an Introduction to Quantum Information Processing

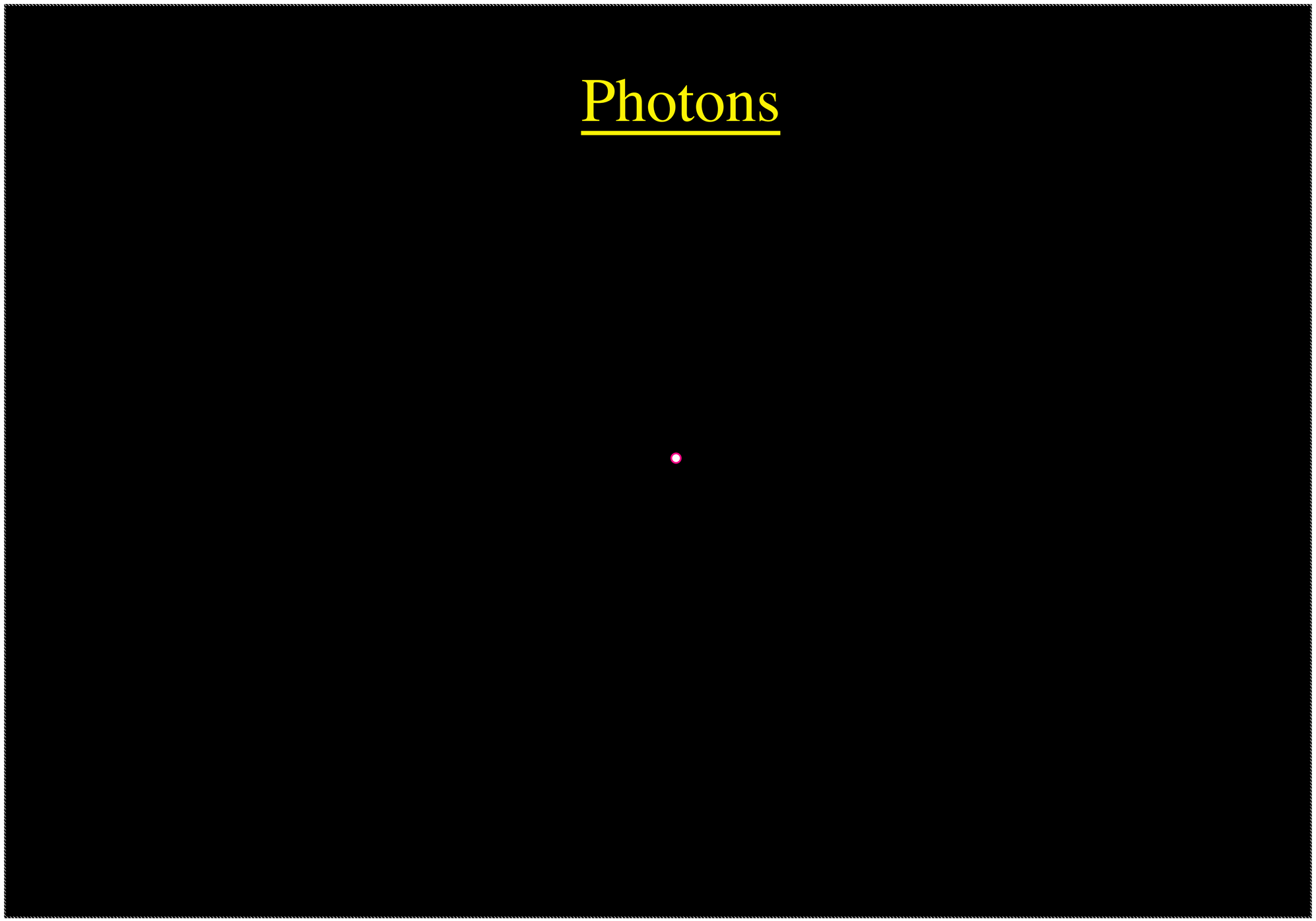
Claude Crépeau

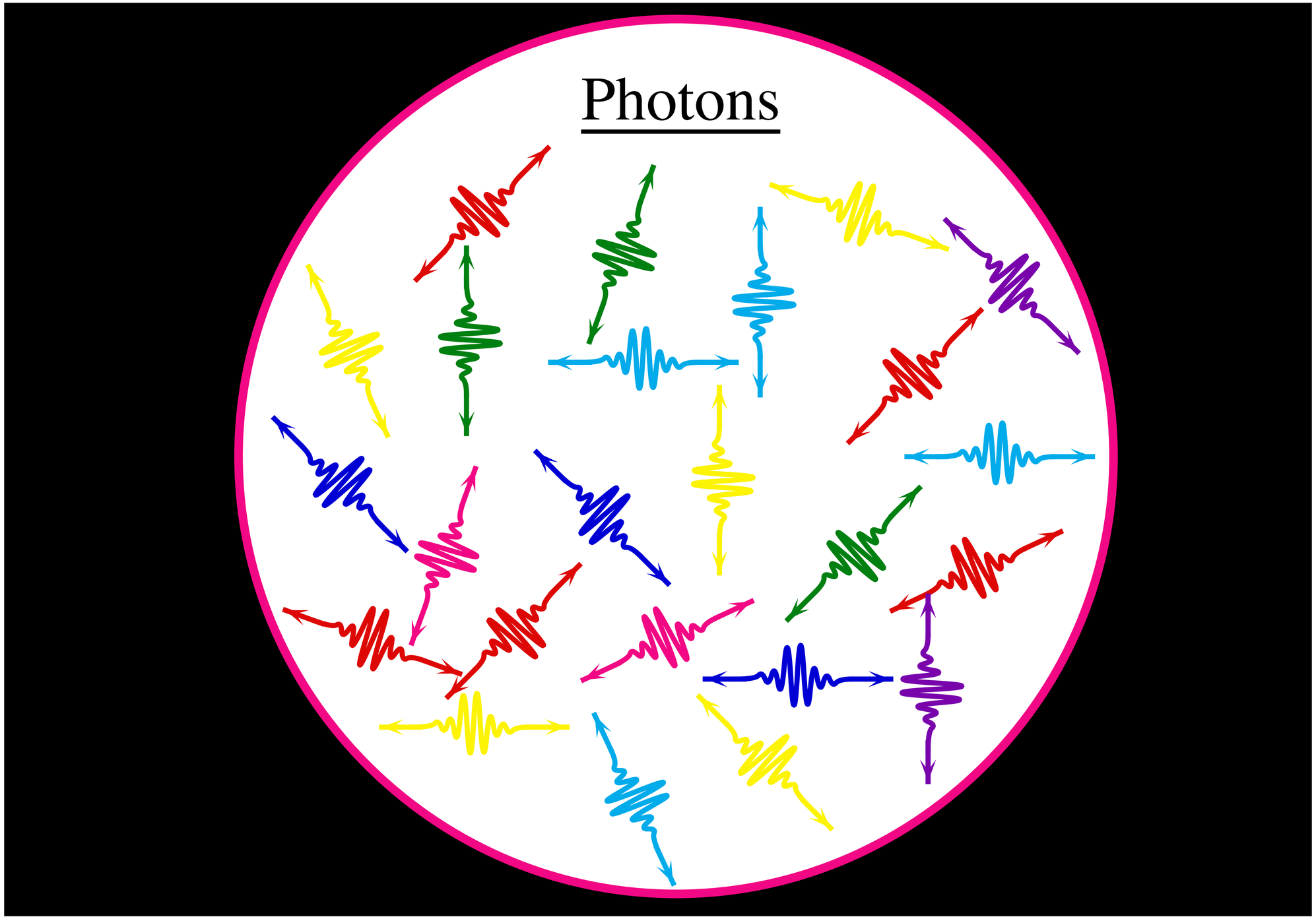
School of Computer Science
McGill University

(1)

Quantum Information

Photons



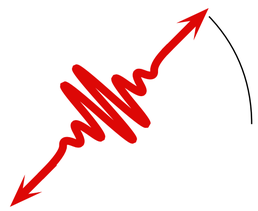


Photons

Bits & QuBits

0: 

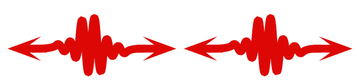
1: 

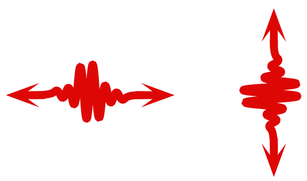


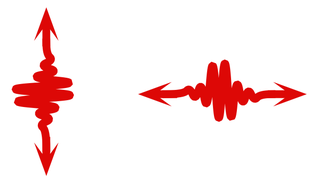
$\theta = \mathrm{Cos}_\theta$  $+ \ \mathrm{Sin}_\theta$ 

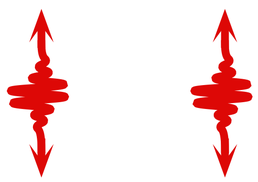
$|\Psi\rangle = C_0$  $+ \ C_1$ 

$C_i, C_{ij} \in \mathbb{C}$

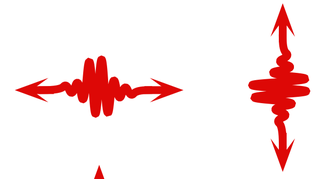
00: 

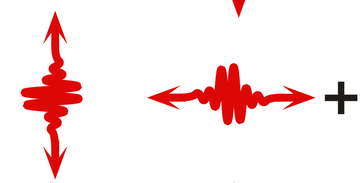
01: 

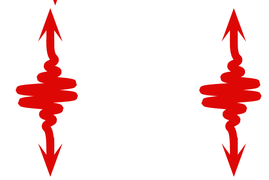
10: 

11: 

$|\Psi\rangle = C_{00}$  $+$

C_{01}  $+$

C_{10}  $+$

C_{11} 

standard notations

Basis vectors: $|0\rangle$ and $|1\rangle$

standard notations

Basis vectors: $|0\rangle$ and $|1\rangle$

Arbitrary states: $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$
such that $|\alpha|^2+|\beta|^2=1$

$\alpha,\beta \in \mathbb{C}$

standard notations

Basis vectors: $|0\rangle$ and $|1\rangle$

Arbitrary states: $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$
such that $|\alpha|^2+|\beta|^2=1$

Arbitrary multi-states: $\alpha,\beta,\delta,\gamma\in\mathbb{C}$

$$|\psi\rangle=\alpha|00\rangle+\beta|01\rangle+\delta|10\rangle+\gamma|11\rangle$$

such that $|\alpha|^2+|\beta|^2+|\delta|^2+|\gamma|^2=1$

standard notations

Conjugate: if $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle=\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$

then $\langle\psi|=\alpha^*\langle 0|+\beta^*\langle 1|=(\alpha^*\ \beta^*)$

standard notations

Conjugate: if $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle=\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$

then $\langle\psi|=\alpha^*\langle 0|+\beta^*\langle 1|=(\alpha^*\ \beta^*)$

Scalar product: $\langle\psi|\phi\rangle=\langle\psi|\bullet|\phi\rangle$

$\langle 0|0\rangle=\langle 1|1\rangle=1$ and $\langle 0|1\rangle=\langle 1|0\rangle=0$

standard notations

Conjugate: if $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle=\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$

then $\langle\psi|=\alpha^*\langle 0|+\beta^*\langle 1|=(\alpha^*\ \beta^*)$

Scalar product: $\langle\psi|\phi\rangle=\langle\psi|\bullet|\phi\rangle$

$\langle 0|0\rangle=\langle 1|1\rangle=1$ and $\langle 0|1\rangle=\langle 1|0\rangle=0$

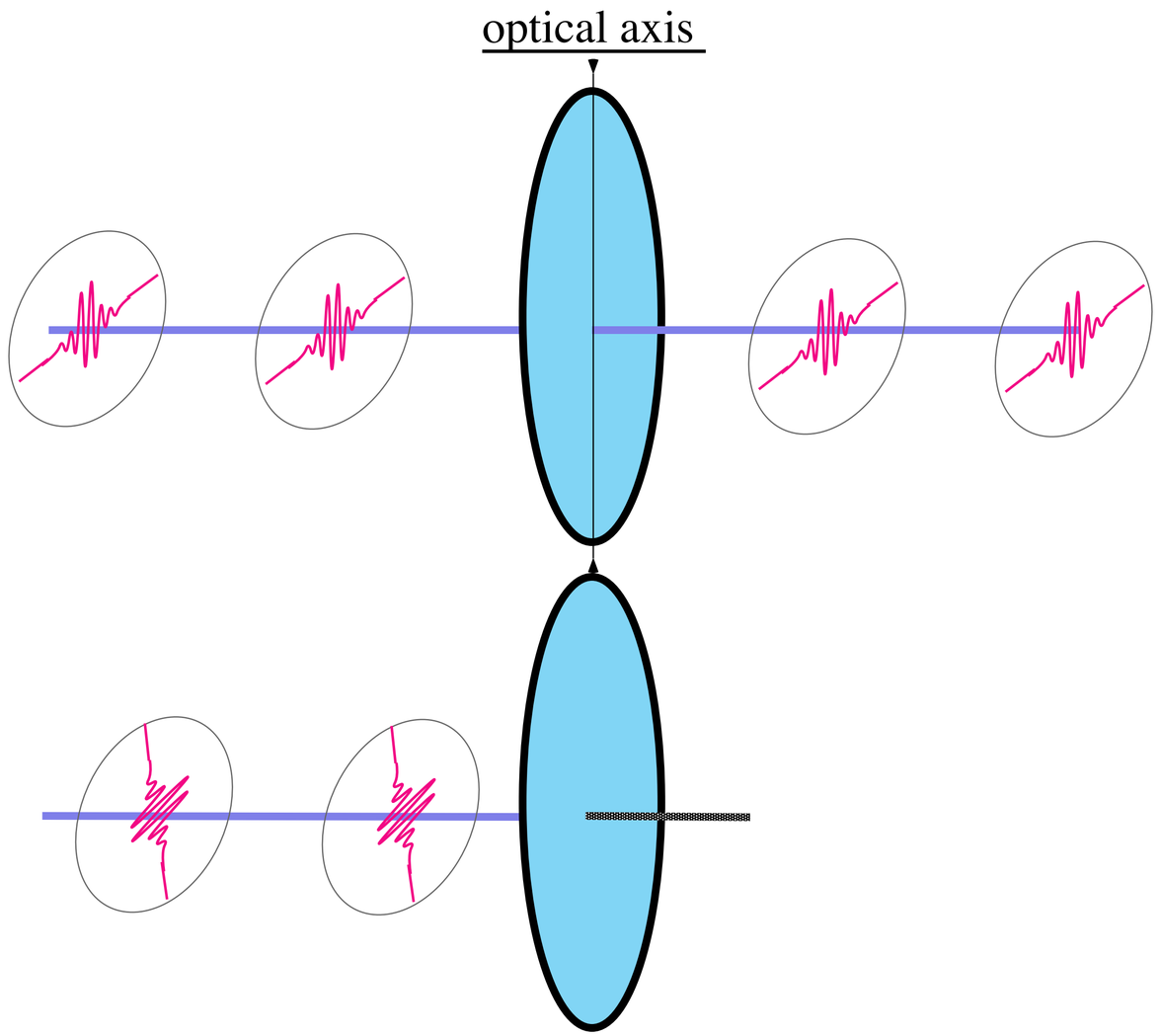
Tensor product: $|\phi\rangle\langle\psi|=|\phi\rangle\bullet\langle\psi|$

$|0\rangle\langle 0|=\begin{pmatrix}1&0\\0&0\end{pmatrix}$ $|0\rangle\langle 1|=\begin{pmatrix}0&1\\0&0\end{pmatrix}$... $|1\rangle\langle 1|=\begin{pmatrix}0&0\\0&1\end{pmatrix}$

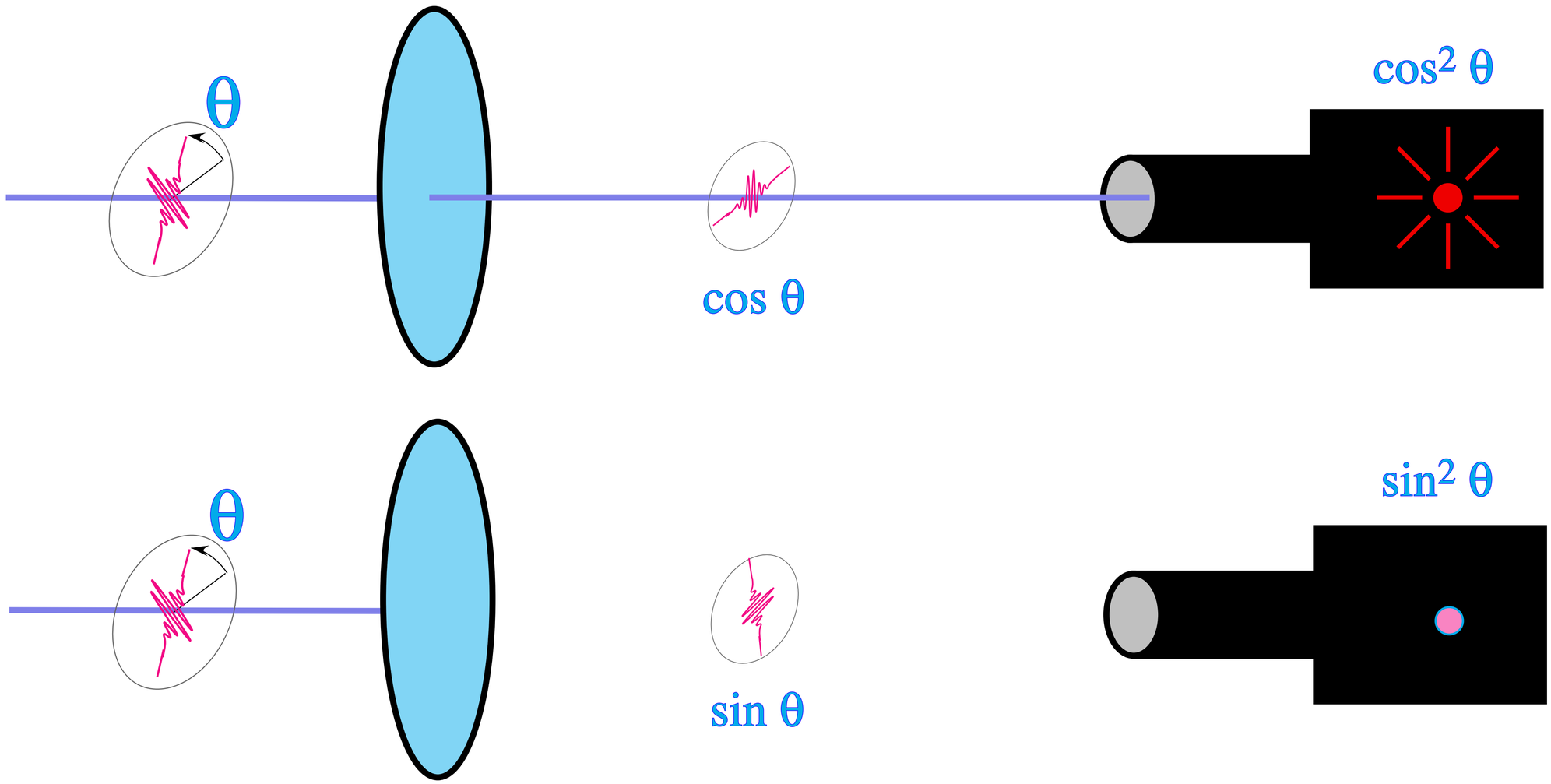
(2)

Quantum Measurements

Polarizing Filter



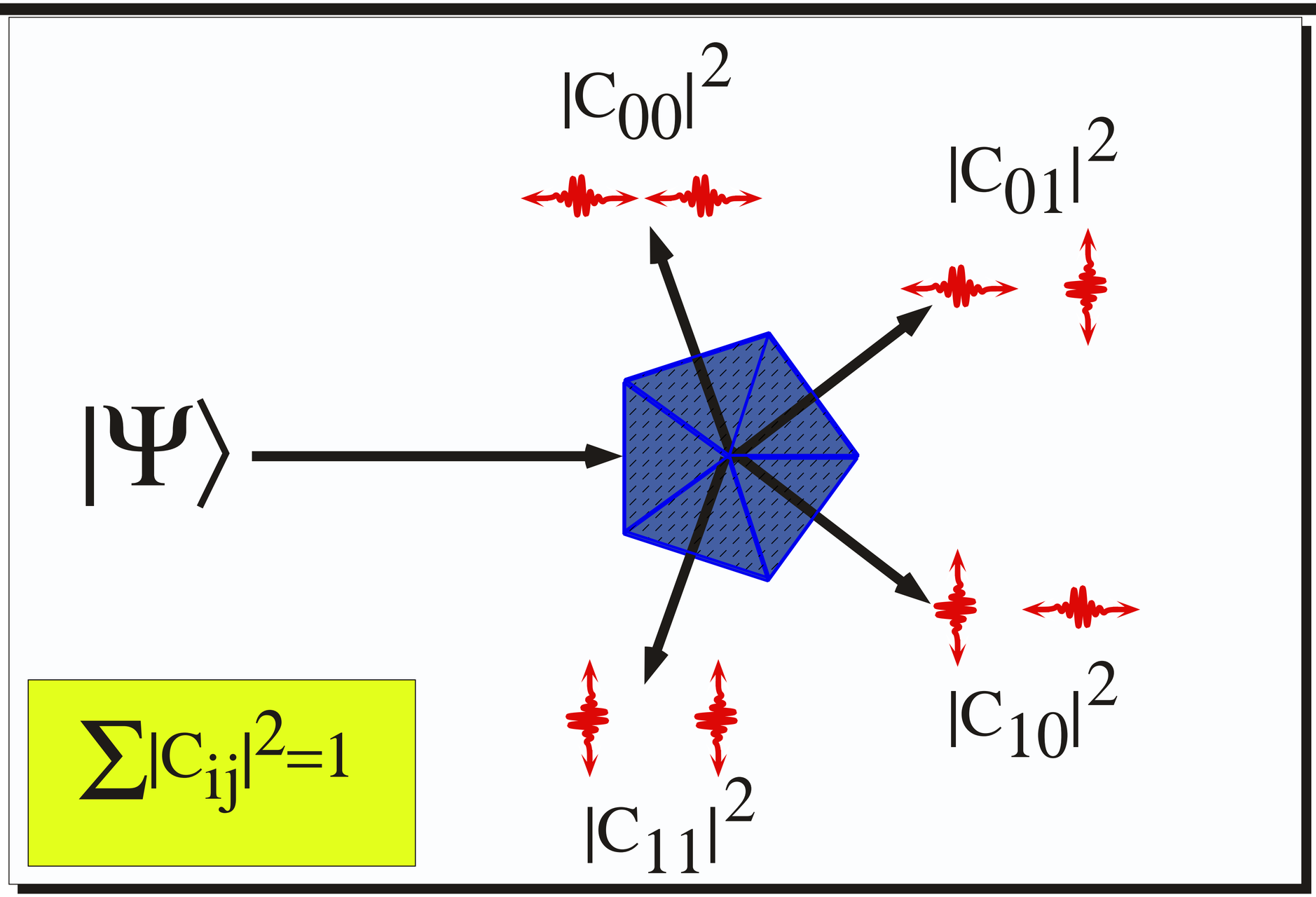
Polarizing Filter and photodetectors



Photons

Projective Measurements

$|\Psi\rangle = C_{00}$ + C_{01} + C_{10} + C_{11}



standard notations

Projector: (state) $P_\psi = |\psi\rangle\langle\psi|$

(space) $P = \Sigma P_i$ where $P_i P_{i'} = \delta_{i,i'} P_i$

standard notations

Projector: (state) $P_\psi = |\psi\rangle\langle\psi|$

(space) $P = \Sigma P_i$ where $P_i P_{i'} = \delta_{i,i'} P_i$

Measurement: $\{ P_m \}$

$$\Sigma P_m = I, \quad P_m P_{m'} = \delta_{m,m'} P_m$$

standard notations

Projector: (state) $P_\psi = |\psi\rangle\langle\psi|$

(space) $P = \Sigma P_i$ where $P_i P_{i'} = \delta_{i,i'} P_i$

Measurement: $\{ P_m \}$

$$\Sigma P_m = I, \quad P_m P_{m'} = \delta_{m,m'} P_m$$

Measuring: $\Pr[m] = \langle\phi|P_m|\phi\rangle$

standard notations

Projector: (state) $P_\psi = |\psi\rangle\langle\psi|$

(space) $P = \Sigma P_i$ where $P_i P_{i'} = \delta_{i,i'} P_i$

Measurement: $\{ P_m \}$

$$\Sigma P_m = I, \quad P_m P_{m'} = \delta_{m,m'} P_m$$

Measuring: $Pr[m] = \langle\phi|P_m|\phi\rangle$

Resulting: $P_m|\phi\rangle / \sqrt{Pr[m]}$

example

Projectors: $P_0 = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

$P_1 = |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

example

Projectors: $P_0 = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

$$P_1 = |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Measurement: $\{ P_0, P_1 \}$

$$\sum P_m = I, \quad P_0 P_1 = P_1 P_0 = 0$$

example

Projectors: $P_0 = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

$$P_1 = |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Measurement: $\{ P_0, P_1 \}$

$$\sum P_m = I, \quad P_0 P_1 = P_1 P_0 = 0$$

Measuring: $\Pr[m] = \langle \phi | P_m | \phi \rangle$

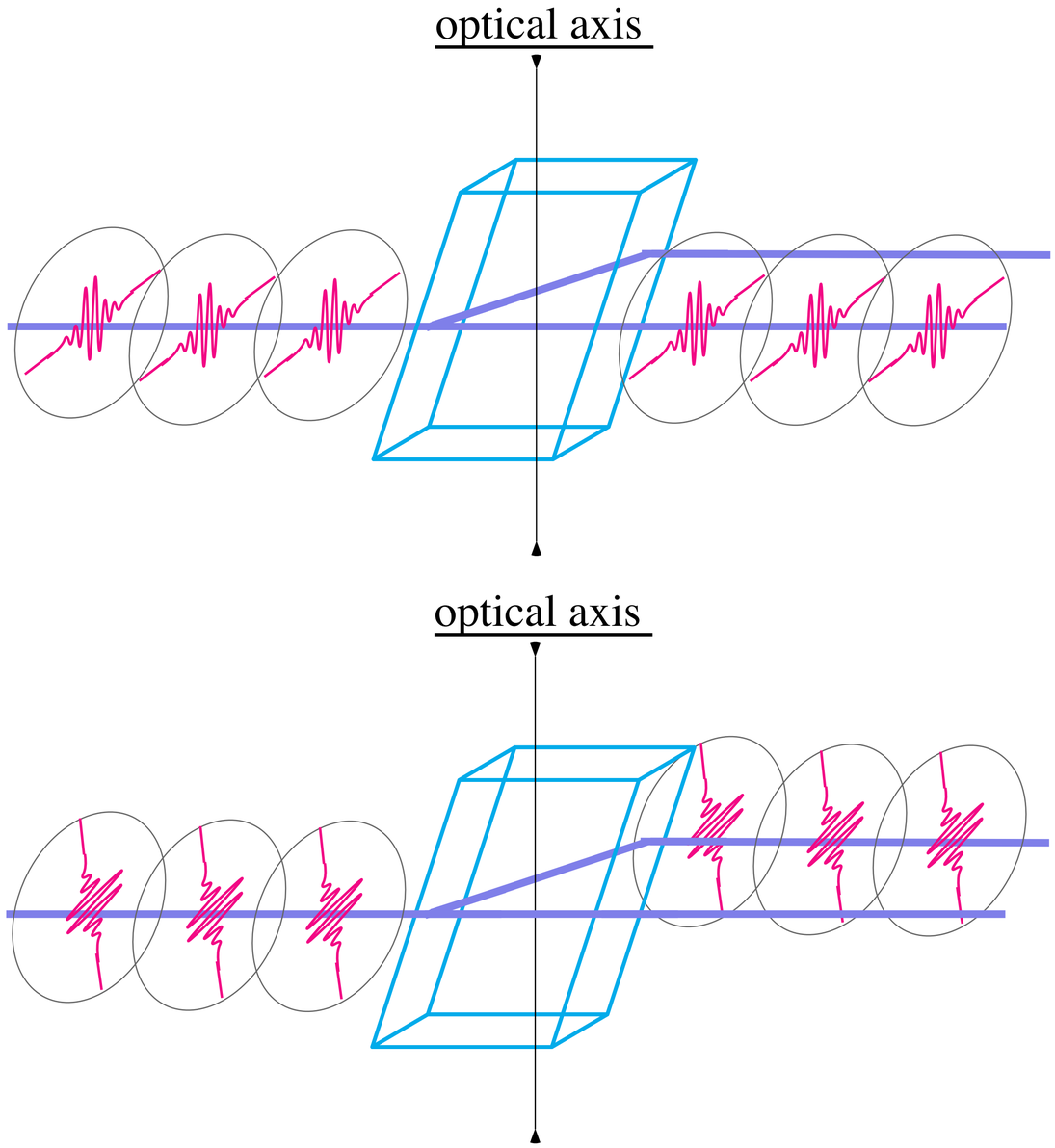
$$\alpha^* \langle 0| + \beta^* \langle 1| \; P_0 \; \alpha|0\rangle + \beta|1\rangle = \alpha^* \alpha = |\alpha|^2$$

$$\alpha^* \langle 0| + \beta^* \langle 1| \; P_1 \; \alpha|0\rangle + \beta|1\rangle = \beta^* \beta = |\beta|^2$$

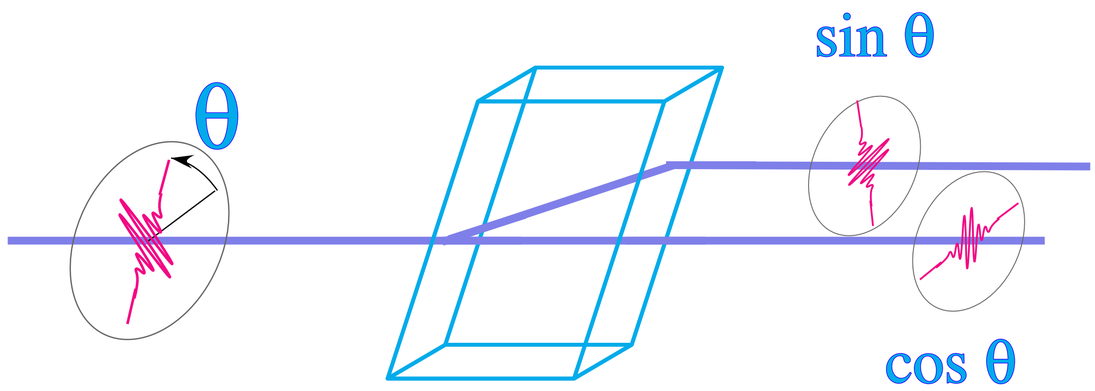
(3)

Quantum Computations

Calcite Crystal



Calcite Crystal



Photons

Quantum Evolution: Unitary Operators

$$|\Psi\rangle \xrightarrow{\boxed{U}} |\Psi'\rangle$$

$$\xrightarrow{\boxed{U}} |\Psi_0\rangle$$

$$\xrightarrow{\boxed{U}} |\Psi_1\rangle$$

$$C_0 \xrightarrow{} + C_1 \xrightarrow{\boxed{U}} C_0|\Psi_0\rangle + C_1|\Psi_1\rangle$$

standard notations

Unitary Operators: $U^\dagger U = U U^\dagger = I$

standard notations

Unitary Operators: $U^\dagger U = U U^\dagger = I$

linear: $U(\alpha|0\rangle + \beta|1\rangle) = \alpha U|0\rangle + \beta U|1\rangle$

standard notations

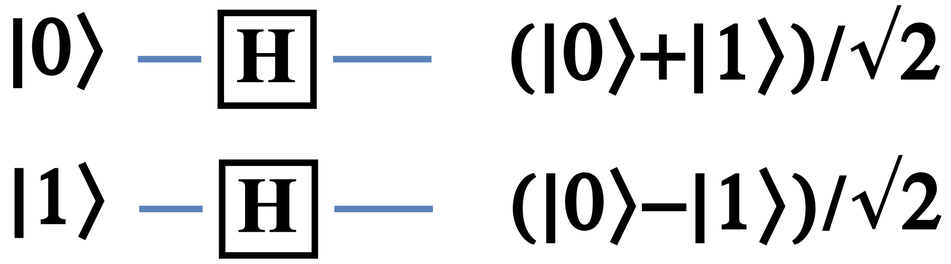
Unitary Operators: $U^\dagger U = U U^\dagger = I$

linear: $U(\alpha|0\rangle + \beta|1\rangle) = \alpha U|0\rangle + \beta U|1\rangle$

preserves scalar products:

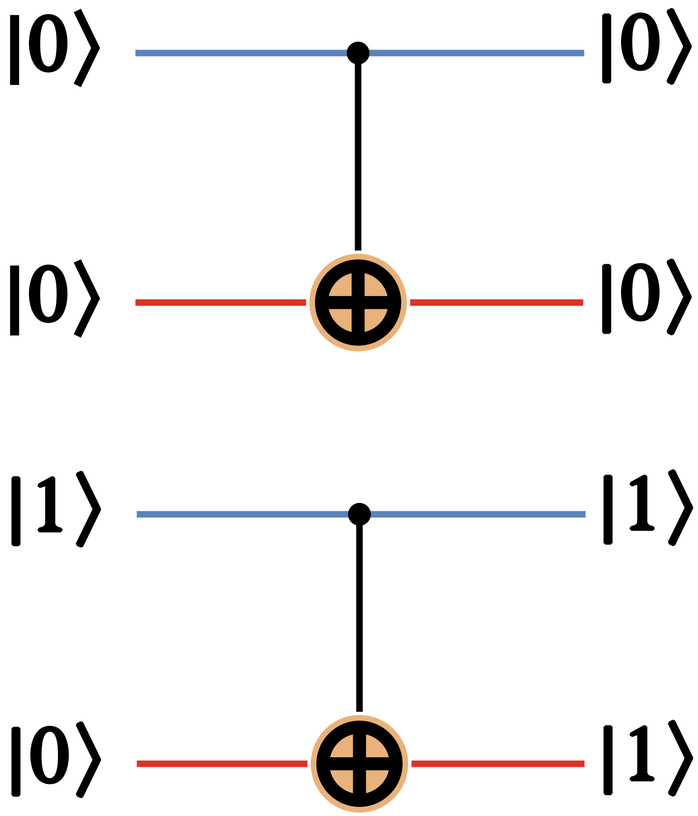
$$(\langle\psi|U^\dagger)(U|\phi\rangle)$$
$$= \langle\psi|U^\dagger U|\phi\rangle = \langle\psi|I|\phi\rangle = \langle\psi|\phi\rangle$$

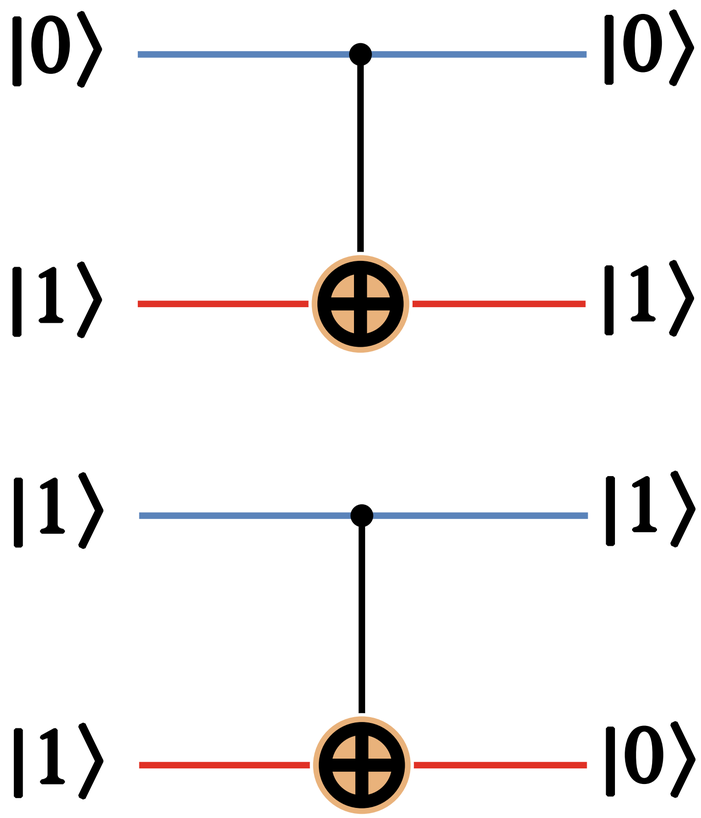
example: Hadamard

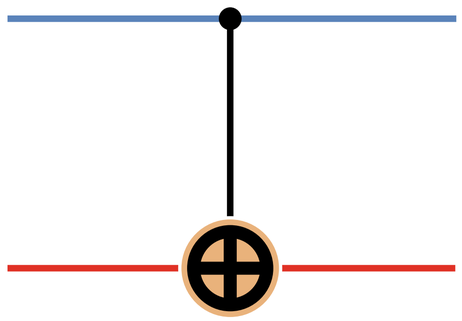


$$\boxed{H} = 1/\sqrt{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

example: Control-NOT





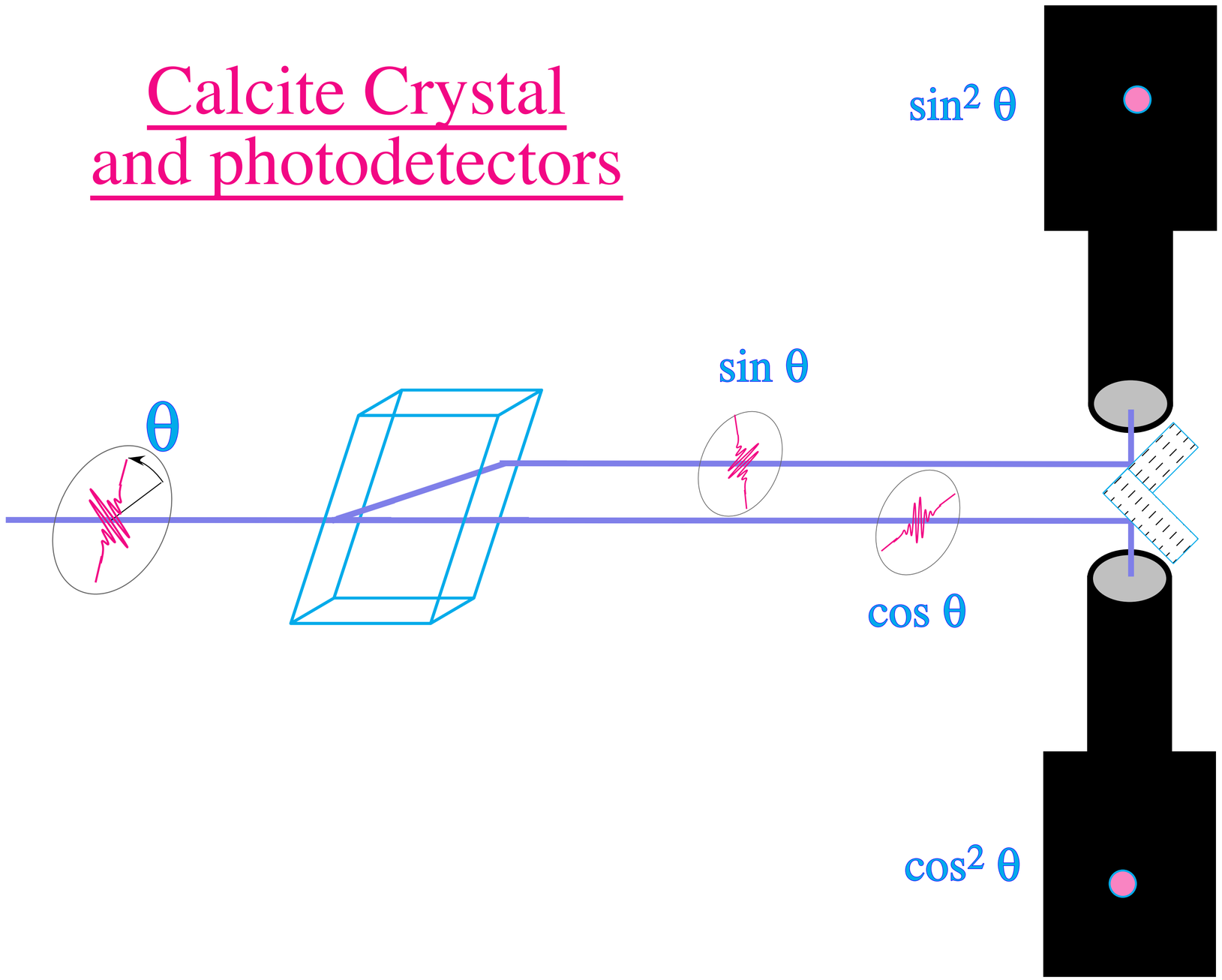


$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

(4)

General Measurements

Calcite Crystal and photodetectors



standard notations

Measurement: $\{ P_m U \}$:(larger state)

$$\Sigma P_m = I, \quad P_m P_{m'} = \delta_{m,m'} P_m$$

standard notations

Measurement: $\{ P_m U \}$:(larger state)

$$\Sigma P_m = I, \quad P_m P_{m'} = \delta_{m,m'} P_m$$

Measuring:

$$\Pr[m] = \langle 0^n | \langle \phi | U^\dagger P_m U | \phi \rangle | 0^n \rangle$$

standard notations

Measurement: $\{ P_m U \}$:(larger state)

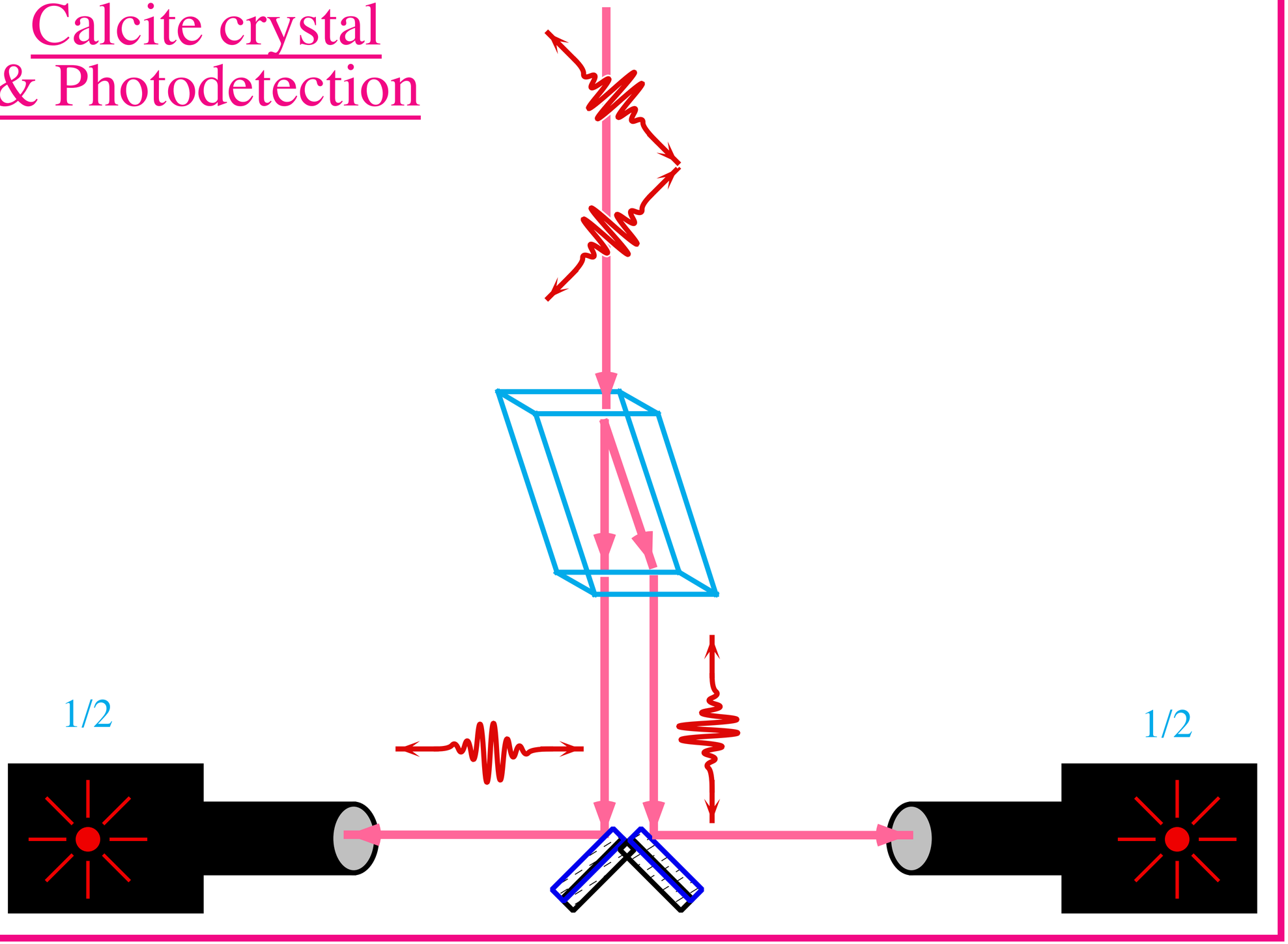
$$\Sigma P_m = I, \quad P_m P_{m'} = \delta_{m,m'} P_m$$

Measuring:

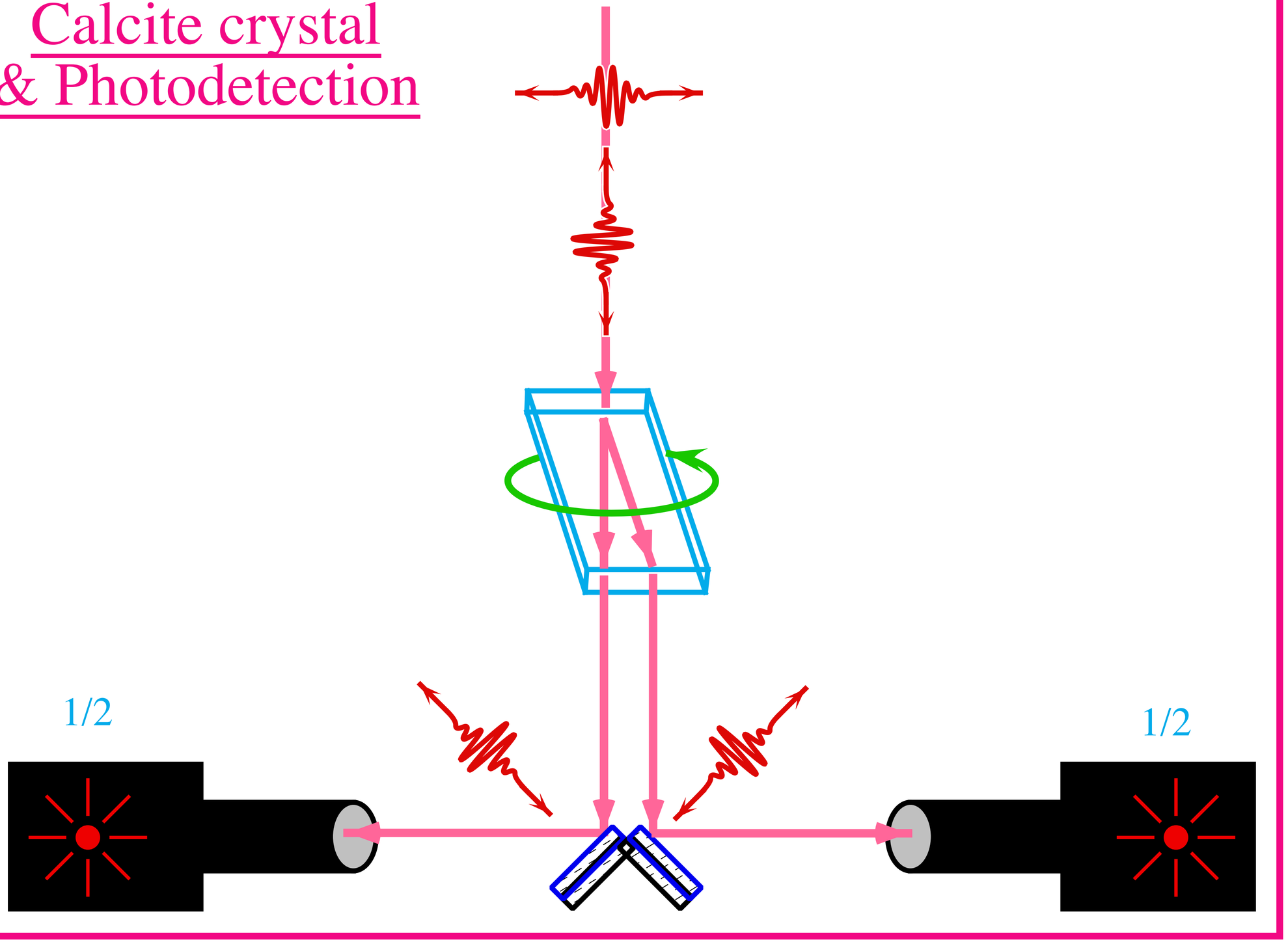
$$Pr[m] = \langle 0^n | \langle \phi | U^\dagger P_m U | \phi \rangle | 0^n \rangle$$

Resulting: $P_m U |\phi\rangle |0^n\rangle / \sqrt{Pr[m]}$

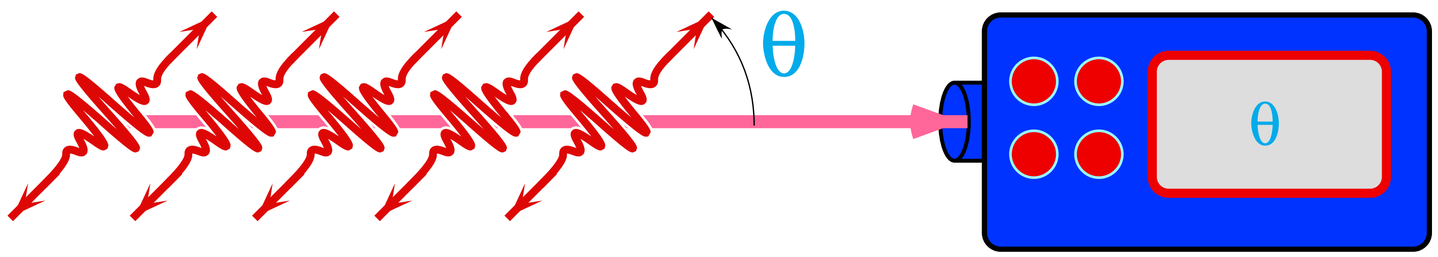
Calcite crystal & Photodetection



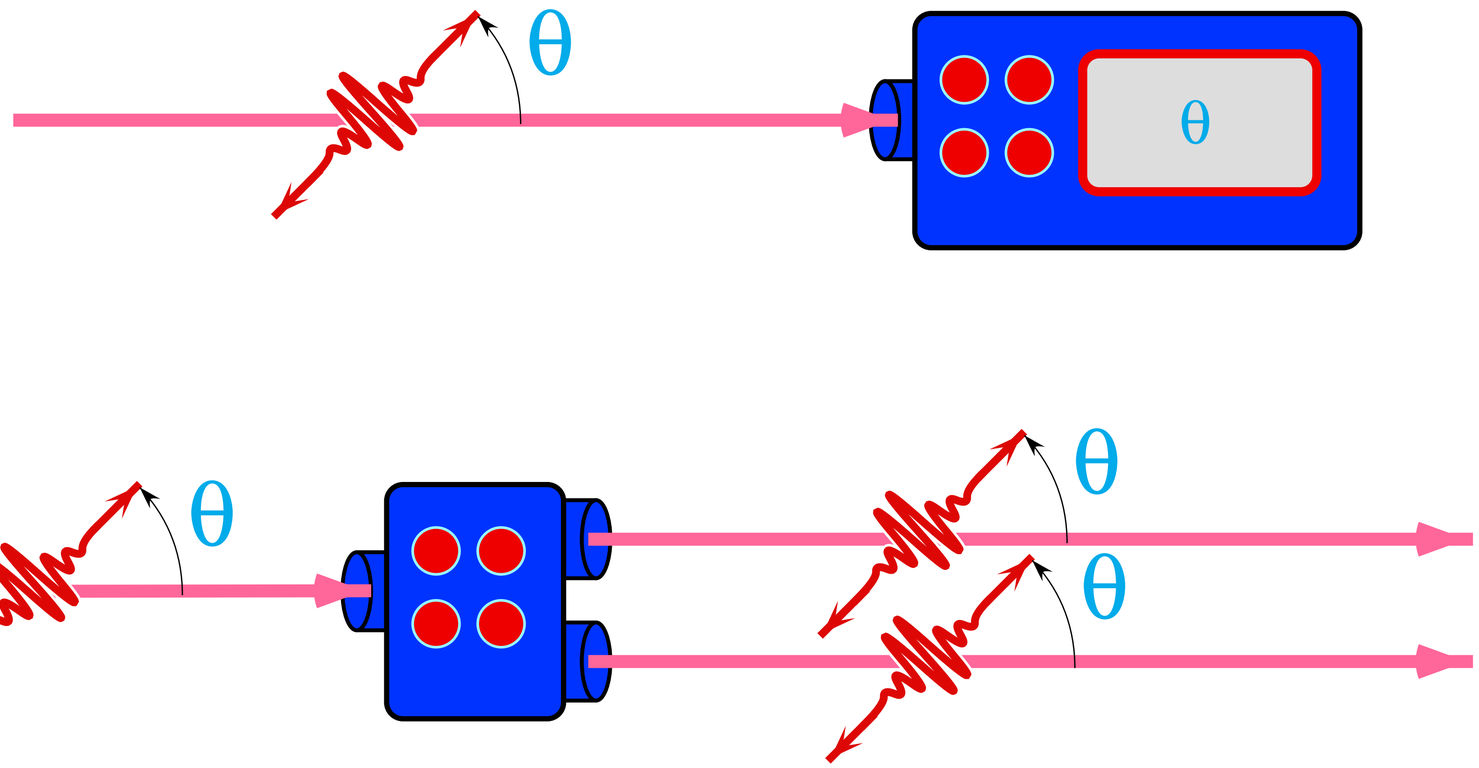
Calcite crystal & Photodetection



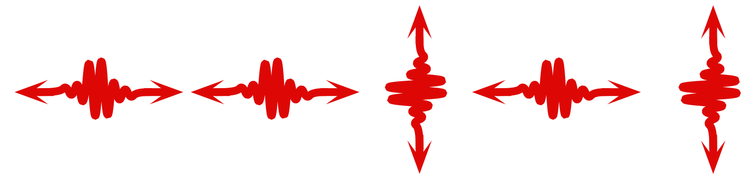
POSSIBLE!



IMPOSSIBLE!



Classical & Quantum Information

0011011110001 10 Classical	Quantum 
Copying: Yes	NO
Measuring: Yes	partial
Broadcasting: Yes	NO
Superposing: NO	Yes
Interfering: NO	Yes

(5)

Quantum Entanglement

$$|¿?\rangle = {}^{1}/_{\sqrt{2}}\,|\mathbf{01}\rangle - {}^{1}/_{\sqrt{2}}\,|\mathbf{10}\rangle$$

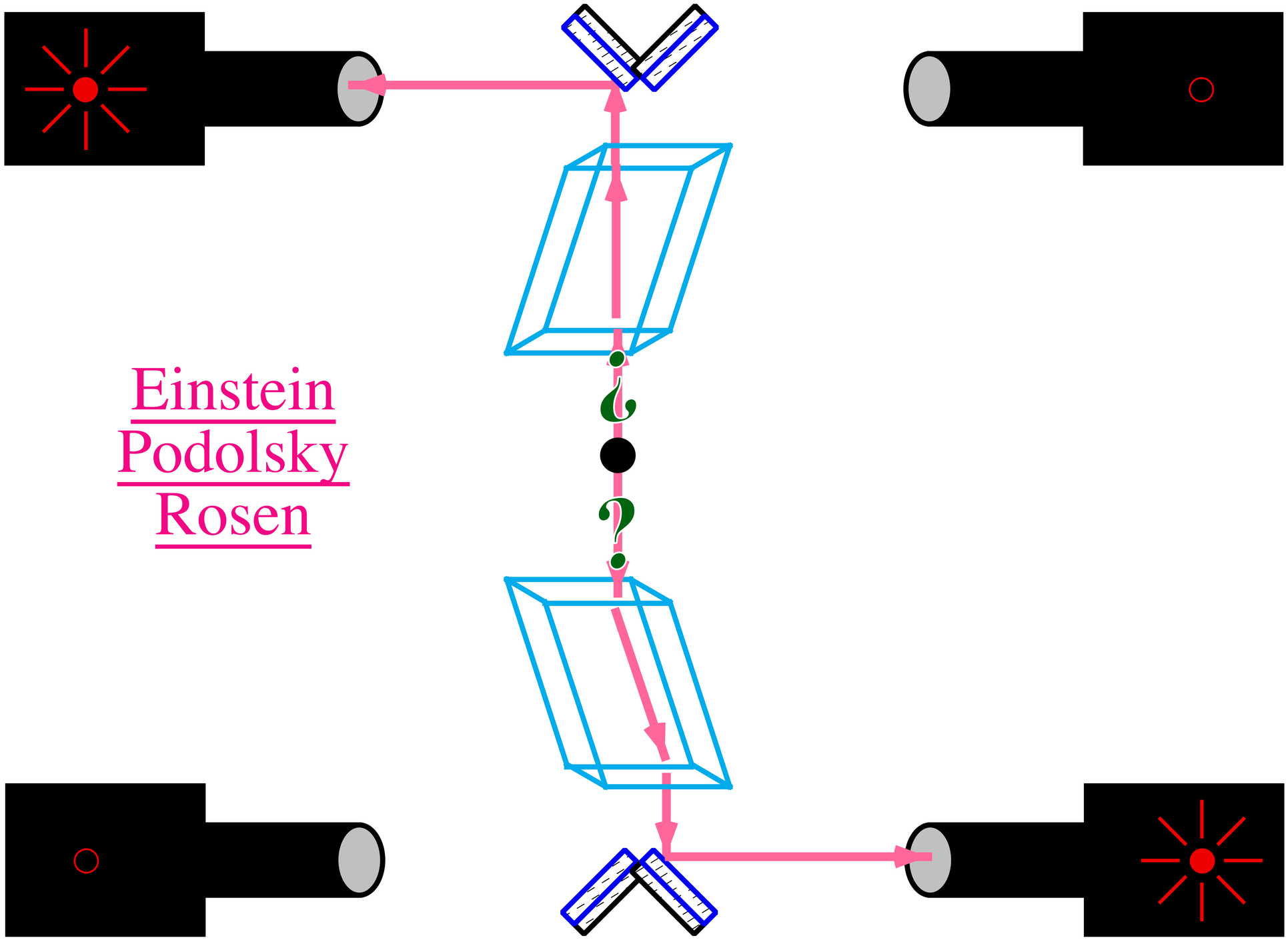
Albert Einstein

Boris Podolsky

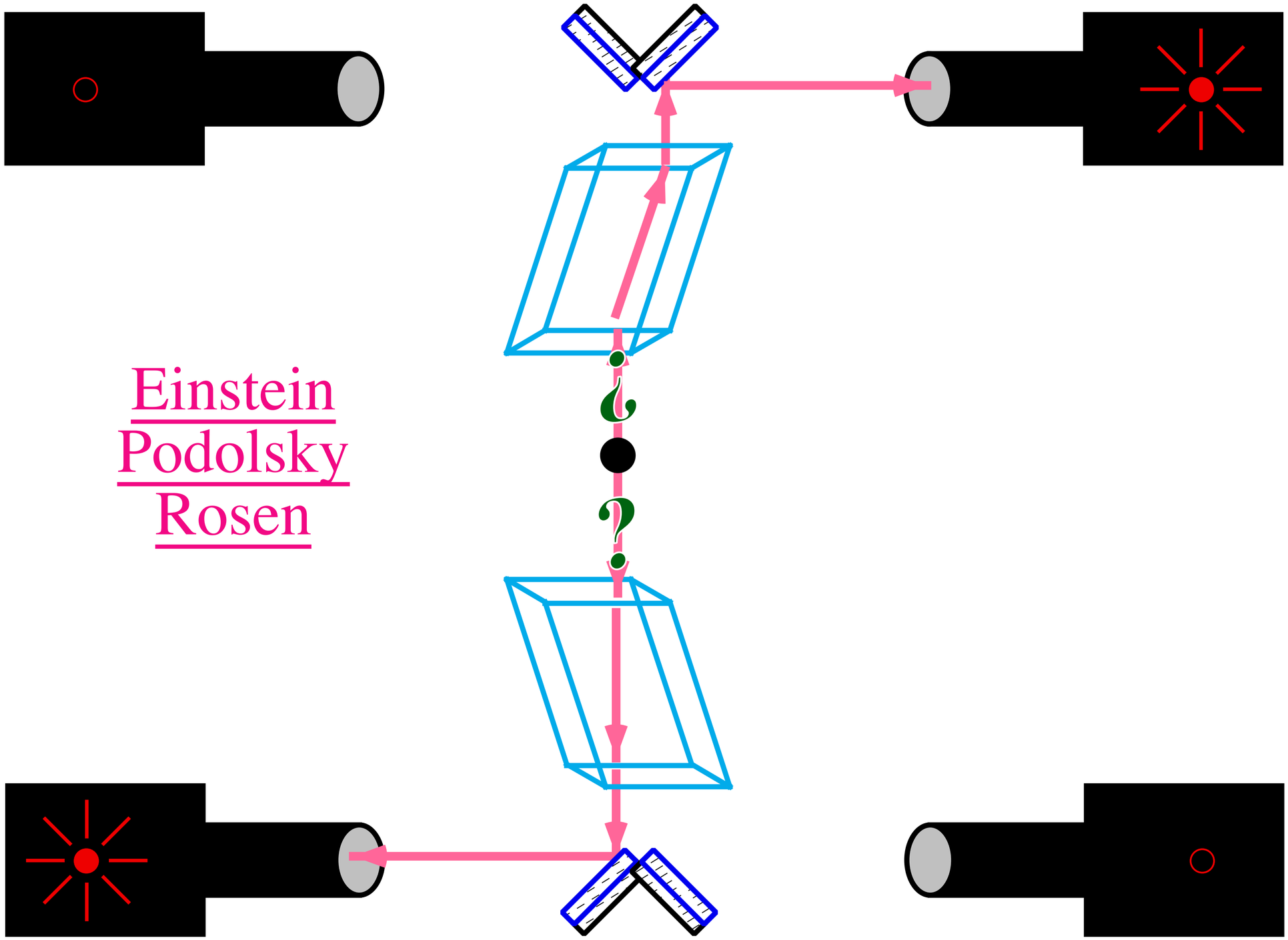
Nathan Rosen

EPR

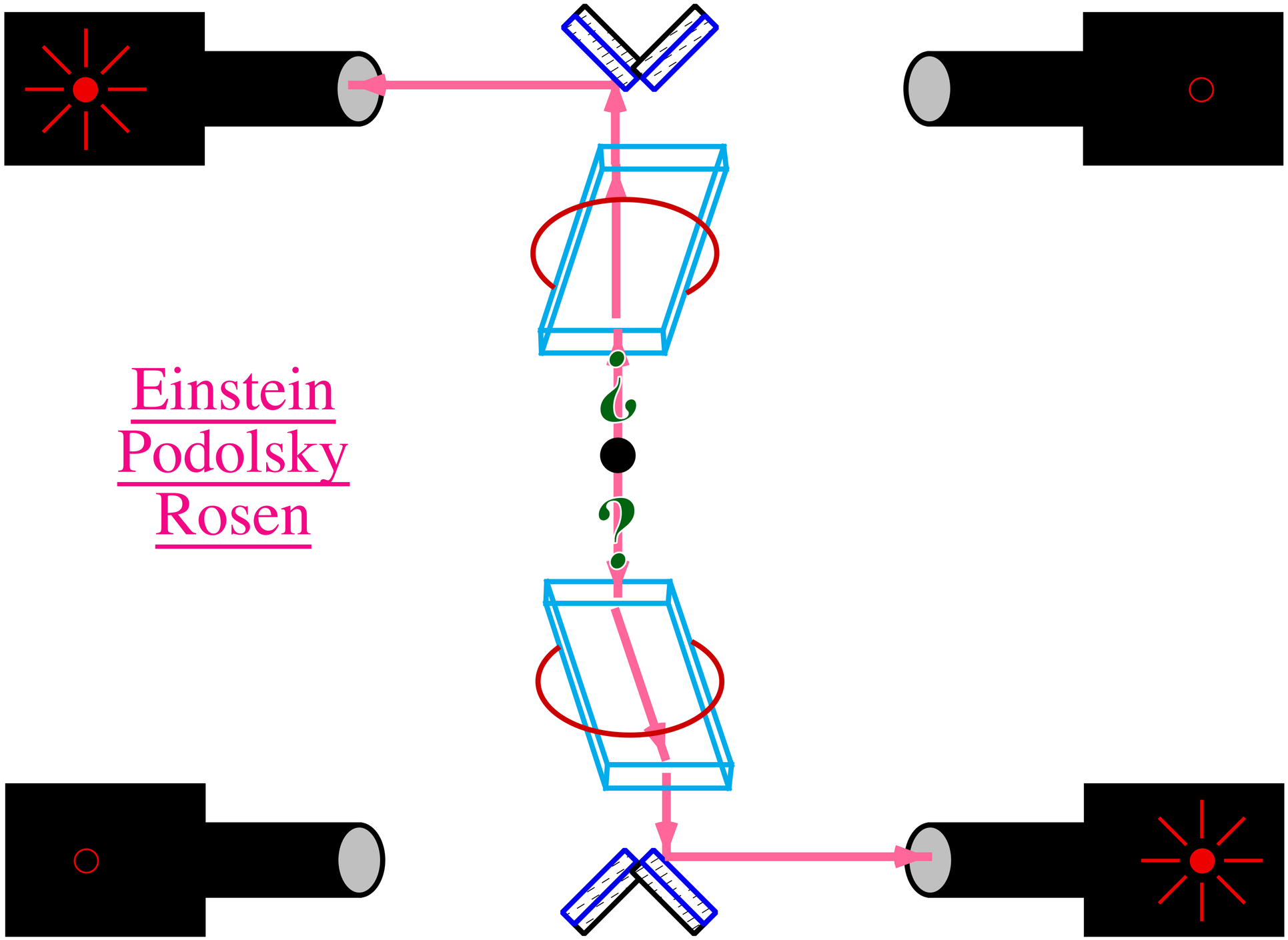
Einstein
Podolsky
Rosen



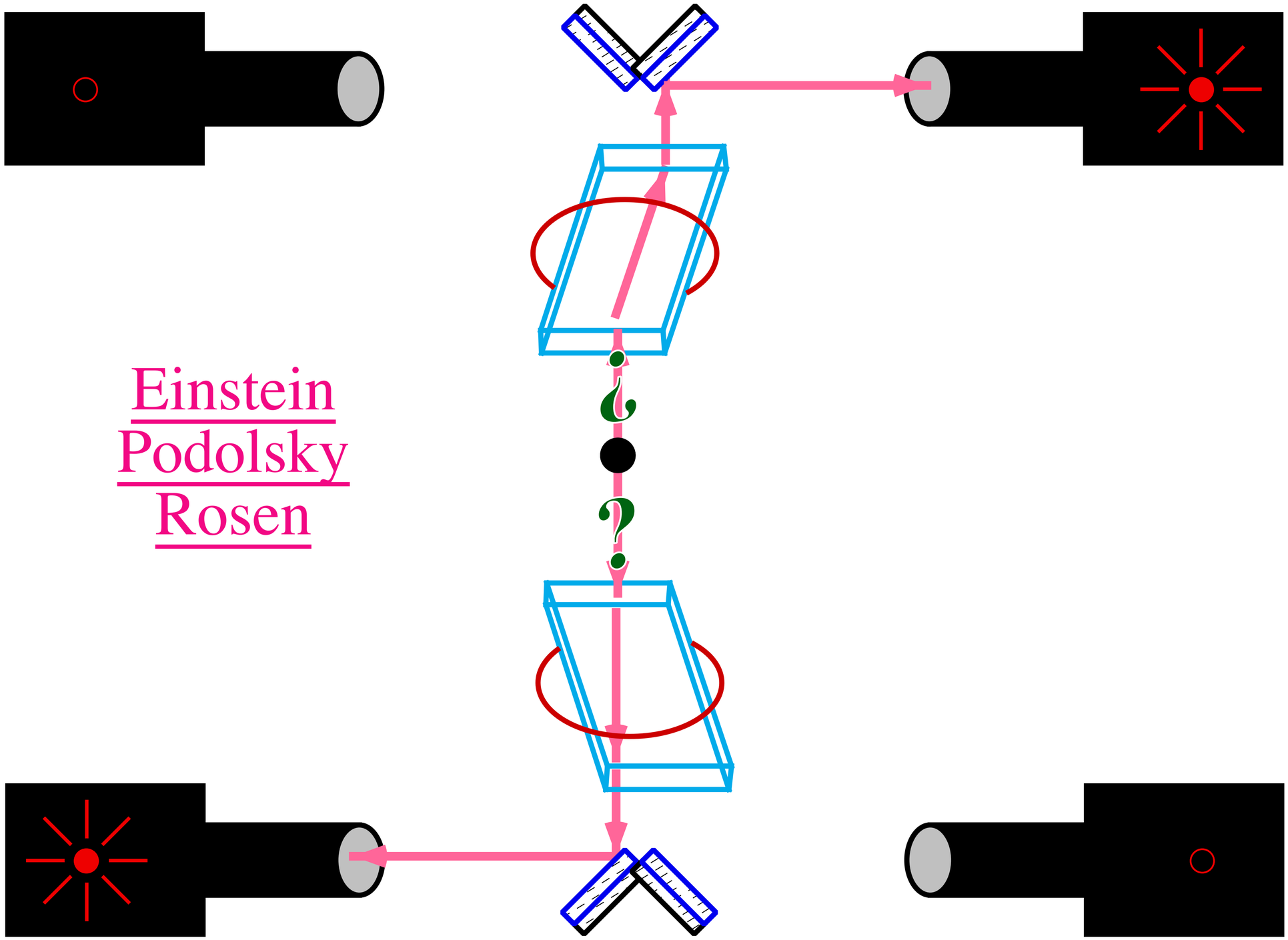
Einstein
Podolsky
Rosen



Einstein
Podolsky
Rosen

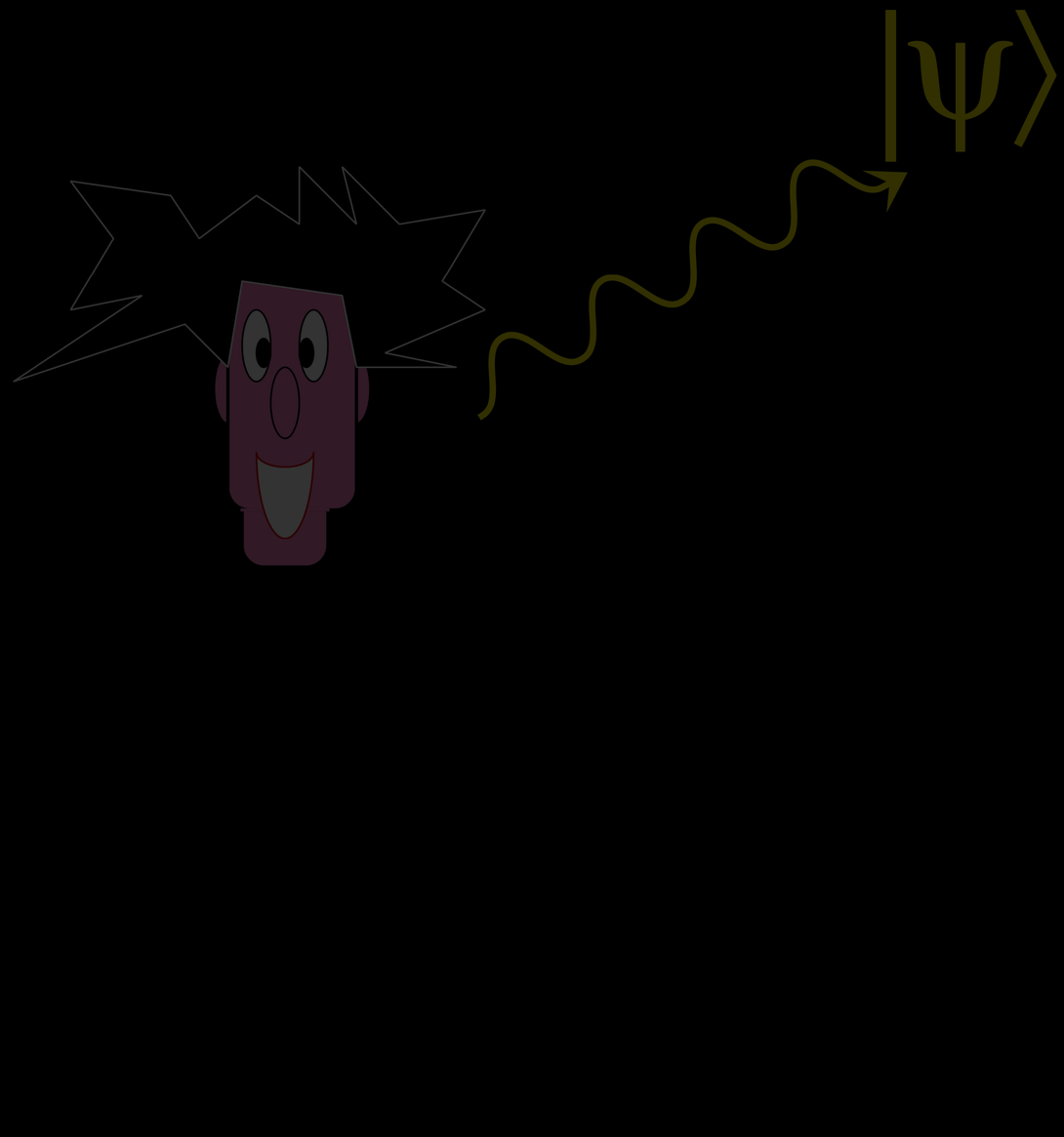


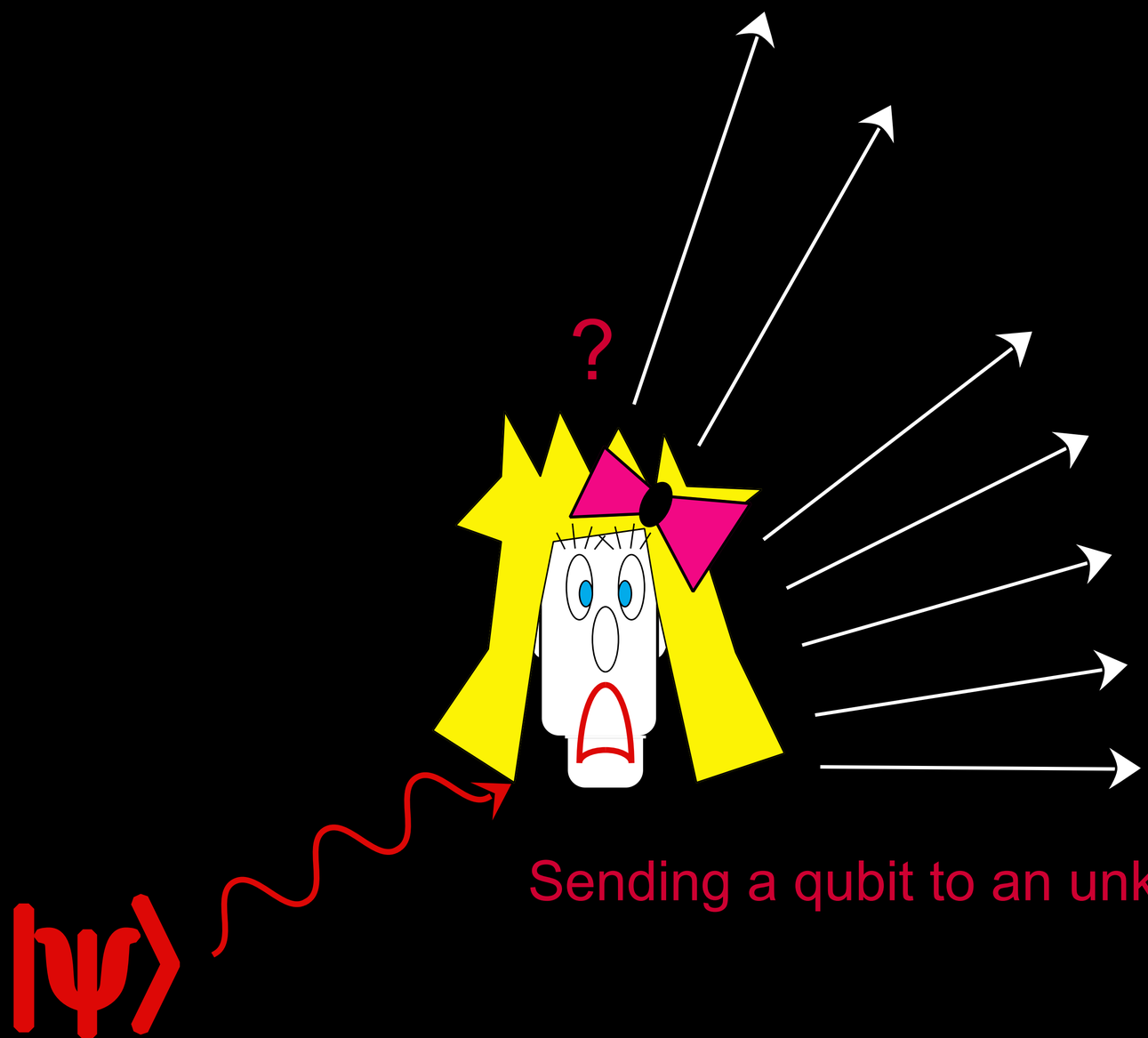
Einstein
Podolsky
Rosen



(6)

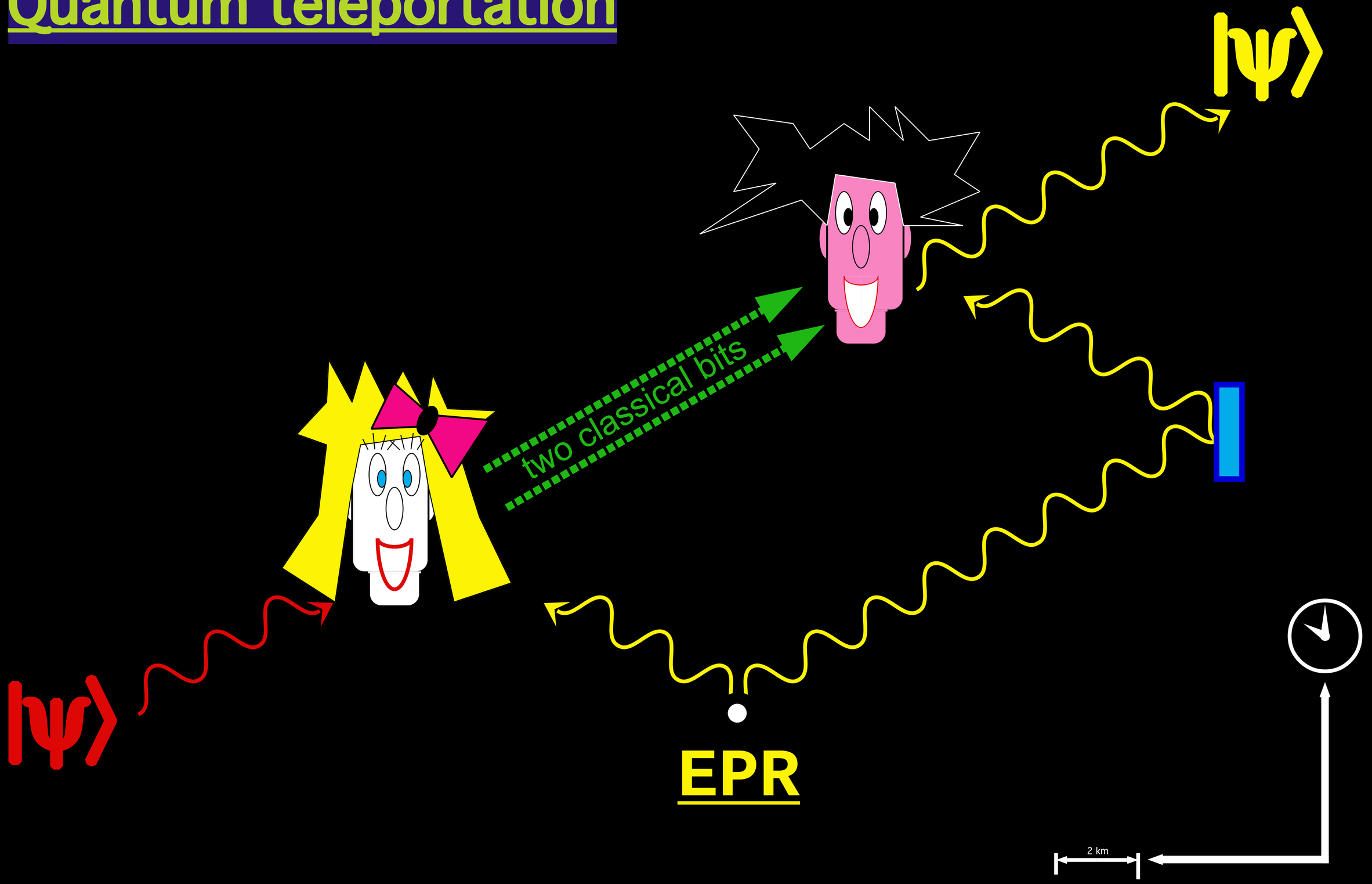
Quantum Teleportation



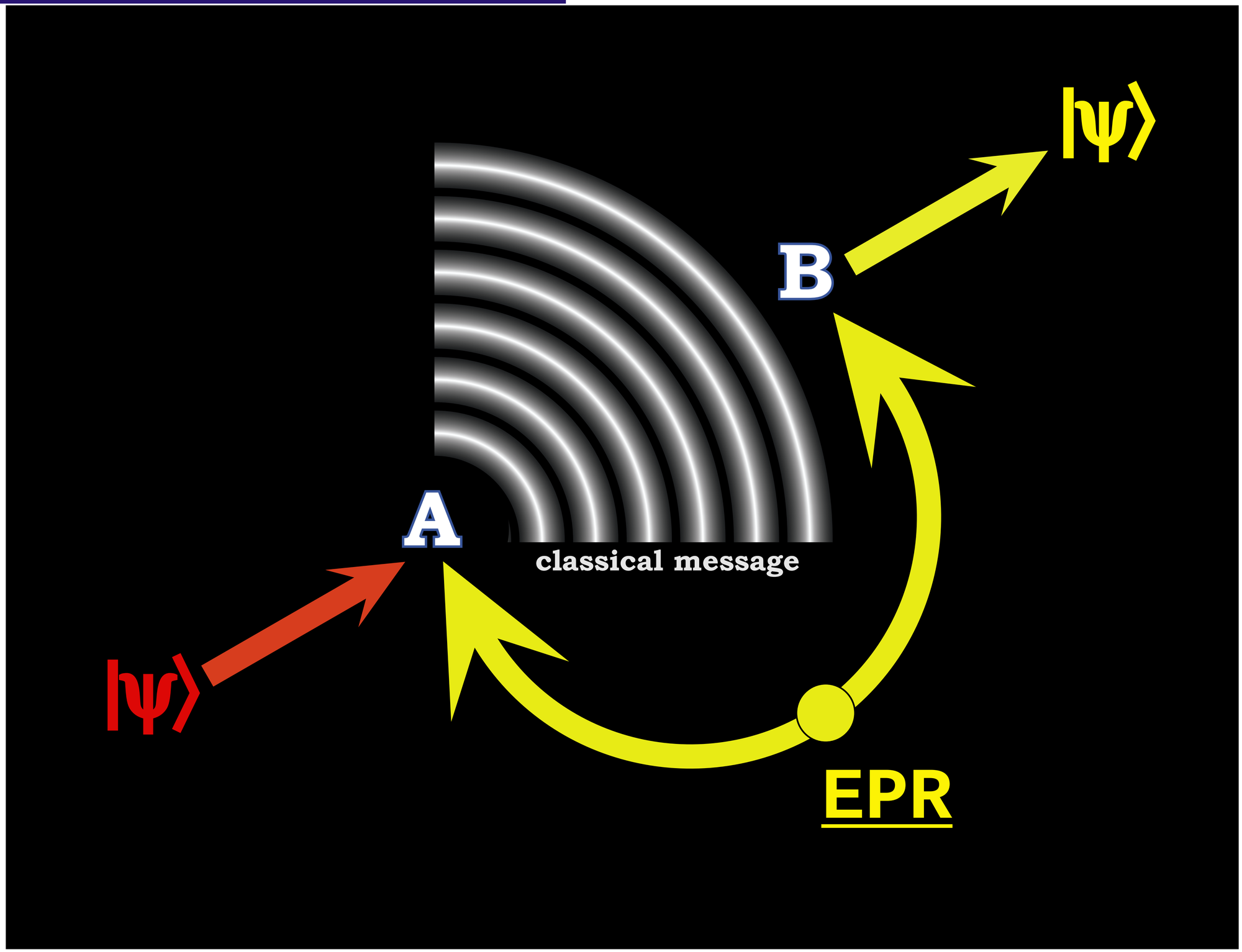


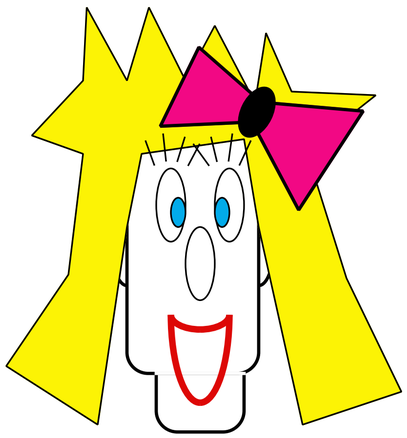
Sending a qubit to an unknown location...?

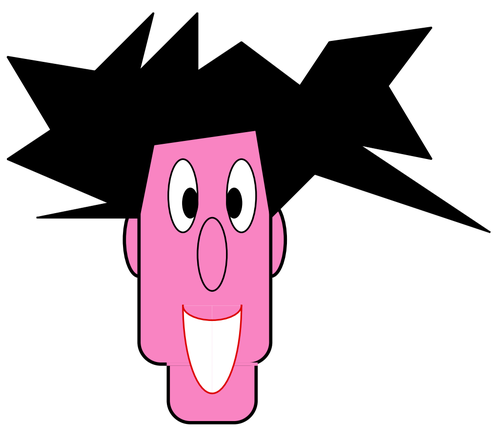
Quantum teleportation

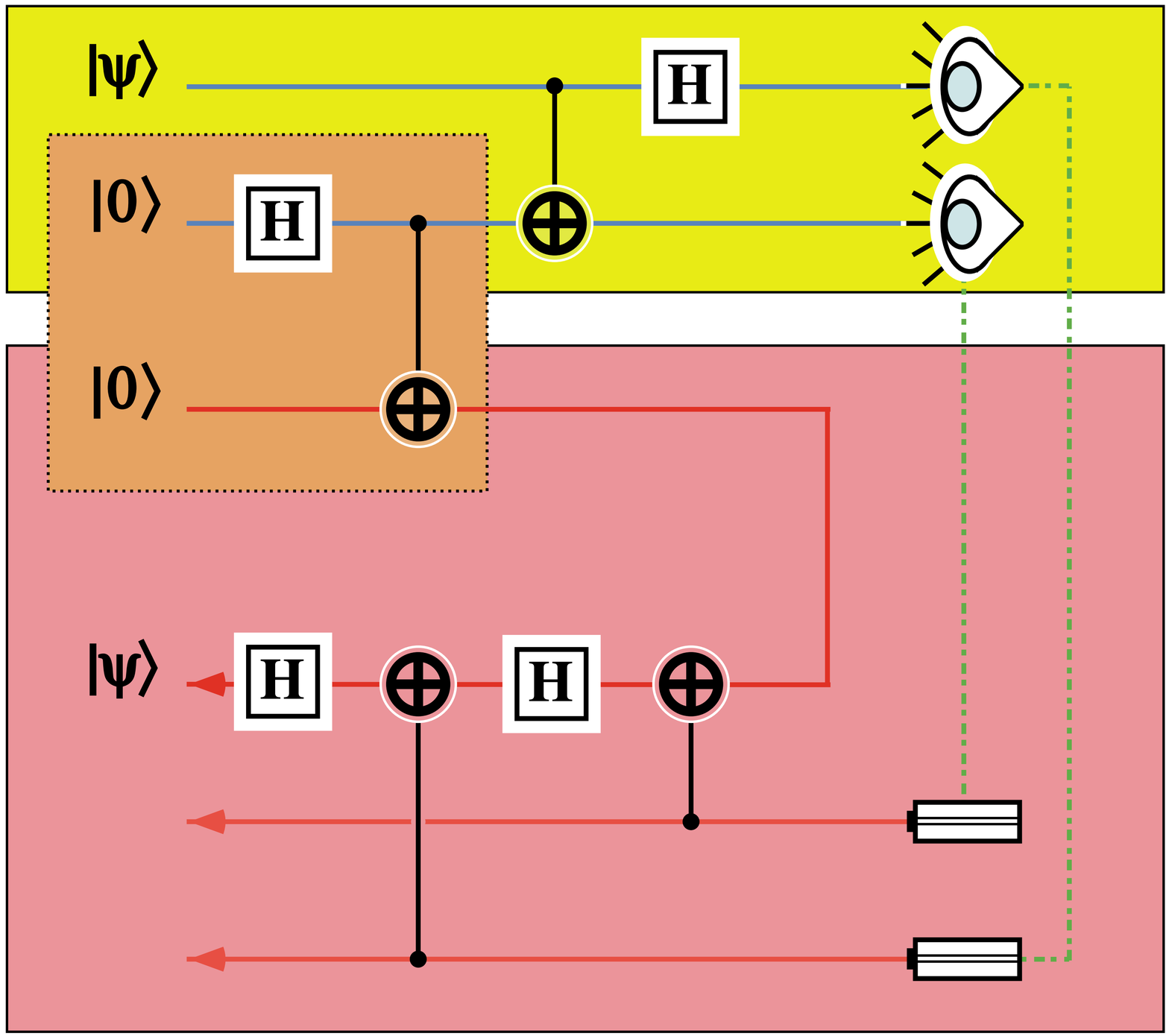


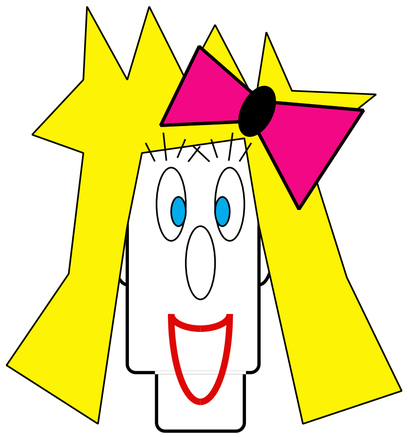
Quantum “broadcasting”

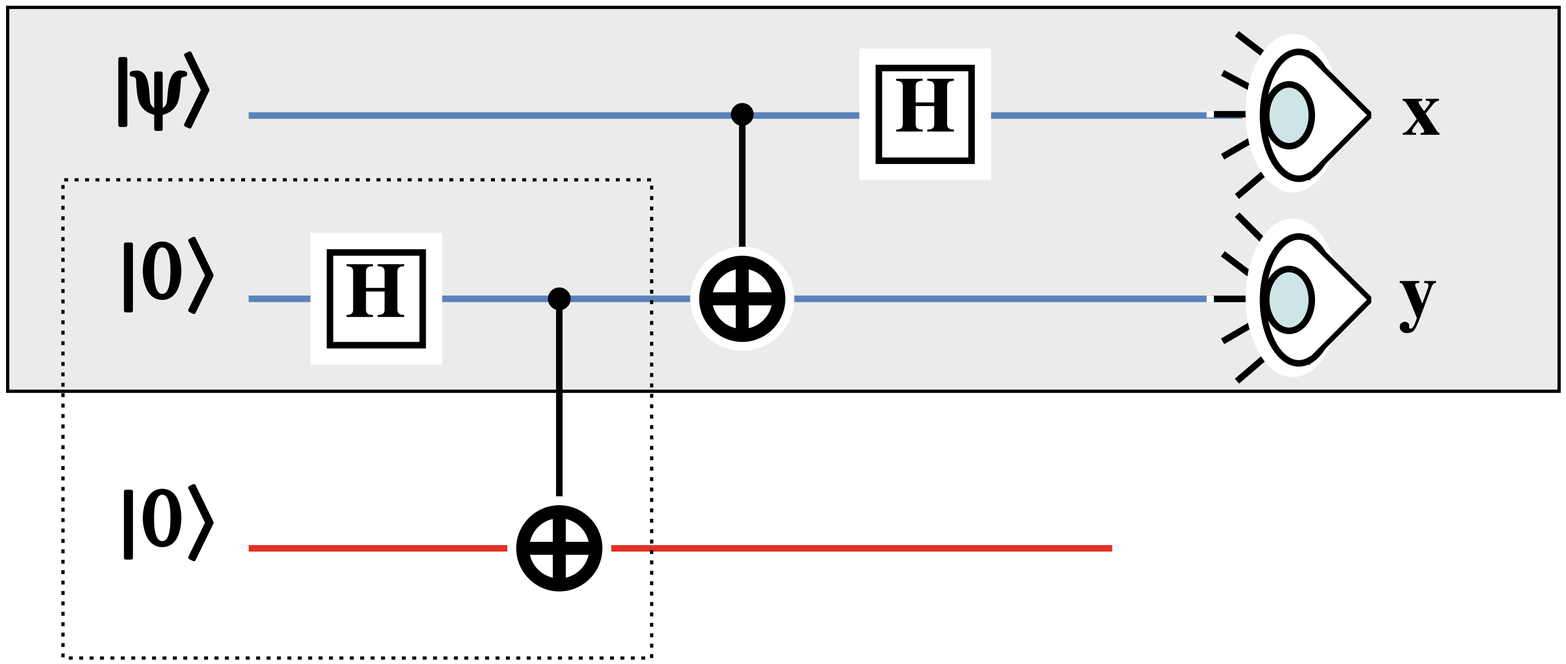












$|\psi\rangle|0\rangle|0\rangle$

H $|\psi\rangle(|0\rangle+|1\rangle)|0\rangle$

⊕ $|\psi\rangle(|0\rangle|0\rangle+|1\rangle|1\rangle)$

$(\alpha|0\rangle+\beta|1\rangle)(|00\rangle+|11\rangle)$

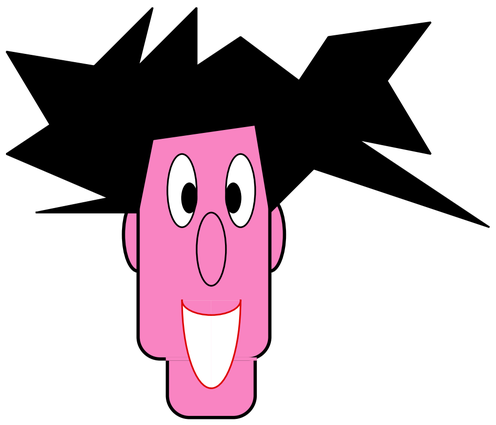
$\alpha|0\rangle|00\rangle+\alpha|0\rangle|11\rangle+\beta|1\rangle|00\rangle+\beta|1\rangle|11\rangle$

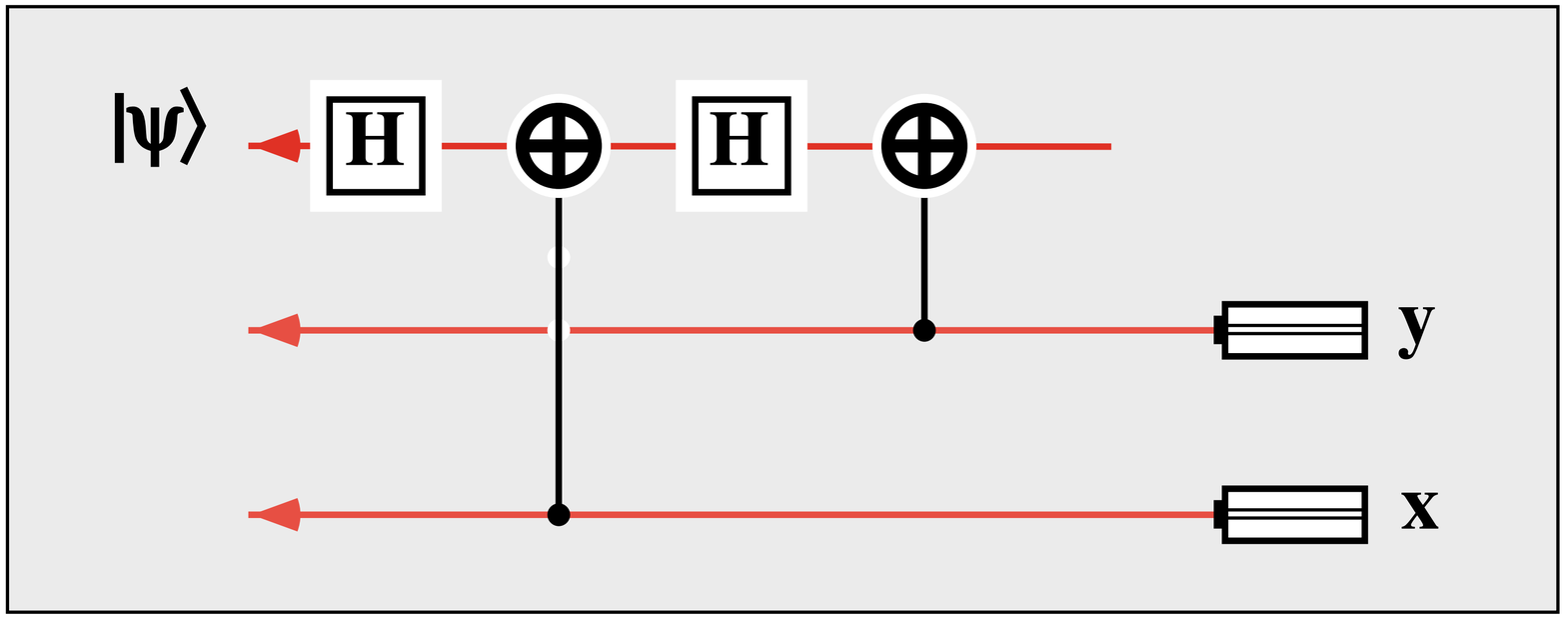
⊕ $\alpha|0\rangle|00\rangle+\alpha|0\rangle|11\rangle+\beta|1\rangle|10\rangle+\beta|1\rangle|01\rangle$

H $\alpha(|0\rangle+|1\rangle)|00\rangle+\alpha(|0\rangle+|1\rangle)|11\rangle+\beta(|0\rangle-|1\rangle)|10\rangle+\beta(|0\rangle-|1\rangle)|01\rangle$

$|00\rangle(\alpha|0\rangle+\beta|1\rangle)+|01\rangle(\alpha|1\rangle+\beta|0\rangle)+|10\rangle(\alpha|0\rangle-\beta|1\rangle)+|11\rangle(\alpha|1\rangle-\beta|0\rangle)$

$|xy\rangle(\alpha|y\rangle+(-1)^{x}\beta|\neg y\rangle)$





$|xy\rangle(\alpha|y\rangle+(-1)^{x}\beta|\neg y\rangle)$

$\oplus$ $|xy\rangle(\alpha|0\rangle+(-1)^{x}\beta|1\rangle)$

H $|xy\rangle(\alpha(|0\rangle+|1\rangle)+(-1)^{x}\beta(|0\rangle-|1\rangle))$

$\oplus$ $|xy\rangle(\alpha(|x\rangle+|\neg x\rangle)+(-1)^{x}\beta(|x\rangle-|\neg x\rangle))$

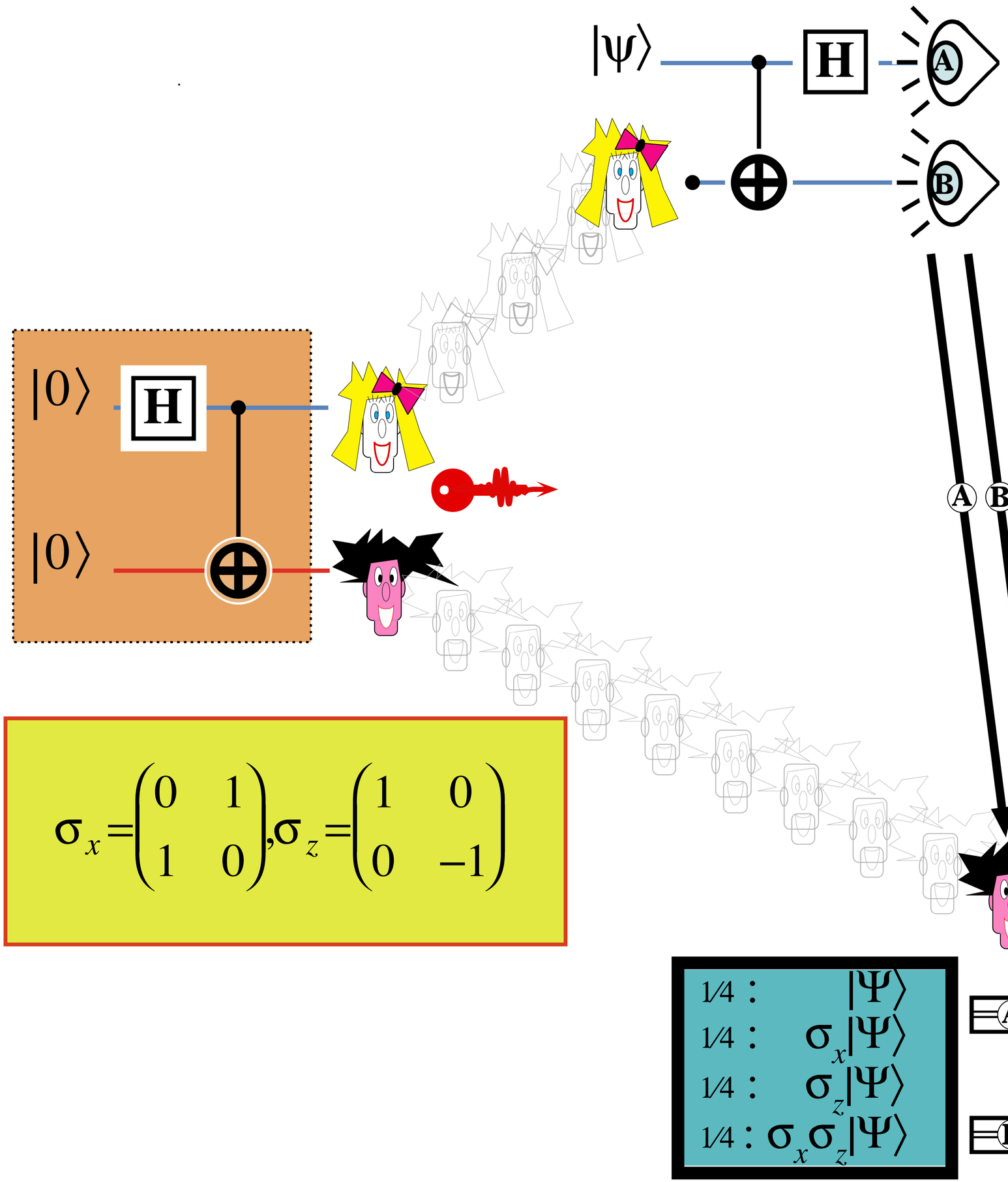
H $|xy\rangle(\alpha([|0\rangle+(-1)^{x}|1\rangle]+[|0\rangle+(-1)^{\neg x}|1\rangle])$

$+(-1)^{x}\beta([|0\rangle+(-1)^{x}|1\rangle]-[|0\rangle+(-1)^{\neg x}|1\rangle]))$

$|xy\rangle(\alpha|0\rangle+\beta|1\rangle)$

$|xy\rangle|\psi\rangle$

Summary



$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

1/4 : $|\Psi\rangle$

1/4 : $\sigma_x|\Psi\rangle$

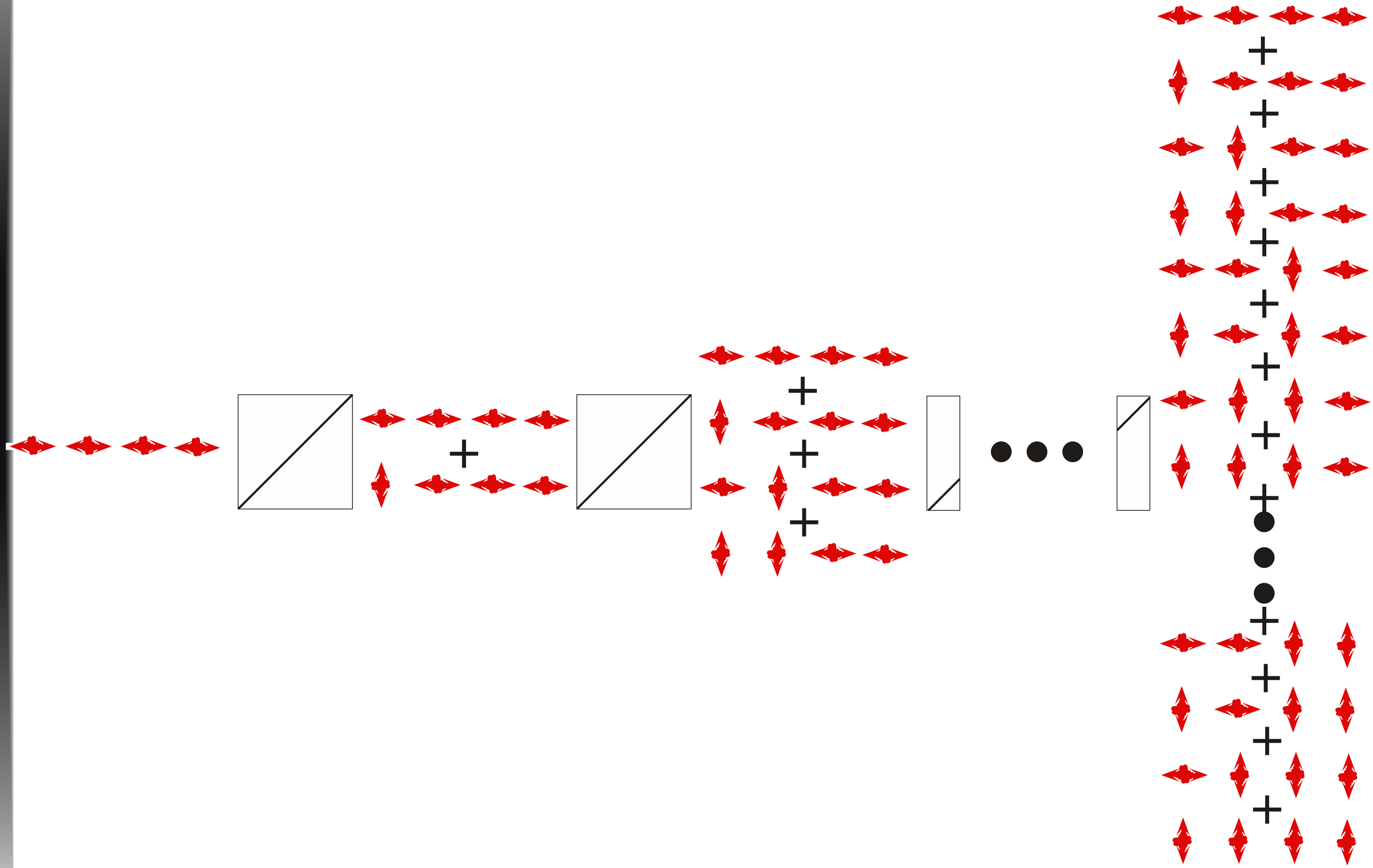
1/4 : $\sigma_z|\Psi\rangle$

1/4 : $\sigma_x\sigma_z|\Psi\rangle$

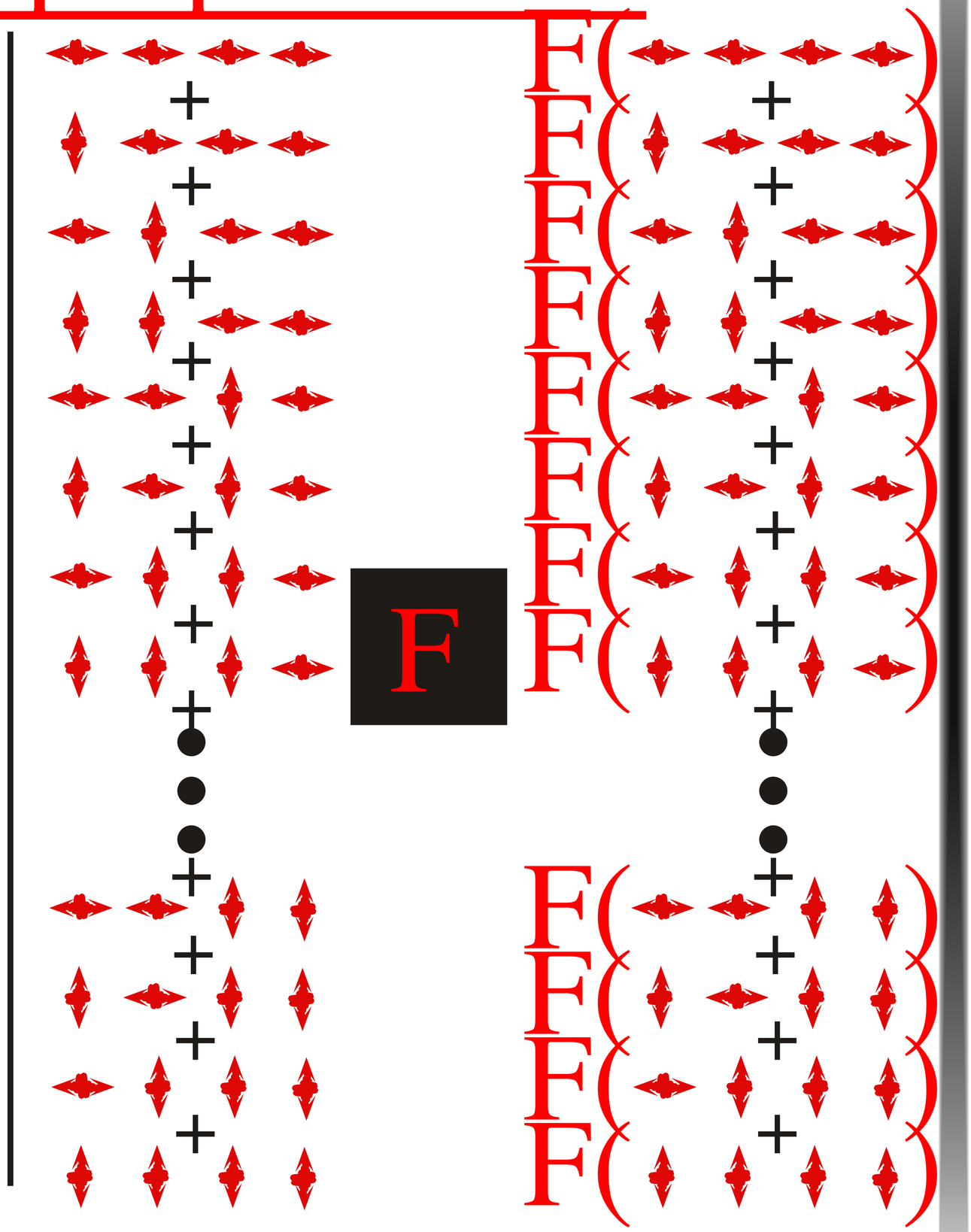
(7)

Quantum Factoring

Quantum Superposition



Quantum Superposition



Quantum Factoring

Given $n=pq$ and $\phi(n)=(p-1)(q-1)$

it is easy to find p and q because

$\phi(n)=(p-1)(q-1)=pq-p-q+1=n-p-(n/p)+1$

$p+(n/p)+n-\phi(n)+1=0$

$p^2+(n-\phi(n)+1)p+n=0$ has solutions:

$p=(-b\pm\sqrt{4ac})/2a \quad (a=1,\ b=n-\phi(n)+1,\ c=n)$

Quantum Factoring

Euler's theorem

$$a^{\phi(n)} \bmod n = 1$$

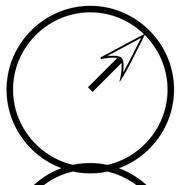
$$F(a,r,n) := (a^r \bmod n, r, n)$$

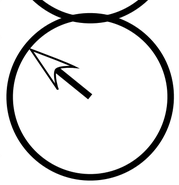
$$F(a,r,n) := (\circlearrowright, r, n)$$

$$F(a,k\phi(n),n) := (\circlearrowright, k\phi(n), n)$$

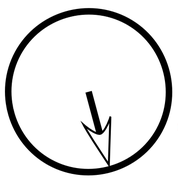
Quantum Factoring

$F(a,r,n) := (a^r \bmod n, r, n)$

$F(a_1,r,n) := ($  $,r,n)$

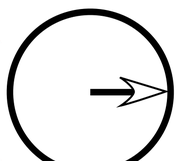
$F(a_2,r,n) := ($  $,r,n)$

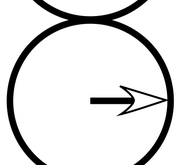
...

$F(a_i,r,n) := ($  $,r,n)$

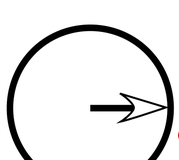
but

.

$F(a_1,k\phi(n),n) := ($  $,k\phi(n),n)$

$F(a_2,k\phi(n),n) := ($  $,k\phi(n),n)$

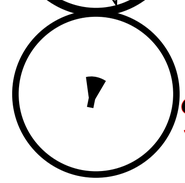
...

$F(a_i,k\phi(n),n) := ($  $,k\phi(n),n)$

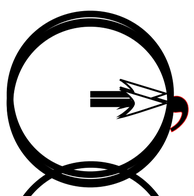
Quantum Factoring

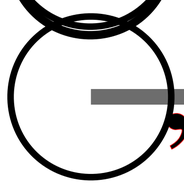
$F(a,r,n):=(a^r \bmod n,r,n)$

$F(*,r,n):=($  $,r,n)$

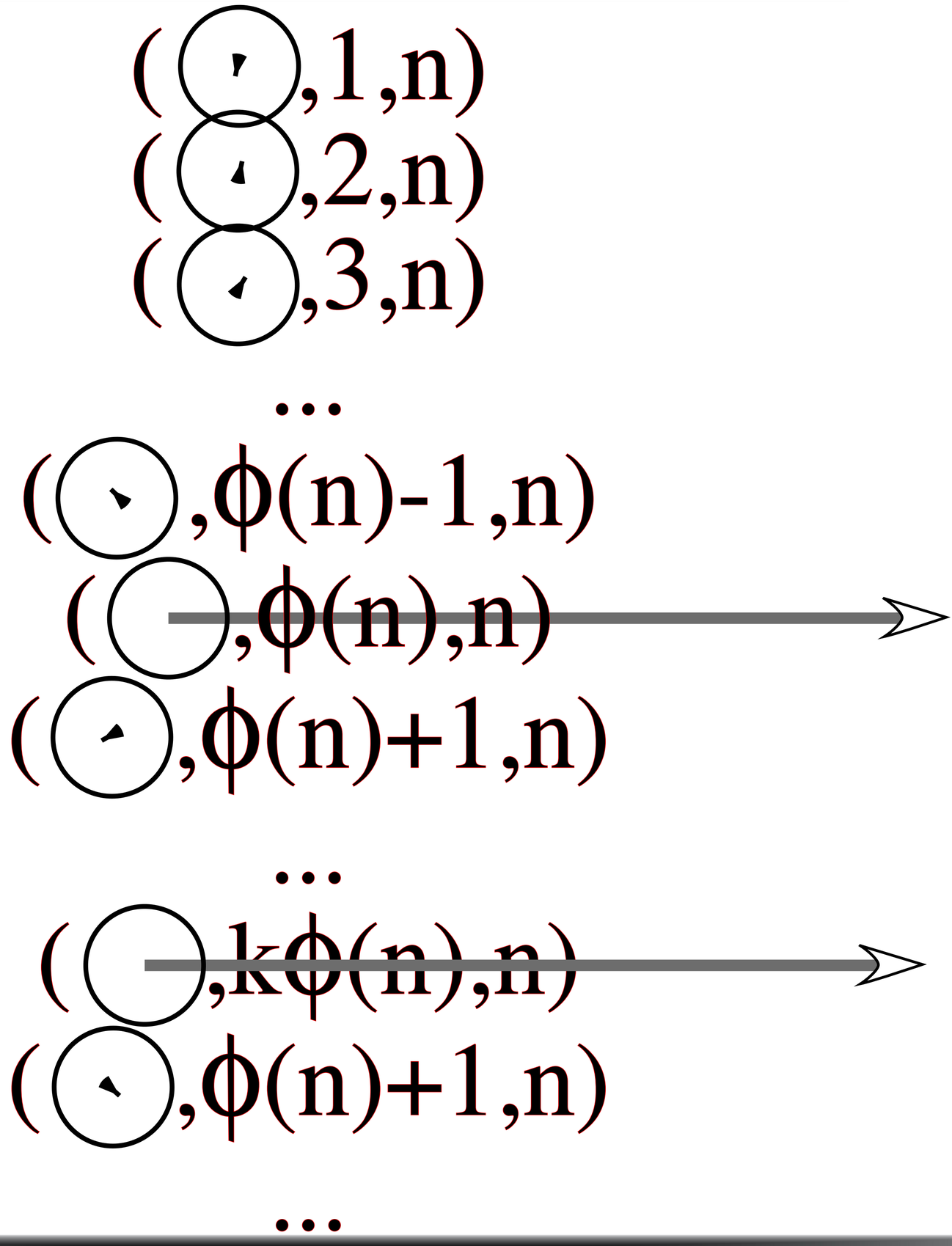
. $=($  $,r,n)$

but .

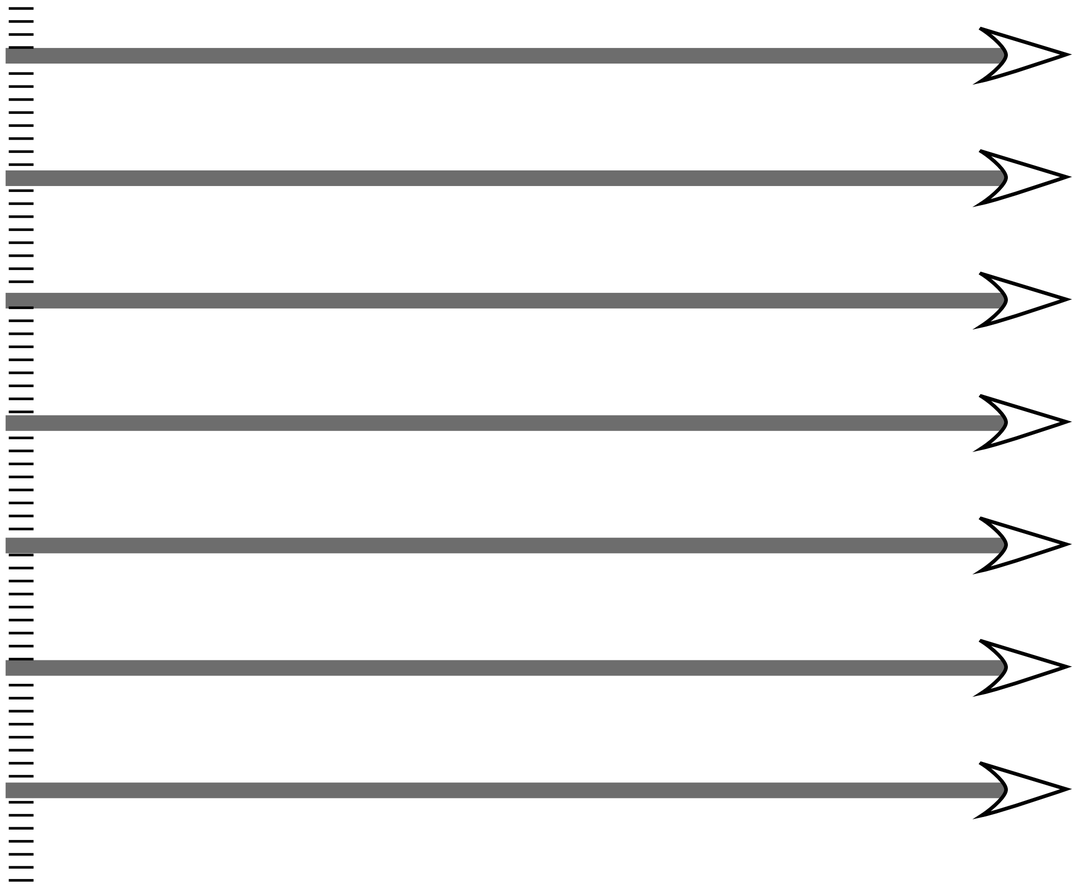
$F(*,k\phi(n),n):=($  $,k\phi(n),n)$

$F(*,k\phi(n),n):=($  $,k\phi(n),n)$

Quantum Factoring



Quantum Factoring



Quantum Factoring

Construct the superposition
for all r and all a of

$(a^r \bmod n, r, n)$

measure r, and with high
probability $r = k\phi(n)$
for some integer k

repeat to obtain $r' = k'\phi(n)$
$\gcd(r,r') = \phi(n)$.

an Introduction to Quantum Information Theory

Claude Crépeau

School of Computer Science
McGill University