Quantum key distribution: Presentation I

Basic protocols (1984-1996)

11/04/2023

No Cloning theorem

$$U|0\rangle|0\rangle \rightarrow |0\rangle|0\rangle \qquad U|1\rangle|0\rangle \rightarrow |1\rangle|1\rangle$$

$$U(\alpha|0\rangle + \beta|1\rangle)|0\rangle \rightarrow \alpha|00\rangle + \beta|11\rangle \neq (\alpha|0\rangle + \beta|1\rangle)^{\otimes 2}$$

QKD: steps

Quantum phase

1. Generation,
2. transmission,
3. reception

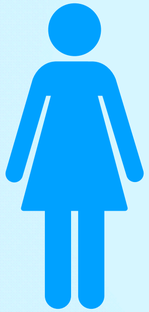
Classical phase

1. Basis reconciliation, Eavesdropping check
2. Sifting
3. Error correction
4. Privacy amplification

QKD: Basic requirement

Alice

Channel (Transmission)



Bob

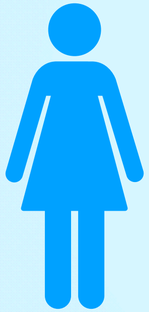
Generation

Measurement

QKD: Basic requirement

Alice

Channel (Transmission)



Bob

Fiber, free space, satellite

Different noises— refractive index fluctuation

Generation
(CV/ DV/ Single photon/ Entanglement)

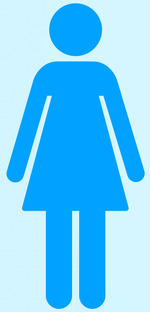
Measurement

SnSPD, ADP, homodyne detection

QKD: Basic requirement

Alice

Channel (Transmission)



Bob

Fiber, free space, satellite

Different noises— mainly related refractive index fluctuation
Polarisation dispersion, interferometric instability,

Generation
(CV/ DV/ Single photon/ Entanglement)

Measurement

SnSPD, ADP, homodyne detection

One theoretical requirement: non-existence of a classical joint probability scheme for all the observables used in the protocol.

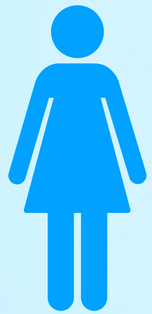
Various practical requirements/challenges:

1. Extraction of a key in a noisy channel.
2. Non-perfect single photon sources.
3. Non-ideal detectors.
4. Losses/ noises in the channel.

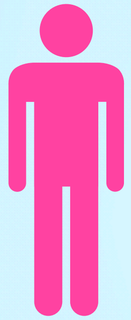
Leave the experimental aspects aside for a moment!

Just the initial protocols!

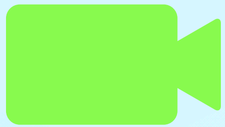
BB84 protocol: first ever protocol (P & M)

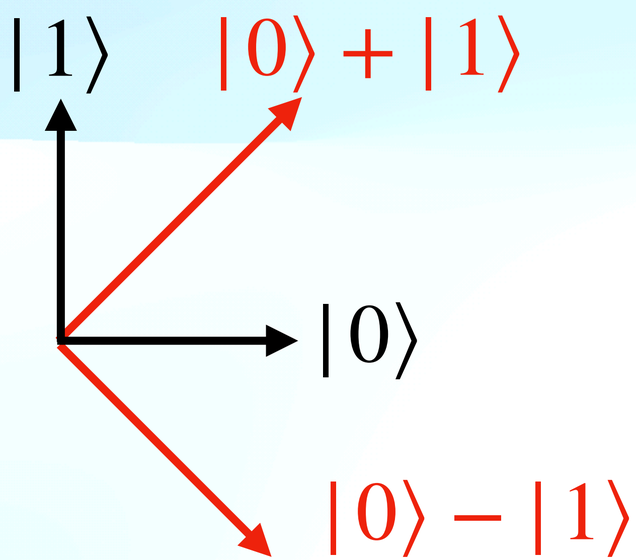


Alice

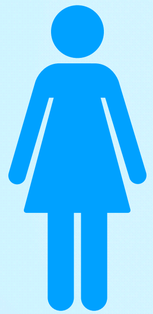


Bob



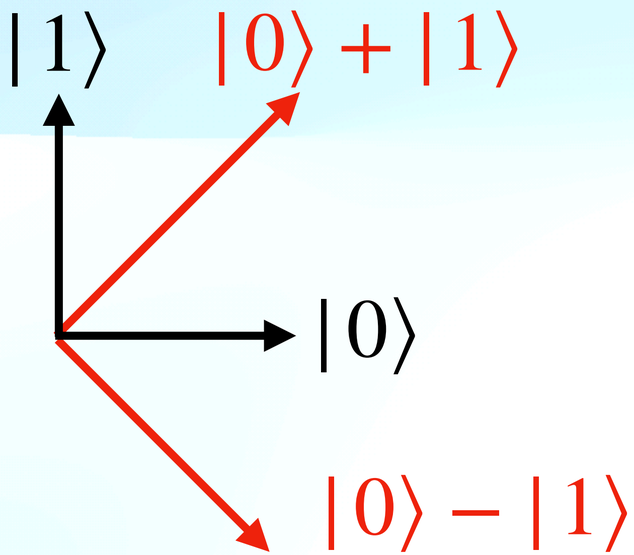


BB84 protocol: first ever protocol



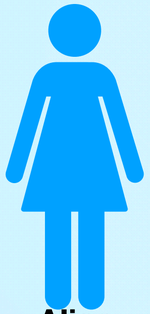
Alice

Bob



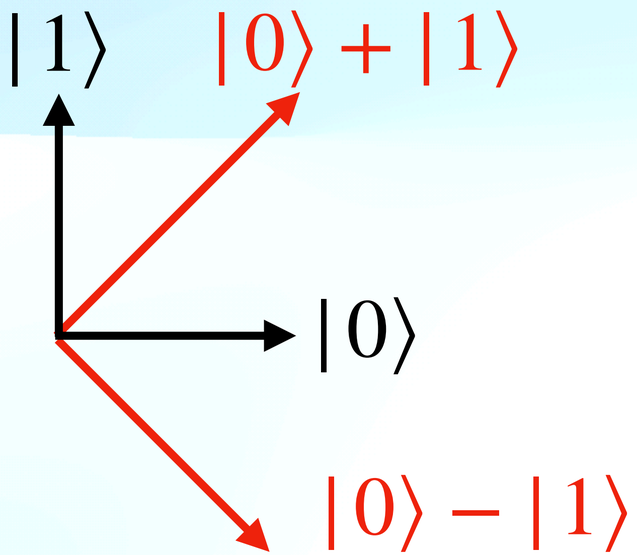
Noiseless channel

BB84 protocol: first ever protocol



Alice

Bob



Noiseless channel

$\{|0\rangle, |1\rangle\}$

$\{|0\rangle + |1\rangle, |0\rangle - |1\rangle\}$

Key generation rule

Sent bit	Measurement basis	Stipulation
$\|0\rangle, \|1\rangle$	$\|0\rangle, \|1\rangle$	Key generation/ security check
	$\|0\rangle \pm \|1\rangle$	Discard
$\|0\rangle \pm \|1\rangle$	$\|0\rangle, \|1\rangle$	Discard
	$\|0\rangle \pm \|1\rangle$	Key generation/ security check

Secret key rate=0.5 bits per transmission

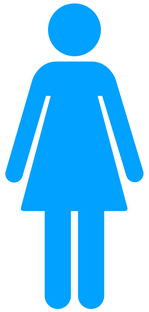
Two key questions regarding security

1. Information-theoretic security (forget the source of any noise, just calculate)
2. Physical layer security

One question regarding implementation

1. How `well' do the experiments mimic theoretical requirements?

Six-state protocol



Alice

$$\{|0\rangle, |1\rangle\}$$

$$\{|0\rangle + |1\rangle, |0\rangle - |1\rangle\}$$

$$\{|0\rangle + i|1\rangle, |0\rangle - i|1\rangle\}$$

Eve's detection probability increases

Bob

$$\{|0\rangle, |1\rangle\}$$

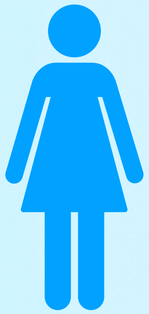
$$\{|0\rangle + |1\rangle, |0\rangle - |1\rangle\}$$

$$\{|0\rangle + i|1\rangle, |0\rangle - i|1\rangle\}$$

What's the advantage over BB84 protocol?

Secret key rate=0.33 bits per transmission/ higher disturbance caused by Eve.

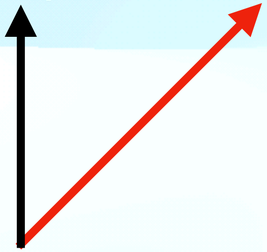
B92 protocol: QKD with minimal number of states



Alice

Bob

$|1\rangle \quad |0\rangle + |1\rangle$

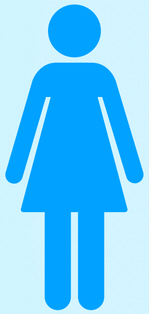


$\{|0\rangle, |1\rangle\}$

$\{|0\rangle + |1\rangle, |0\rangle - |1\rangle\}$

Noiseless channel

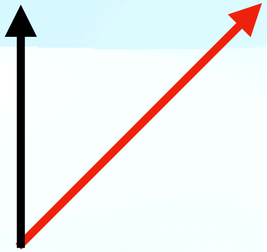
B92 protocol: QKD with minimal number of states



Alice

Bob

$|1\rangle \quad |0\rangle + |1\rangle$

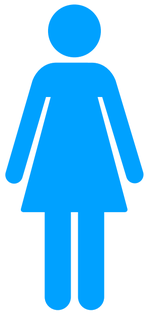


$\{|0\rangle, |1\rangle\}$

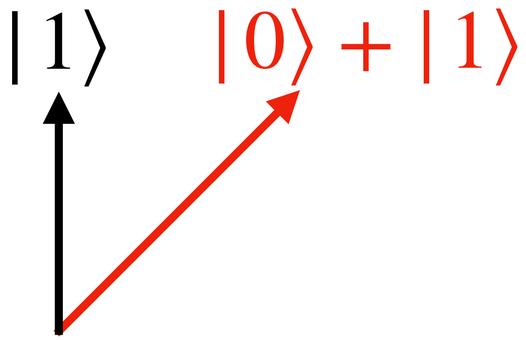
$\{|0\rangle + |1\rangle, |0\rangle - |1\rangle\}$

Noiseless channel

B92 protocol: QKD with minimal number of states



Alice



Noiseless channel

Bob

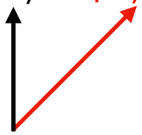
$\{|0\rangle, |1\rangle\}$

$\{|0\rangle + |1\rangle, |0\rangle - |1\rangle\}$

B92 protocol: QKD with minimal number of states

Alice

$|1\rangle \quad |0\rangle + |1\rangle$



Noiseless channel

Bob

$\{|0\rangle, |1\rangle\}$

$\{|0\rangle + |1\rangle, |0\rangle - |1\rangle\}$

Key generation rule

An example of unambiguous state discrimination

State sent by Alice	Post-measurement state of Bob
$\|0\rangle$	$\|0\rangle$
	$\|0\rangle + \|1\rangle, \|0\rangle - \|1\rangle$
$\|0\rangle + \|1\rangle$	$\|0\rangle, \|1\rangle$
	$\|0\rangle + \|1\rangle$

If Bob gets $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, Alice has sent $|0\rangle$.

If Bob gets $|1\rangle$, Alice has sent $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

Key generation rule

An example of unambiguous state discrimination

State sent by Alice	Post-measurement state of Bob
$\|0\rangle$	$\|0\rangle$
	$\|0\rangle + \|1\rangle, \|0\rangle - \|1\rangle$
$\|0\rangle + \|1\rangle$	$\|0\rangle, \|1\rangle$
	$\|0\rangle + \|1\rangle$

If Bob gets $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$,
Alice has sent $|0\rangle$.

If Bob gets $|1\rangle$,
Alice has sent
$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

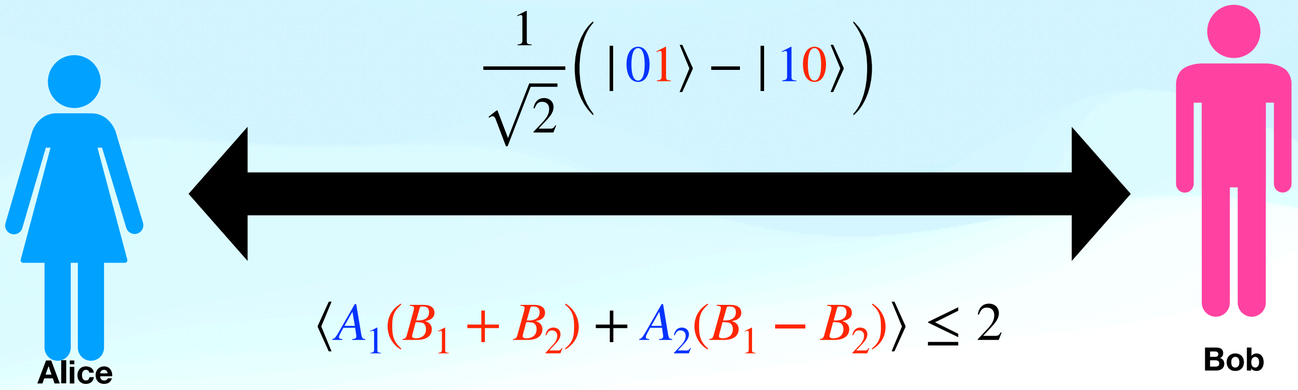
Key generation rule

An example of unambiguous state discrimination

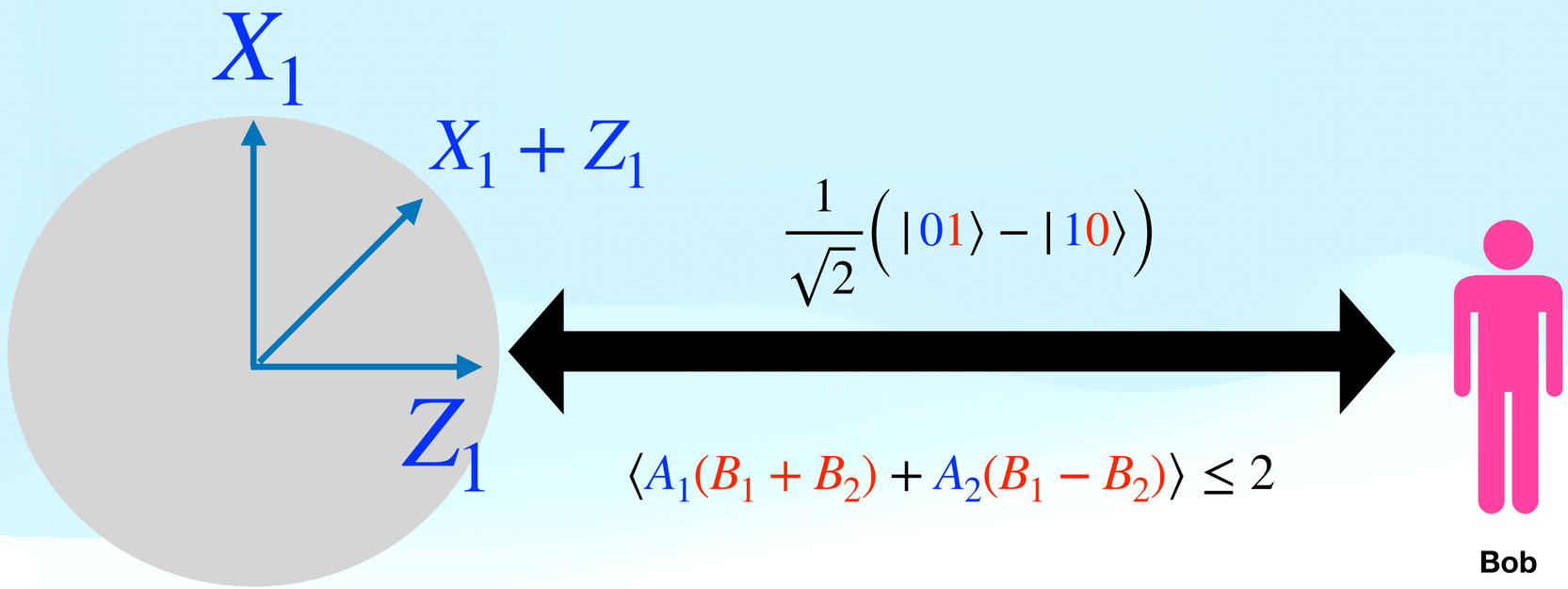
$\|0\rangle$	$\|0\rangle$
	$\|0\rangle + \|1\rangle, \|0\rangle - \|1\rangle$
$\|0\rangle + \|1\rangle$	$\|0\rangle, \|1\rangle$
	$\|0\rangle + \|1\rangle$

Used in CiZi paper

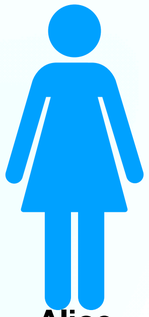
E91 protocol: Entanglement-based protocol



E91 protocol: Entanglement-based protocol

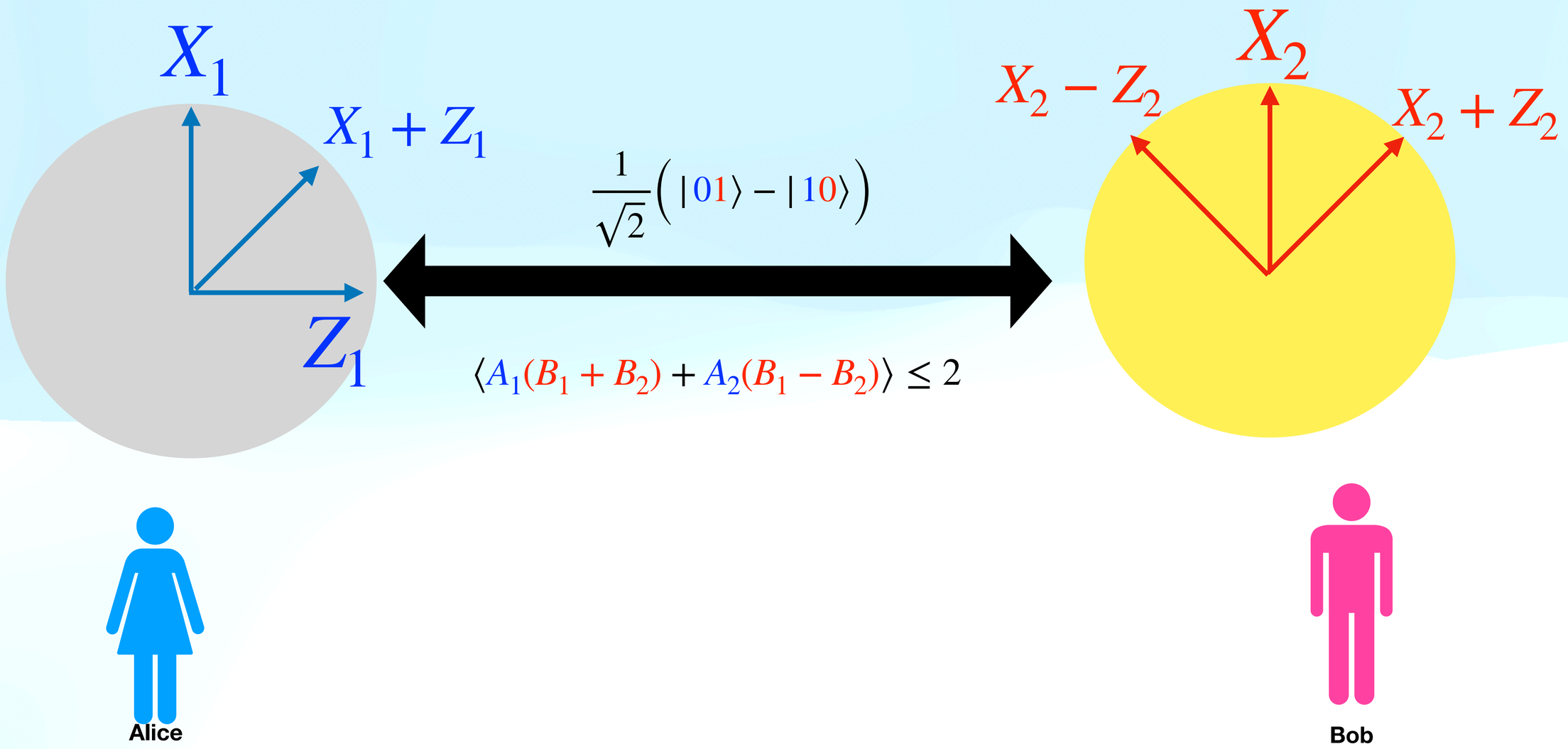


Bob

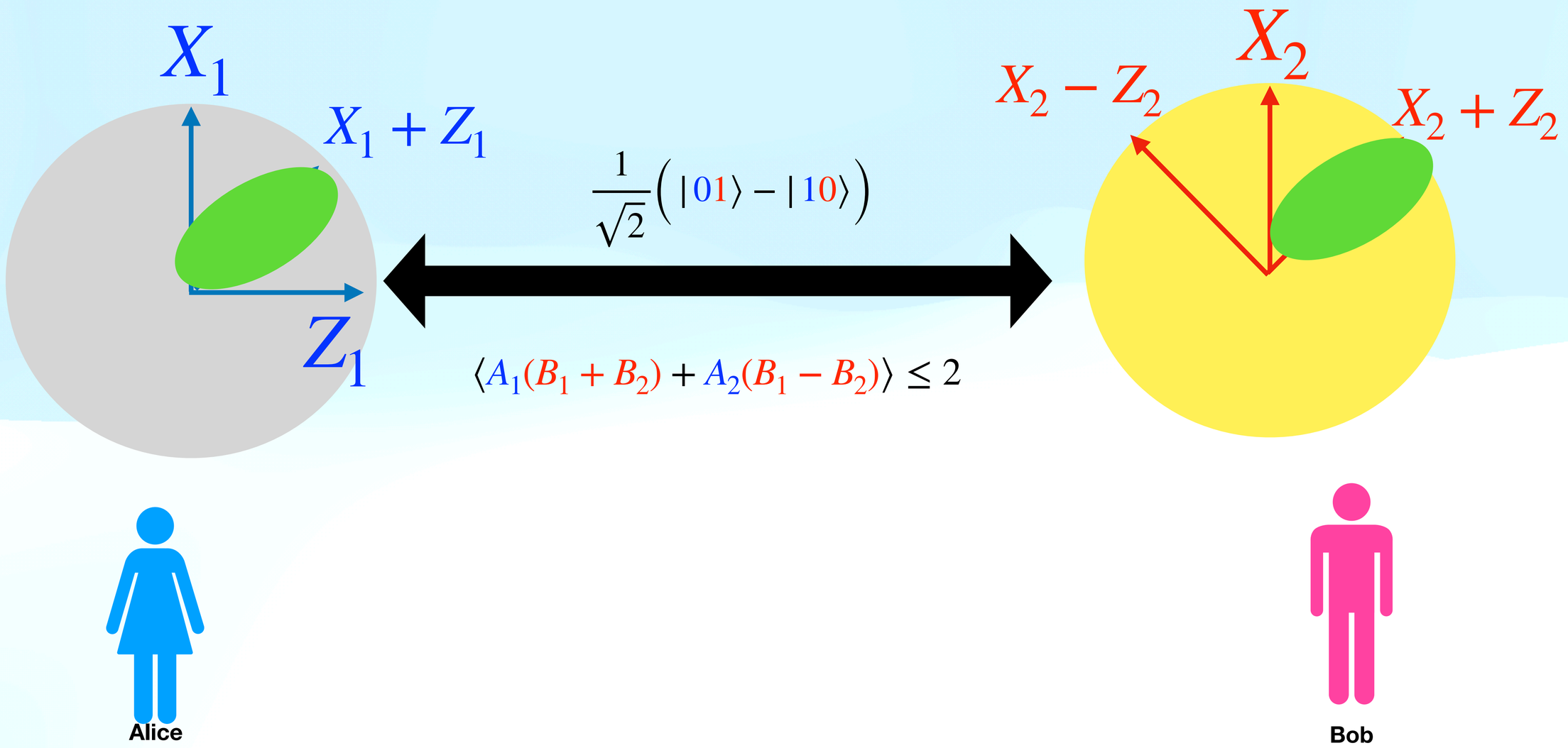


Alice

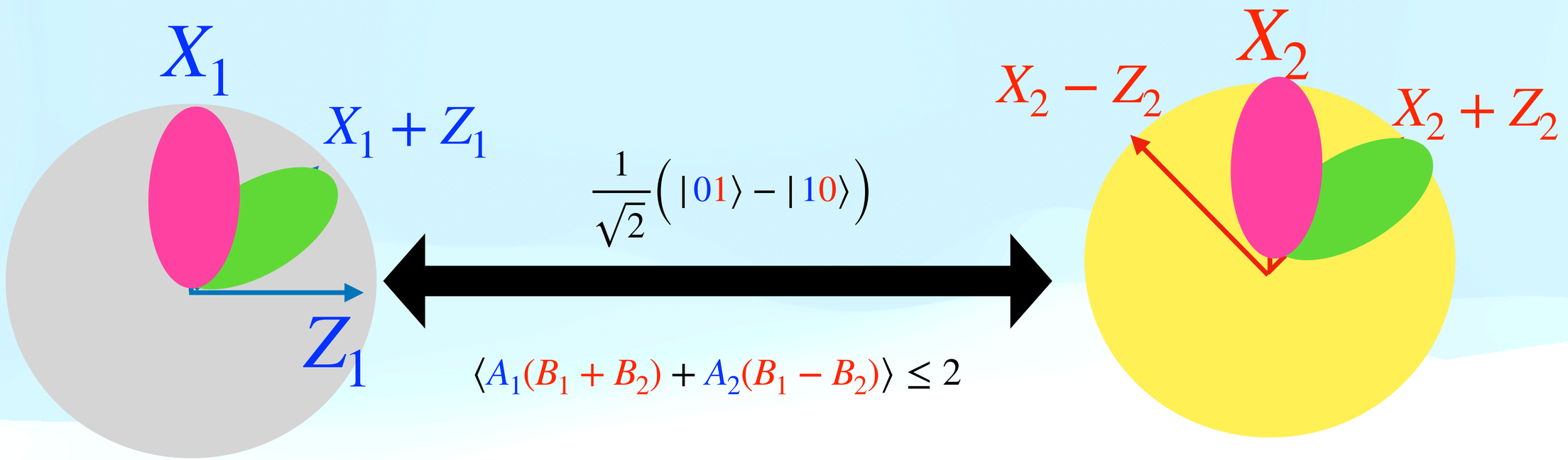
E91 protocol: Entanglement-based protocol



E91 protocol: Entanglement-based protocol



E91 protocol: Entanglement-based protocol

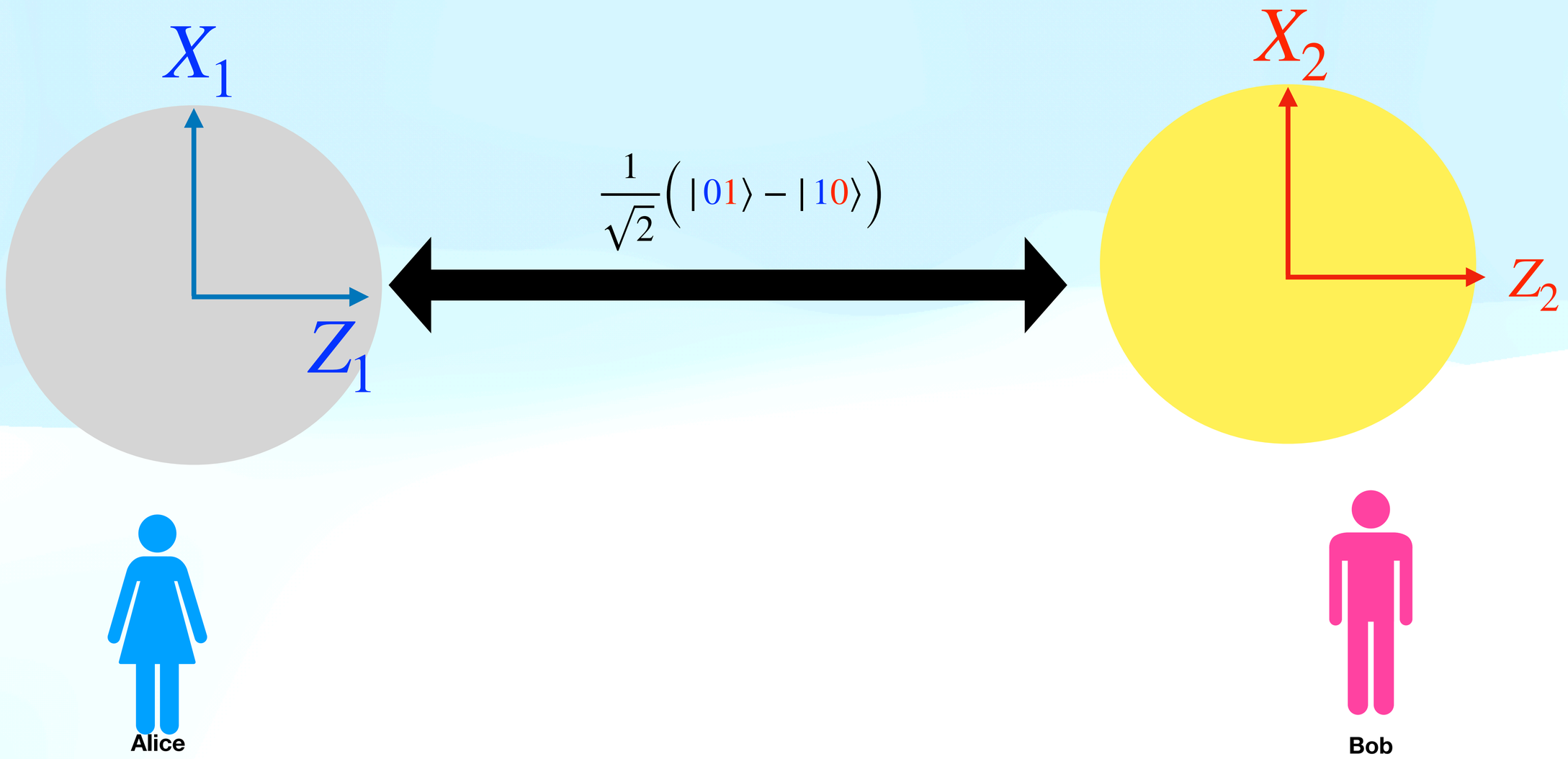


Alice

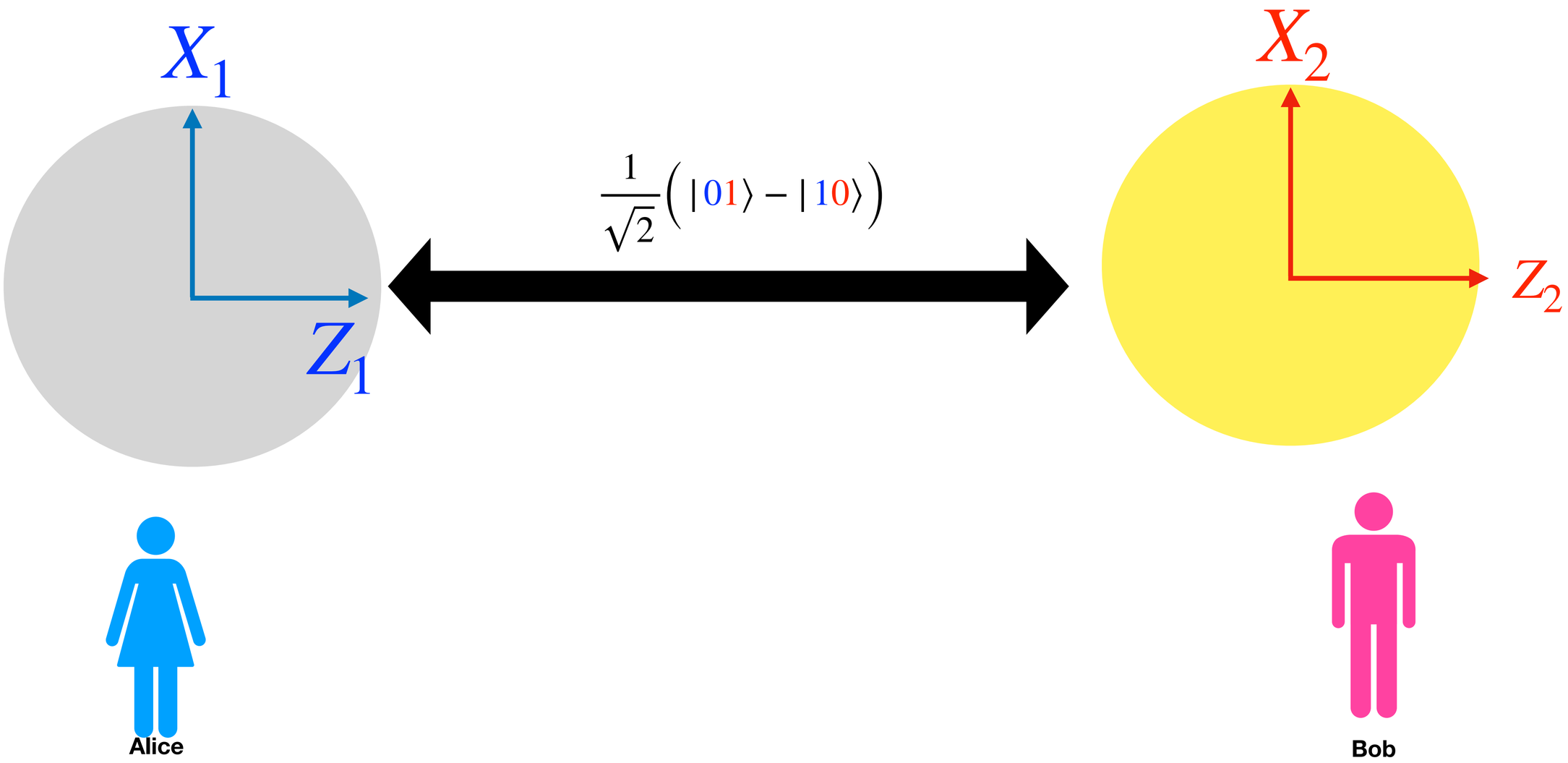
Key generation rate=2/9 bits per transmission

Bob

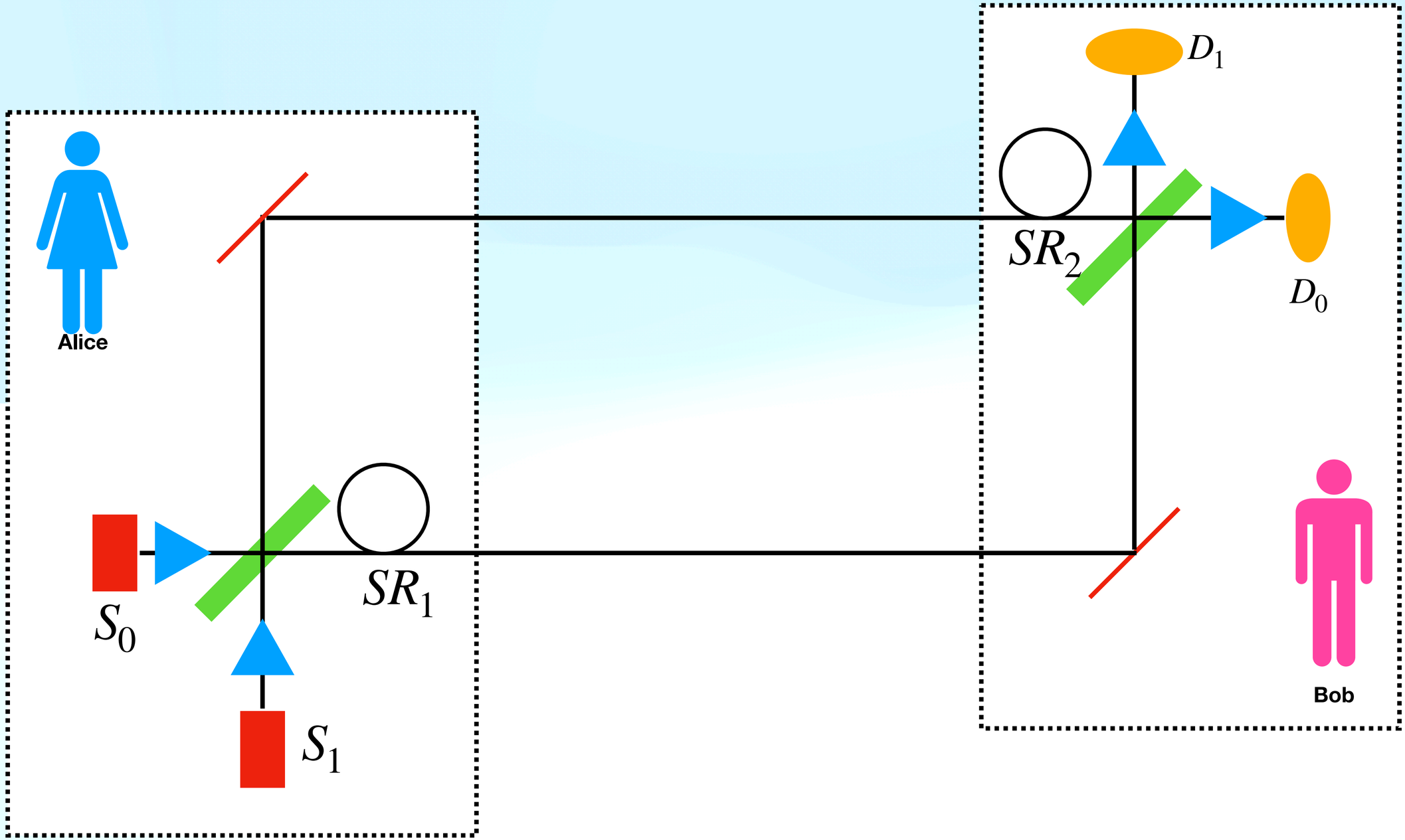
BBM 92 protocol: Entanglement-based protocol



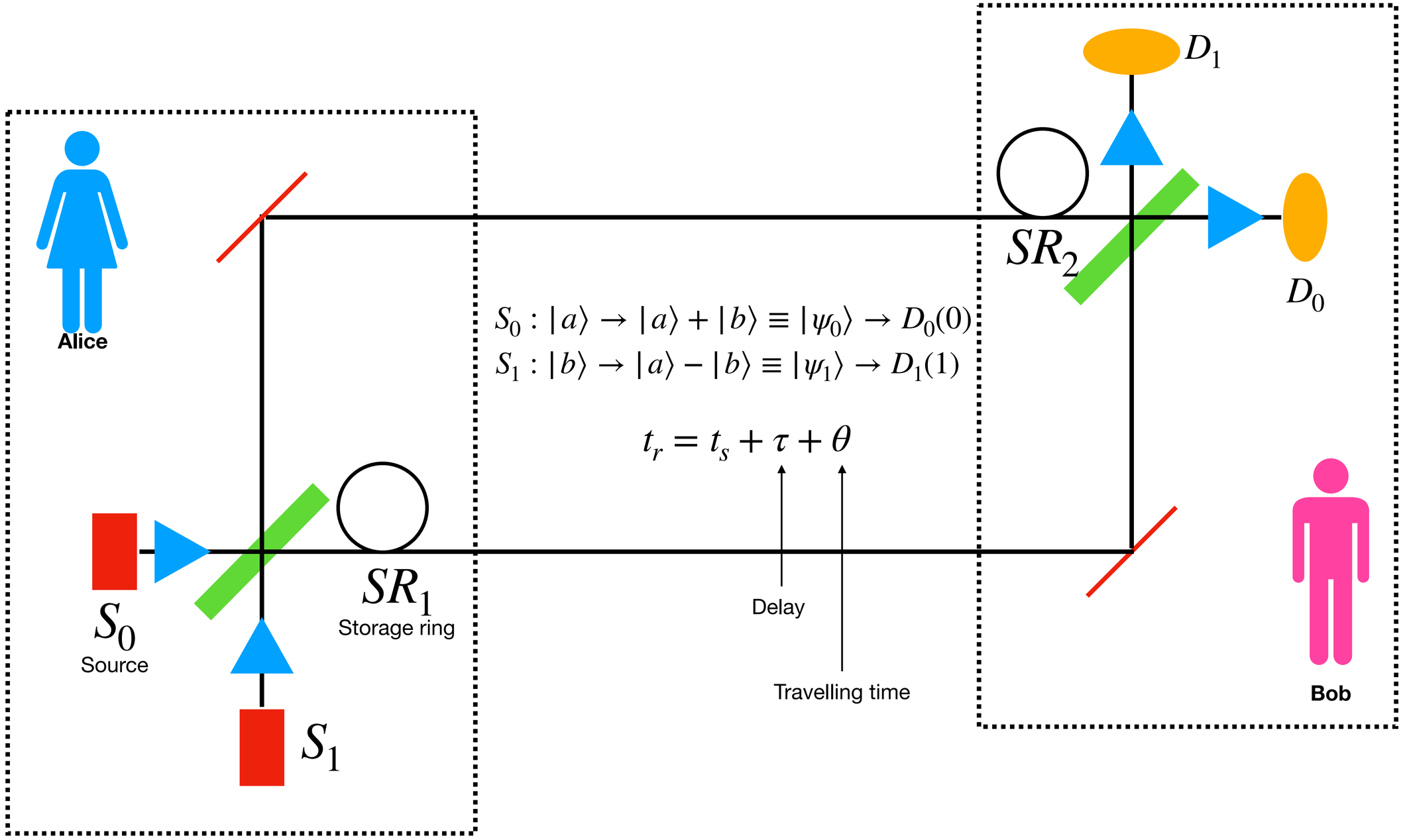
BBM 92 protocol: Entanglement-based protocol



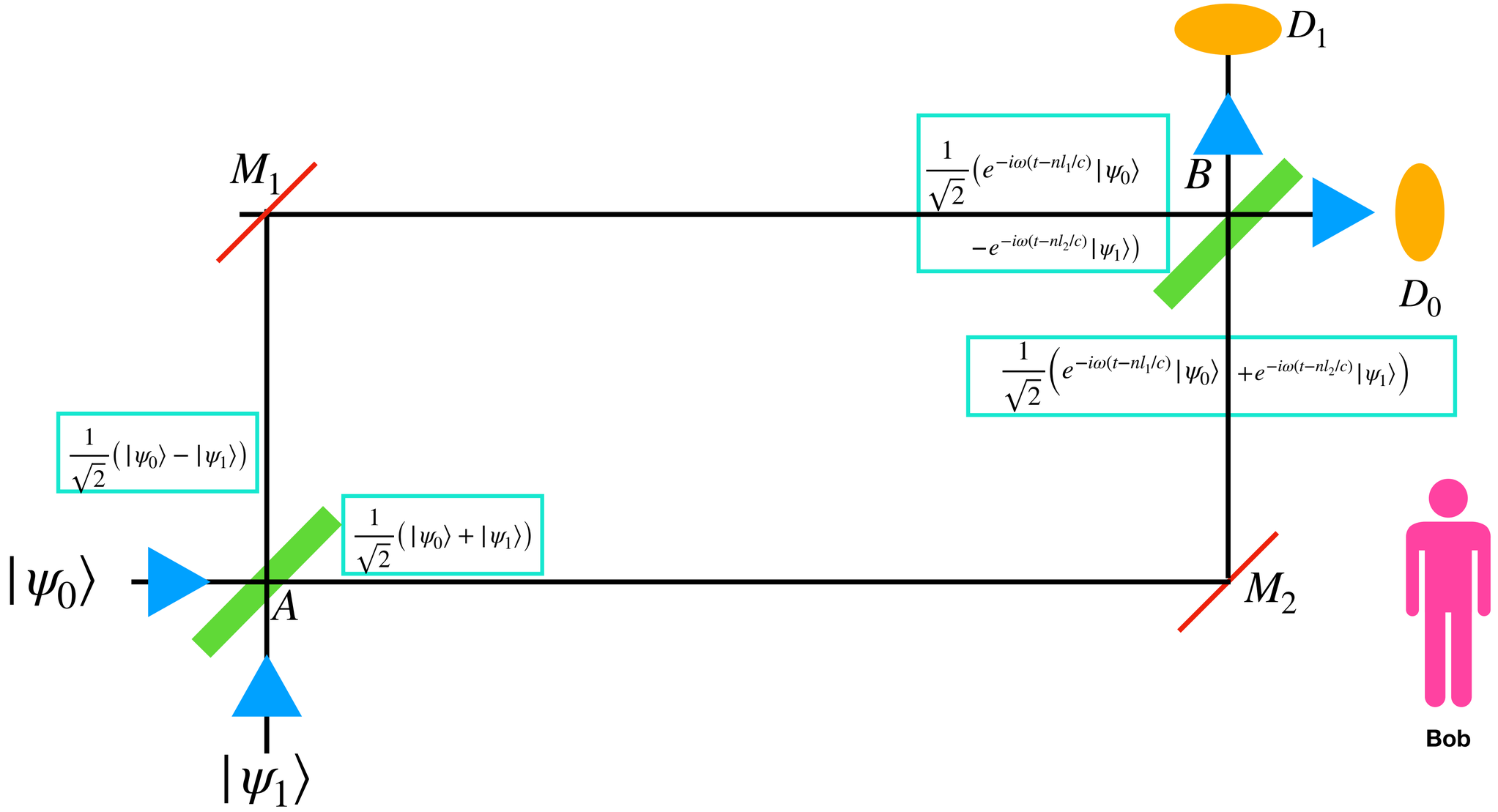
Goldenberg-Vaidman protocol (1995)-based on orthogonal states



Goldenberg-Vaidman protocol (1995)-based on orthogonal states



Goldenberg-Vaidman protocol (1995)-based on orthogonal states



Formal equivalence between entanglement based QKD and P & M QKD

P & M QKD protocol

$$\{\,|\phi_i\rangle, p_i\}$$

Need not be orthogonal

Formal equivalence between entanglement based QKD and P & M QKD

P & M QKD protocol

$$\{\, |\phi_i\rangle, p_i \}$$

Need not be orthogonal

Entanglement-based QKD protocol

$$\sum_i \sqrt{p_i}\, |i\rangle\, |\phi_i\rangle$$

Orthonormal

Formal equivalence between entanglement based QKD and P & M QKD

P & M QKD protocol

$$\{\, |\phi_i\rangle, p_i \}$$

Need not be orthogonal

Used in layered paper

Entanglement-based QKD protocol

$$\sum_i \sqrt{p_i}\, |i\rangle\, |\phi_i\rangle$$

Orthonormal

Topics covered in the last presentation

ONLY PROTOCOLS:

BB84, B92, E91, six state, BBM92, GV protocol

Formal equivalence between P&M and entanglement-based QKD protocols

Topics covered in the last presentation

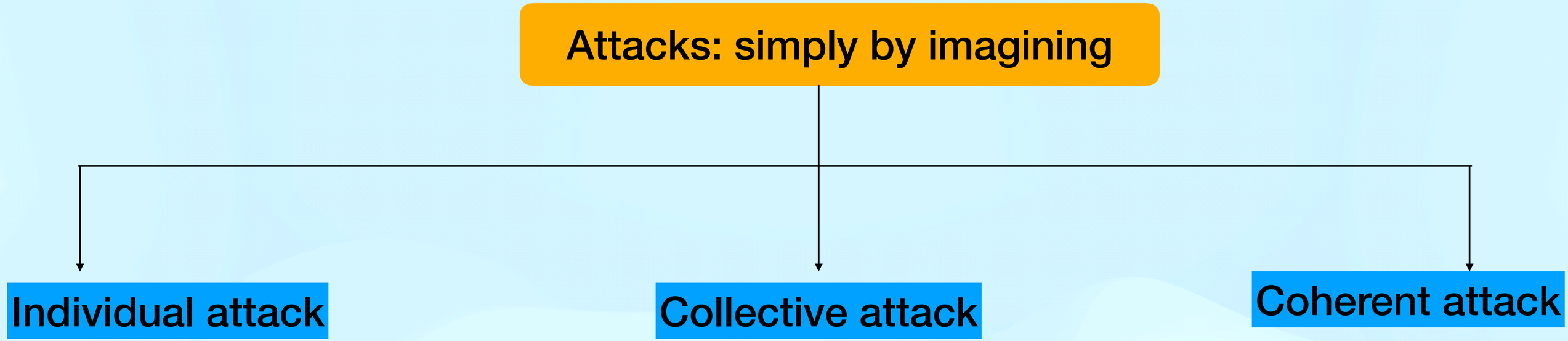
ONLY PROTOCOLS:

BB84, B92, E91, six state, BBM92, GV protocol

Formal equivalence between P&M and entanglement-based QKD protocols

Topics for today's presentation

Attacks: individual attacks, collective attacks on BB84 protocols
Photon-number-splitting attack on BB84 protocol


Attacks: simply by imagining
Individual attack
Collective attack
Coherent attack

Attacks: simply by imagining

Individual attack

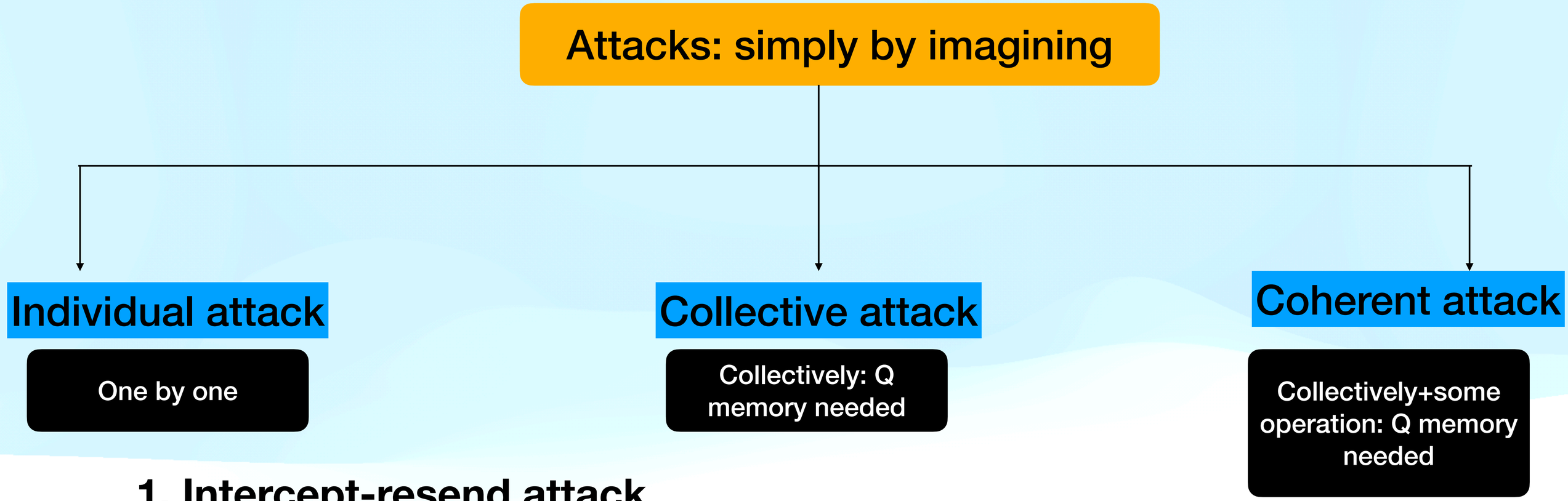
One by one

Collective attack

Collectively: Q memory needed

Coherent attack

Collectively+some operation: Q memory needed



1. Intercept-resend attack

2. Entangle-and-measure attack

Attacks: arising from the gap between theoretical assumptions and experimental implementation

Attacks: arising from the gap between theoretical assumptions and experimental implementation: side channel attack

PYL555: Quantum Mechanics
(II Minor Solutions)

10 Oct, 2015 4 PM – 5 PM

Question 1. All questions are in $D = 2$ spatial dimensions except when explictly stated.

(a) (5 marks) A particle of mass m is constrained to the $X-Y$ plane. If it is in a potential $V(x,y) = \frac{1}{2}k_1x^2 + \frac{1}{2}k_2y^2$, $k_1 > k_2$, find the expectation value of $\vec{r}^2$ in the first excited state.

Solution: The energy levels are given by $\hbar\Big\{n_1\omega_1 + n_2\omega_2 + \frac{1}{2}(\omega_1+\omega_2)\Big\}$. The first excited state corresponds to $n_1 = 0,\ n_2 = 1$. Hence $\langle\vec{r}^2\rangle = \frac{\hbar}{m}(\omega_1 + 3\omega_2)$; Note that $\omega^2 = \frac{k}{m}$.

(b) (5 marks) Construct the radial momentum operator in $D = 4$ spatial dimensions.
Solution: Use the definition $p_r = \frac{1}{2}(\vec{p}\cdot\hat{r}+\hat{r}\cdot\vec{p})$. Use also that $\vec{\nabla}_D\cdot\vec{r} = D$. You will get $p_r = -i\hbar(\partial_r + \frac{3}{2r})$.

(c) (10 marks) A particle is in the second excited state of the Morse potential

$$V(r) = V_0\Big(\exp(-2\alpha r) - 2\exp(-\alpha r)\Big).$$

Which of the following wave functions are allowed candidates for the wave function? All constants are positive. Identify the quantum numbers associated with the allowed states.

- (1) $\psi(x,y) = (r-a)(r-b)\exp(-cr^2)$
- (2) $\psi(x,y) = \exp(-ar)\exp(2i\phi)$
- (3) $\psi(x,y) = (r-a)(r-b)\exp(-cr^2)\exp(-2i\phi)$
- (4) $\psi(x,y) = \frac{1}{x^4+a^4}\exp(-by^2)$

Solution: Leading order potential around the minima is of an oscillator. The second excited state has two nodes in the radial wave function. Possible choices are (1) and (3). The first one is an s state and the next belongs to $m = -2$.

(d) (5 marks) A particle of mass m and charge q is constrained to the $X-Y$ plane, with a magnetic field $\vec{B}(\vec{r}) = B\theta(R-r)\hat{k}$. Construct a Hamiltonian for the charged particle.

solution: I will leave this for you to figure out. Use polar coordinates and you get the naswer in no time. What you have to note is that $\vec{A}$ should be continuous at $r = R$.

The End

Attacks: arising from the gap between theoretical assumptions and experimental implementation: side channel attack

PYL555: Quantum Mechanics
(II Minor Solutions)

10 Oct, 2015 4 PM – 5 PM

Question 1. All questions are in $D = 2$ spatial dimensions except when explictly stated.

(a) (5 marks) A particle of mass m is constrained to the $X-Y$ plane. If it is in a potential $V(x,y) = \frac{1}{2}k_1x^2 + \frac{1}{2}k_2y^2$, $k_1 > k_2$, find the expectation value of $\vec{r}^2$ in the first excited state.

Solution: The energy levels are given by $\hbar\Big\{n_1\omega_1 + n_2\omega_2 + \frac{1}{2}(\omega_1+\omega_2)\Big\}$. The first excited state corresponds to $n_1 = 0,\ n_2 = 1$. Hence $\langle\vec{r}^2\rangle = \frac{\hbar}{m}(\omega_1 + 3\omega_2)$; Note that $\omega^2 = \frac{k}{m}$.

Side channel: anything (DOF) not employed in the protocol

$$V(r) = V_0\Big(\exp(-2\alpha r) - 2\exp(-\alpha r)\Big).$$

Which of the following wave functions are allowed candidates for the wave function? All constants are positive. Identify the quantum numbers associated with the allowed states.

- (1) $\psi(x,y) = (r-a)(r-b)\exp(-cr^2)$
- (2) $\psi(x,y) = \exp(-ar)\exp(2i\phi)$
- (3) $\psi(x,y) = (r-a)(r-b)\exp(-cr^2)\exp(-2i\phi)$
- (4) $\psi(x,y) = \frac{1}{x^4+a^4}\exp(-by^2)$

Solution: Leading order potential around the minima is of an oscillator. The second excited state has two nodes in the radial wave function. Possible choices are (1) and (3). The first one is an s state and the next belongs to $m = -2$.

(d) (5 marks) A particle of mass m and charge q is constrained to the $X-Y$ plane, with a magnetic field $\vec{B}(\vec{r}) = B\theta(R-r)\hat{k}$. Construct a Hamiltonian for the charged particle.

solution: I will leave this for you to figure out. Use polar coordinates and you get the naswer in no time. What you have to note is that $\vec{A}$ should be continuous at $r = R$.

The End

An example of side channel attack

Stems from an implicit assumption: in BB84, we have two-level systems only.
If this assumption is not fulfilled, then?

An example of side channel attack

Stems from an implicit assumption: in BB84, we have two-level systems only. If this assumption is not fulfilled, then?

$$\frac{1}{2}\Big(|00\rangle_{zz}\langle 00| + |11\rangle_{zz}\langle 11|\Big)_{12}\frac{1}{2}\Big(|00\rangle_{xx}\langle 00| + |11\rangle_{xx}\langle 11|\Big)_{34}$$

Attacks: arising from the gap between theoretical assumptions and experimental implementation: side channel attack

$$|\,|\alpha|\,e^{i\theta}\rangle \longleftarrow$$ Weak coherent pulse

$$\frac{1}{2\pi}\int_0^{2\pi} d\theta\,|\alpha\rangle\langle\alpha| = \sum_{n=0}^{\infty} e^{-|\alpha|^2}\frac{|\alpha|^n}{n!}|n\rangle\langle n| \leftarrow$$ Multiphoton components

Attacks: arising from the gap between theoretical assumptions and experimental implementation: side channel attack

$$|\,|\alpha|\,e^{i\theta}\rangle \longleftarrow$$ Weak coherent pulse

$$\frac{1}{2\pi}\int_0^{2\pi} d\theta\,|\alpha\rangle\langle\alpha| = \sum_{n=0}^{\infty} e^{-|\alpha|^2}\frac{|\alpha|^n}{n!}|n\rangle\langle n| \leftarrow$$ Multiphoton components

$$\alpha = 0.1 \implies |0.1\rangle = \sqrt{0.90}\,|0\rangle + \sqrt{0.09}\,|1\rangle + \sqrt{0.002}\,|2\rangle + \cdots$$

Attacks: arising from the gap between theoretical assumptions and experimental implementation: side channel attack

$$|\,|\alpha|\,e^{i\theta}\rangle \longleftarrow$$ Weak coherent pulse

$$\frac{1}{2\pi}\int_0^{2\pi} d\theta\,|\alpha\rangle\langle\alpha| = \sum_{n=0}^{\infty} e^{-|\alpha|^2}\frac{|\alpha|^n}{n!}|n\rangle\langle n| \leftarrow$$ Multiphoton components

$$\alpha = 0.1 \implies |0.1\rangle = \sqrt{0.90}\,|0\rangle + \sqrt{0.09}\,|1\rangle + \sqrt{0.002}\,|2\rangle + \cdots$$

No photon at all

Single photon

Two photons

Attacks: arising from the gap between theoretical assumptions and experimental implementation: side channel attack

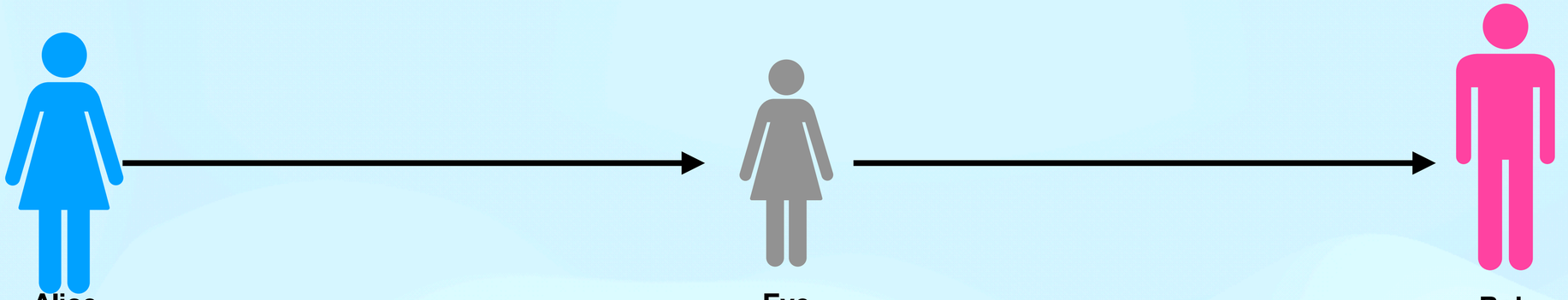
$$|\,|\alpha|\,e^{i\theta}\rangle \longleftarrow$$ Weak coherent pulse

$$\frac{1}{2\pi}\int_0^{2\pi} d\theta\,|\alpha\rangle\langle\alpha| = \sum_{n=0}^{\infty} e^{-|\alpha|^2}\frac{|\alpha|^n}{n!}|n\rangle\langle n| \leftarrow$$ Multiphoton components

$$\alpha = 0.1 \implies |0.1\rangle = \sqrt{0.90}\,|0\rangle + \sqrt{0.09}\,|1\rangle + \sqrt{0.002}\,|2\rangle + \cdots$$

Same point with entanglement based sources or isn' it? ←To be looked into

Intercept-resend attack for BB84 protocol



Intercept-resend attack for BB84 protocol: individual attack

$$|\theta\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

$$|\theta^{\perp}\rangle = \sin\frac{\theta}{2}|0\rangle - e^{-i\phi}\cos\frac{\theta}{2}|1\rangle$$

Intercept-resend attack for BB84 protocol: individual attack

$$|\theta\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

$$|\theta^{\perp}\rangle = \sin\frac{\theta}{2}|0\rangle - e^{-i\phi}\cos\frac{\theta}{2}|1\rangle$$

$$P(0|\theta) = P(1|\theta^{\perp}) = \cos^2\frac{\theta}{2} := P_E^Z$$

Intercept-resend attack for BB84 protocol: individual attack

$$|\theta\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

$$|\theta^{\perp}\rangle = \sin\frac{\theta}{2}|0\rangle - e^{-i\phi}\cos\frac{\theta}{2}|1\rangle$$

$$P(0|\theta) = P(1|\theta^{\perp}) = \cos^2\frac{\theta}{2} := P_E^Z$$

$$P(+|\theta) = P(-|\theta^{\perp}) = \frac{1+\sin\theta\cos\phi}{2} := P_E^X$$

Intercept-resend attack for BB84 protocol: individual attack

$$|\theta\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

$$|\theta^{\perp}\rangle = \sin\frac{\theta}{2}|0\rangle - e^{-i\phi}\cos\frac{\theta}{2}|1\rangle$$

$$P(0|\theta) = P(1|\theta^{\perp}) = \cos^2\frac{\theta}{2} := P_E^Z$$

$$P(+|\theta) = P(-|\theta^{\perp}) = \frac{1+\sin\theta\cos\phi}{2} := P_E^X$$

$$I_E^Z = 1 - H_2\left(P_E^Z\right) \qquad I_E^X = 1 - H_2\left(P_E^X\right)$$

Intercept-resend attack for BB84 protocol: individual attack

$$|\theta\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

$$|\theta^{\perp}\rangle = \sin\frac{\theta}{2}|0\rangle - e^{-i\phi}\cos\frac{\theta}{2}|1\rangle$$

$$P(0|\theta) = P(1|\theta^{\perp}) = \cos^2\frac{\theta}{2} := P_E^Z$$

$$P(+|\theta) = P(-|\theta^{\perp}) = \frac{1+\sin\theta\cos\phi}{2} := P_E^X$$

$$I_E^Z = 1 - H_2(P_E^Z) \qquad I_E^X = 1 - H_2(P_E^X)$$

$$I_E = \frac{I_E^Z + I_E^X}{2}$$

Breidbart basis: $\theta = \frac{\pi}{4}, \phi = 0$

$P_E^Z = P_E^X := P_E \leftarrow$ Eve's overall probability of guessing

$P_E = \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right)$ $\quad I_{\mathrm{AE}} \approx 0.4$ bit

Breidbart basis: $\theta = \frac{\pi}{4}, \phi = 0$

$$P_E^Z = P_E^X := P_E \leftarrow$$ Eve's overall probability of guessing

$$P_E = \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right) \qquad I_{\mathrm{AE}} \approx 0.4 \text{ bit}$$

QBER

$$P(1|0) = P(1|\theta)P(\theta|0) + P(1|\theta^{\perp})P(\theta^{\perp}|0) = \frac{\sin^2\theta}{2}$$

$$P(+|-) = P(+|\theta)P(\theta|-) + P(+|\theta^{\perp})P(\theta^{\perp}|-) = \frac{1}{4}\left(1 - \sin^2\theta\cos^2\phi\right)$$

Breidbart basis: $\theta = \frac{\pi}{4}, \phi = 0$

$$P_E^Z = P_E^X := P_E \leftarrow$$ Eve's overall probability of guessing

$$P_E = \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right) \qquad I_{\mathrm{AE}} \approx 0.4 \text{ bit}$$

QBER

$$P(1|0) = P(1|\theta)P(\theta|0) + P(1|\theta^{\perp})P(\theta^{\perp}|0) = \frac{\sin^2\theta}{2}$$

$$P(+|-) = P(+|\theta)P(\theta|-) + P(+|\theta^{\perp})P(\theta^{\perp}|-) = \frac{1}{4}\left(1 - \sin^2\theta\cos^2\phi\right)$$

$$P_{\mathrm{err}} = \frac{P_{\mathrm{err}}^Z + P_{\mathrm{err}}^X}{2} = \frac{1 + (1 - \cos^2\phi)\sin^2\theta}{4}$$

$$I_{AB} = 1 - h(\mathrm{QBER})$$

$$I_{\mathrm{AB}} \approx 0.19 \text{ bit}$$

Breidbart basis: $\theta = \frac{\pi}{4}, \phi = 0$

$$P_E^Z = P_E^X := P_E \leftarrow$$ Eve's overall probability of guessing

$$P_E = \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right) \qquad I_{\mathrm{AE}} \approx 0.06 \text{ bit}$$

QBER

$$P(1|0) = P(1|\theta)P(\theta|0) + P(1|\theta^{\perp})P(\theta^{\perp}|0) = \frac{\sin^2\theta}{2}$$

$$P(+|-) = P(+|\theta)P(\theta|\quad) + P(+|\theta^{\perp})P(\theta^{\perp}|-) = \frac{1}{4}\left(1 - \sin^2\theta\cos^2\phi\right)$$

$$P_{\mathrm{err}} = \frac{P^Z \quad \mathrm{err}}{2} = \frac{1 + (1 - \cos^2\phi)\sin^2\theta}{4}$$

Key distribution NOT possible

$$I_{AB} = 1 - h(\mathrm{QBER})$$

$$I_{\mathrm{AB}} \approx 0.19 \text{ bit}$$

Optimal eavesdropping strategy of the BB84 protocol

$$U|0\rangle|E\rangle = |0\rangle|F_0\rangle + |1\rangle|D_0\rangle$$

$$U|1\rangle|E\rangle = |1\rangle|F_1\rangle + |0\rangle|D_1\rangle$$

$|F_{0,1}\rangle$ And $|D_{0,1}\rangle$ ← **Nonorthogonal and unnormalised**

Optimal eavesdropping strategy of the BB84 protocol

Minimum dimension of ancilla=4

$$U|0\rangle|E\rangle = |0\rangle|F_0\rangle + |1\rangle|D_0\rangle$$

$$U|1\rangle|E\rangle = |1\rangle|F_1\rangle + |0\rangle|D_1\rangle$$

$|F_{0,1}\rangle$ And $|D_{0,1}\rangle$ ← **Nonorthogonal and unnormalised**

$$U|a\rangle|E\rangle = |a\rangle|F_a\rangle + |a^{\perp}\rangle|D_a\rangle; \quad |a\rangle \in \{|0\rangle, |1\rangle, |\pm\rangle\}$$

$$\langle a|a^{\perp}\rangle = 0$$

$$2|F_{\pm}\rangle = |F_0\rangle + |F_1\rangle \pm |D_0\rangle \pm |D_1\rangle$$

$$2|D_{\pm}\rangle = |F_0\rangle - |F_1\rangle \mp |D_0\rangle \pm |D_1\rangle$$

Optimal eavesdropping strategy of the BB84 protocol

$$U|a\rangle|E\rangle = |a\rangle|F_a\rangle + |a^{\perp}\rangle|D_a\rangle; \quad |a\rangle \in \{|0\rangle, |1\rangle, |\pm\rangle\} \quad \langle a|a^{\perp}\rangle = 0$$

$$U|0\rangle|E\rangle = |0\rangle|F_0\rangle + |1\rangle|D_0\rangle \qquad U|1\rangle|E\rangle = |1\rangle|F_1\rangle + |0\rangle|D_1\rangle$$

$|F_{0,1}\rangle$ And $|D_{0,1}\rangle$ ← **Nonorthogonal and unnormalised**

$$2|F_{\pm}\rangle = |F_0\rangle + |F_1\rangle \pm |D_0\rangle \pm |D_1\rangle$$

$$2|D_{\pm}\rangle = |F_0\rangle - |F_1\rangle \mp |D_0\rangle \pm |D_1\rangle$$

Symmetric attack

$$\langle F_a|F_a\rangle = F, \langle D_a|D_a\rangle = D, \langle F_a|F_a^{\perp}\rangle = F\cos x, \langle D_a|D_a^{\perp}\rangle = D\cos y\,.$$

Optimal eavesdropping strategy of the BB84 protocol

$$U|a\rangle|E\rangle = |a\rangle|F_a\rangle + |a^{\perp}\rangle|D_a\rangle; \quad |a\rangle \in \{|0\rangle, |1\rangle, |\pm\rangle\} \quad \langle a|a^{\perp}\rangle = 0$$

$$U|0\rangle|E\rangle = |0\rangle|F_0\rangle + |1\rangle|D_0\rangle \qquad U|1\rangle|E\rangle = |1\rangle|F_1\rangle + |0\rangle|D_1\rangle$$

$|F_{0,1}\rangle$ And $|D_{0,1}\rangle$ ← **Nonorthogonal and unnormalised**

$$2|F_{\pm}\rangle = |F_0\rangle + |F_1\rangle \pm |D_0\rangle \pm |D_1\rangle$$

$$2|D_{\pm}\rangle = |F_0\rangle - |F_1\rangle \mp |D_0\rangle \pm |D_1\rangle$$

$$\langle F_a|F_a\rangle = F, \langle D_a|D_a\rangle = D, \langle F_a|F_a^{\perp}\rangle = F\cos x, \langle D_a|D_a^{\perp}\rangle = D\cos y\,.$$

$$|F_0\rangle = \begin{pmatrix} \sqrt{F} \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |F_1\rangle = \begin{pmatrix} \sqrt{F}\cos x \\ 0 \\ 0 \\ \sqrt{F}\sin x \end{pmatrix} \quad |D_0\rangle = \begin{pmatrix} 0 \\ \sqrt{D} \\ 0 \\ 0 \end{pmatrix} \quad |D_1\rangle = \begin{pmatrix} 0 \\ \sqrt{D}\cos y \\ \sqrt{D}\sin y \\ 0 \end{pmatrix}$$

Optimal eavesdropping strategy of the BB84 protocol

$$F = 1 - D; \quad D = \frac{1 - \cos x}{2 - \cos x + \cos y}$$

Obtained by putting $\langle F_{\pm} | F_{\pm} \rangle = \langle F_0 | F_0 \rangle = \langle F_1 | F_1 \rangle$

For this choice: $\langle F_a | F_a \rangle = F, \langle D_a | D_a \rangle = D, \langle F_a | F_a^{\perp} \rangle = F \cos x, \langle D_a | D_a^{\perp} \rangle = D \cos y$.

The attack acts symmetrically in the two bases.

$$I_{AB} = \frac{1}{2}(1 - H_2(D))$$

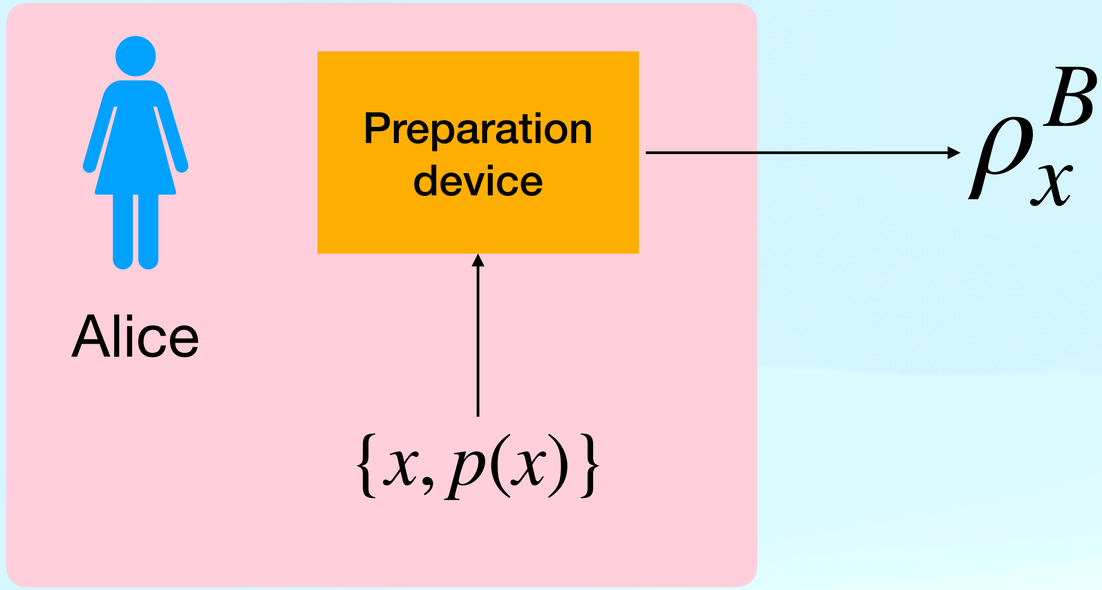
$$\rho_E(u) = |F_u\rangle\langle F_u| + |D_u\rangle\langle D_u| = F|f_u\rangle\langle f_u| + D|d_u\rangle\langle d_u|; \quad |f_u\rangle = F^{-1/2}|F_u\rangle, |d_u\rangle = D^{-1/2}|D_u\rangle$$

$$\chi_{AE} = S(\rho_E) - \frac{1}{2}[S(\rho_E(u)) - S[\rho_E(u \oplus 1)]]$$

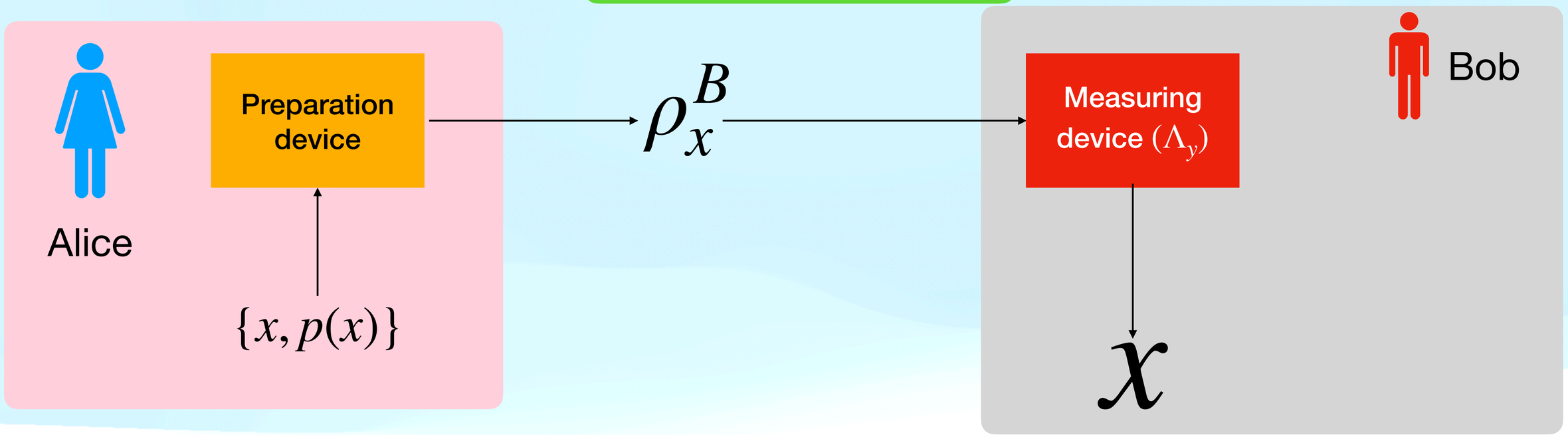
$$S[\rho_E(u)] = S[\rho_E(u \oplus 1)] = h(D); I_{AB} = 1 - h(D)$$

$$R_{DW} = I(A,B) - \chi_{AE} = 1 - 2h(D)$$

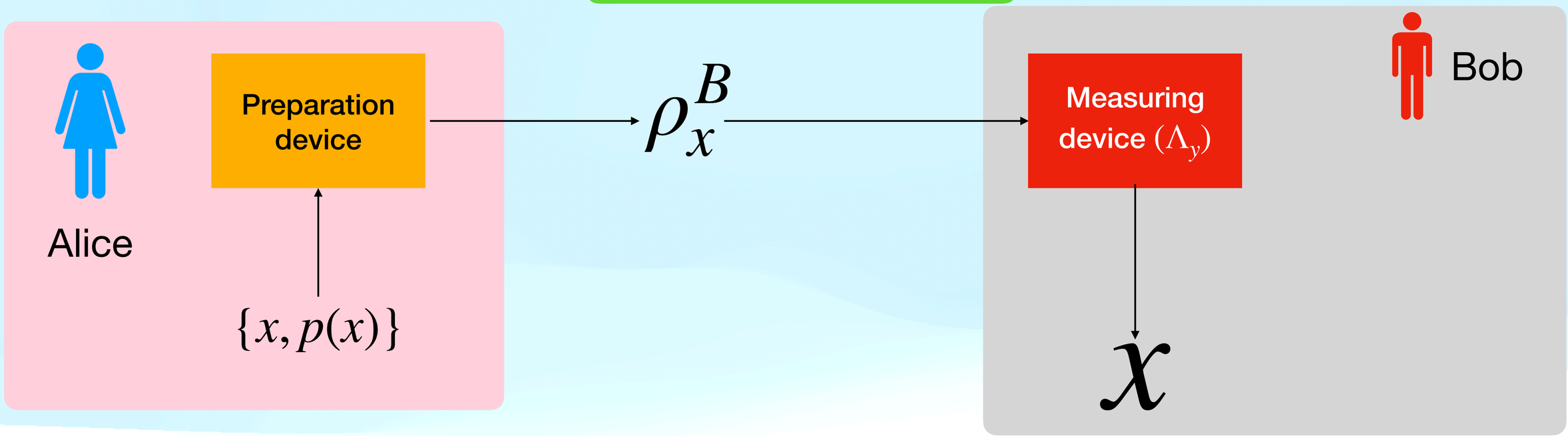
Holevo information: task under consideration



Holevo information: task under consideration

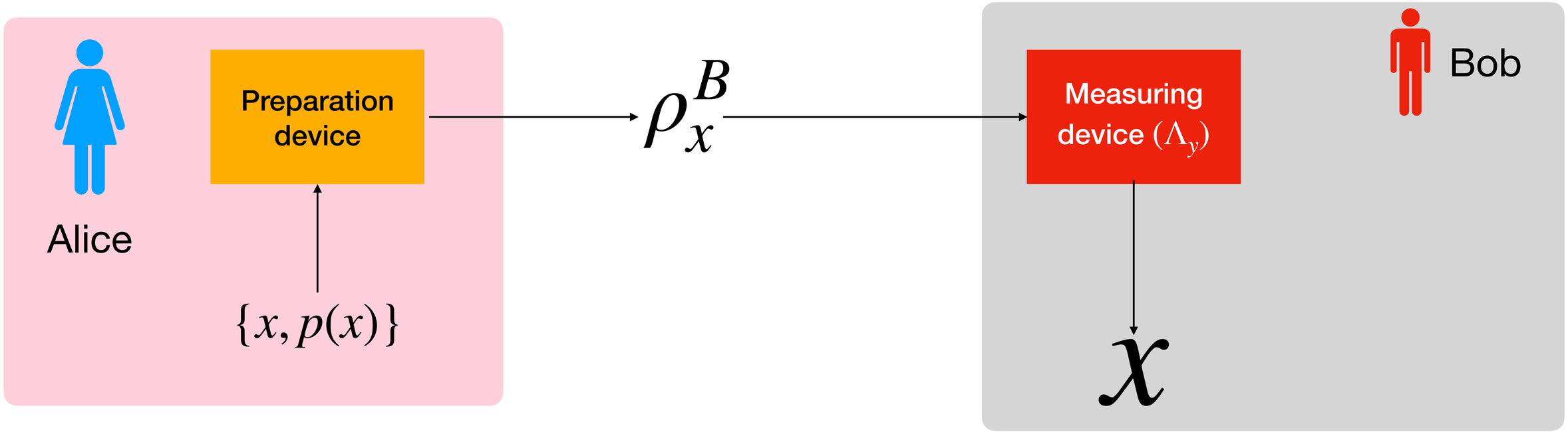


Holevo information: task under consideration



$$I_{acc}(\mathscr{E}) = \max_{\{\Lambda_y\}} I(X;Y)$$

Holevo information: task under consideration



$$I_{acc}(\mathscr{E}) = \max_{\{\Lambda_y\}} I(X;Y)$$

Upper bounded by

$$\chi(\mathscr{E}) \equiv H(\rho^B) - \sum_x p_X(x) H\left(\rho_x^B\right)$$

Holevo information: brief introduction

Alice prepares a classical ensemble $\mathscr{E} = \{p_X(x), \rho_x^B\}$ and then hands this ensemble to Bob without telling him the classical index x .

The expected density operator of this ensemble is

$$\rho^B \equiv \sum_x p_X(x)\rho_x^B$$

Holevo information: brief introduction

Alice prepares a classical ensemble $\mathscr{E} = \{p_X(x), \rho_x^B\}$ and then hands this ensemble to Bob without telling him the classical index x .

The expected density operator of this ensemble is

$$\rho^B \equiv \sum_x p_X(x)\rho_x^B$$

This density operator characterises the state from Bob's perspective because he does not have knowledge of classical index x .

Holevo information: brief introduction

Alice prepares a classical ensemble $\mathscr{E} = \{p_X(x), \rho_x^B\}$ and then hands this ensemble to Bob without telling him the classical index x. The expected density operator of this ensemble is

$$\rho^B \equiv \sum_x p_X(x)\rho_x^B$$

This density operator characterises the state from Bob's perspective because he does not have knowledge of classical index x.

His task is to determine the classical index x by performing some measurement on his system B.

The accessible information quantifies Bob's information gain after performing some optimal measurement $\{\Lambda_y\}$ on his system B:

$$I_{acc}(\mathscr{E}) = \max_{\{\Lambda_y\}} I(X;Y)$$

Holevo information: brief introduction

Suppose that Alice prepares a classical ensemble $\mathscr{E} = \{p_X(x), \rho_x^B\}$ and then hands this ensemble to Bob without telling him the classical index x. The expected density operator of this ensemble is

$$\rho^B \equiv \sum_x p_X(x)\rho_x^B$$

This density operator characterises the state from Bob's perspective because he does not have knowledge of classical index x.

His task is to determine the classical index x by performing some measurement on his system B.

The accessible information quantifies Bob's information gain after performing some optimal measurement $\{\Lambda_y\}$ on his system B:

$$I_{acc}(\mathscr{E}) = \max_{\{\Lambda_y\}} I(X;Y)$$

Where Y is a random variable corresponding to the outcome of the ensemble.

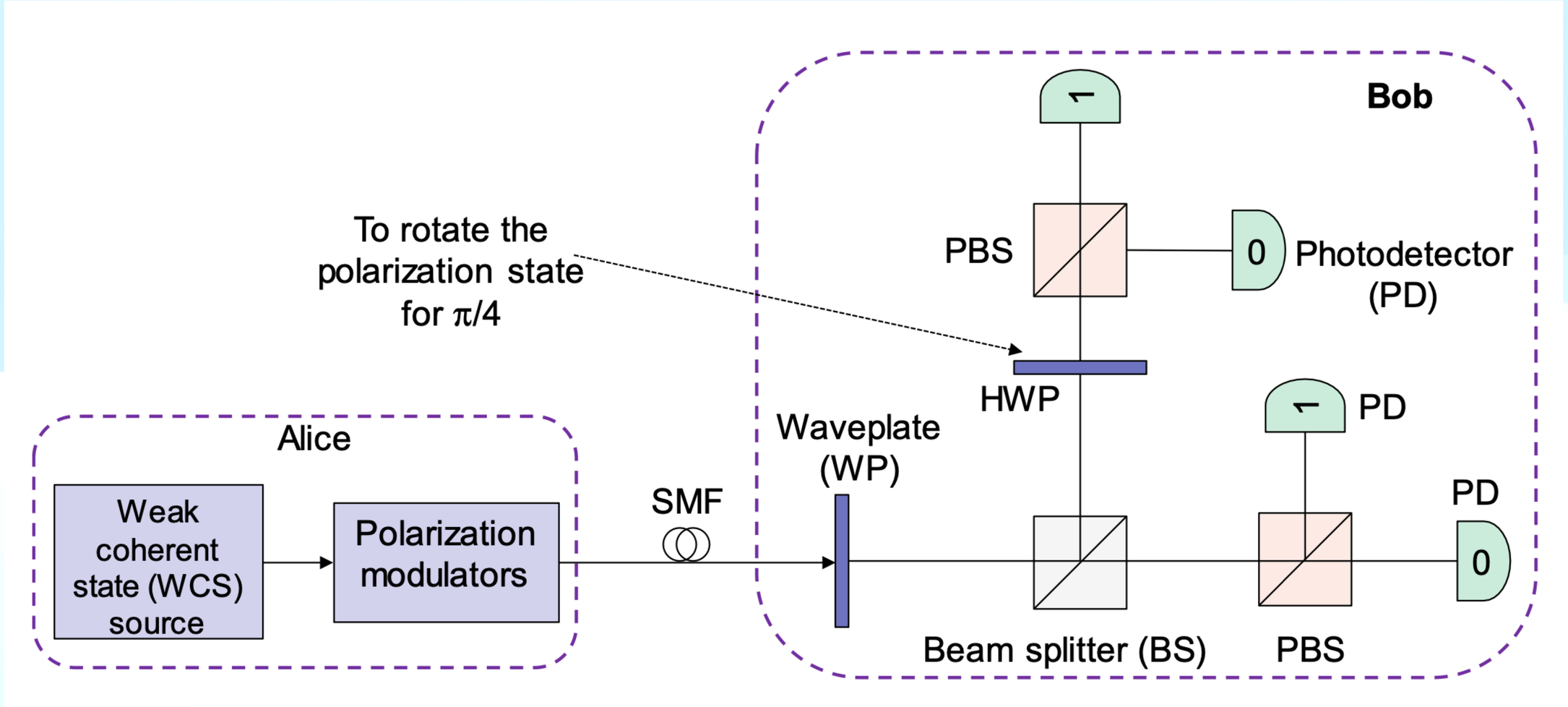
In general, this quantity is hard to calculate.

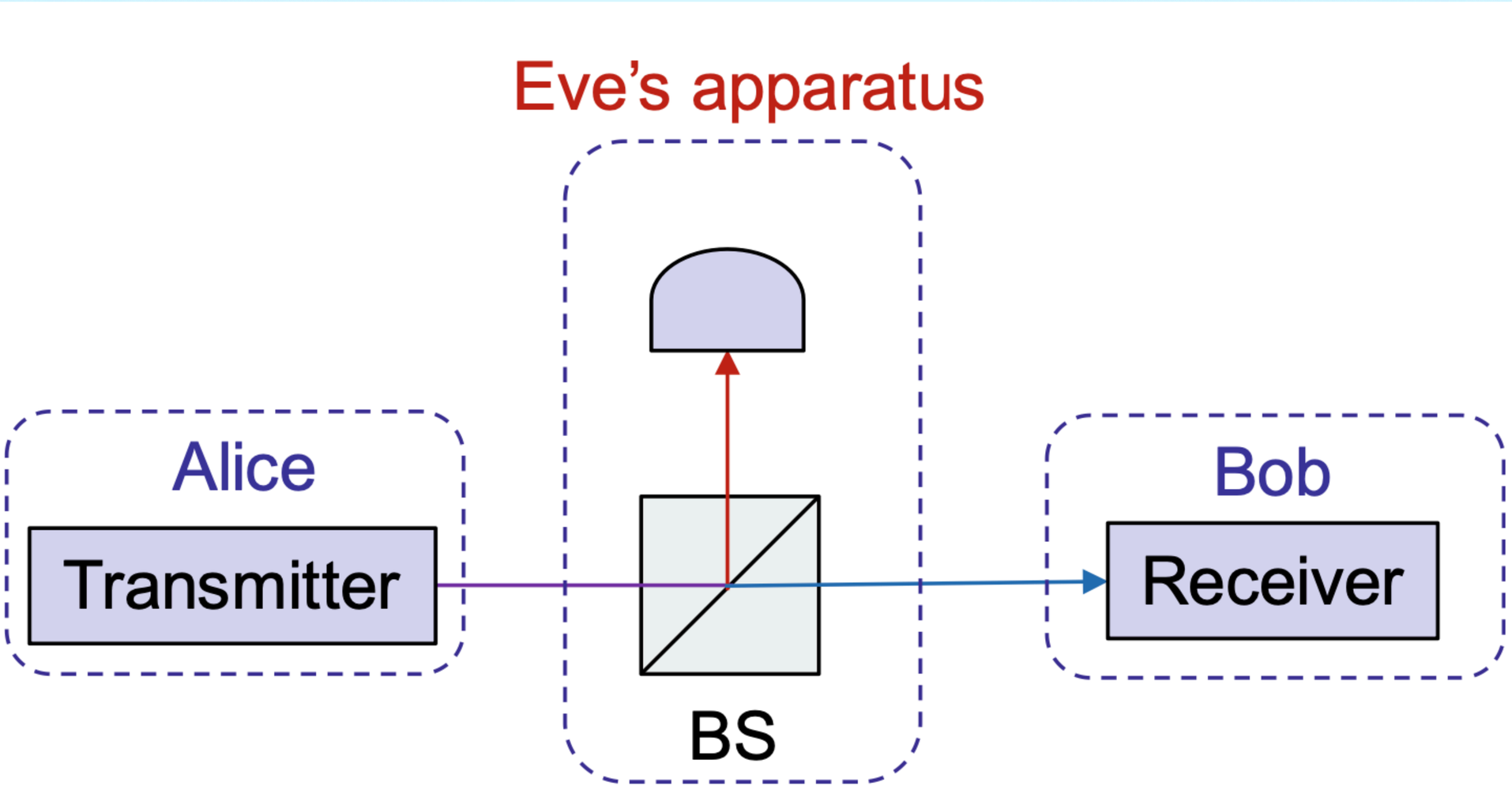
Holevo information provides a useful upper bound.

$$\chi(\mathscr{E}) \equiv H(\rho^B) - \sum_x p_X(x) H\left(\rho_x^B\right)$$

Change of theme
Attacks based on side channels

Schematic for experimental implementation Polarisation based BB84 protocol




Eve's apparatus
Alice
Transmitter
BS
Bob
Receiver

Decoy state based QKD protocol

$$\rho_\mu = \sum_{n=0}^{\infty} P_\mu(n) \, |n\rangle\langle n| \qquad P_\mu(n) = \frac{\mu^n e^{-\mu}}{n!}$$

Decoy state based QKD protocol

$$\rho_\mu = \sum_{n=0}^{\infty} P_\mu(n)\,|n\rangle\langle n| \qquad P_\mu(n) = \frac{\mu^n e^{-\mu}}{n!}$$

The gain of the protocol Q_μ

The success probability that Bob's detector clicks when triggered by Alice's pulse.

Gain: the ratio of the number of Bob's detection events (where Bob chooses the same basis as Alice) to Alice's number of emitted signals.

QBER: the error rate of Bob's detection events for the case that Alice and Bob use the same basis.

Problem: Very hard to obtain a good lower bound on and a good upper bound on e_1.

One Solution: prior art methods (as in GLLP) make the most pessimistic assumption that all multiphoton signals emitted by Alice will be received by Bob.

Key point of the decoy state idea:

Alice prepares a set of additional states—decoy states, in addition to standard BB84 states.

Those decoy states are used for the purpose of detecting eavesdropping attacks only, whereas the standard BB84 states are used for key generation only.

Only difference between the decoy state and the standard BB84 states: Their intensities (i.e., their photon number distributions).

By measuring the yields and QBER of decoy states, the authors show that Alice and Bob can obtain reliable bounds to Ω and e_1, thus allowing them to surpass all prior art results substantially.

General theory of new decoy state schemes.

Assumptions:

Alice: can prepare phase-randomized coherent states and can turn her power up and down for each signal.

This may be achieved by using standard commercial variable optical attenuators (VOAs).

Let $|\sqrt{\mu}e^{i\theta}\rangle$ denote a weak coherent state emitted by Alice.

Assuming that the phase, θ, of all signals is totally randomized, the probability distribution for the number of photons of the signal state follows a Poisson distribution with some parameter μ.

That is to say that, with a probability $p_n = \frac{\mu^n e^{-\mu}}{n!}$, Alice's signal will have n photons.

We have assumed that Alice can prepare any Poissonian (with parameter μ) mixture of photon number states and, moreover, Alice can vary the parameter, μ, for each individual signal.

Q_μ: Gain for a coherent state $|\sqrt{\mu}e^{i\theta}\rangle$.

(The random mixture $|\sqrt{\mu}e^{i\theta}\rangle$ randomised over all values of θ as the phase is assumed to be totally randomized.)

$$Q_\mu = Y_0 e^{-\mu} + Y_1 e^{-\mu}\mu + Y_2 e^{-\mu}\frac{\mu^2}{2} + \cdots + Y_n e^{-\mu}\frac{\mu^n}{n!} + \cdots$$

Y_n: the yield of n photon signal.

Y_0: the detection events due to background including dark counts and stray light from timing pulses.

.

The QBER can depend on the photon number.

e_n : the QBER of an n-photon signal.

The QBER E_μ for a coherent state $|\sqrt{\mu}e^{i\theta}\rangle$:

$$Q_\mu E_\mu = Y_0 e^{-\mu} e_0 + Y_1 e^{-\mu}\mu e_1 + Y_2 e^{-\mu}(\mu^2/2) e_2 + \cdots + Y_n e^{-\mu}(\mu^n/n!) e_n + \cdots$$

Essence of the decoy state idea

***A* decoy and a signal**: have the same characteristics (wavelength, timing information, etc.).

Eve: cannot distinguish a decoy state from a signal state.

The only piece of information available to Eve: the number of photons in a signal.

The yield, Y_n, and QBER, e_n: can depend on <u>only</u> the photon number, n, but not which distribution (decoy or signal) the state is from.

Essence of the decoy state idea

$$Y_n(\text{signal}) = Y_n(\text{decoy}) = Y_n$$

$$e_n(\text{signal}) = e_n(\text{decoy}) = e_n$$

Assumption: Alice will pick an infinite number of possible intensities (all non- negative values of μ) for decoy states.

Purpose served: Alice and Bob can experimentally measure the yield Q_μ and the QBER e_μ.

Relations between the variables $Q'_\mu s$ and $Y'_n s$ and between $E'_\mu s$ and $e'_n s$: linear.

$\{Q'_\mu s\}$ and $\{E'_\mu s\}$ measured from their experiments $\Longrightarrow$ $\{Y'_n s\}$ and $\{e'_n s\}$.

Alice and Bob can constrain simultaneously the yields, Y_n, and QBER, e_n, simultaneously for *all* n.

Suppose Alice and Bob know their channel property well (Well characterised channel).

They know what range of values of Y_n's and e_n's is acceptable.

Any attack by Eve that will change the value of any one of the Y_n's and e_n's substantially will, in principle, be caught with high probability by our decoy state method.

Therefore, in order to avoid being detected, the eavesdropper, Eve, has very limited options in her eavesdropping attack.

Yield.

(a) $n = 0$. In the absence of eavesdropping, Y_0: given by the background detection event rate p_{dark} of the system.

(b) $n \geq 1$. Two sources of Y_n : (i) the detection of signal photons η_n and (ii) the background event p_{dark} .

$$Y_n = \eta_n + p_{\text{dark}} - \eta_n p_{\text{dark}} \approx \eta_n + p_{\text{dark}}$$

10^{-3} 10^{-5}

η : overall transmission probability of each photon.

Normal channel: independence between the behaviors of the *n photons*.

The transmission efficiency for n-photon signals η_n:

$$\eta_n = 1 - (1 - \eta)^n$$

(For a small η and ignore the dark count $Y_n = n\eta$.)

QBER in a realistic experiment:

(a) If the signal is a vacuum, Bob's detection is due to background including dark counts and stray light due to timing pulses. Assuming that the two detectors have equal background event rates, then the output is totally random and the error rate is 50%. That is, the QBER for the vacuum $e_0 = 1/2$.

(b) If the signal has $n \geq 1$ photons, it also has some error rate, say e_n.

e_n comes from two parts, erroneous detections and background contribution,

$$e_n = \frac{1}{Y_n}\left(e_{\text{detector}}\eta_n + \frac{1}{2}p_{\text{dark}} \right)$$

where e_{detector} is independent of n.
The values of Y_n and e_n can be experimentally verified by Alice and Bob using our decoy state method. Any attempt by Eve to change them significantly will almost always be caught.

Combining decoy state idea with GLLP.—Suppose key *generation is done on signal state* $|\sqrt{\mu}e^{i\theta}\rangle$.

In principle, Alice and Bob can isolate the single-photon signals and apply privacy amplification to them only.

Therefore, generalizing the work in GLLP, we find Eq. (1) where the gain of the signal state, $Q_\mu = \sum_{k=0}^{\infty} Y_k e^{-\mu} \frac{\mu^k}{k!}$

and the fraction of Bob's detection events that have originated from single-photon signals emitted by Alice is given by:

$$\Omega = \frac{Q_1}{Q_\mu}.$$

Where

$$Q_1 = Y_1 \mu e^{-\mu}.$$

Assumption: error correction protocols can achieve the fundamental (Shannon) limit.

However, practical error correction protocols are generally inefficient. A simple way to take this inefficiency into account is to introduce a function, $f(e)> 1$, of the QBER, e. By doing so, we find that the key generation rate for practical protocols is given by:

$$S \geq q\{-Q_\mu f(E_\mu) H_2(E_\mu) + Q_1(1 - H_2(e))\}$$

Decoy state based QKD protocol

$$\rho_\mu = \sum_{n=0}^{\infty} P_\mu(n) \, |n\rangle\langle n| \qquad P_\mu(n) = \frac{\mu^n e^{-\mu}}{n!}$$

The gain of the protocol Q_μ

The success probability that Bob's detector clicks when triggered by Alice's pulse.

QBER E_μ

The overall error affecting the detection.

Ω : **Fraction of Bob's detection events corresponding to single-photon pulses emitted by Alice.**

$$1 - \Omega = \frac{\sum_{n>1} P_\mu}{Q_\mu}$$

ΩQ_μ : A lower bound for the probability Q_1 that Bob's detector clicks when Alice sends a single-photon state

$\frac{E_\mu}{\Omega} \rightarrow$ An upper bound for the QBER e_1 associated with the detection of the single photon pulses.

$Q_\mu f(E_\mu) H_2(E_\mu)$: **Number of bits sacrificed per use after applying error correction to the entire data (generated from both single- and multi photon pulses)**

EC effciency

$$R^{re}_{BB84} = \frac{1}{2} Q_\mu \left\{ \Omega \left(1 - H_2(E_\mu \Omega^{-1}) \right) - f(E_\mu) H_2(E_\mu) \right\}$$

Due to Gottesman-Lo-Lutkenhaus -Preskill

Have presented hand wavingly without the procedure for $f(E_\mu)$.

A factor due to experimental losses

$$R^{re}_{BB84} = \frac{1}{2} Q_\mu \left\{ \Omega \left(1 - H_2(E_\mu \Omega^{-1}) \right) - f(E_\mu) H_2(E_\mu) \right\}$$

Due to Gottesman-Lo-Lutkenhaus -Preskill

Have presented hand wavingly without the procedure for $f(E_\mu)$.

$$R_{BB84}^{re} = \frac{1}{2} Q_\mu \left\{ \Omega \left(1 - H_2(E_\mu \Omega^{-1}) \right) - f(E_\mu) H_2(E_\mu) \right\}$$

Due to Gottesman-Lo-Lutkenhaus -Preskill

Have presented hand wavingly without the procedure for $f(E_\mu)$.

If Alice sends different values of light intensity μ,

then $Q_\mu = \sum_{n=0}^{\infty} Y_n \frac{\mu^n e^{-\mu}}{n!}$;

$$E_\mu = \frac{1}{Q_\mu} \sum_{n=0}^{\infty} e_n Q_n = \frac{1}{Q_\mu} \sum_{n=0}^{\infty} e_n Y_n \frac{\mu^n e^{-\mu}}{n!}$$

Become linearly independent.

$$R_{BB84}^{re} = \frac{1}{2} Q_\mu \left\{ \Omega \left(1 - H_2(E_\mu \Omega^{-1}) \right) - f(E_\mu) H_2(E_\mu) \right\}$$

Due to Gottesman-Lo-Lutkenhaus -Preskill

Have presented hand wavingly without the procedure for $f(E_\mu)$.

Control parameter: number of pulses with different μ

If Alice sends different values of light intensity μ,

then $Q_\mu = \sum_{n=0}^{\infty} Y_n \frac{\mu^n e^{-\mu}}{n!}$;

$$E_\mu = \frac{1}{Q_\mu} \sum_{n=0}^{\infty} e_n Q_n = \frac{1}{Q_\mu} \sum_{n=0}^{\infty} e_n Y_n \frac{\mu^n e^{-\mu}}{n!}$$

Become linearly independent.

BREAK!

CSS Code [n, k] code

Generator matrix G: maps messages to their equivalents in code spaces.

Code $\rightarrow y = Gx \leftarrow$ Message

CSS Code [n, k] code

Generator matrix G: maps messages to their equivalents in code spaces.

Code $\rightarrow y = Gx \leftarrow$ Message

$0 \rightarrow (0,0,0)^T$ $1 \rightarrow (1,1,1)^T$

CSS Code [n, k] code

Generator matrix G: maps messages to their equivalents in code spaces.

Code $\rightarrow y = Gx \leftarrow$ Message

$0 \rightarrow (0,0,0)^T$ $\quad$ $1 \rightarrow (1,1,1)^T$

$G = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ $\quad$ $Hx = 0$

$(n-k) \times n$ Matrix with entries in $\{0,1\}$

CSS Code [n, k] code

Generator matrix G: maps messages to their equivalents in code spaces.

Code $\rightarrow y = Gx \leftarrow$ Message

$0 \rightarrow (0,0,0)^T$ $\quad$ $1 \rightarrow (1,1,1)^T$

$G = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ $\quad$ $Hx = 0$

$(n-k) \times n$ Matrix with entries in $\{0,1\}$

$(n-k)$ Linearly independent vectors orthogonal to the columns of G.

$$H = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

If an error e occurs, $y' \rightarrow y + e$

Since $Hy = 0$ for all codewords y, it follows that

$$Hy' = Hy + He = He \leftarrow$$ Error syndrome

If an error e occurs, $y' \to y + e$

Since $Hy = 0$ for all codewords y, it follows that

$$Hy' = Hy + He = He \leftarrow \text{Error syndrome}$$

Different error syndromes

$$He_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad He_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad He_3 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

If an error e occurs, $y' \to y + e$

Since $Hy = 0$ for all codewords y, it follows that

$$Hy' = Hy + He = He \leftarrow \text{ Error syndrome}$$

Different error syndromes

$$He_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad He_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad He_3 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Makes it possible to read off the error from syndromes.

$d(x, y) \to$ Hamming distance

The number of positions in which the two bit strings differ

How many errors can such a code correct?

$$d(C) = \min_{x,y \in C, x \neq y} d(x, y)$$

$$C \rightarrow \text{An } [n, k, d] \text{ code}$$

A code with distance $(2t + 1)$ for some integer $'t'$ can be used to correct upto $'t'$ errors, simply by decoding the corrupted message $'y'$ as the unique codeword y that satisfies

$$d(y, y') \leq t\,.$$

Quantum error correction

An $[n, k_1]$ code C_1 An $[n, k_2]$ code C_2 $C_2 \subset C_1$

C_1 And $C_2^{\perp}$ Both can correct upto t errors.

For any codeword $x \in C_1$, we define the quantum state,

$$|x + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle$$

$|C_2|$: Cardinality of C_2

Crucial point: Bit flip and phase flip errors are corrected independent of each other.

Bit flip $|x\rangle \rightarrow |x + e_{\text{bit}}\rangle$

Phase flip $|x\rangle \rightarrow (-1)^{x \cdot e_{\text{phase}}} |x\rangle$

Bit flip $|x\rangle \to |x + e_{\text{bit}}\rangle$

Phase flip $|x\rangle \to (-1)^{x \cdot e_{\text{phase}}} |x\rangle$

Observation: Bit flip error $\xrightarrow{\text{Hadamard}}$ Phase flip error

$$|x'\rangle \to |x' + e_{\text{phase}}\rangle$$

$$|x + e_2\rangle \to \frac{1}{\sqrt{2^{k+1}}} \sum_{y \in C_2} (-1)^{(x+y) \cdot e_{\text{phase}}} |x + y + e_{\text{bit}}\rangle$$

Bit flip $|x\rangle \to |x + e_{\text{bit}}\rangle$

Phase flip $|x\rangle \to (-1)^{x \cdot e_{\text{phase}}} |x\rangle$

Observation: Bit flip error $\xrightarrow{\text{Hadamard}}$ Phase flip error

$$|x'\rangle \to |x' + e_{\text{phase}}\rangle$$

$$|x + e_2\rangle \to \frac{1}{\sqrt{2^{k+1}}} \sum_{y \in C_2} (-1)^{(x+y) \cdot e_{\text{phase}}} |x + y + e_{\text{bit}}\rangle$$

To compute the syndrome, we apply the parity check matrix H_1 of the code C_1 and store the result in the Ancilla state:

$$|x + y + e_{\text{bit}}\rangle \to |x + y + e_{\text{bit}}\rangle |H_1(x + y + e_{\text{bit}})\rangle = |x + y + e_{\text{bit}}\rangle |H_1 e_{\text{bit}}\rangle$$

Bit flip $|x\rangle \rightarrow |x + e_{\text{bit}}\rangle$

Phase flip $|x\rangle \rightarrow (-1)^{x \cdot e_{\text{phase}}} |x\rangle$

Observation: Bit flip error $\xrightarrow{\text{Hadamard}}$ Phase flip error

$$|x'\rangle \rightarrow |x' + e_{\text{phase}}\rangle$$

$$|x + e_2\rangle \rightarrow \frac{1}{\sqrt{2^{k+1}}} \sum_{y \in C_2} (-1)^{(x+y) \cdot e_{\text{phase}}} |x + y + e_{\text{bit}}\rangle$$

To compute the syndrome, we apply the parity check matrix H_1 of the code C_1 and store the result in the Ancilla state:

$$|x + y + e_{\text{bit}}\rangle \rightarrow |x + y + e_{\text{bit}}\rangle |H_1(x + y + e_{\text{bit}})\rangle = |x + y + e_{\text{bit}}\rangle |H_1 e_{\text{bit}}\rangle$$

To detect the error, measure the Ancilla state, discard it and apply NOT gate on the qubits where a bit flip has occurred.

This removes all the bit flip errors and the resulting state is:

$$\frac{1}{\sqrt{2^{k_2}}} \sum_{y \in C_2} (-1)^{(x+y)\cdot e_{\text{phase}}} |x+y\rangle$$

This removes all the bit flip errors and the resulting state is:

$$\frac{1}{\sqrt{2^{k_2}}} \sum_{y \in C_2} (-1)^{(x+y)\cdot e_{\text{phase}}} |x+y\rangle$$

$$\frac{1}{\sqrt{2^{k_2}}} \sum_{y \in C_2} (-1)^{(x+y)\cdot e_{\text{phase}}} |x+y\rangle \xrightarrow{H} \frac{1}{\sqrt{2^{n+k_2}}} \sum_{z} \sum_{y \in C_2} (-1)^{(x+y)\cdot (e_{\text{phase}}+z)} |z\rangle$$

This removes all the bit flip errors and the resulting state is:

$$\frac{1}{\sqrt{2^{k_2}}}\sum_{y\in C_2}(-1)^{(x+y)\cdot e_{\text{phase}}}|x+y\rangle$$

$$\frac{1}{\sqrt{2^{k_2}}}\sum_{y\in C_2}(-1)^{(x+y)\cdot e_{\text{phase}}}|x+y\rangle \xrightarrow{H} \frac{1}{\sqrt{2^{n+k_2}}}\sum_{z}\sum_{y\in C_2}(-1)^{(x+y)\cdot(e_{\text{phase}}+z)}|z\rangle$$

If $z'\in C^{\perp}$, then $\sum_{y\in C_2}(-1)^{y\cdot z'}=|C_2|$, while if $z'\notin C^{\perp}$, $\sum_{y\in C_2}(-1)^{y\cdot z'}=0$. So,

$$\frac{1}{\sqrt{2^{n-k_2}}}\sum_{z'\in C_2^{\perp}}(-1)^{x\cdot z'}|z'+e_{\text{phase}}\rangle$$

This removes all the bit flip errors and the resulting state is:

$$\frac{1}{\sqrt{2^{k_2}}}\sum_{y\in C_2}(-1)^{(x+y)\cdot e_{\text{phase}}}|x+y\rangle$$

$$\frac{1}{\sqrt{2^{k_2}}}\sum_{y\in C_2}(-1)^{(x+y)\cdot e_{\text{phase}}}|x+y\rangle \xrightarrow{H} \frac{1}{\sqrt{2^{n+k_2}}}\sum_{z}\sum_{y\in C_2}(-1)^{(x+y)\cdot(e_{\text{phase}}+z)}|z\rangle$$

If $z'\in C^{\perp}$, then $\sum_{y\in C_2}(-1)^{y\cdot z'}=|C_2|$, while if $z'\notin C^{\perp}$, $\sum_{y\in C_2}(-1)^{y\cdot z'}=0$. So,

$$\frac{1}{\sqrt{2^{n-k_2}}}\sum_{z'\in C_2^{\perp}}(-1)^{x\cdot z'}|z'+e_{\text{phase}}\rangle$$

Exactly the same form as that of a bit-flip error described the vector e_{phase}.

Shor-Preskill proof for security of BB84 protocol

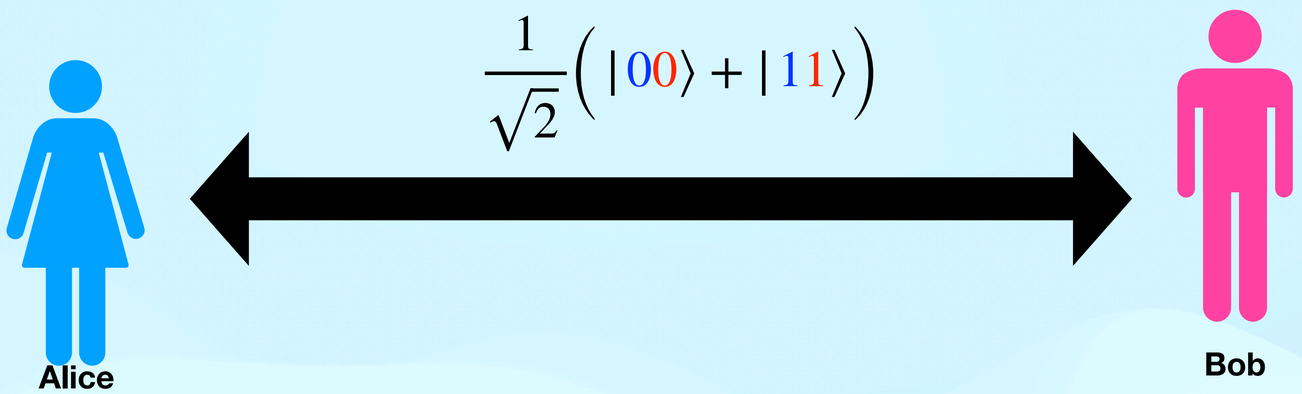
Shor-Preskill proof for security of BB84 protocol

Key result: Key generation rate: $1 - 2h(\epsilon)$

Shor-Preskill proof for security of BB84 protocol

Key result: Key generation rate: $1 - 2h(\epsilon)$

Entanglement-based version of BB84 protocol



Alice and Bob distribute a sequence of m of these states, i.e.,

$$|\Phi^+\rangle_{AB}^{\otimes m} = |\Phi^+\rangle_{AB} \otimes |\Phi^+\rangle_{AB} \otimes \cdots \otimes |\Phi^+\rangle_{AB}$$

In practice, they will share a mixed state ρ .

Entanglement-based version of BB84 protocol

1.Alice creates $2n$ qubit pairs in the state $|\Phi^+\rangle^{\otimes 2n}$ with $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Entanglement-based version of BB84 protocol

1. Alice creates $2n$ qubit pairs in the state $|\Phi^+\rangle^{\otimes 2n}$ with $|\Phi^+\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big)$.
2. She randomly selects n of these qubits that will later be used to estimate the errors in the qubit pairs.

Entanglement-based version of BB84 protocol

1. Alice creates $2n$ qubit pairs in the state $|\Phi^+\rangle^{\otimes 2n}$ with $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
2. She randomly selects n of these qubits that will later be used to estimate the errors in the qubit pairs.
3. Alice selects a random classical bit string $b = (b_1, b_2, \cdots, b_{2n})$ of length $2n$. When $b_i = 1$, she applies a Hadamard transform to her half of the corresponding qubit pair.

Entanglement-based version of BB84 protocol

1. Alice creates $2n$ qubit pairs in the state $|\Phi^+\rangle^{\otimes 2n}$ with $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
2. She randomly selects n of these qubits that will later be used to estimate the errors in the qubit pairs.
3. Alice selects a random classical bit string $b = (b_1, b_2, \cdots, b_{2n})$ of length $2n$. When $b_i = 1$, she applies a Hadamard transform to her half of the corresponding qubit pair.
4. She sends the other half of all qubit pairs to Bob.

Entanglement-based version of BB84 protocol

1. Alice creates $2n$ qubit pairs in the state $|\Phi^+\rangle^{\otimes 2n}$ with $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
2. She randomly selects n of these qubits that will later be used to estimate the errors in the qubit pairs.
3. Alice selects a random classical bit string $b = (b_1, b_2, \cdots, b_{2n})$ of length $2n$. When $b_i = 1$, she applies a Hadamard transform to her half of the corresponding qubit pair.
4. She sends the other half of all qubit pairs to Bob.
5. Alice announces the string b and the positions of the check qubits.

Entanglement-based version of BB84 protocol

1. Alice creates $2n$ qubit pairs in the state $|\Phi^+\rangle^{\otimes 2n}$ with $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
2. She randomly selects n of these qubits that will later be used to estimate the errors in the qubit pairs.
3. Alice selects a random classical bit string $b = (b_1, b_2, \cdots, b_{2n})$ of length $2n$. When $b_i = 1$, she applies a Hadamard transform to her half of the corresponding qubit pair.
4. She sends the other half of all qubit pairs to Bob.
5. Alice announces the string b and the positions of the check qubits.
6. Bob applies a Hadamard transformation to those qubits for which $b_i = 1$.

Entanglement-based version of BB84 protocol

1. Alice creates $2n$ qubit pairs in the state $|\Phi^+\rangle^{\otimes 2n}$ with $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
2. She randomly selects n of these qubits that will later be used to estimate the errors in the qubit pairs.
3. Alice selects a random classical bit string $b = (b_1, b_2, \cdots, b_{2n})$ of length $2n$. When $b_i = 1$, she applies a Hadamard transform to her half of the corresponding qubit pair.
4. She sends the other half of all qubit pairs to Bob.
5. Alice announces the string b and the positions of the check qubits.
6. Bob applies a Hadamard transformation to those qubits for which $b_i = 1$.
7. Alice and Bob measure the check qubits in the computational basis $\{|0\rangle, |1\rangle\}$ to estimate the error rate. If more than t errors occur, they abort the protocol.

Entanglement-based version of BB84 protocol

1. Alice creates $2n$ qubit pairs in the state $|\Phi^+\rangle^{\otimes 2n}$ with $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
2. She randomly selects n of these qubits that will later be used to estimate the errors in the qubit pairs.
3. Alice selects a random classical bit string $b = (b_1, b_2, \cdots, b_{2n})$ of length $2n$. When $b_i = 1$, she applies a Hadamard transform to her half of the corresponding qubit pair.
4. She sends the other half of all qubit pairs to Bob.
5. Alice announces the string b and the positions of the check qubits.
6. Bob applies a Hadamard transformation to those qubits for which $b_i = 1$.
7. Alice and Bob measure the check qubits in the computational basis $\{|0\rangle, |1\rangle\}$ to estimate the error rate. If more than t errors occur, they abort the protocol.
8. If the number of errors is below than t, Alice and Bob use the error correction codes C_1 and C_2 to correct the errors in the n remaining bits and obtain $|\Phi^+\rangle^{\otimes m}$.

Entanglement-based version of BB84 protocol

1. Alice creates $2n$ qubit pairs in the state $|\Phi^+\rangle^{\otimes 2n}$ with $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
2. She randomly selects n of these qubits that will later be used to estimate the errors in the qubit pairs.
3. Alice selects a random classical bit string $b = (b_1, b_2, \cdots, b_{2n})$ of length $2n$. When $b_i = 1$, she applies a Hadamard transform to her half of the corresponding qubit pair.
4. She sends the other half of all qubit pairs to Bob.
5. Alice announces the string b and the positions of the check qubits.
6. Bob applies a Hadamard transformation to those qubits for which $b_i = 1$.
7. Alice and Bob measure the check qubits in the computational basis $\{|0\rangle, |1\rangle\}$ to estimate the error rate. If more than t errors occur, they abort the protocol.
8. If the number of errors is below than t, Alice and Bob use the error correction codes C_1 and C_2 to correct the errors in the n remaining bits and obtain $|\Phi^+\rangle^{\otimes m}$.
9. They measure the state $|\Phi^+\rangle^{\otimes m}$ in the computational basis to obtain the shred secret key.

Lemma

Let $\epsilon \geq 0$ and ρ_{AB} be a bipartite quantum system such that

$$F\left(\rho_{AB}, |\phi^+\rangle^{\otimes m}\right) \geq 1 - \epsilon^2.$$

Then the two $n-$bit strings resulting from local measurements of ρ_{AB} in the computational basis are $\epsilon-$secure keys (with respect to an adversary who controls a purifying system of ρ_{AB}.)

Lemma

Let $\epsilon \geq 0$ and ρ_{AB} be a bipartite quantum system such that

$$F\left(\rho_{AB}, |\phi^{+}\rangle^{\otimes m}\right) \geq 1 - \epsilon^{2}.$$

Then the two $n-$bit strings resulting from local measurements of ρ_{AB} in the computational basis are $\epsilon-$secure keys (with respect to an adversary who controls a purifying system of ρ_{AB}.)

Purifying system

$|\psi_{ABE}\rangle$ Such that $\rho_{AB} = Tr_{E}\left(|\psi_{ABE}\rangle\langle\psi_{ABE}|\right)$

$$\rho_{E} = Tr_{AB}\left(|\psi_{ABE}\rangle\langle\psi_{ABE}|\right)$$

Criterion for a protocol to be secure:

$$\frac{1}{2}\left|\left|\rho_{ABE}-\rho_{UU}\otimes\rho_{E}\right|\right|_{1}\leq\epsilon,$$

$$\rho_{UU}=\sum_{u\in\mathcal{S}}\frac{1}{|\mathcal{S}|}|u\rangle\langle u|\otimes|u\rangle\langle u|$$

$$F\left(\rho_{ABE},|\Phi^{+}\rangle^{\otimes m}\otimes\sigma_{E}\right)=F\left(\rho_{AB},|\phi^{+}\rangle^{\otimes m}\right)$$

$$\frac{1}{2}\left|\left|\rho_{ABE}-||\Phi^{+}\rangle^{\otimes m}\otimes\sigma_{E}\right|\right|_{1}\leq\sqrt{1-F\left(\rho_{ABE},|\Phi^{+}\rangle^{\otimes m}\otimes\sigma_{E}\right)}$$

Relation between trace distance and fidelity

$$=\sqrt{1-F\left(\rho_{AB},|\Phi^{+}\rangle^{\otimes m}\right)}$$

$$\leq\sqrt{1-(1-\epsilon^{2})}=\epsilon$$

Quantum measurements do allow an interpretation in terms of classical probability theory if the observables that are considered refer to only one basis.

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle \pm |11\rangle\Big), \quad |\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}\Big(|01\rangle \pm |10\rangle\Big)$$

In the protocol, the three errors are generated by $\sigma_x, \sigma_y, \sigma_z$.

Nothing $(\mathbf{1})$	$\|\Phi^+\rangle \rightarrow \|\Phi^+\rangle$
Bit flip (σ_x)	$\|\Phi^+\rangle \rightarrow \|\Psi^+\rangle$
Phase flip (σ_z)	$\|\Phi^+\rangle \rightarrow \|\Phi^-\rangle$
Bit+phase (σ_y)	$\|\Phi^+\rangle \rightarrow \|\Psi^-\rangle$

Detectors of errors: POVM

Detector of bit-flip

$$\Pi_{bf} = |\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-|$$

Detector of phase-flip

$$\Pi_{pe} = |\Phi^-\rangle\langle\Phi^-| + |\Psi^-\rangle\langle\Psi^-|$$

$$\Pi_{bf} = \frac{1}{2}(\mathbf{1} \otimes \mathbf{1} - \sigma_z \otimes \sigma_z)$$

$$\Pi_{pe} = \frac{1}{2}(\mathbf{1} \otimes \mathbf{1} - \sigma_x \otimes \sigma_x)$$

Reduction to the prepare-and-measure version

The measurement of n check pairs in step 8 is simply used to estimate the error rate.

Instead of using entangled states, Alice can equivalently prepare and send n single qubit states to Bob. This changes sets 1, 2 and 8 of the protocol to:

Entanglement-based version of BB84 protocol

1. Alice creates n random check bits and n qubit pairs in the state $|\Phi^+\rangle^{\otimes n}$. She encodes n qubits as $|0\rangle$ or $|1\rangle$ according to the check bits.
2. She randomly chooses n out of $2n$ positions to put in the check qubits. In the remaining positions, she puts in one half of each state $|\Phi^+\rangle$.
3. Alice selects a random classical bit string $b = (b_1, b_2, \cdots, b_{2n})$ of length $2n$. When $b_i = 1$, she applies a Hadamard transform to her half of the corresponding qubit pair.
4. She sends the other half of all qubit pairs to Bob.
5. Alice announces the string b and the positions of the check qubits.
6. Bob applies a Hadamard transformation to those qubits for which $b_i = 1$.
7. Alice and Bob measure the check qubits in the computational basis $\{|0\rangle, |1\rangle\}$ to estimate the error rate. If more than t errors occur, they abort the protocol.
8. Bob measures the n check qubits in the $\{|0\rangle, |1\rangle\}$ basis and publicly shares the result with Alice. If more than t bits disagree, they abort the protocol.
9. They measure the state $|\Phi^+\rangle^{\otimes m}$ in the computational basis to obtain the shred secret key.

How to remove the remaining n entangled pairs?

Two classical linear error correction codes C_1 (encoding k_1 bits into n bits) and C_2 (encoding k_2 bits into n bits), a $[n, m]$ CSS code of C_1 over C_2 encodes $m = k_1 - k_2$ qubits into n qubits and corrects upto t errors.

Position of bit-flip error: parity check matrix H_1 of the classical code C_1

Information about the phase-error: parity check matrix $H_2^{\perp}$ of the classical dual code $C_2^{\perp}$

A codeword in this code is always of the form

$$|x_k + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x_k + y\rangle,$$

x_k: a representative of one of the 2^m cosets of C_2 in C_1.

x_k : a vector x indexed by a string k .

$$|x_k, v, w\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{v \cdot y} |x_k + y + w\rangle$$

x_k : a vector x indexed by a string k .

$$|x_k, v, w\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{v \cdot y} |x_k + y + w\rangle$$

$[n, m]$ CSS Codes of C_1 over C_2.

These states form an orthonormal basis of a 2^n dimensional Hilbert space.

x_k : a vector x indexed by a string k .

$$|x_k, v, w\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{v \cdot y} |x_k + y + w\rangle$$

$[n, m]$ CSS Codes of C_1 over C_2.

These states form an orthonormal basis of a 2^n dimensional Hilbert space.

We show that there are $2^{k_1 - k_2}$ distinct values of x_k, 2^{n-k_1} distinct values of w and 2^{k_2} distinct values of v .

x_k : a vector x indexed by a string k .

$$|x_k, v, w\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{v \cdot y} |x_k + y + w\rangle$$

$[n, m]$ CSS Codes of C_1 over C_2.

These states form an orthonormal basis of a 2^n dimensional Hilbert space.

We show that there are $2^{k_1 - k_2}$ distinct values of x_k, 2^{n-k_1} distinct values of w and 2^{k_2} distinct values of v .

I. If $x_k - x_k' \in C_2$, then $|x_k + C_2\rangle = |x_k' + C_2\rangle$, which implies that the state $|x_k + C_2\rangle$ only depends on the coset C_1/C_2 in which x_k is contained. Since there are 2^m such cosets, there are 2^m distinct values of x_k .

x_k : a vector x indexed by a string k .

$$|x_k, v, w\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{v \cdot y} |x_k + y + w\rangle$$

$[n, m]$ CSS Codes of C_1 over C_2.

These states form an orthonormal basis of a 2^n dimensional Hilbert space.

We show that there are $2^{k_1 - k_2}$ distinct values of x_k, 2^{n-k_1} distinct values of w and 2^{k_2} distinct values of v .

I. If $x_k - x_k' \in C_2$, then $|x_k + C_2\rangle = |x_k' + C_2\rangle$, which implies that the state $|x_k + C_2\rangle$ only depends on the coset C_1/C_2 in which x_k is contained. Since there are 2^m such cosets, there are 2^m distinct values of x_k .

2. Suppose that $|x_k, v, w\rangle = |x_k, v', w\rangle$. This implies that $v \cdot y = v' \cdot Y$ for all $y \in C_2$, and therefore $(v - v') \cdot y = 0$ for all $y \in C_2$. This means that $v - v' \in K$, where K is the row space of the parity check matrix H_2 of C_2. The rows of H_2 span the space of all the vectors that are orthogonal to the codewords y of C_2.

Therefore, the requirement for two states $|x_k, v, w\rangle$ and $|x_k, v', w\rangle$ to be distinct states is $v - v' \notin K$, which directly implies $v + K \neq v' + K$ (which is a property of cosets). Since H_2 has $n - k_2$ linearly independent rows, v has $2^{n-(n-k_2)} = 2^{k_2}$ distinct values.

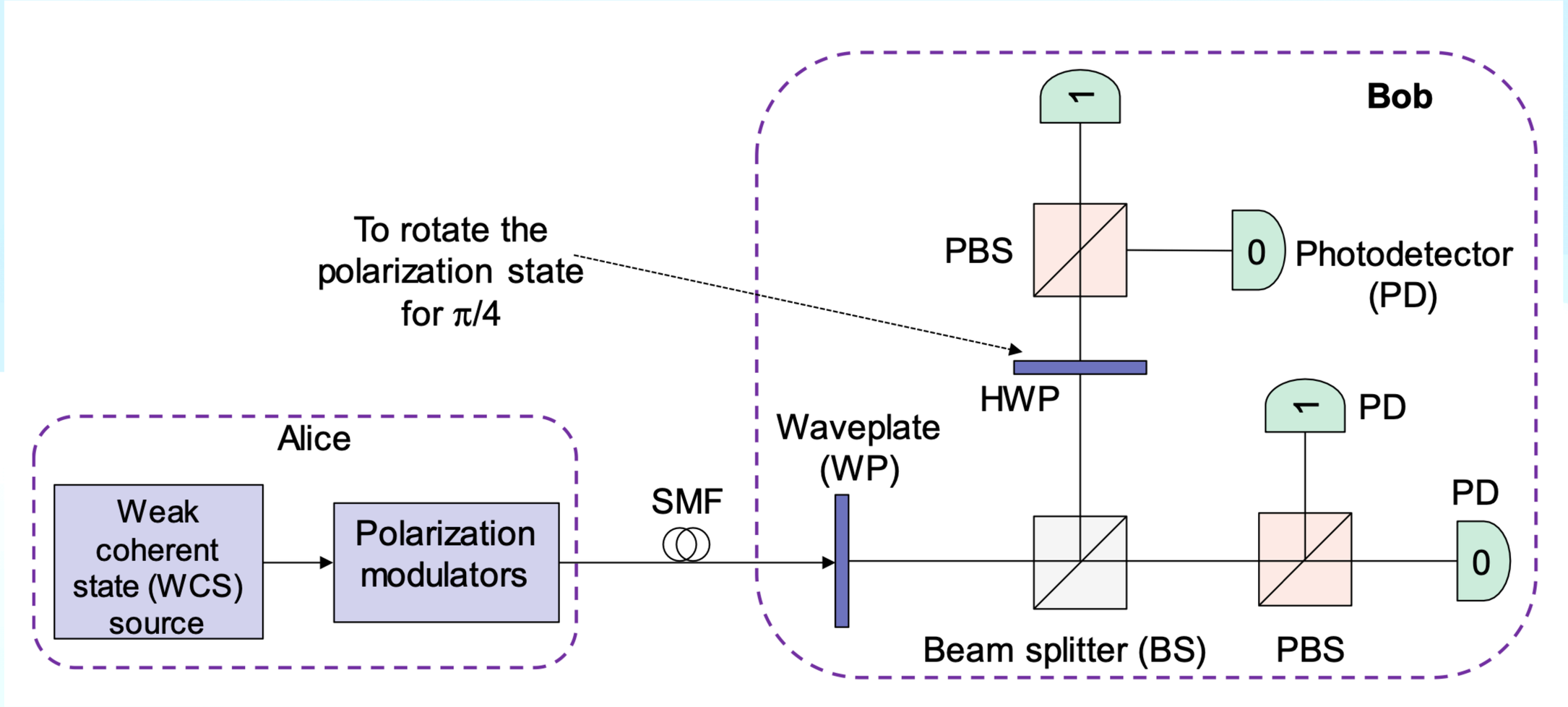
III. With a similar argument as in I, the values of w depend on the coset of C_1 in a 2^n dimensional Hilbert space in which w is contained, which implies that there are 2^{n-k_1} distinct values of w .

Orthonormality of the states

If x_k and x_k' belong to different cosets of C_1/C_2, then there are no codewords $y, y' \in C_2$ such that $x_k + y = x_k' + y'$. Hence, the states are orthonormal. A similar argument can be given in the current situation.

Consider the cosets of $C_2 \in F_2^n$ (the set of all $n-$ bit strings. For two distinct states $|x_k, v, w\rangle$ and $|x_k', v', w'\rangle, x_k + w$ and $x_k' + w$ belong to different cosets of F_2^n/C_2, and therefore, there are no $y, y' \in C_2$ such that $x_k + w + y = x_k' + w' + y'$; hence the two states are orthonormal.)

Schematic for experimental implementation Polarisation based BB84 protocol



The very first demonstration of QC was a table-top experiment performed at the IBM laboratory in the early 1990s over a distance of 30 cm (Bennett, Bessette, et al., 1992)

Experimental Quantum Cryptography[1]

Charles H. Bennett

IBM Research, Yorktown Heights, New York, NY 10598, U.S.A.

François Bessette, Gilles Brassard, and Louis Salvail

Département IRO, Université de Montréal, C.P. 6128, succursale "A", Montréal (Québec), Canada H3C 3J7

John Smolin

Physics Department, University of California at Los Angles, Los Angeles, CA 90024, U.S.A.

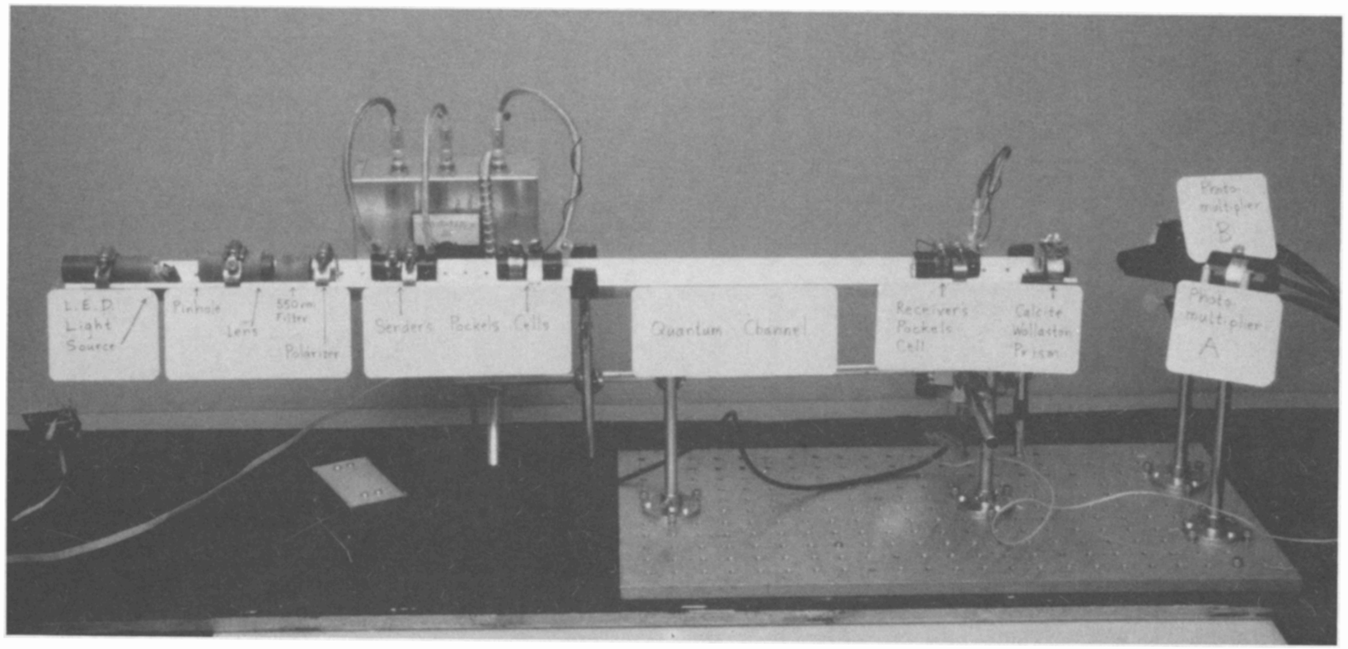


Fig. 2. Photograph of the apparatus.

Incoherent green light flashes are produced by Light Emitting Diode (LED) on the left, collimated into a beam by Pinhole and Lens, then pass through a 550 nm Filter and a horizontal Polarizer. Sender's Pockels Cells convert the horizontal polarization into an arbitrary sequence of the four polarization states (horizontal, vertical, left-circular, and right-circular). After traversing the quantum channel, a 32 cm free air optical path, the beam passes through Receiver's Pockels Cell, which, if energized, converts rectilinear into circular polarizations and vice versa. Finally, a calcite Wollaston prism splits the beam into horizontally and vertically polarized components, in which individual photons are detected by Photomultiplier tubes A and B, respectively.

There are two main possibilities. Either one chooses a wavelength around 800 nm, for which efficient photon counters are commercially available, or one chooses a wavelength compatible with today’s telecom- munications optical fibers, i.e., near 1300 or 1550 nm. The first choice requires free-space transmission or the use of special fibers, hence the installed telecommunica- tions networks cannot be used. The second choice re- quires the improvement or development of new detec- tors, not based on silicon semiconductors, which are transparent above a wavelength of 1000 nm.

In the case of transmission using optical fibers, it is still unclear which of the two alternatives will turn out to be the best choice. If QC finds niche markets, it is con- ceivable that special fibers will be installed for that pur- pose. But it is equally conceivable that new commercial detectors will soon make it much easier to detect single photons at telecommunications wavelengths. Actually, the latter possibility is very likely, as several research groups and industries are already working on it. There is another good reason to bet on this solution: the quality of telecommunications fibers is much higher than that of any special fiber; in particular, the attenuation is much lower (this is why the telecommunications industry chose these wavelengths): at 800 nm, the attenuation is about 2 dB/km (i.e., half the photons are lost after 1.5 km), while it is only of the order of 0.35 and 0.20 dB/km at 1300 and 1550 nm, respectively (50% loss after about 9 and 15 km).

In the case of free-space transmission, the choice of wavelength is straightforward, since the region where good photon detectors exist—around 800 nm—coincides with that where absorption is low. However, free-space transmission is restricted to line-of-sight links and is very weather dependent.

In principle, the resulting decrease in bit rate could be compensated for thanks to the achiev- able gigahertz modulation rates of telecommunications lasers. But in practice, the problem comes from the de- tectors' dark counts (i.e., a click without a photon's ar- riving). Indeed, the detectors must be active for all pulses, including the empty ones. Hence the total dark counts increase with the laser's modulation rate, and the ratio of detected photons to dark counts (i.e., the signal- to-noise ratio) decreases with m (see Sec. IV.A). The problem is especially severe for longer wavelengths, at which photon detectors based on indium gallium ar- senide semiconductors (InGaAs) are needed (see Sec. III.C), since the noise of these detectors explodes if they are opened too frequently (in practice with a rate larger than a few megahertz). This prevents the use of really low photon numbers, smaller than approximately 1%. Most experiments to date have relied on m50.1, mean-ing that 5% of the nonempty pulses contain more than one photon. However, it is important to stress that, as pointed out by Lu¨ tkenhaus (2000), there is an optimal m

Photon pairs generated by parametric downconversion

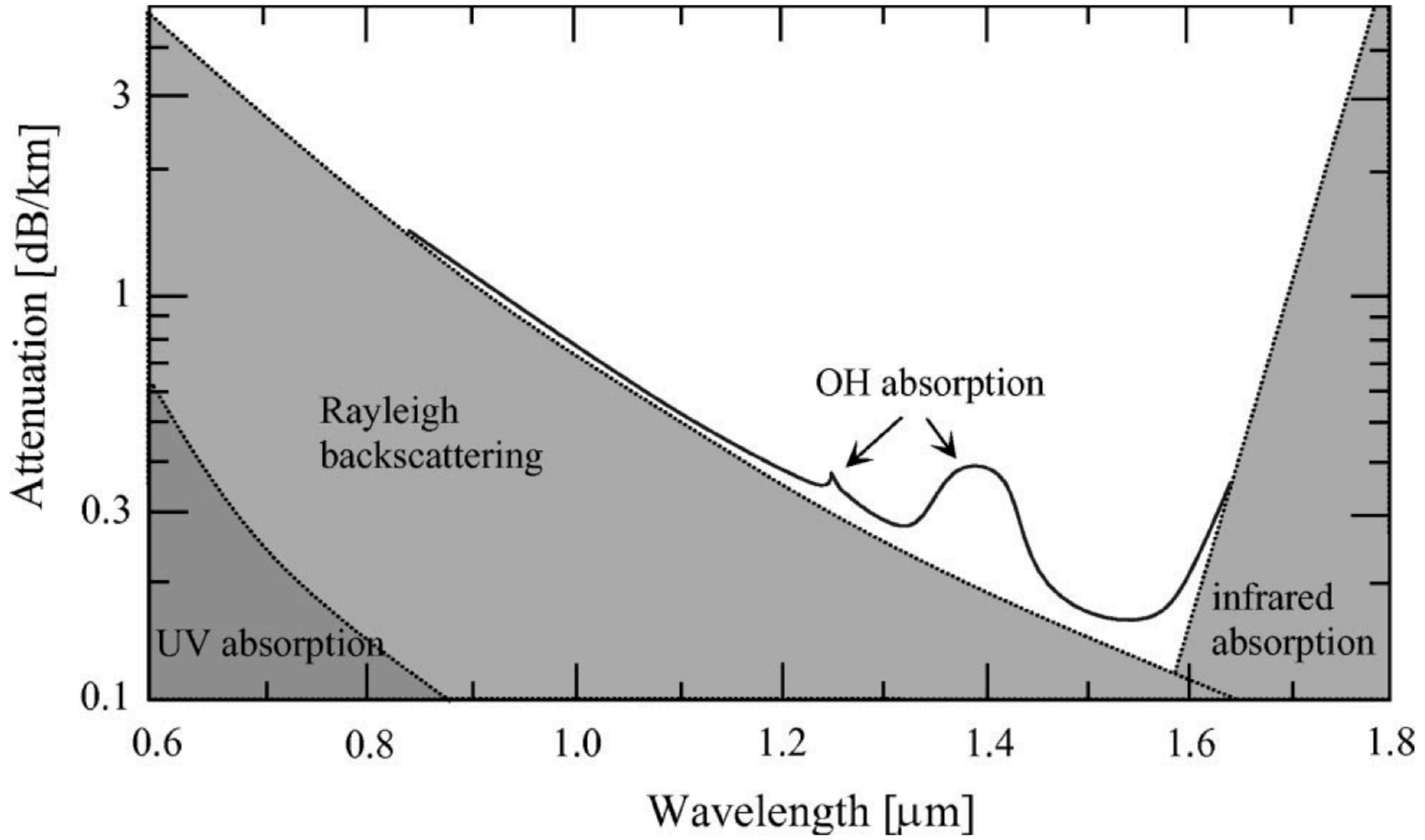
Another way to create pseudo-single-photon states is the generation of photon pairs and the use of one photon as a trigger for the other one (Hong and Mandel, 1986). In contrast to the sources discussed earlier, the second detector must be activated only whenever the first one has detected a photon, hence when m51, and not whenever a pump pulse has been emitted, therefore circumventing the problem of empty pulses.

The photon pairs are generated by spontaneous para- metric downconversion in a x (2) nonlinear crystal.16 In this process, the inverse of the well-known frequency doubling, one photon spontaneously splits into two daughter photons—traditionally called signal and idler photons—conserving total energy and momentum. In this context, momentum conservation is called phase matching and can be achieved despite chromatic disper- sion by exploiting the birefringence of the nonlinear crystal. Phase matching allows one to choose the wave- length and determines the bandwidth of the downcon- verted photons. The latter is in general rather large and varies from a few nanometers up to some tens of na- nometers. For the nondegenerate case one typically gets a bandwith of 5 – 10 nm, whereas in the degenerate case (where the central frequency of both photons is equal), the bandwidth can be as large as 70 nm.

This photon-pair creation process is very inefficient; typically it takes some 1010 pump photons to create one pair in a given mode.17 The number of photon pairs per mode is thermally distributed within the coherence time of the photons and follows a Poissonian distribution for larger time windows (Walls and Milburn, 1995). With a pump power of 1 mW, about 106 pairs per second can be collected in single-mode fibers. Accordingly, in a time window of roughly 1 ns, the conditional probability of finding a second pair, having already detected one, is 106 3 102 9 ' 0.1% . In the case of continuous pumping, this time window is given by the detector resolution. Tol- erating, for example, 1% of these multipair events, one can generate 107 pairs per second using a realistic

10-mW pump. To detect, for example, 10% of the trigger photons, the second detector has to be activated 106 times per second. In comparison, the example of 1% of multiphoton events corresponds in the case of faint laser pulses to a mean photon number of m50.02. In order to get the same number (106) of nonempty pulses per sec- ond, a pulse rate of 50 MHz is needed. For a given pho- ton statistics, photon pairs thus allow one to work with lower pulse rates (e.g., 50 times lower) and hence re- duced detector-induced errors. However, due to limited coupling efficiency in optical fibers, the probability of finding the sister photon after detection of the trigger photon in the respective fiber is in practice less than 1. This means that the effective photon number is not 1 but rather m'2/3 (Ribordy et al., 2001), still well above m 5 0.02.

Figure 5 shows one of our sources creating entangled photon pairs at a wavelength of 1310 nm, as used in tests of Bell’s inequalities over 10 kilometers (Tittel et al., 1998). Although not as simple as faint laser sources, diode-pumped photon-pair sources emitting in the near infrared can be made compact, robust, and rather handy.


Attenuation [dB/km]
3
1
0.3
0.1
0.6
0.8
1.0
1.2
1.4
1.6
1.8
Wavelength [μm]
Rayleigh
backscattering
OH absorption
UV absorption
infrared
absorption

Individual quantum systems are usually two-level sys- tems, called qubits. During their propagation they must be protected from environmental noise. Here “environ- ment” refers to everything outside the degree of free- dom used for the encoding, which is not necessarily out- side the physical system. If, for example, the information is encoded in the polarization state, then the optical fre- quencies of the photon are part of the environment. Hence coupling between the polarization and the optical frequency has to be mastered18 (e.g., by avoiding wave- length-sensitive polarizers and birefringence). Moreover, the sender of the qubits should avoid any correlation between the polarization and the spectrum of the pho- tons.

Light is guided in optical fibers thanks to the refrac- tive index profile n(x,y) across the section of the fibers (traditionally, the z axis is along the propagation direc- tion). Over the last 25 years, a lot of effort has gone into reducing transmission losses—initially several dB per km—and today the attenuation is as low as 2 dB/km at 800-nm wavelength, 0.35 dB/km at 1310 nm, and 0.2 dB/km at 1550 nm (see Fig. 6). It is amusing to note that the dynamical equation describing optical pulse propa- gation (in the usual slowly varying envelope aproxima- tion) is identical to the Schro¨ dinger equation, with V(x,y)52n(x,y) (Snyder, 1983). Hence a positive bump in the refractive index corresponds to a potential well. The region of the well is called the fiber core. If the

core is large, many bound modes exist, corresponding to many guided modes in the fiber. Such fibers are called multimode fibers, They usually have cores 50 mm in di- ameter. The modes couple easily, acting on the qubit like a nonisolated environment. Hence multimode fibers are not appropriate as quantum channels (see, however, Townsend, 1998a, 1998b). If, however, the core is small enough (diameter of the order of a few wavelengths), then a single spatial mode is guided. Such fibers are called single-mode fibers. For telecommunications wave- lengths (i.e., 1.3 and 1.5 mm), their core is typically 8 mm in diameter. Single-mode fibers are very well suited to carry single quanta. For example, the optical phase at the output of a fiber is in a stable relation with the phase at the input, provided the fiber does not become elon- gated. Hence fiber interferometers are very stable, a fact exploited in many instruments and sensors (see, for ex- ample, Cancellieri, 1993).

Polarization effects in single-mode fibers are a com- mon source of problems in all optical communication schemes, classical as well as quantum ones. In recent years these effects have been the subject of a major re- search effort in classical optical communication (Gisin et al., 1995). As a result, today's fibers are much better than the fibers of a decade ago. Today, the remaining birefringence is small enough for the telecommunica- tions industry, but for quantum communication any

birefringence, even extremely small, will always remain a concern. All fiber-based implementations of QC have to face this problem. This is clearly true for polarization- based systems, but it is equally a concern for phase- based systems, since interference visibility depends on the polarization states. Hence, although polarization ef- fects are not the only source of difficulties, we shall de- scribe them in some detail, distinguishing among four effects: the geometric phase, birefringence, polarization mode dispersion, and polarization-dependent losses.

The geometric phase as encountered when guiding light in an optical fiber is a special case of the Berry phase,19 which results when any parameter describing a property of the system under concern, here the k vector characterizing the propagation of the light field, under- goes an adiabatic change. Think first of a linear polar- ization state, let us say vertical at the input. Will it still be vertical at the output? Vertical with respect to what? Certainly not the gravitational field! One can follow that linear polarization by hand along the fiber and see how it may change even along a closed loop. If the loop stays in a plane, the state after a loop coincides with the input state, but if the loop explores the three dimensions of our space, then the final state will differ from the initial one by an angle. Similar reasoning holds for the axes of elliptical polarization states. The two circular polariza- tion states are the eigenstates. During parallel transport they acquire opposite phases, called the Berry phases. The presence of a geometrical phase is not fatal for quantum communication. It simply means that initially Alice and Bob have to align their systems by defining, for instance, the vertical and diagonal directions (i.e., performing the unitary transformation mentioned be- fore). If these vary slowly, they can be tracked, though this requires active feedback. However, if the variations are too fast, the communication might be interrupted.

Polarization mode dispersion (PMD) is the presence of two different group velocities for two orthogonal po- larization modes. It is due to a delicate combination of two causes. First, birefringence produces locally two group velocities. For optical fibers, this local dispersion is in good approximation equal to the phase dispersion, of the order of a few picoseconds per kilometer. Hence, an optical pulse tends to split locally into a fast mode and a slow mode. But because the birefringence is small, the two modes couple easily. Hence any small imperfec- tion along the fiber produces polarization mode cou- pling: some energy of the fast mode couples into the slow mode and vice versa. PMD is thus similar to a ran- dom walk21 and grows only with the square root of the fiber length. It is expressed in pskm21/2, with values as low as 0.1 pskm21/2 for modern fibers and possibly as high as 0.5 or even 1pskm21/2 for older ones.

Polarization-dependent loss is a differential attenua- tion between two orthogonal polarization modes. This effect is negligible in fibers, but can be significant in components like phase modulators. In particular, some integrated optics waveguides actually guide only one mode and thus behave almost like polarizers (e.g., pro- ton exchange waveguides in LiNbO3). Polarization- dependent losses are usually stable, but if connected to a fiber with some birefringence, the relation between the polarization state and the loss may fluctuate, producing random outcomes (Elamari et al., 1998). Polarization- dependent loss cannot be described by a unitary opera- tor acting in the polarization state space (but it is of course unitary in a larger space (Huttner, Gautier, et al., 1996). Thus it does not preserve the scalar product. In particular, it can turn nonorthogonal states into orthogo- nal ones, which can then be distinguished unambigu- ously (at the cost of some loss; Huttner, Gautier, et al., 1996; Clarke et al., 2000). Note that this attenuation could be used by Eve, especially to eavesdrop on the two-state protocol (Sec. II.D.1).

Hence the broadening of photons featuring nonzero bandwidth, or, in other words, the coupling between fre- quency and position, must be circumvented or con- trolled. This implies working with photons of small bandwidth, or, as long as the bandwidth is not too large, operating close to the wavelength l0 at which chromatic dispersion is zero, i.e., for standard fibers around 1310 nm. Fortunately, fiber losses are relatively small at this wavelength and amount to '0.35 dB/km. This region is called the second telecommunications window.22 There are also special fibers, called dispersion-shifted fibers, with a refractive index profile such that the chromatic

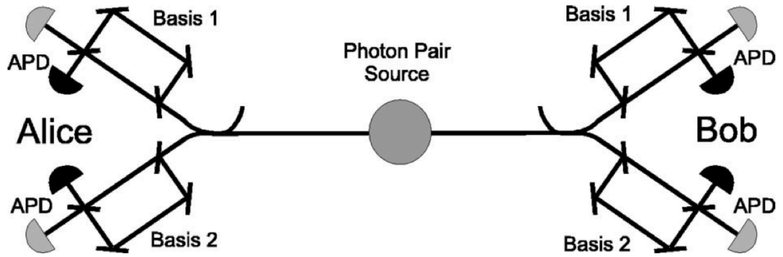


FIG. 23. System for quantum cryptography based on phase-coding entanglement: APD, avalanche photodiode. The photons choose their bases randomly at Alice and Bob's couplers.

The input two-mode Fock basis state $|01\rangle_{n1n2}$ after the first beam splitter (BS) gets transformed to

$$|01\rangle_{n_1n_2} \rightarrow 2^{-1/2}\left(j|01\rangle_{n_3n_4} + |10\rangle_{n_3n_4}\right). \tag{6.16}$$

After the phase shifts in the Mach–Zehnder (MZ) branches get introduced, we can write

$$2^{-1/2}\left(j|01\rangle_{n_3n_4} + |10\rangle_{n_3n_4}\right) \rightarrow 2^{-1/2}\left(je^{-j\phi/2}|01\rangle_{n_3n_4} + e^{j\phi/2}|10\rangle_{n_3n_4}\right), \phi = \phi_A - \phi_B, \tag{6.17}$$

where ϕ_A (ϕ_B) corresponds to the phase shift introduced in the upper (lower) branch belonging to Alice (Bob). After the second BS, the corresponding state will be

$$|01\rangle_{n_3n_4} \rightarrow 2^{-1/2}\left(j|01\rangle_{n_5n_6} + |10\rangle_{n_5n_6}\right), |10\rangle_{n_3n_4} \rightarrow 2^{-1/2}\left(j|10\rangle_{n_5n_6} + |01\rangle_{n_5n_6}\right). \tag{6.18}$$

The overall output state can be represented by

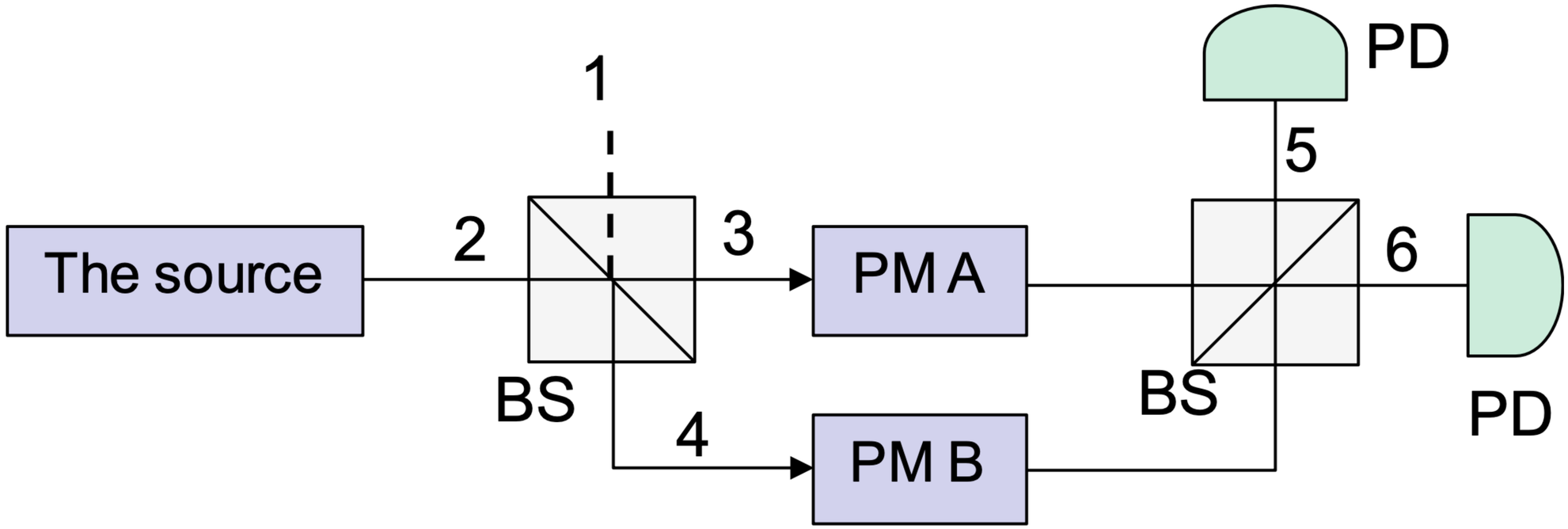
$$|\psi(\phi)\rangle = j\left(\sin(\phi/2)|01\rangle_{n_5n_6} + \cos(\phi/2)|10\rangle_{n_5n_6}\right). \tag{6.19}$$

By setting different phases ϕ we can define the states for BB84 protocol as follows:

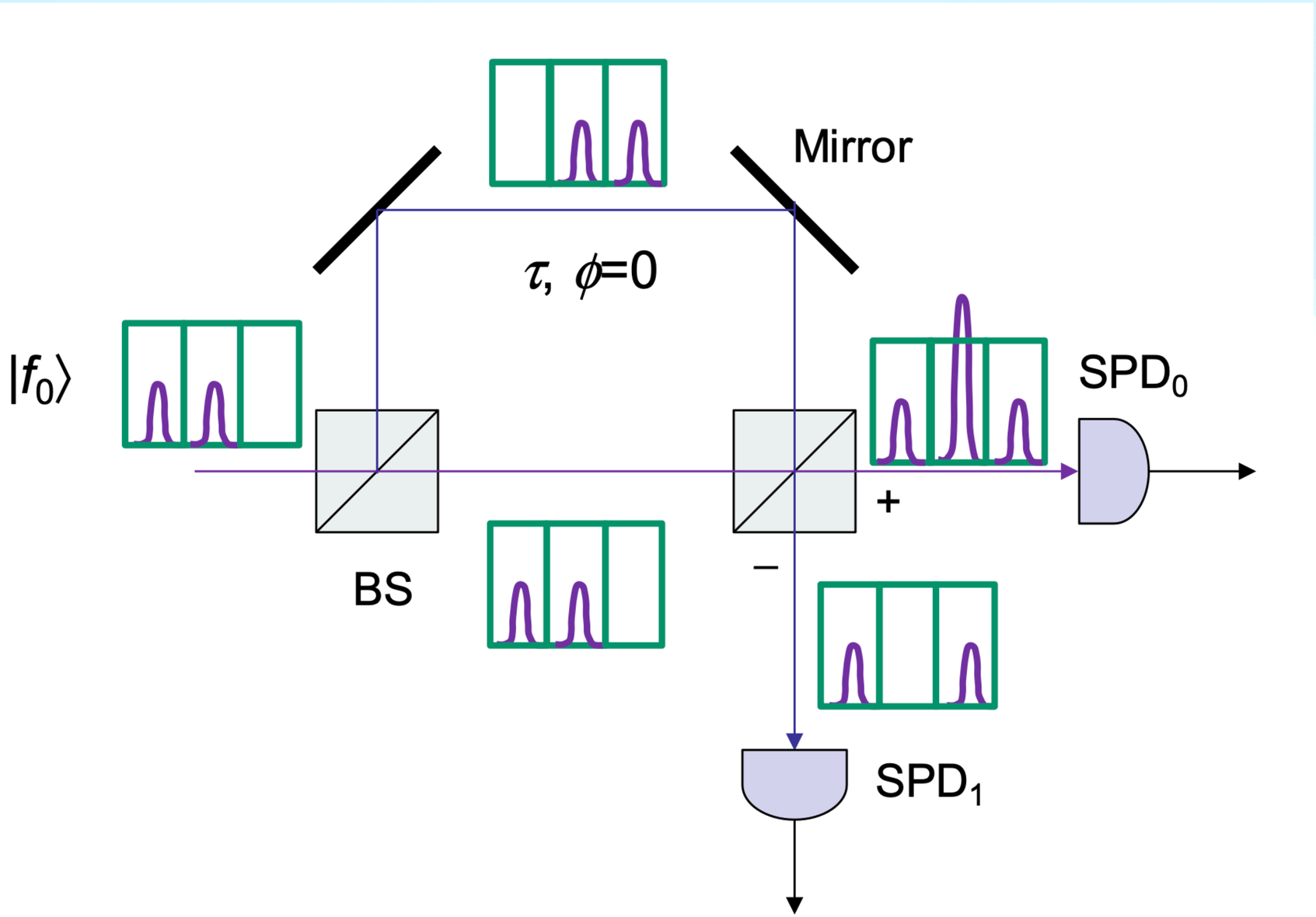
$$\begin{aligned} &|\psi(0)\rangle = j|10\rangle_{n_5n_6} \doteq |0\rangle, \qquad |\psi(\pi)\rangle = j|01\rangle_{n_5n_6} \doteq |1\rangle \\ &|\psi(\pi/2)\rangle = j2^{-1/2}\left(|10\rangle_{n_5n_6} + |01\rangle_{n_5n_6}\right) \doteq |+\rangle, |\psi(-\pi/2)\rangle \\ &\qquad = j2^{-1/2}\left(|10\rangle_{n_5n_6} - |01\rangle_{n_5n_6}\right) \doteq |-\rangle. \end{aligned} \tag{6.20}$$

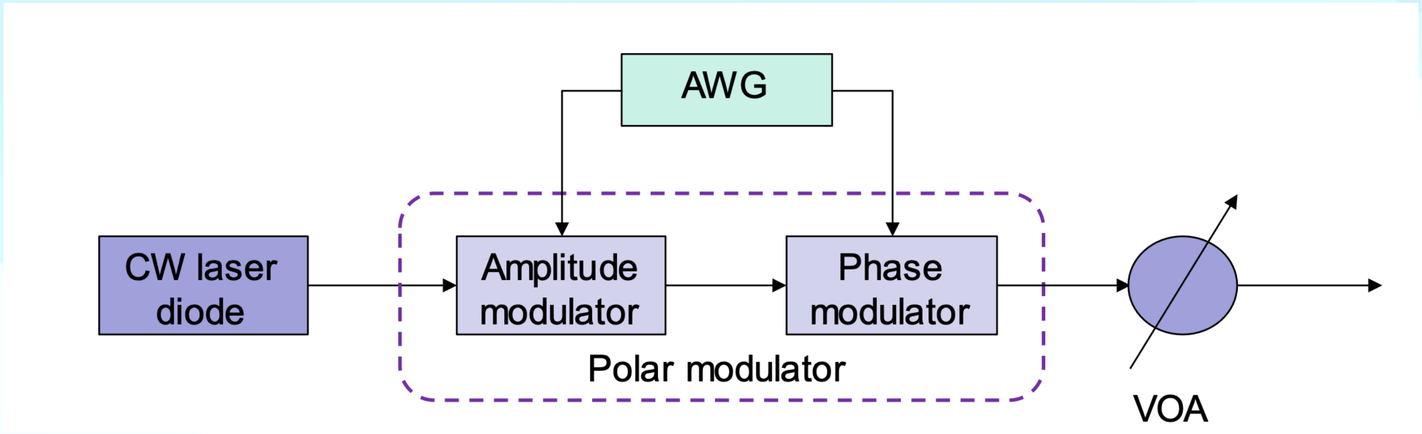
Alice randomly sets the control voltage to introduce the phase shift $\phi_A \in \{-\pi/2,\ 0,\ \pi/2,\ \pi\}$ and therefore randomly selects the state. Bob randomly selects the measurement basis by randomly choosing $\phi_B \in \{0,\ \pi/2\}$. Conclusive measurement occurs when either: (i) $\phi_B = 0$ and $\phi_A \in \{0,\ \pi\}$ or (ii) $\phi_B = \pi/2$ and $\phi_A \in \{-\pi/2,\ \pi/2\}$.

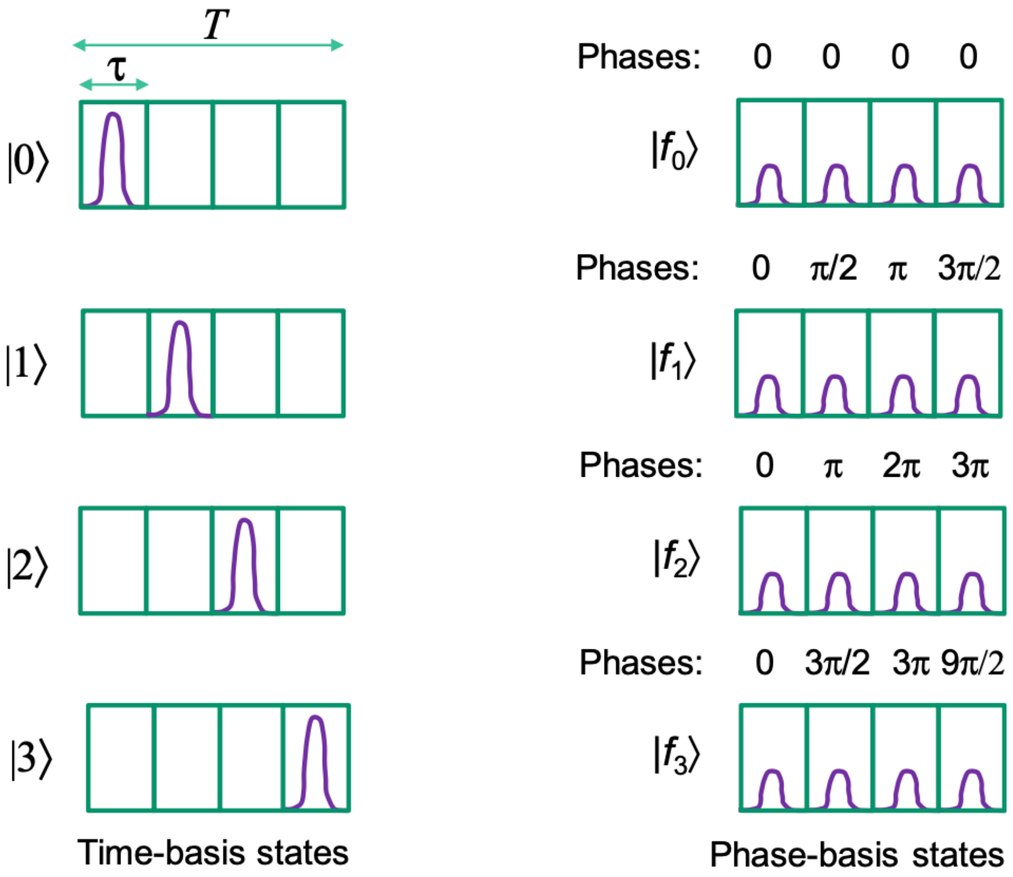
Schematic for experimental implementation
Phase encoding based BB 84 protocol

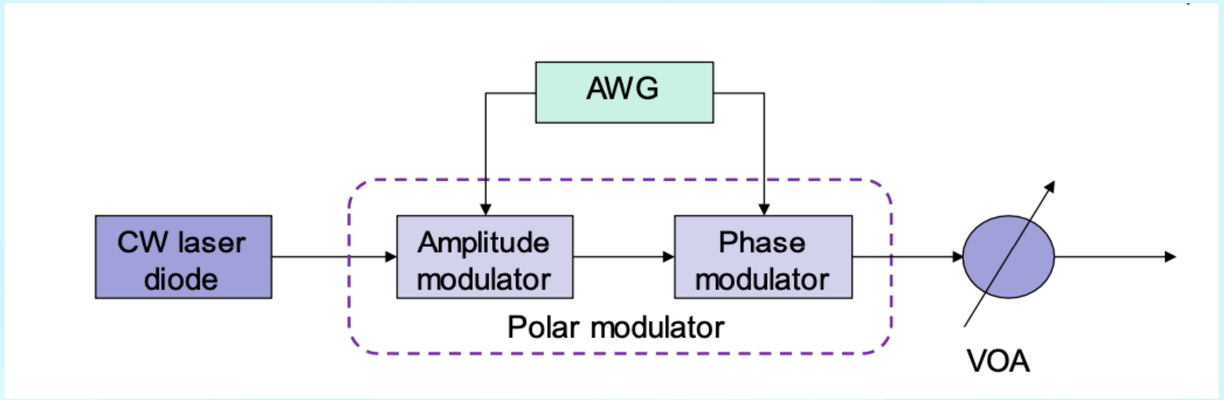


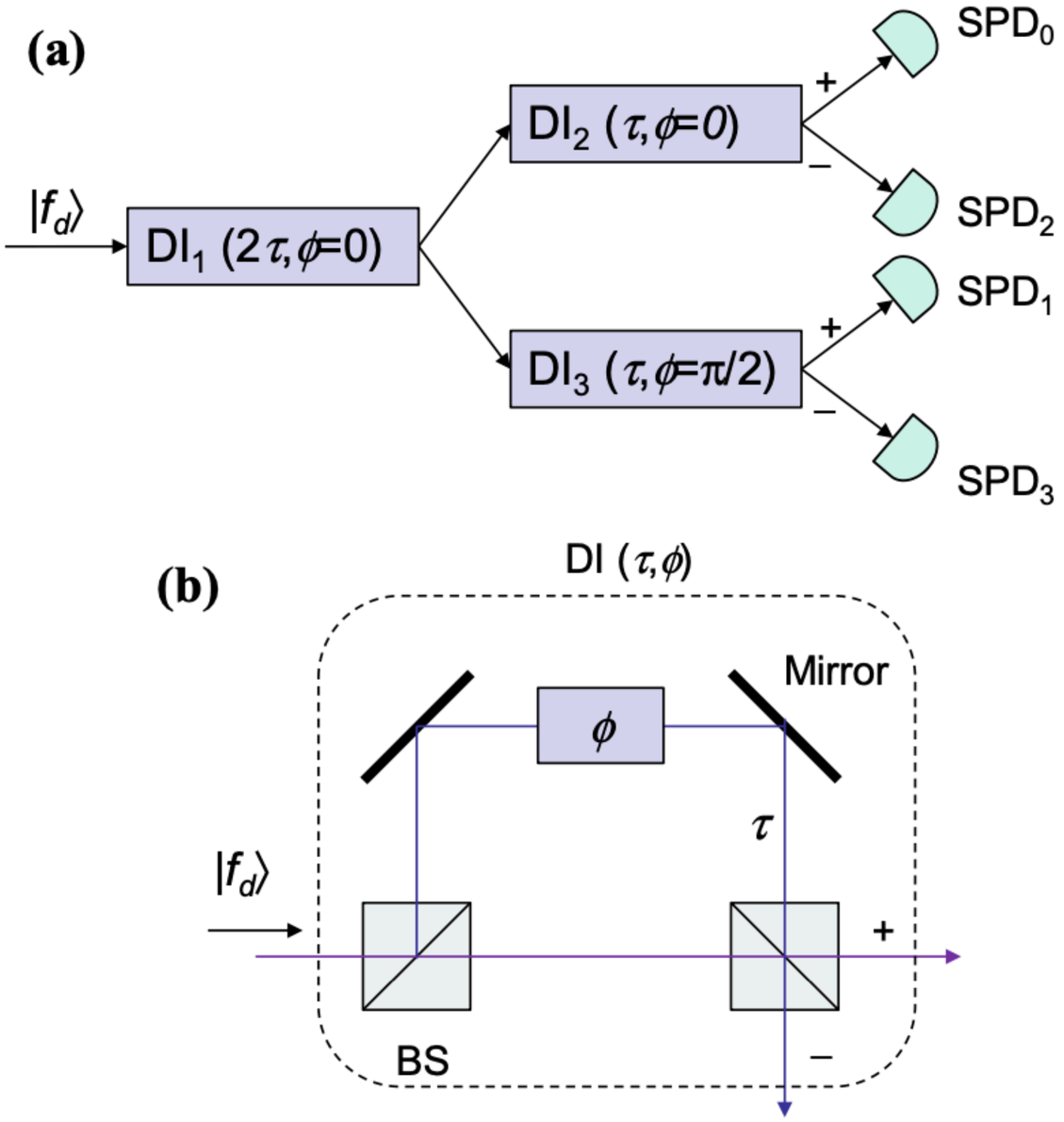
Schematic for experimental implementation
Time encoding based BB 84 protocol

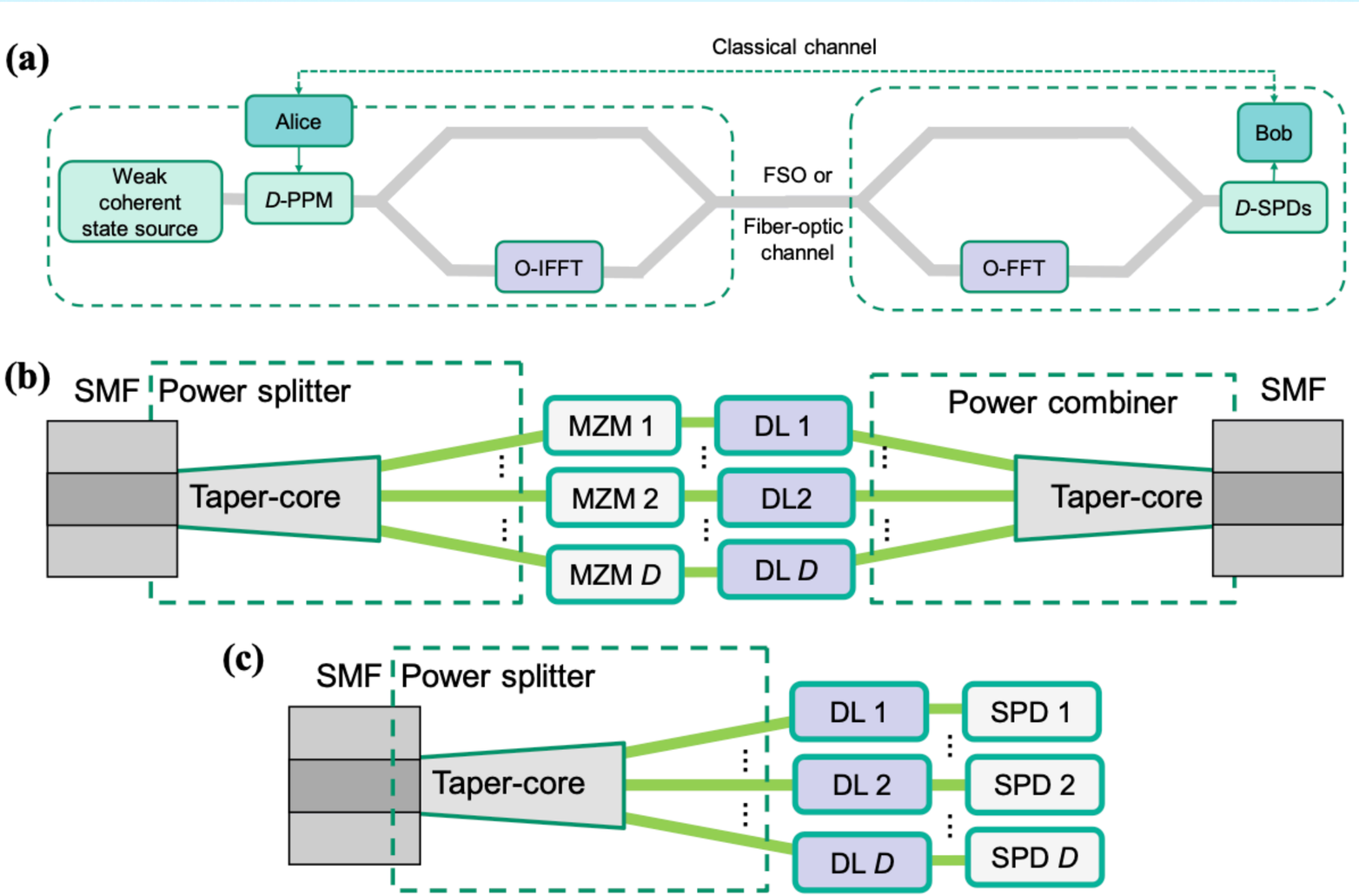



AWG
CW laser diode
Amplitude modulator
Phase modulator
Polar modulator
VOA


T
τ
|0⟩
|1⟩
|2⟩
|3⟩
Time-basis states
Phases: 0 0 0 0
|f0⟩
Phases: 0 π/2 π 3π/2
|f1⟩
Phases: 0 π 2π 3π
|f2⟩
Phases: 0 3π/2 3π 9π/2
|f3⟩
Phase-basis states


AWG
CW laser diode
Amplitude modulator
Phase modulator
Polar modulator
VOA


(a)
$|f_d\rangle$
DI$_1$ (2τ,ϕ=0)
DI$_2$ (τ,ϕ=0)
DI$_3$ (τ,ϕ=π/2)
+
–
+
–
SPD$_0$
SPD$_2$
SPD$_1$
SPD$_3$
(b)
DI (τ,ϕ)
Mirror
ϕ
τ
$|f_d\rangle$
+
–
BS


(a)
Classical channel
Alice
Weak coherent state source
D-PPM
O-IFFT
FSO or
Fiber-optic channel
O-FFT
Bob
D-SPDs
(b)
SMF
Power splitter
Taper-core
MZM 1
MZM 2
MZM D
DL 1
DL2
DL D
Power combiner
Taper-core
SMF
(c)
SMF
Power splitter
Taper-core
DL 1
DL 2
DL D
SPD 1
SPD 2
SPD D

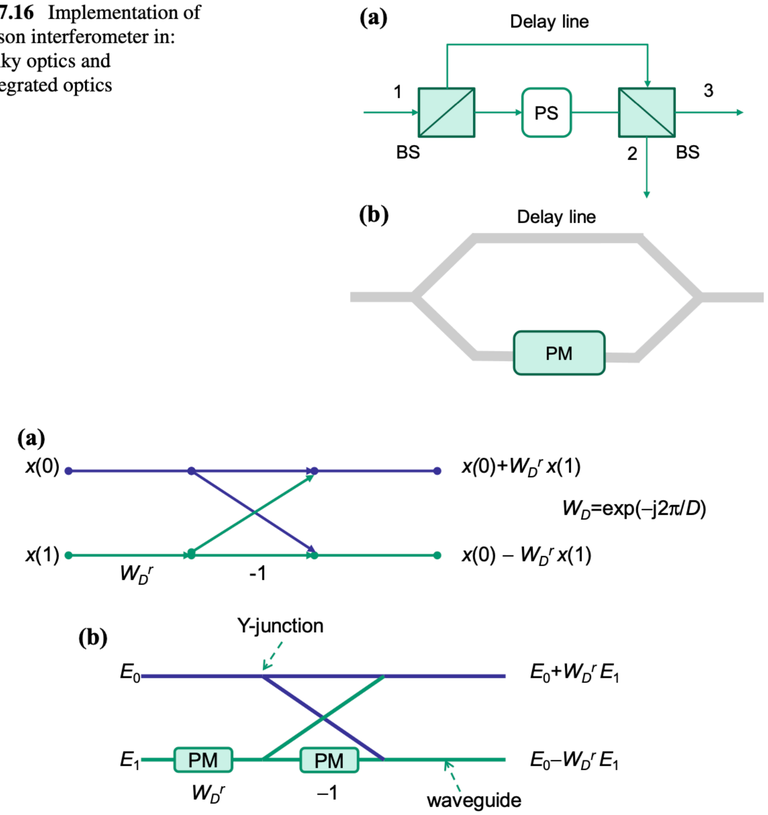
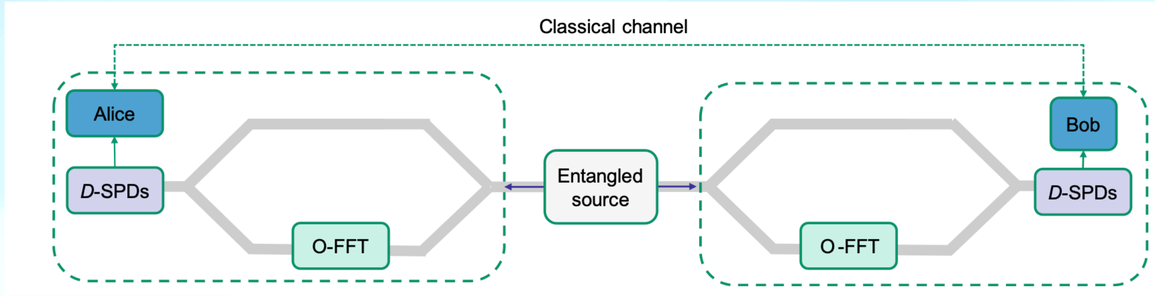
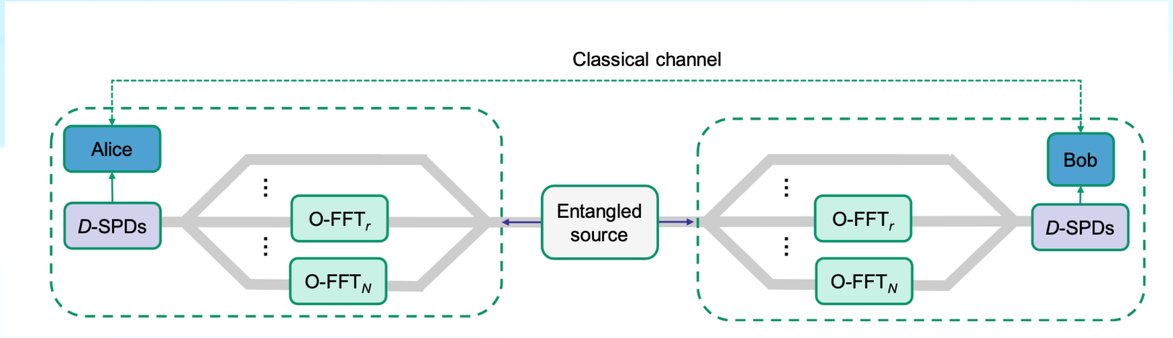
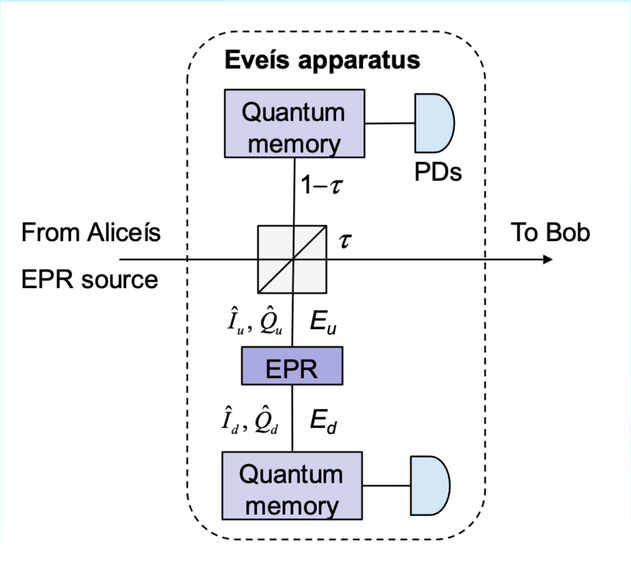
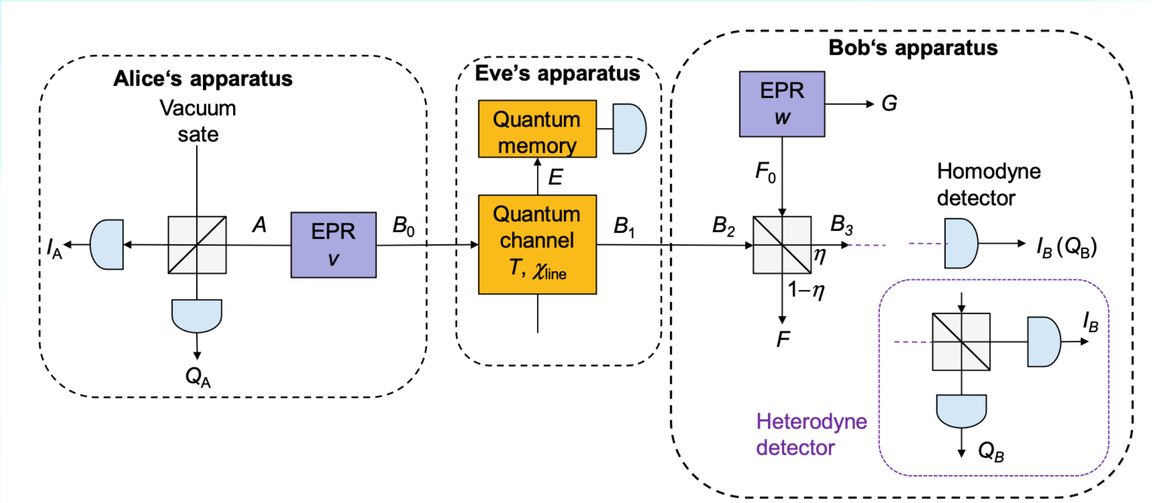


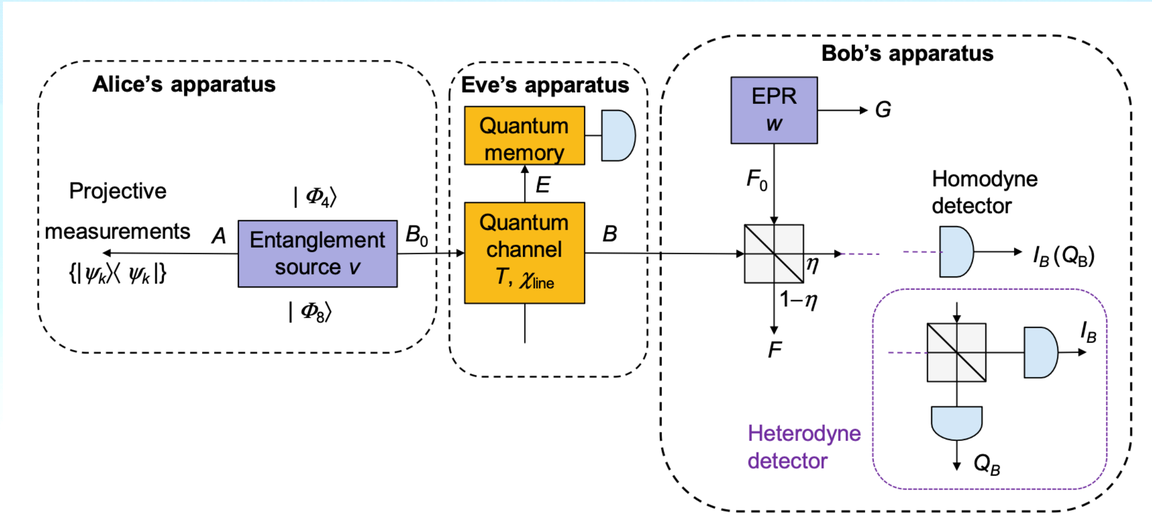
Fig. 7.16 Implementation of Franson interferometer in:
a bulky optics and
b integrated optics


Classical channel
Alice
D-SPDs
O-FFT
Entangled source
Bob
D-SPDs
O-FFT


Classical channel
Alice
D-SPDs
O-FFT$_r$
O-FFT$_N$
Entangled source
Bob
D-SPDs
O-FFT$_r$
O-FFT$_N$


Eveís apparatus
Quantum memory
PDs
1−τ
From Aliceís
EPR source
τ
To Bob
$\hat{I}_u, \hat{Q}_u$
E_u
EPR
$\hat{I}_d, \hat{Q}_d$
E_d
Quantum memory


Alice's apparatus
Vacuum
sate
A
EPR
v
B_0
I_A
Q_A
Eve's apparatus
Quantum
memory
E
Quantum
channel
T, χ_{line}
B_1
Bob's apparatus
EPR
w
G
F_0
B_2
B_3
η
1–η
F
Homodyne
detector
$I_B(Q_B)$
I_B
Q_B
Heterodyne
detector


Alice's apparatus
Projective
measurements
{|ψk⟩⟨ψk|}
A
Entanglement
source v
|Φ4⟩
|Φ8⟩
B0
Eve's apparatus
Quantum
memory
E
Quantum
channel
T, χline
B
Bob's apparatus
EPR
w
G
F0
Homodyne
detector
η
1−η
F
IB (QB)
IB
QB
Heterodyne
detector

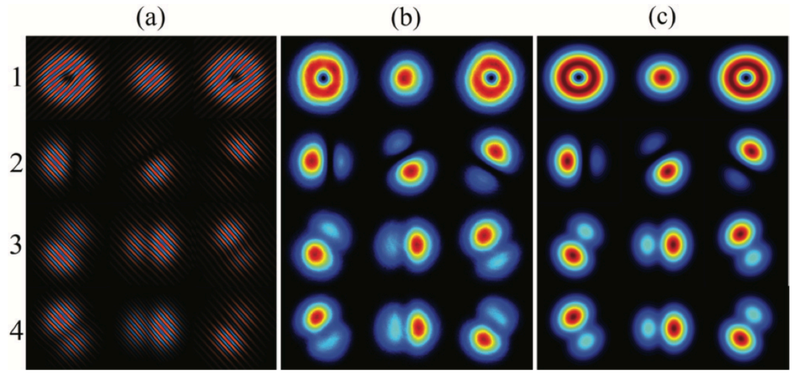
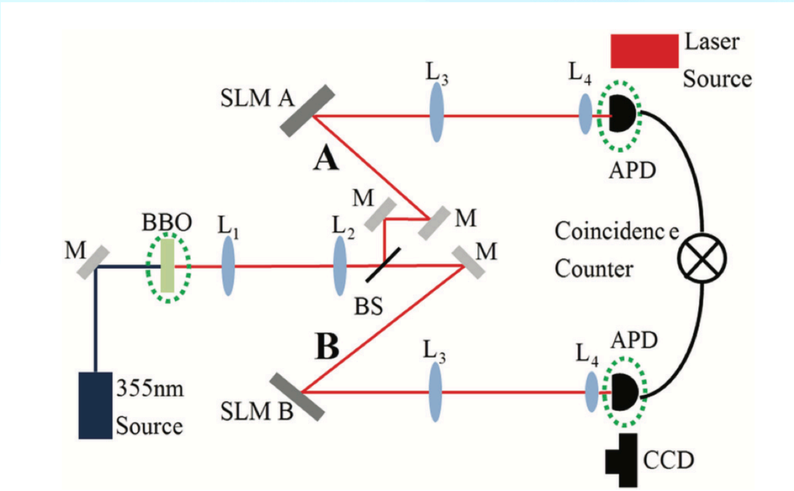


FIG. 1. (Color online) The states for each of the four MUBs for $d = 3$. (a) Images representing the measurement filters (or holograms) for each of the 12 states. (b) Experimentally produced and (c) theoretically calculated intensity profiles of the LG_ℓ modes produced by each hologram. The first row (1) represents the well-known LG basis, sometimes called the OAM basis, as given by Eq. (7).


Laser
Source
SLM A
L3
L4
APD
A
M
M
M
M
BBO
L1
L2
Coincidenc e
Counter
BS
B
APD
L4
L3
355nm
Source
SLM B
CCD

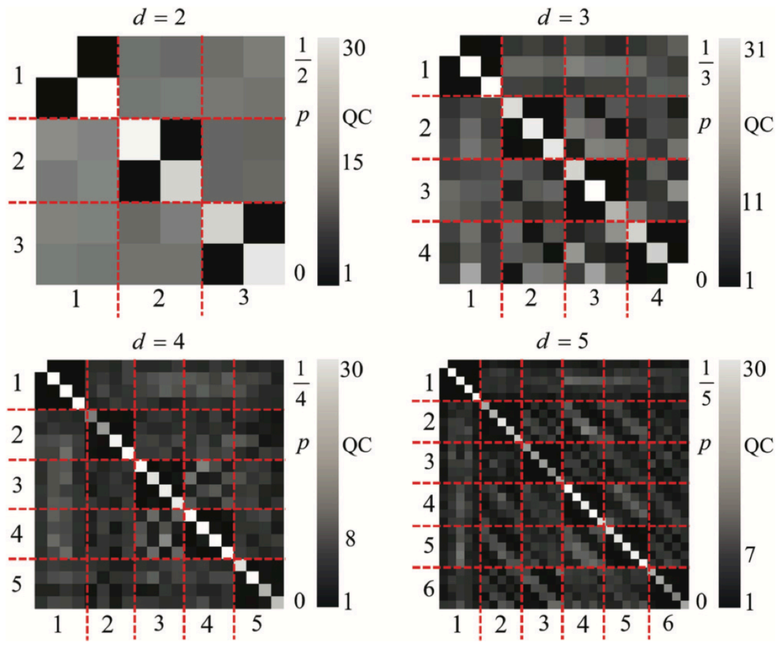
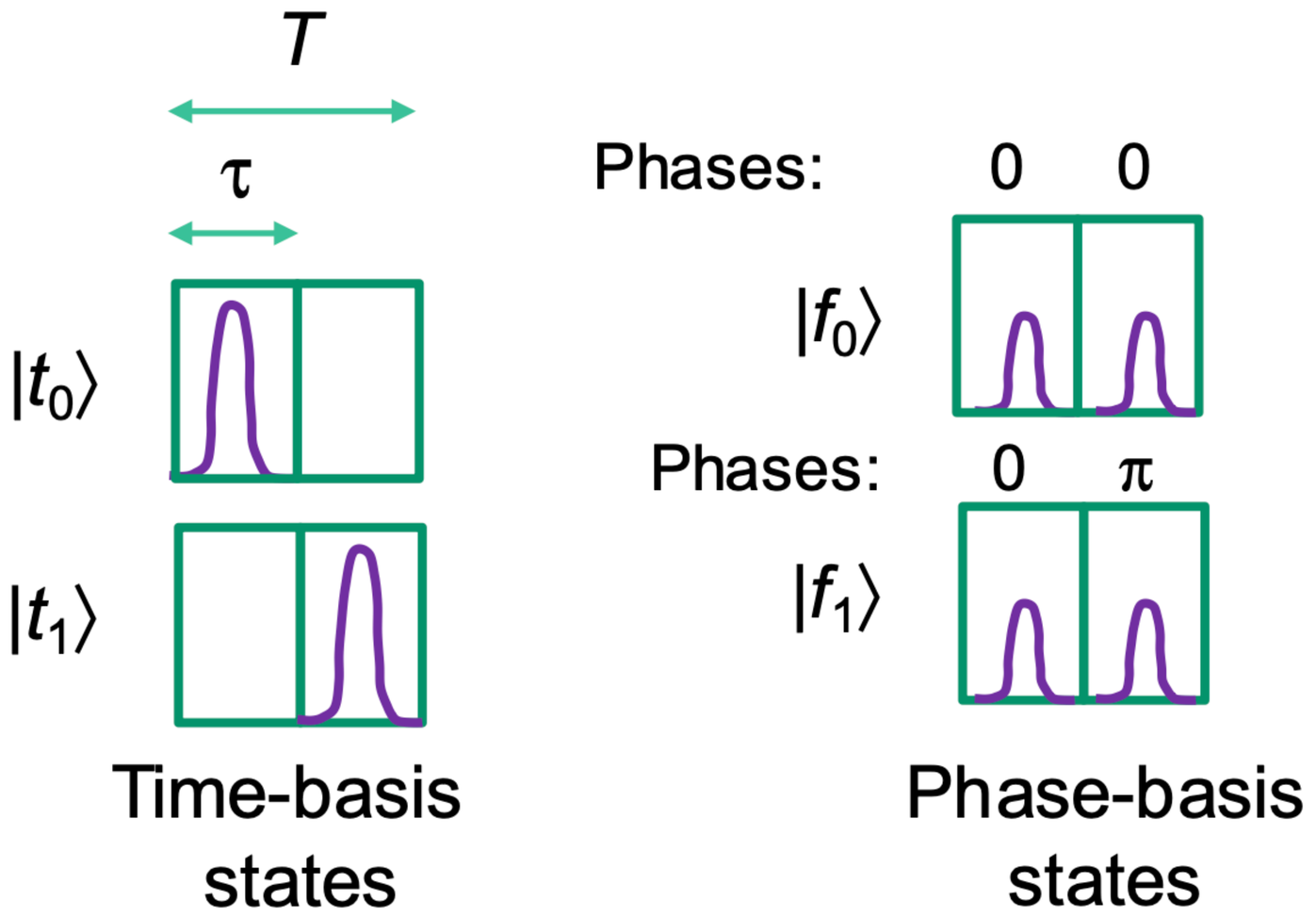
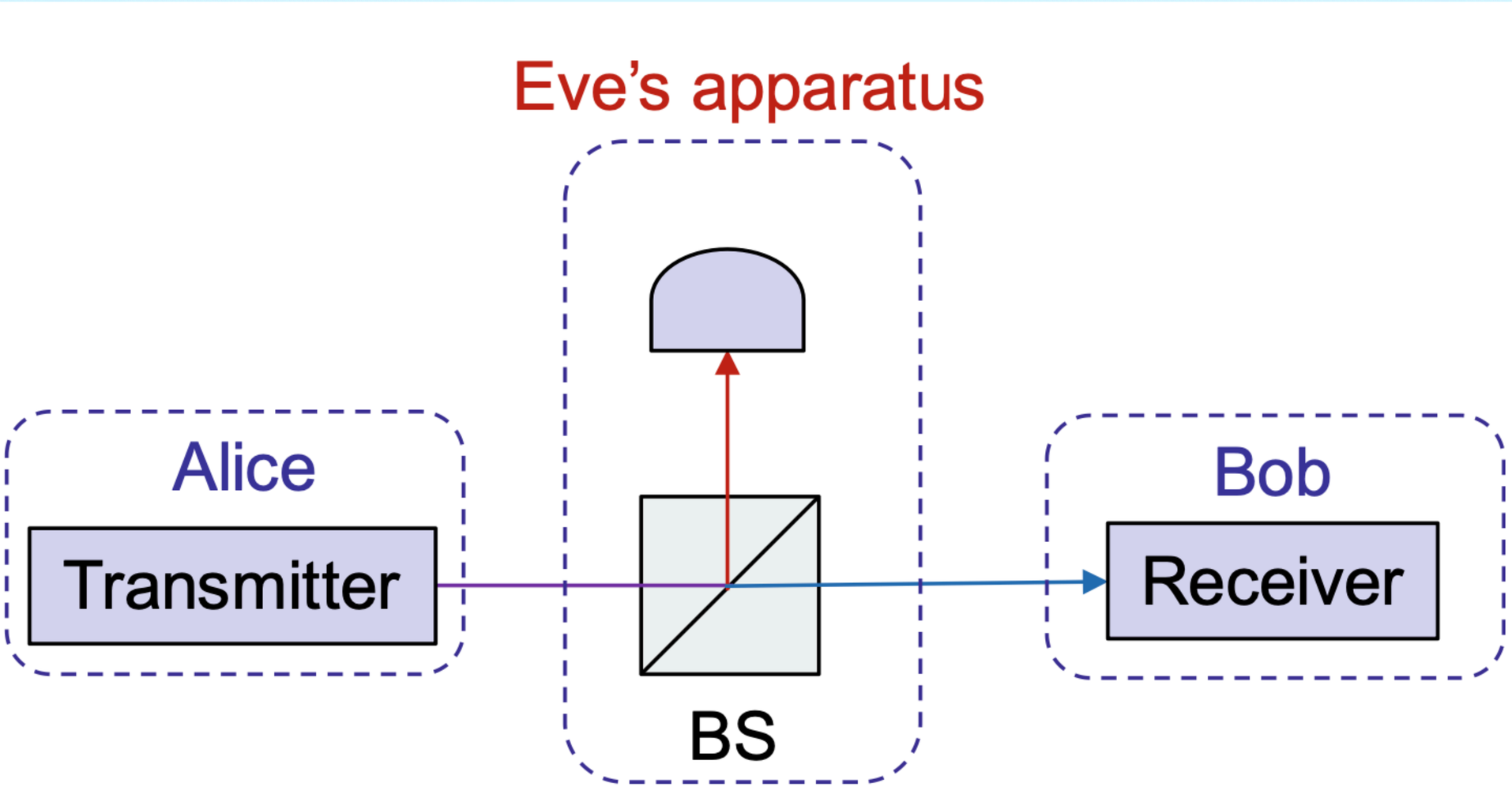


FIG. 4. (Color online) The normalized joint probabilities when SLM A (Alice) and SLM B (Bob) select one of the d states from one of the $d + 1$ bases for the EB scheme.


T
τ
$|t_0\rangle$
$|t_1\rangle$
Time-basis states
Phases: 0 0
$|f_0\rangle$
Phases: 0 π
$|f_1\rangle$
Phase-basis states


Eve's apparatus
Alice
Transmitter
BS
Bob
Receiver

Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations

Valerio Scarani,[1] Antonio Acín,[1] Grégoire Ribordy,[2] and Nicolas Gisin[1]

[1]*Group of Applied Physics, University of Geneva, 20, rue de l'Ecole-de-Médecine, CH-1211 Geneva 4, Switzerland*
[2]*Id-Quantique, rue Cingria 10, CH-1205 Geneva, Switzerland*

(Received 22 November 2002; published 6 February 2004)

We introduce a new class of quantum key distribution protocols, tailored to be robust against photon number splitting (PNS) attacks. We study one of these protocols, which differs from the original protocol by Bennett and Brassard (BB84) only in the classical sifting procedure. This protocol is provably better than BB84 against PNS attacks at zero error.

Six state protocol

$$\langle F_u | F_{u\oplus 1}\rangle = F\cos x;\ \langle D_u | D_{u\oplus 1}\rangle = D\cos y, \langle F_u | D_{u\oplus 1}\rangle = 0,$$