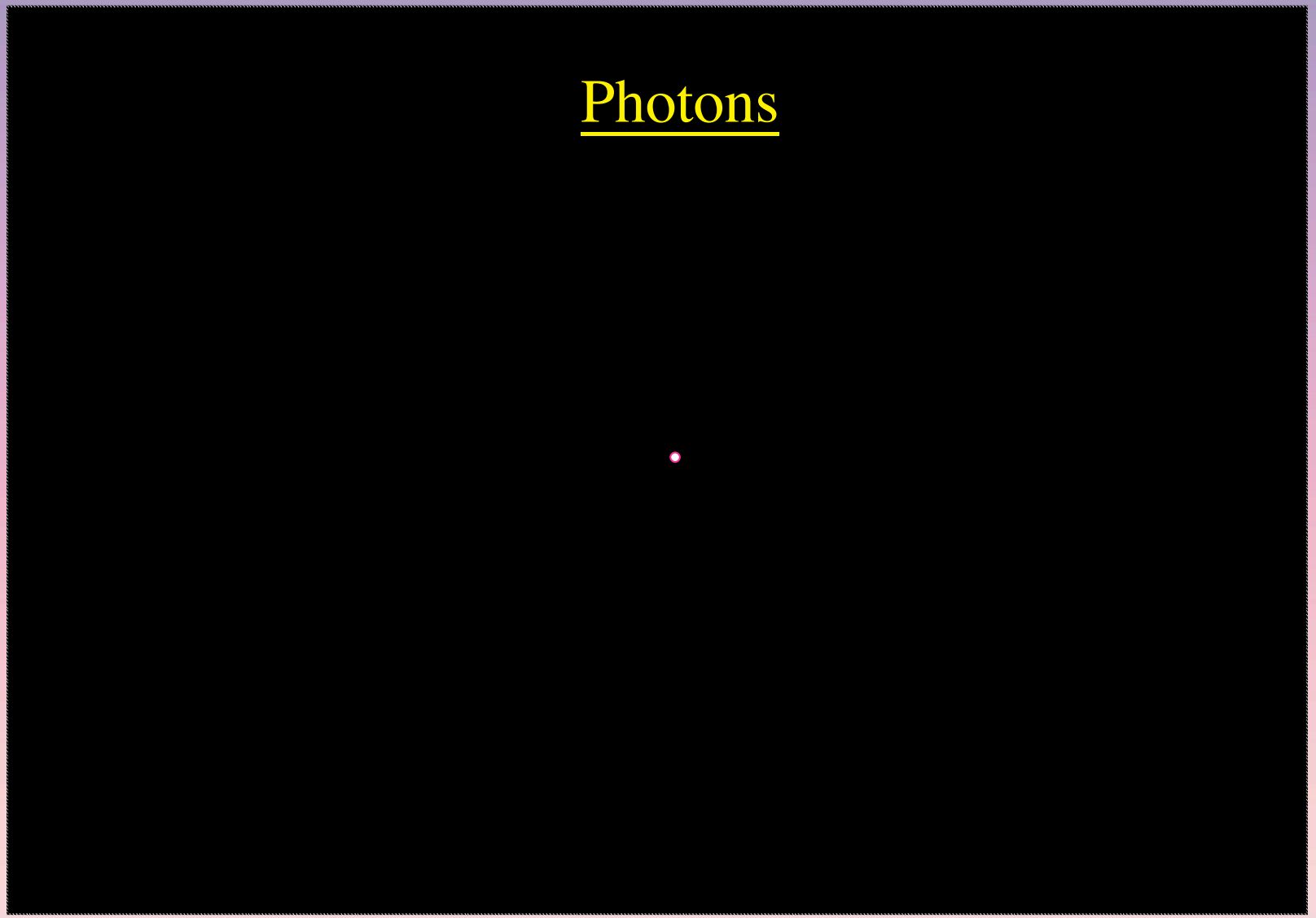
an Introduction to Quantum Information Theory

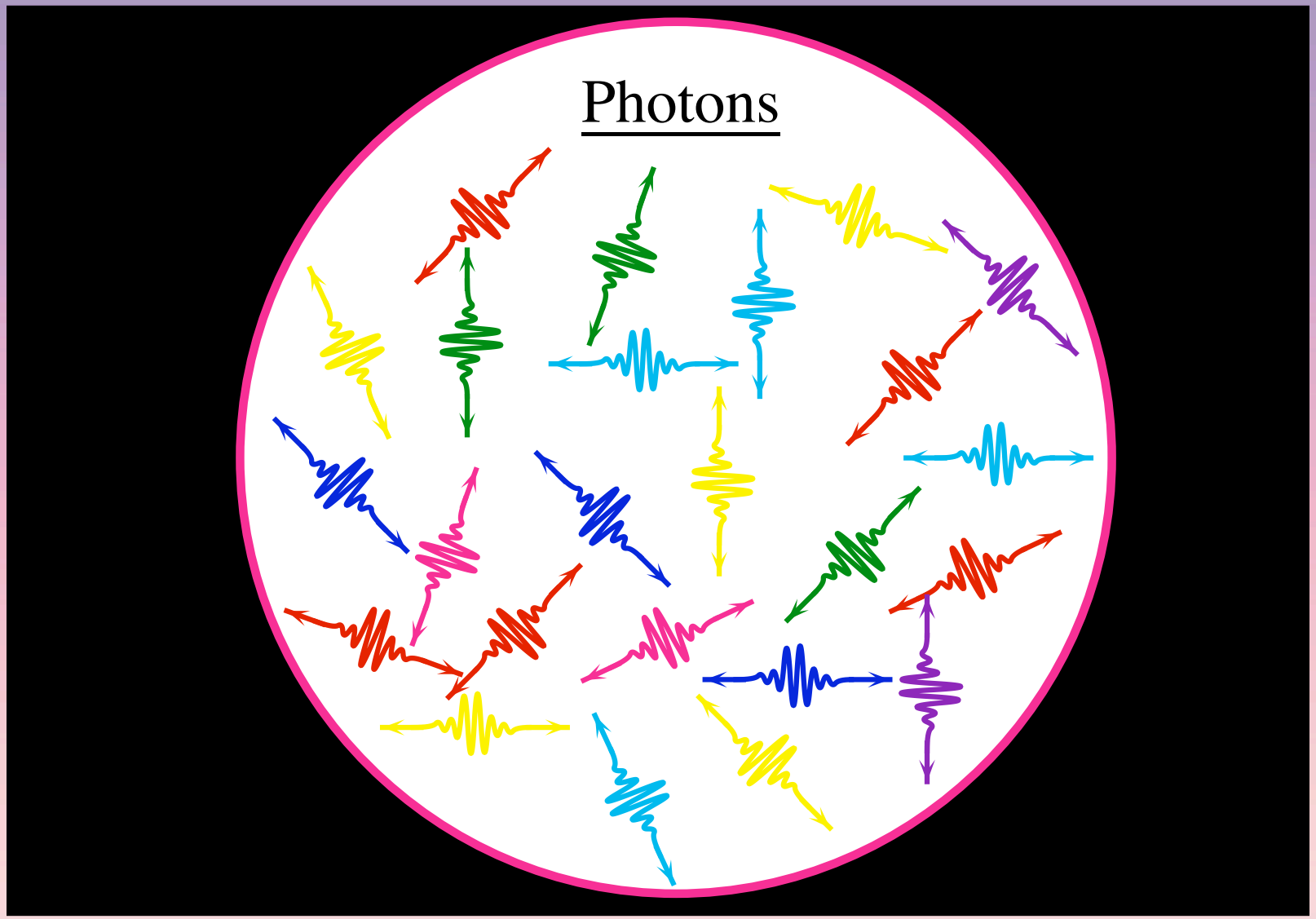
Claude Crépeau

School of Computer Science
McGill University

(1)
Quantum Information

Photons





Photons

Bits & QuBits

0:

1:

$$|\Psi\rangle = c_0 + c_1$$

$$c_i, c_{ij} \in \mathfrak{C}$$

00:

01:

10:

11:

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

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

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

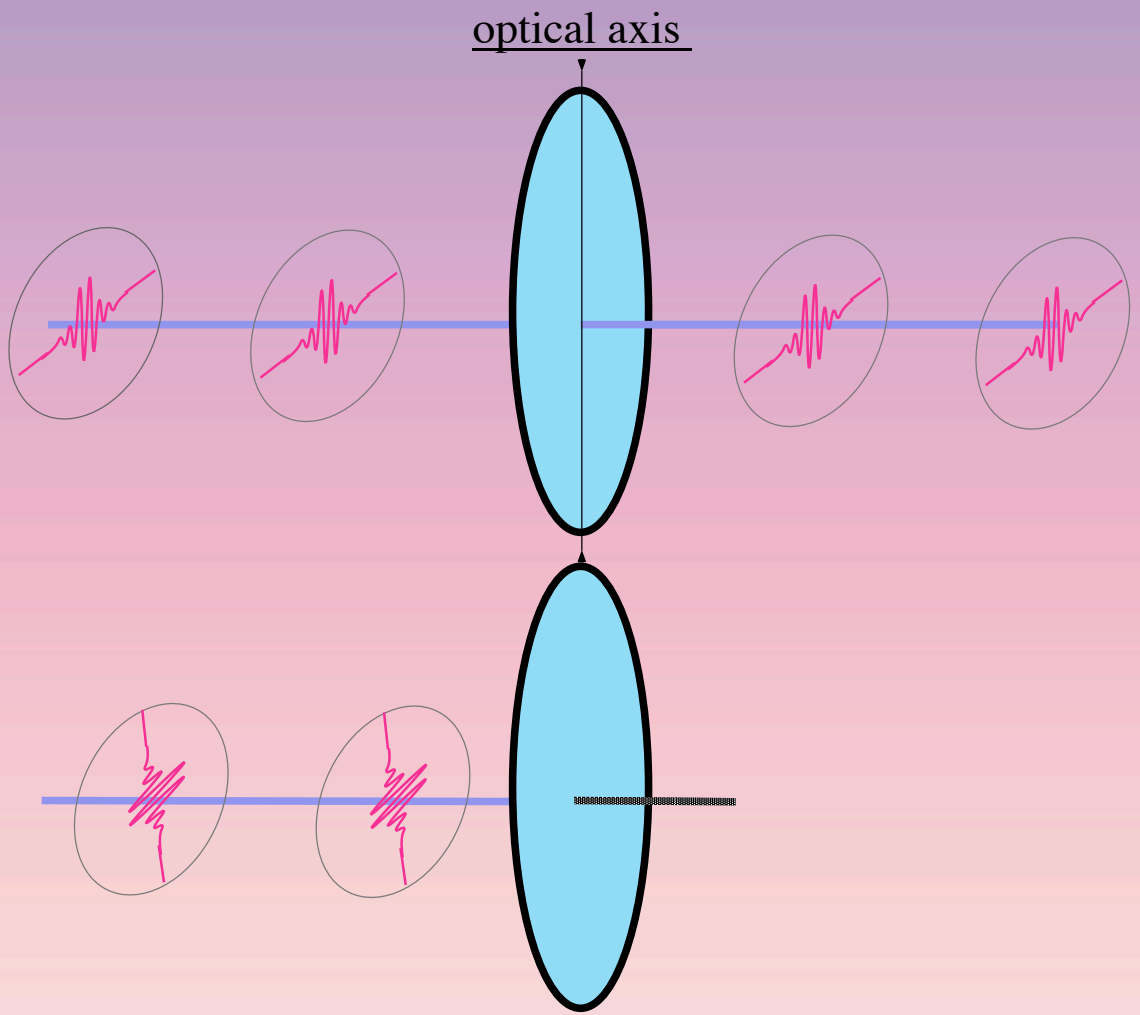
$\langle 0|0\rangle=\langle 1|1\rangle=1$ and $\langle 0|1\rangle=\langle 1|0\rangle=0$

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

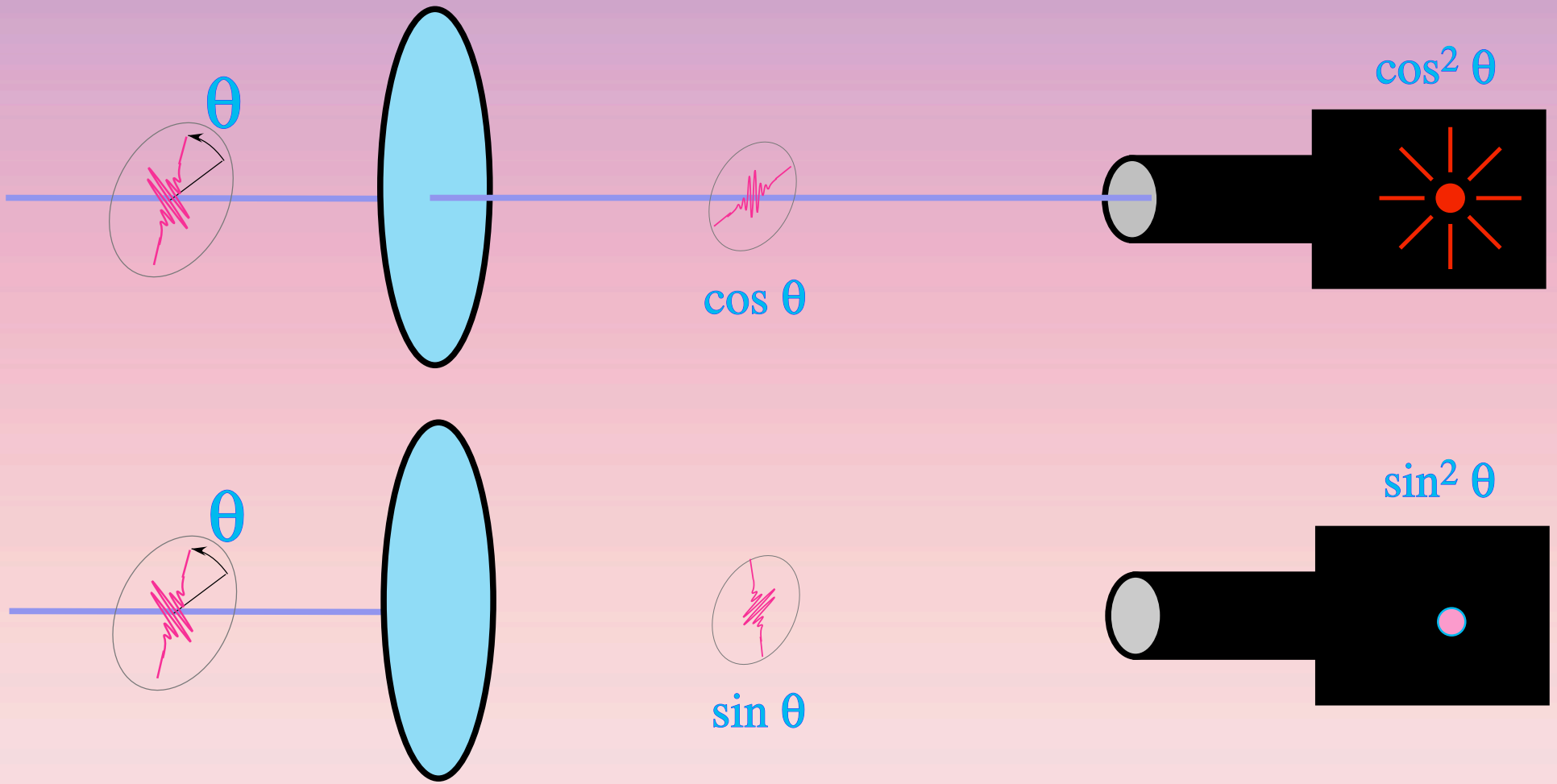
$|0\rangle\otimes|0\rangle=\begin{pmatrix}1&0\\0&0\end{pmatrix}$ $|0\rangle\otimes|1\rangle=\begin{pmatrix}0&1\\0&0\end{pmatrix}$... $|1\rangle\otimes|1\rangle=\begin{pmatrix}0&0\\0&1\end{pmatrix}$

(2)
Quantum Measurements

Polarizing Filter



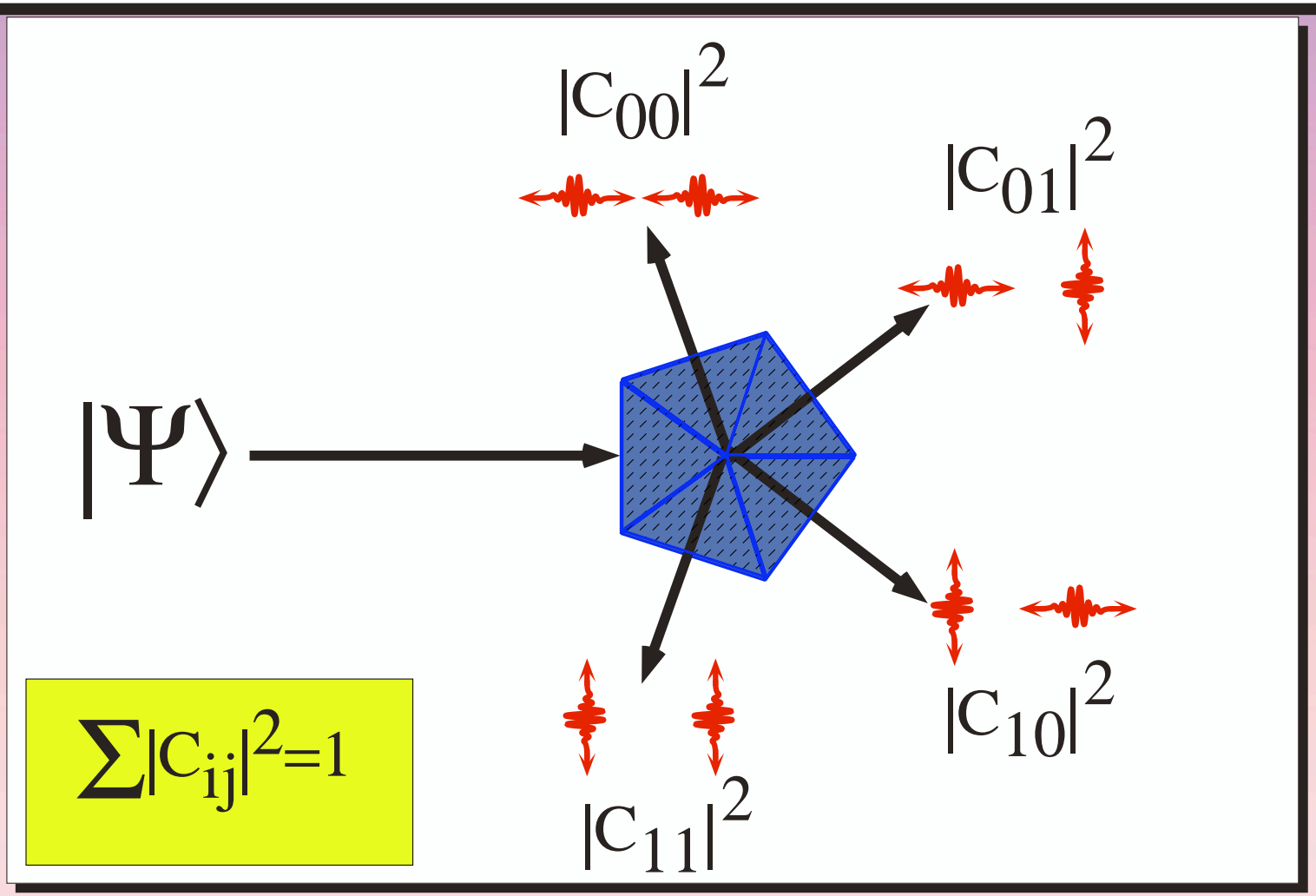
Polarizing Filter and photodetectors



Photons

Projective Measurements

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



standard notations

Projector: $P_\psi = |\psi\rangle\langle\psi|$

$P = \Sigma P_m$, where $P_m P_{m'} = \delta_{m,m'} P_m$

Measurement: $\{ P_m \}$

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

Measuring: $p(m) = \langle\phi|P_m|\phi\rangle$

Resulting: $P_m|\phi\rangle / \sqrt{p(m)}$

example

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

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

Measurement: $\{ P_0, P_1 \}$

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

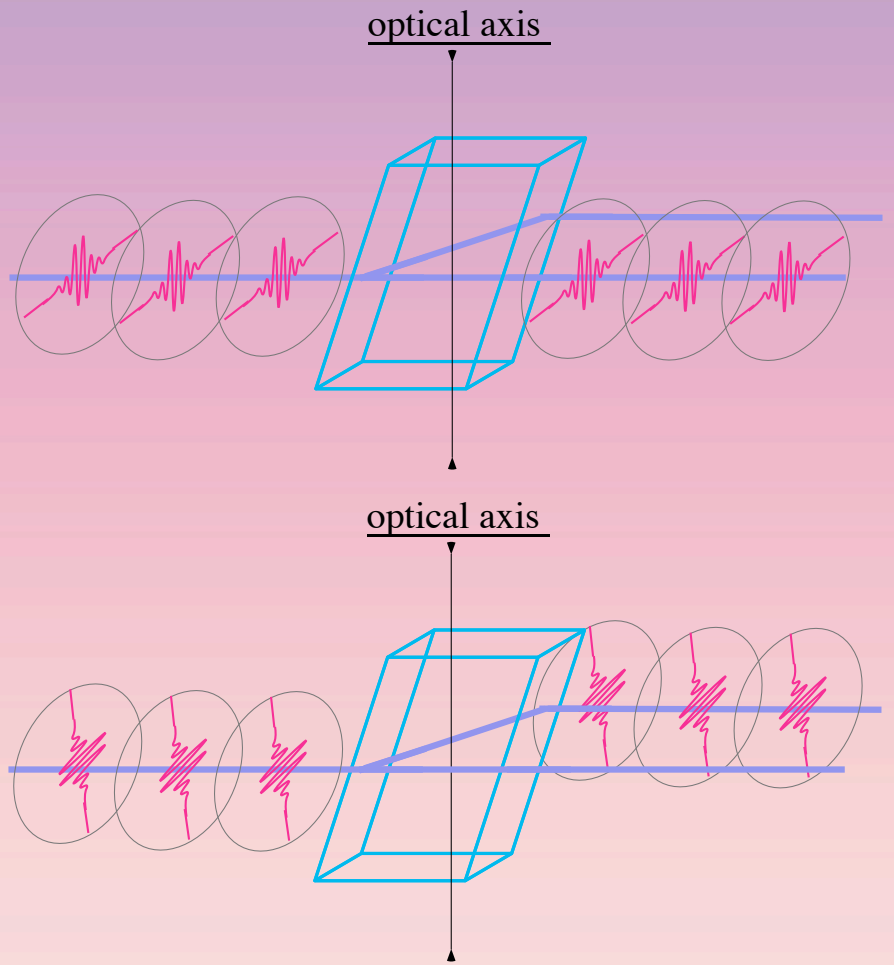
Measuring: $p(m) = \langle \phi | P_m | \phi \rangle$

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

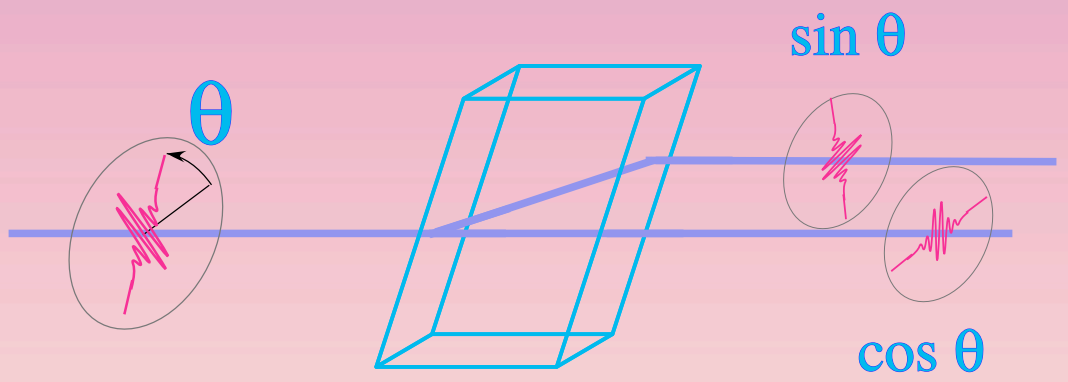
$\alpha^* \langle 0| + \beta^* \langle 1| \; P_1 \; \alpha|0\rangle + \beta|1\rangle = \beta^* \beta = |\beta|^2$

(3)
Quantum Computations

Calcite Crystal



Calcite Crystal

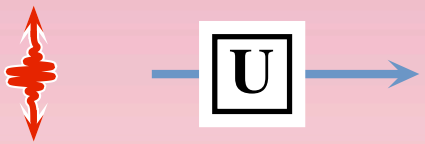


Photons

Quantum Evolution: Unitary Operators

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

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



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

$$\xrightarrow{U} c_0|\Psi_0\rangle + c_1|\Psi_1\rangle$$

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: calcite crystal

Basis states: $|\phi\pi\rangle$, ϕ: polarizaton {0,1}
π: path {low,high}

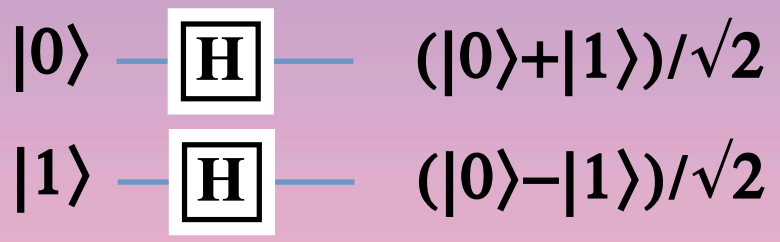
Input states: $(\alpha|0\rangle+\beta|1\rangle)|low\rangle$

Operator: U: $|0x\rangle \rightarrow |0x\rangle$ $\quad U=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$

$|1x\rangle \rightarrow |1\neg x\rangle$

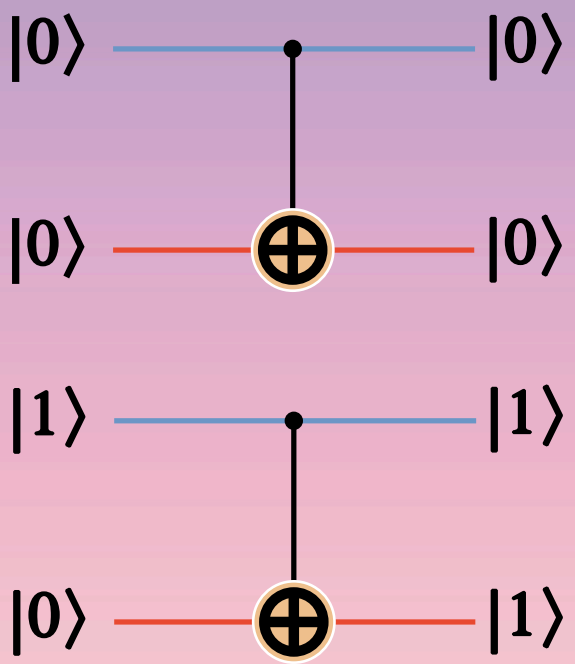
Output states: $\alpha|0\ low\rangle+\beta|1\ high\rangle$

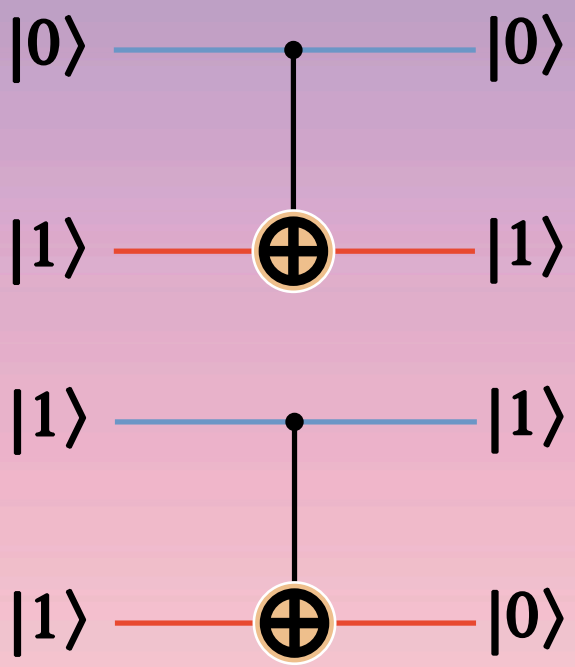
example: Hadamard

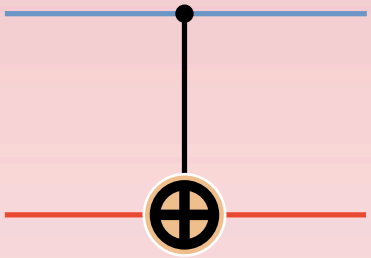


$$H = 1/\sqrt{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

example: Control-NOT



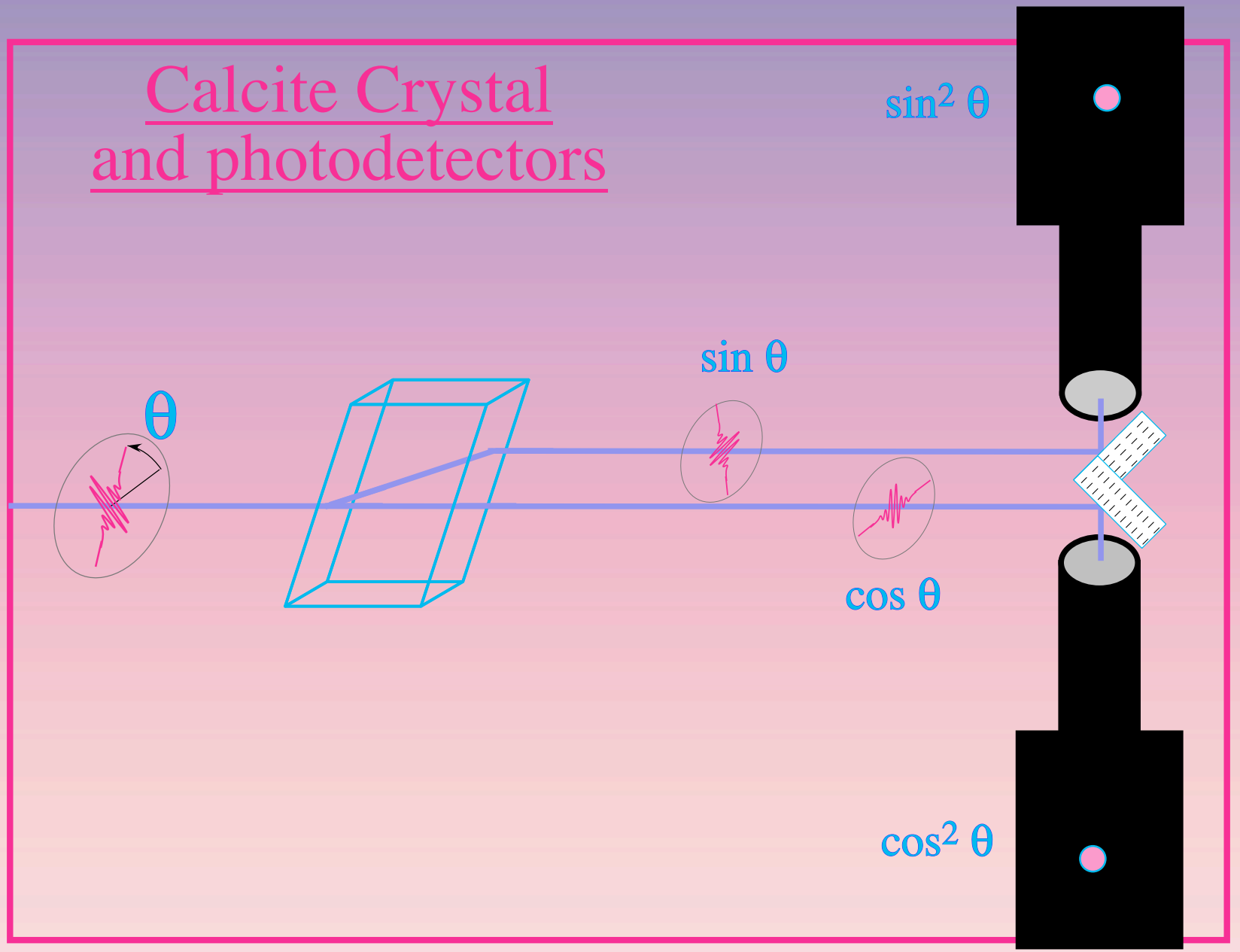




$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

(4)
General Measurements

Calcite Crystal and photodetectors



standard notations

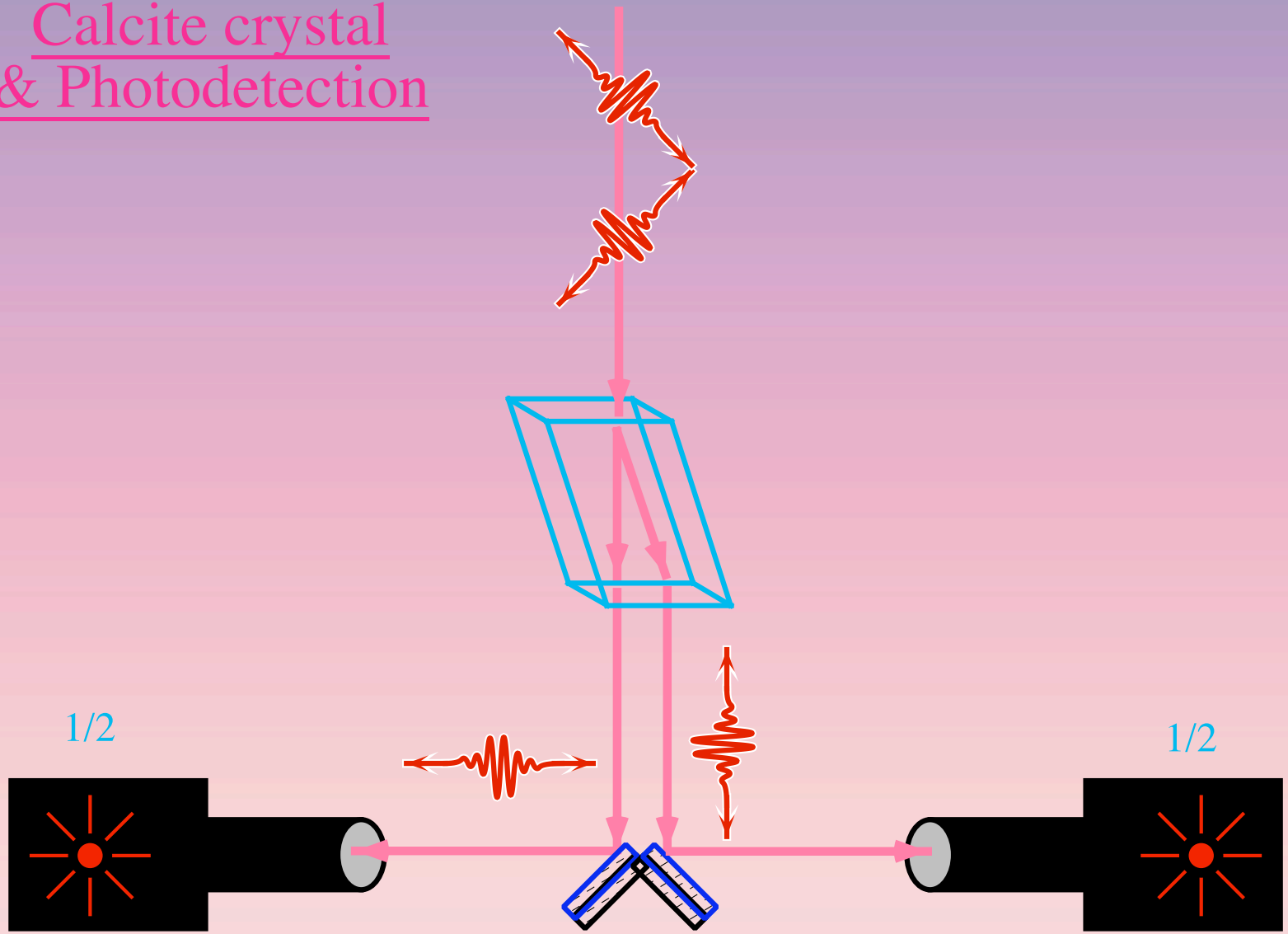
Measurement: $\{ P_m U \}$

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

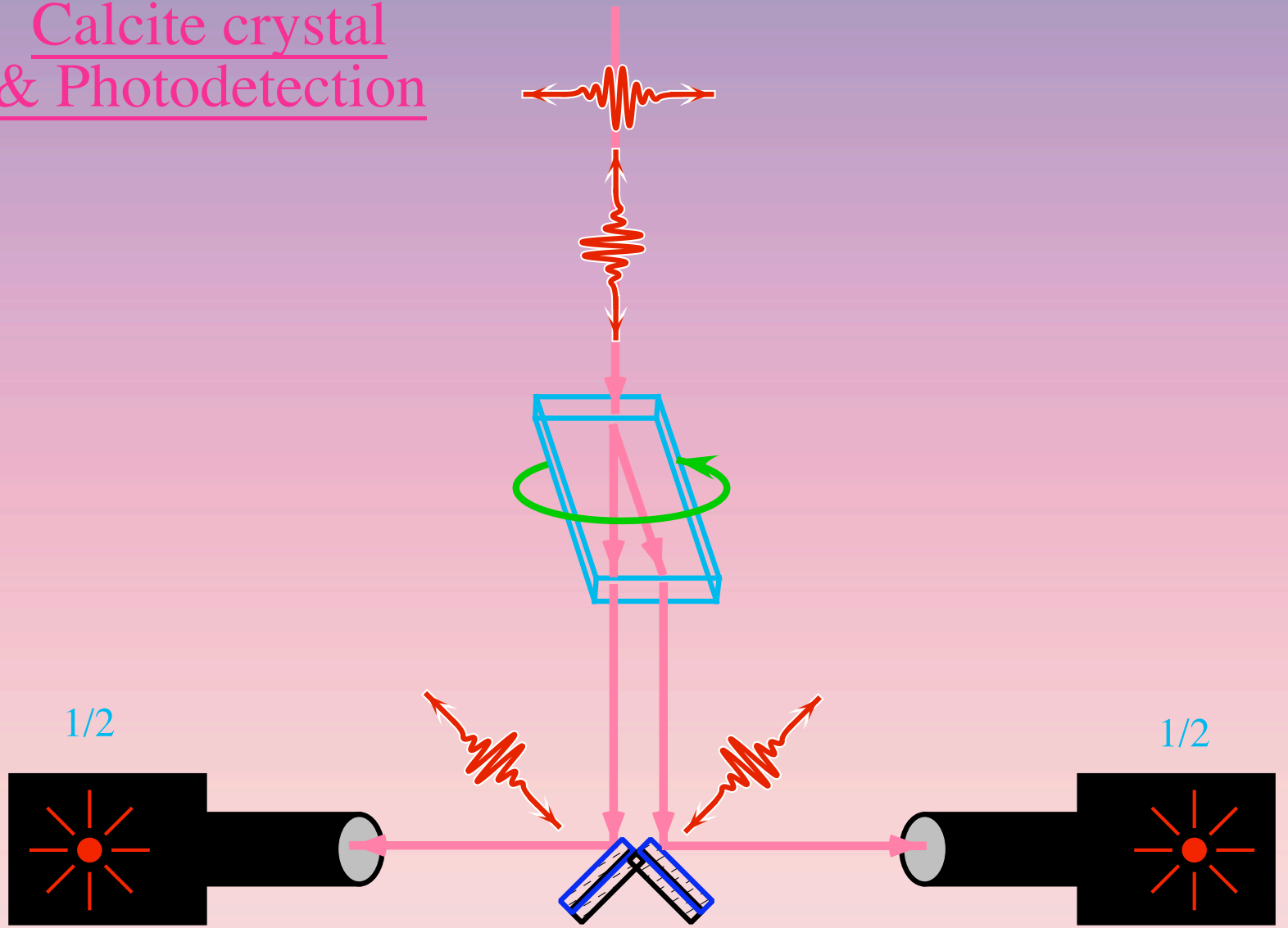
Measuring: $p(m) = \langle\phi|\langle 0|U^\dagger P_m U|\phi\rangle|0\rangle$

Resulting: $P_m U|\phi\rangle|0\rangle / \sqrt{p(m)}$

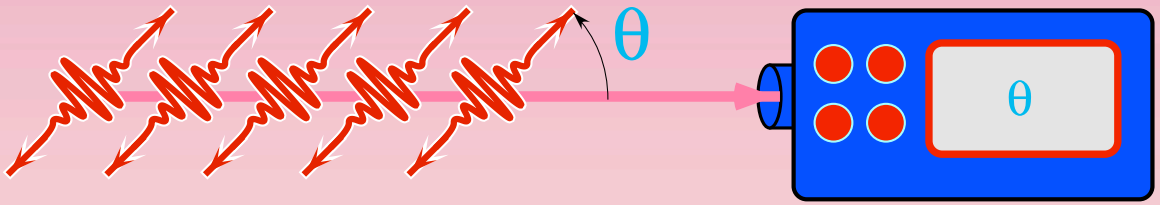
Calcite crystal & Photodetection



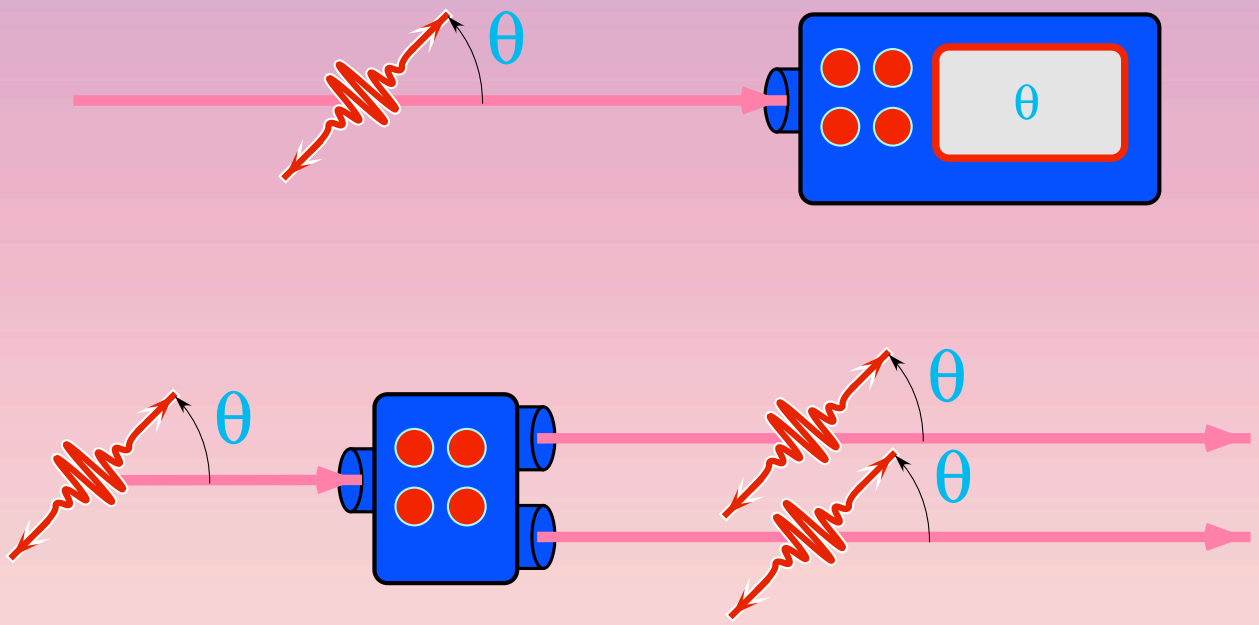
Calcite crystal & Photodetection



POSSIBLE!



IMPOSSIBLE!



Classical & Quantum Information

0011011100110 Classical	Quantum
Copying: Yes	NO
Measuring: Yes	partial
Broadcasting: Yes	NO
Superposing: NO	Yes
Interfering: NO	Yes

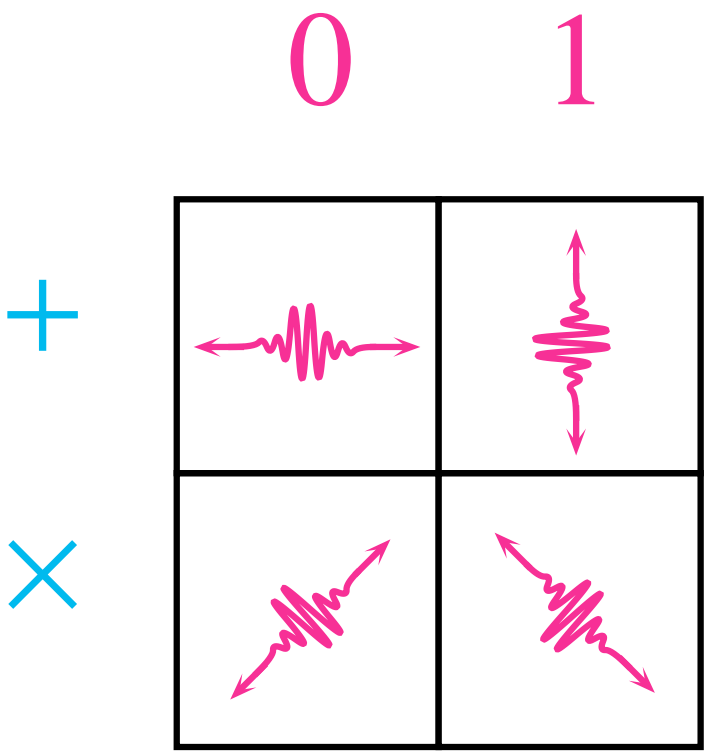
an Introduction to Quantum Information Theory

Claude Crépeau

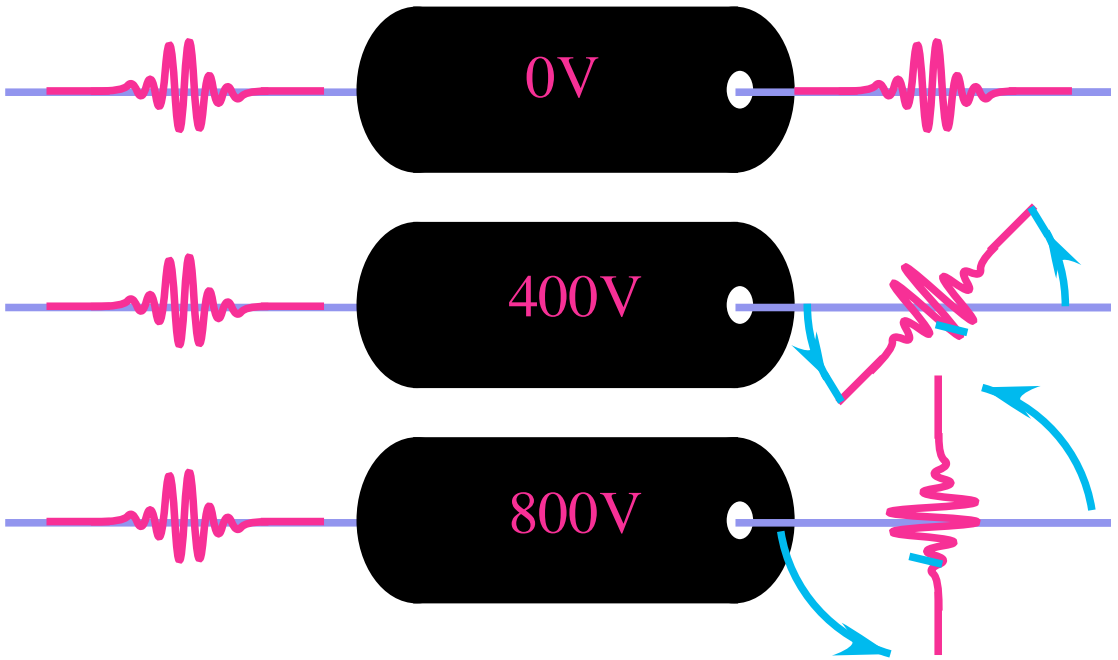
School of Computer Science
McGill University

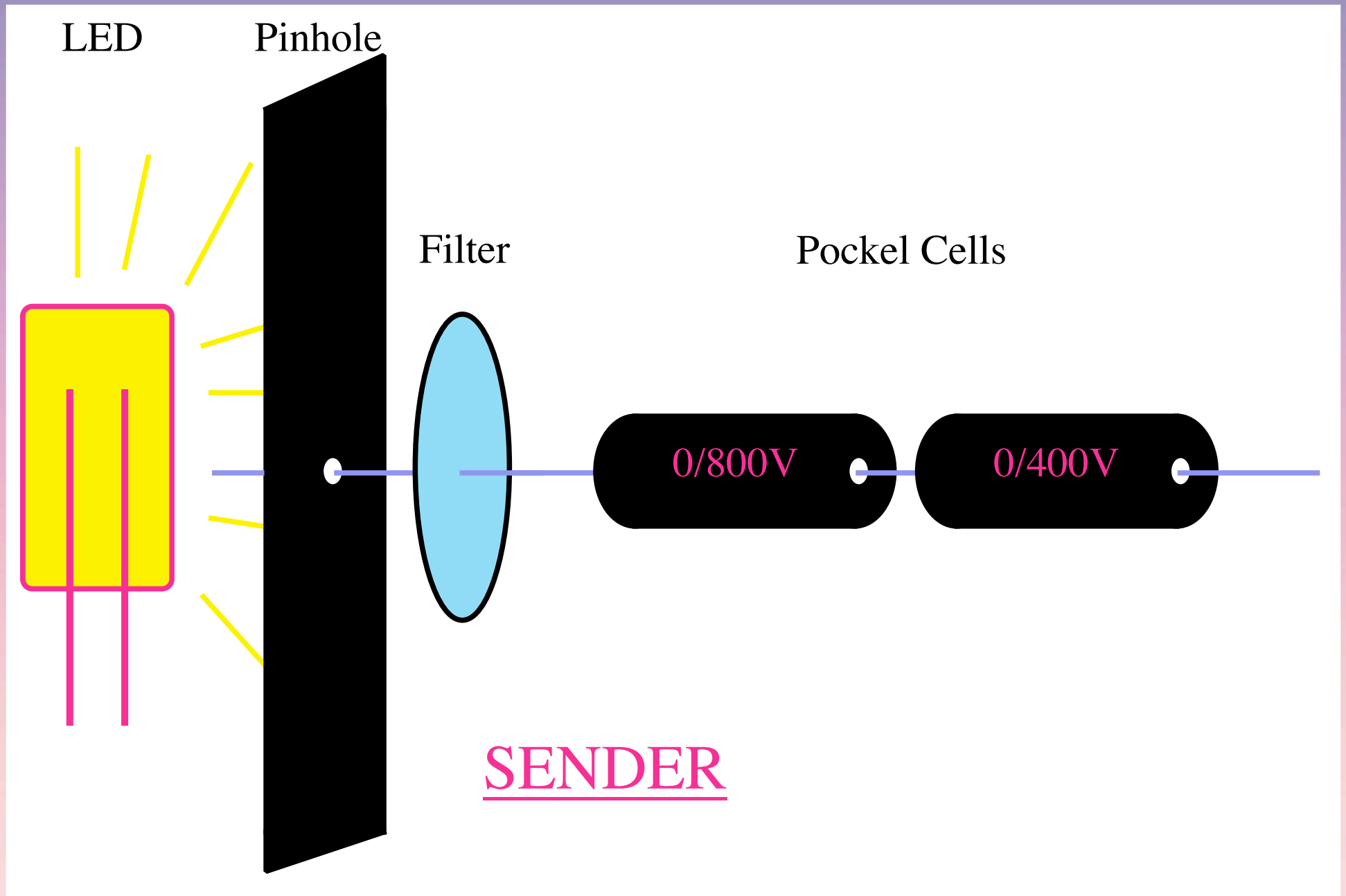
(8)
Quantum Cryptography

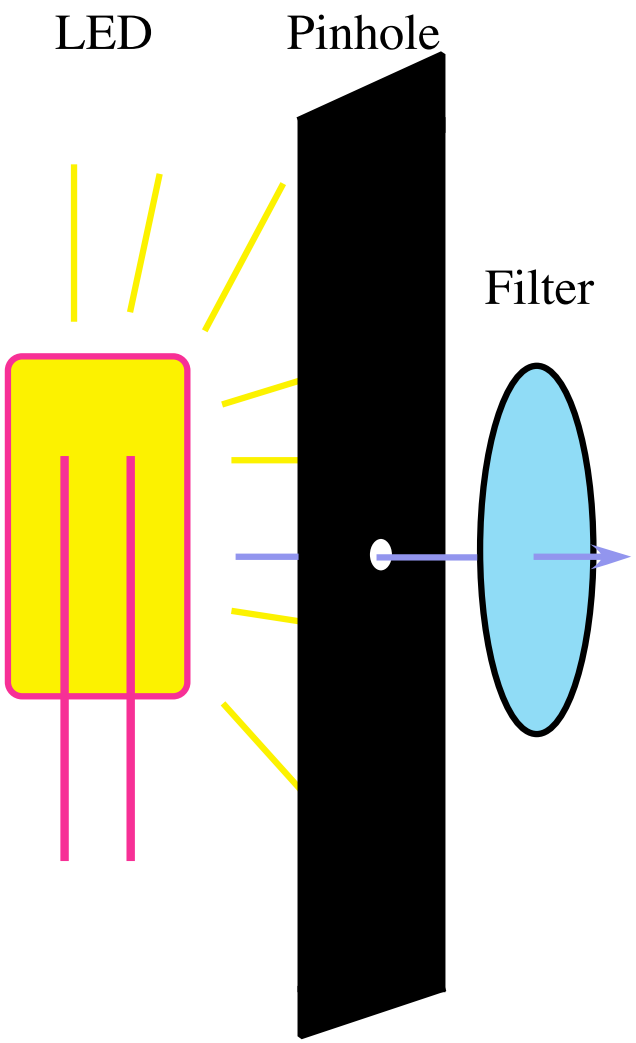
Ambiguous Coding Scheme



Pockel Cells







Light source:

~ 1/10 photon per pulse

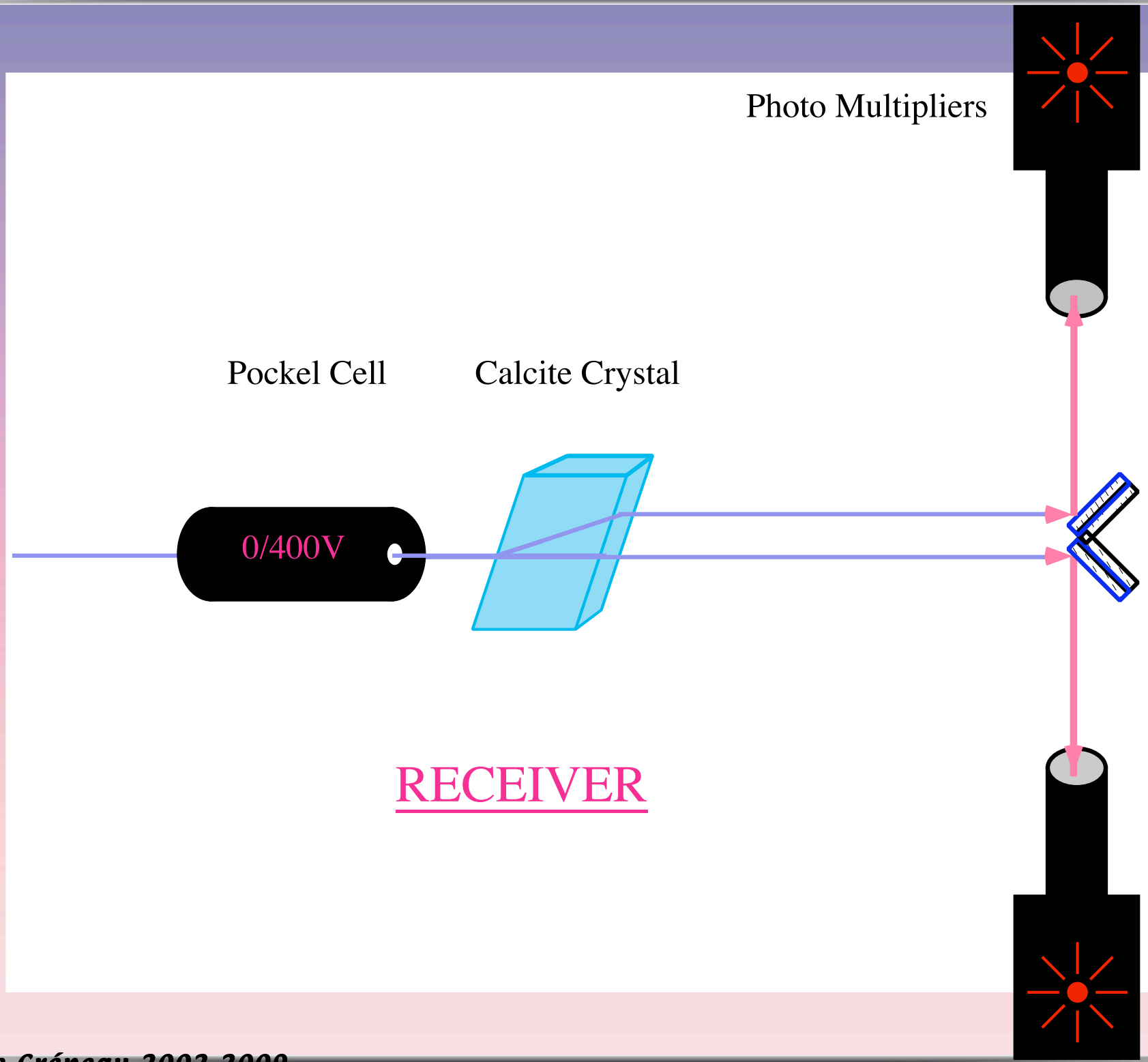
n = #photons per pulse follows a

Poisson distribution $\Pr(n \leq x) = 1\text{-}e^{-x/10}$

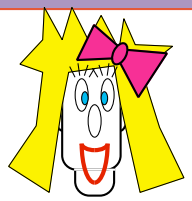
Problem:

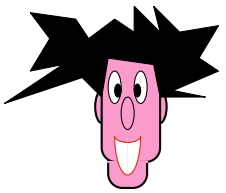
• may transmit multiple correlated

polarized photons



Q-distribution of keys



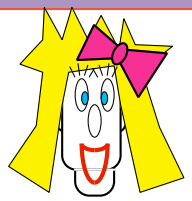


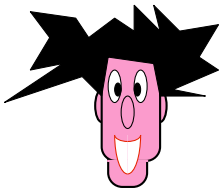
A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	×	×	+	+	×	+	+	+	×	+	+	×	×	×	+	×	×	×	+	+	×	+	×	+
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0
A:	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	0			0		1			1		0					1	0			1		0	0	0
B:	0			0		1			1		0					1	0			1		0	0	0
A:	0			0		1			1		0					1	1			1		0	0	0
A:	0					1					0						1							0
B:	=					=					=						≠							=
B:				0					1							1				1		0	0	
A:				0					1							1				1		0	0	

20%

Bennett- Brassard

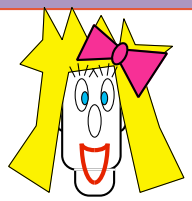
Q-distribution of keys

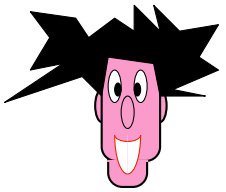




A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+

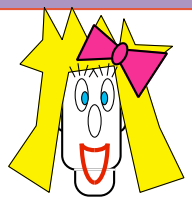
Q-distribution of keys

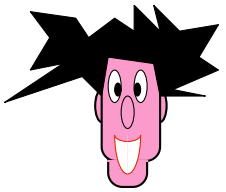




A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	×	×	+	+	×	+	+	+	×	+	+	×	×	×	+	×	×	×	+	+	×	+	×	+
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0

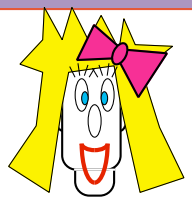
Q-distribution of keys

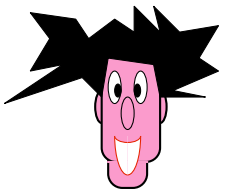




A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	×	×	+	+	×	+	+	+	×	+	+	×	×	×	+	×	×	×	+	+	×	+	×	+
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0
A:	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+

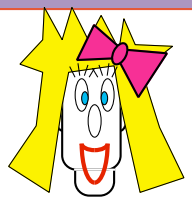
Q-distribution of keys

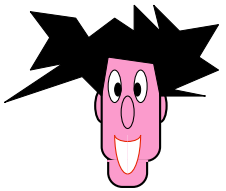




A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	×	×	+	+	×	+	+	+	×	+	+	×	×	×	+	×	×	×	+	+	×	+	×	+
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0
A:	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	0			0		1			1		0					1	0			1		0	0	0
B:	0			0		1			1		0					1	0			1		0	0	0
A:	0			0		1			1		0					1	1			1		0	0	0

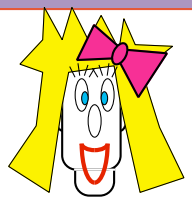
Q-distribution of keys

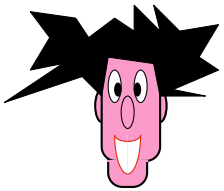




B:	0		0	1		1	0		1	0		1	0	0	0
A:	0		0	1		1	0		1	1		1	0	0	0

Q-distribution of keys

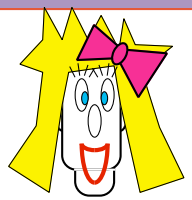


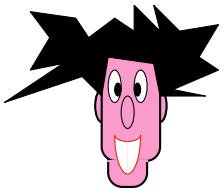


B:	0		0		1		1		0		1	0		1		0	0	0
A:	0		0		1		1		0		1	1		1		0	0	0
A:	0				1				0			1						0
B:	=				=				=			↑						=

20%

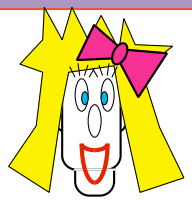
Q-distribution of keys

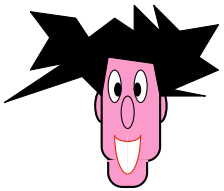




B:	=		=		=			↑				=		20%
B:		0		1			1		1	0	0			
A:		0		1			1		1	0	0			

Q-distribution of keys





B:	0	1	1	1	0	0
A:	0	1	1	1	0	0

20%

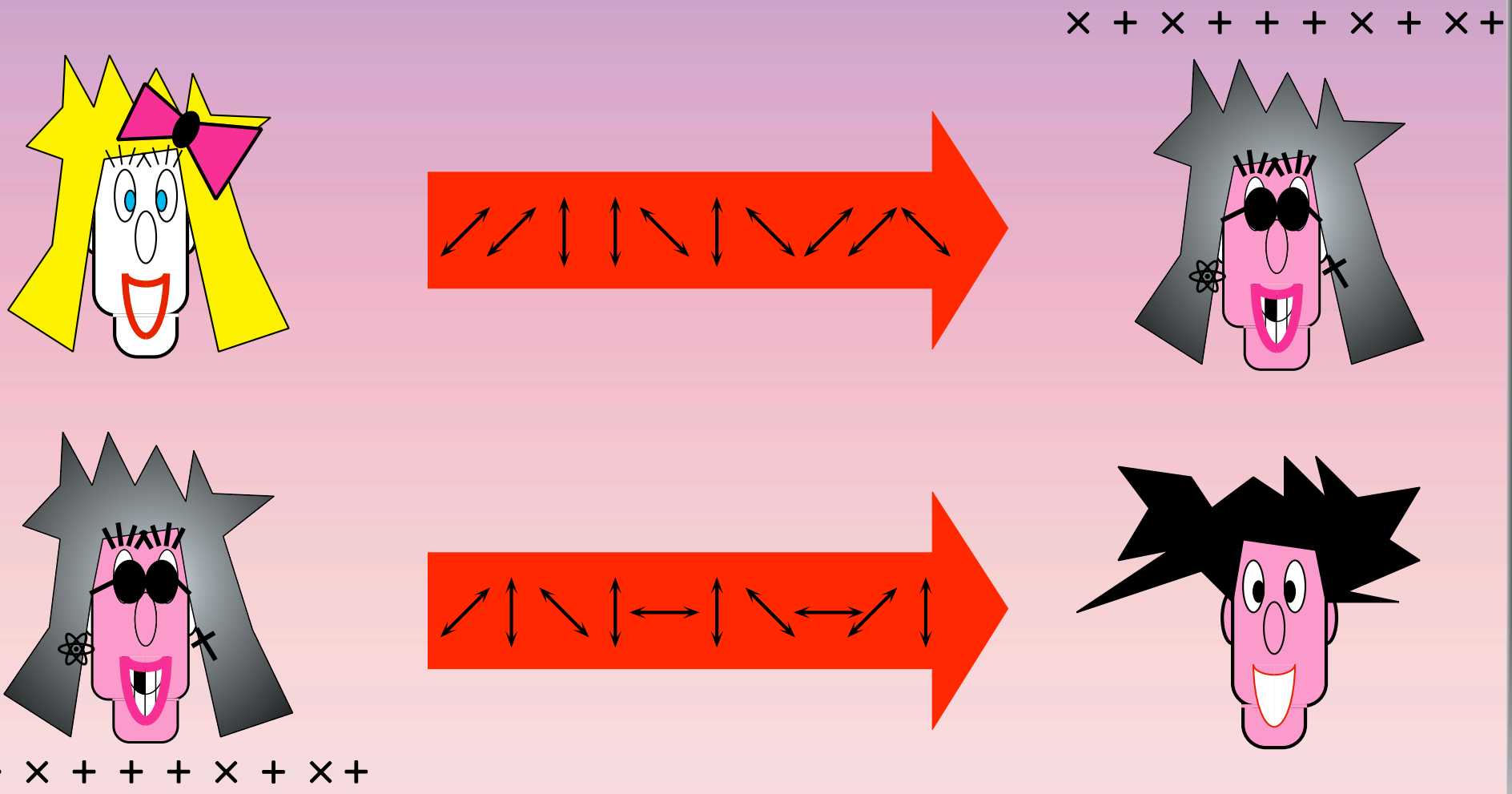
Q-distribution of keys

• • • • •

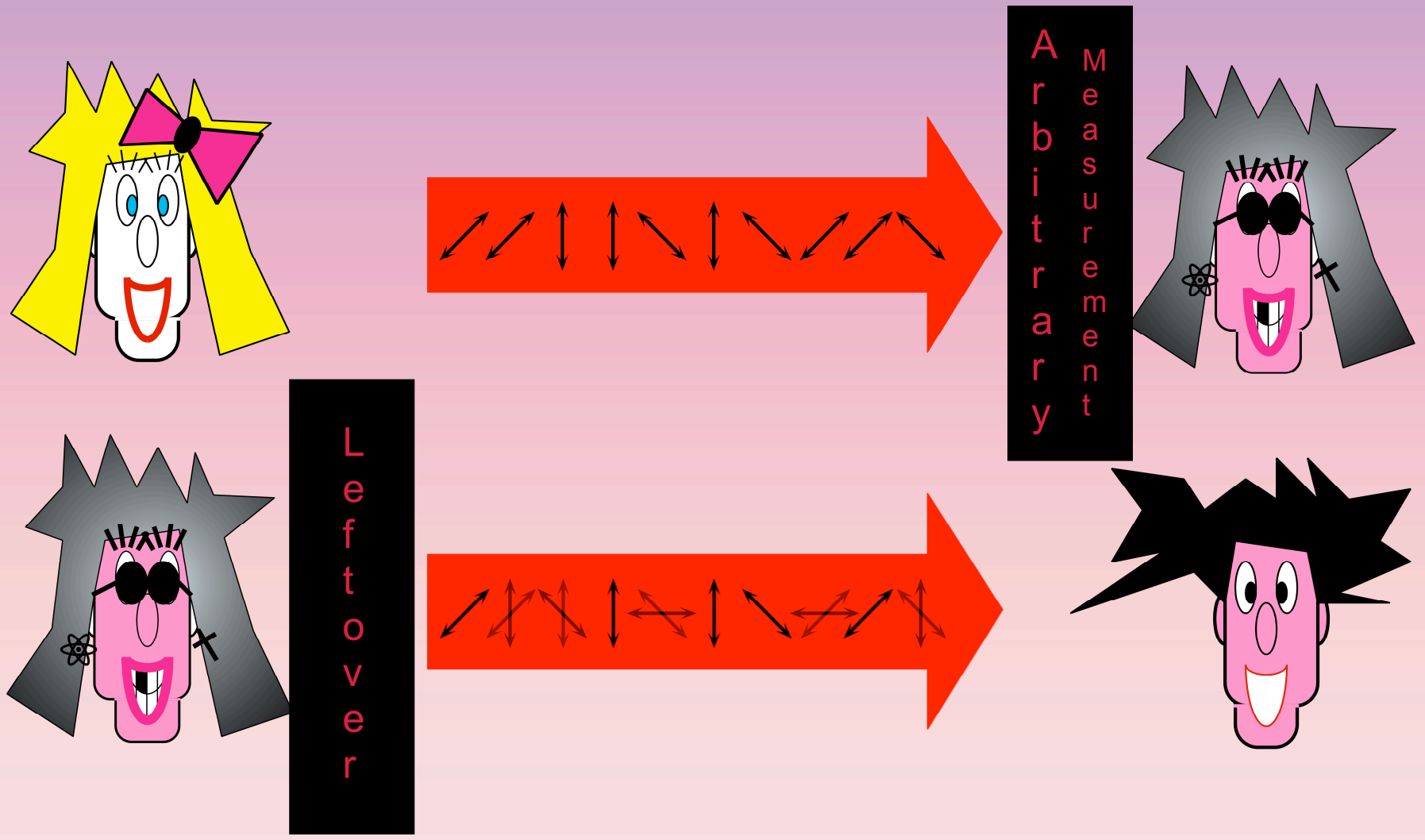
- Produces raw classical key
- Observed error rate indicates amount of eavesdropper information
- Error-correction is used to fix errors
- Random hash function is used to distill a smaller secret classical key

• • • • •

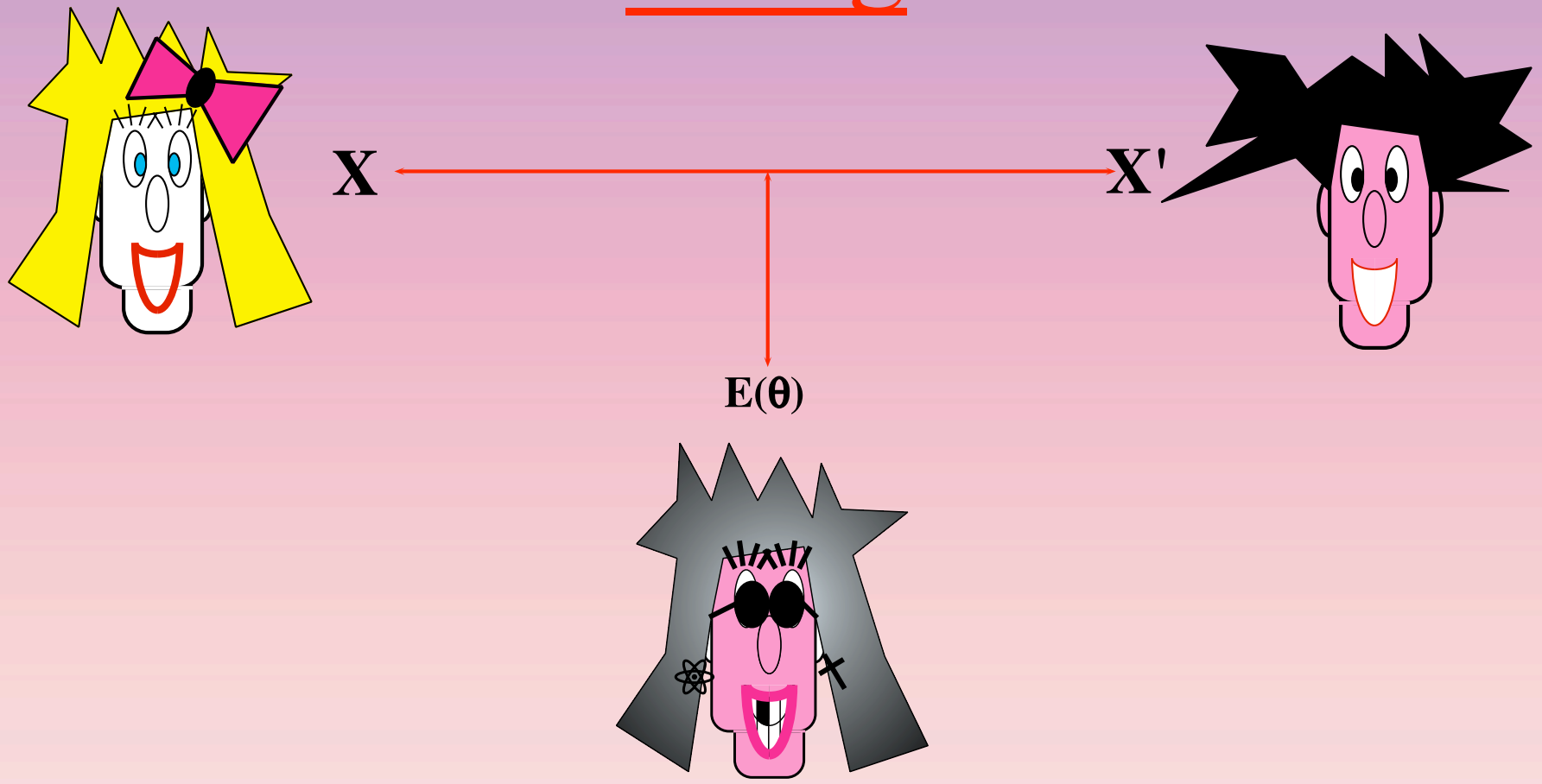
Information <--> Errors (intercept resend)



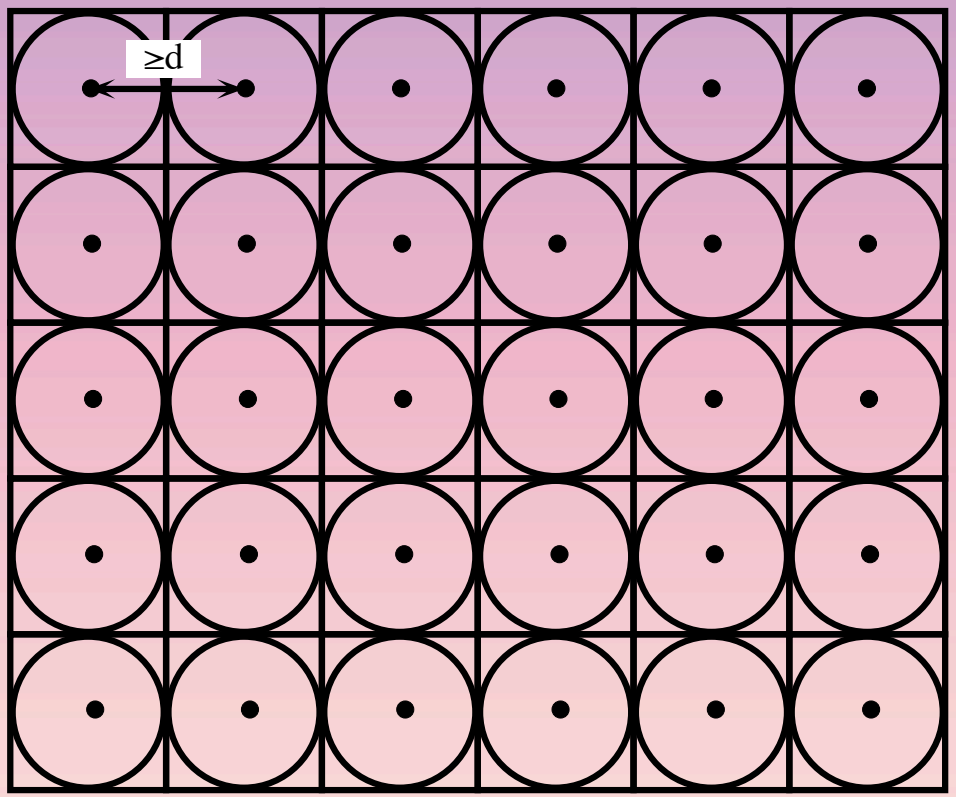
Information <--> Errors (general)



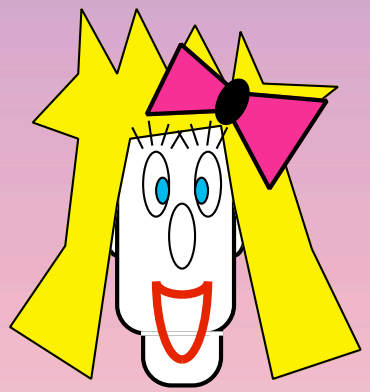
Mostly Identical Partly Secret String



(classical) error-correcting codes

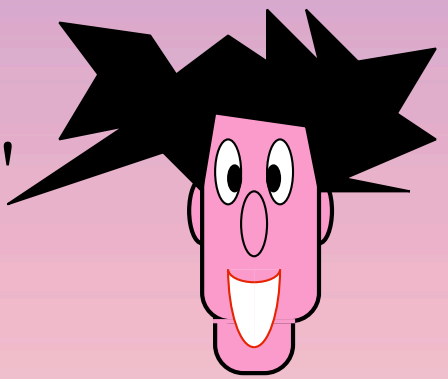


Identical Partly Secret String



X

W

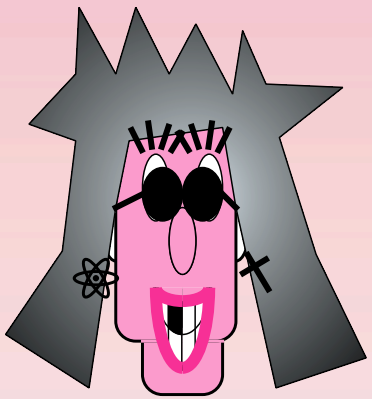


X'

C

W:=C⊕X

E:=E(θ)+W

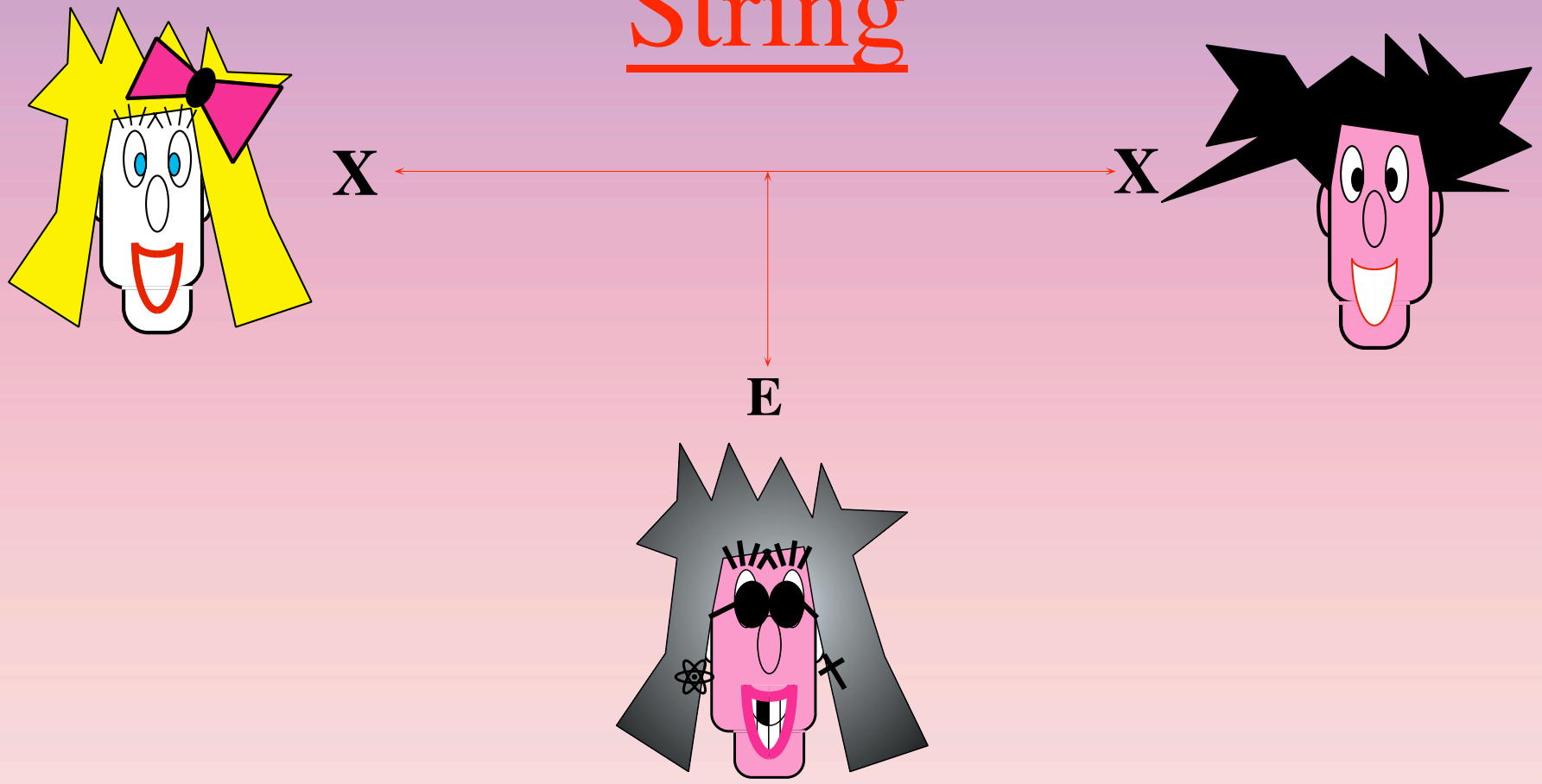


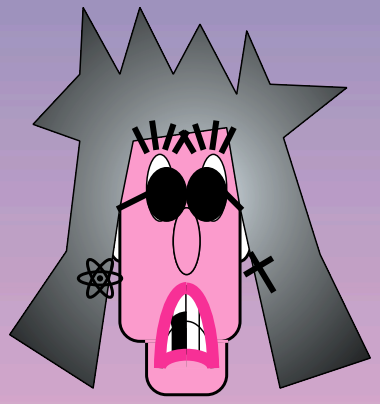
C'

C':=W⊕X'

X:=C⊕W

Identical Partly Secret String

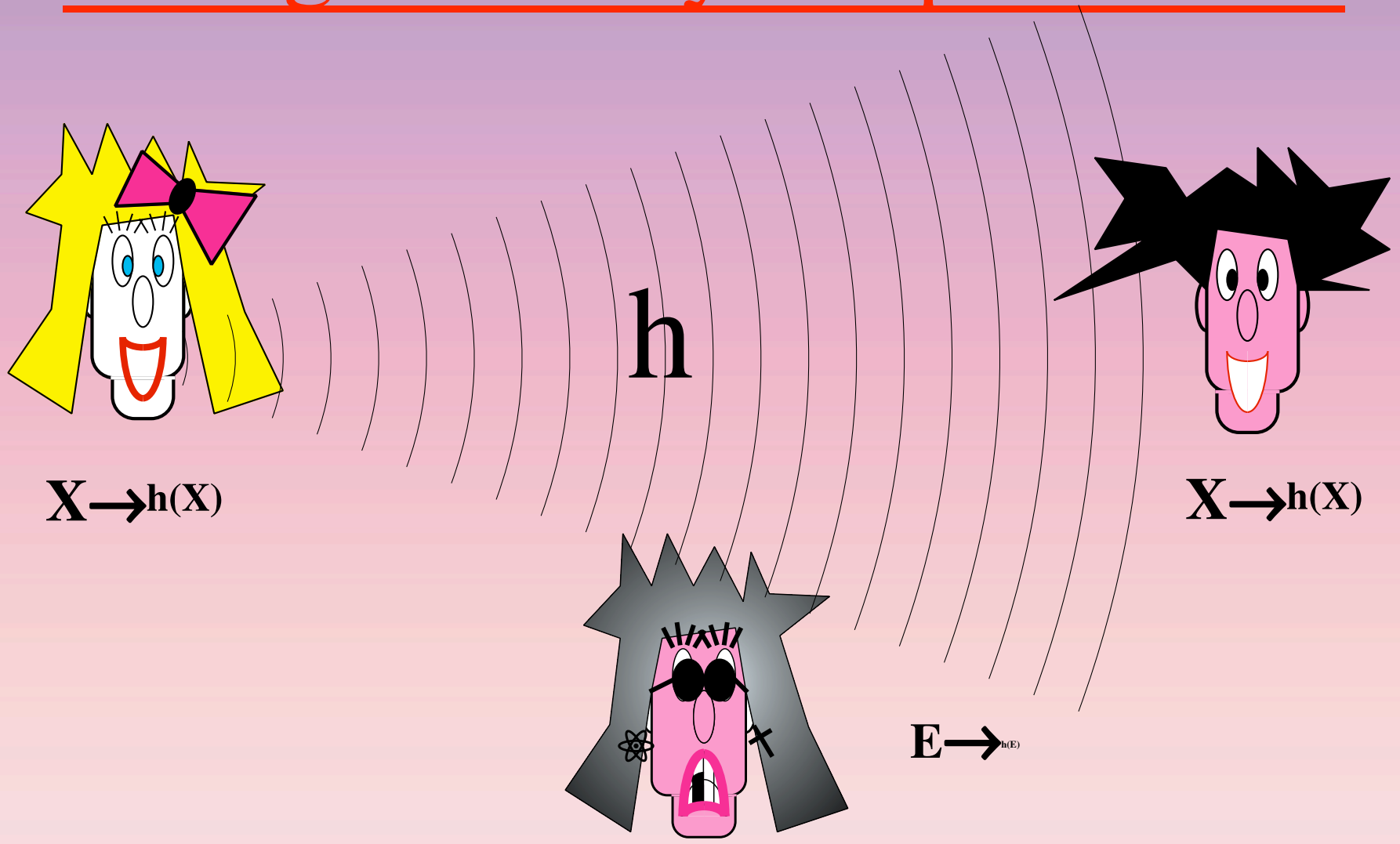




in BB84, Eve's information at this point (before privacy amplification) contains:

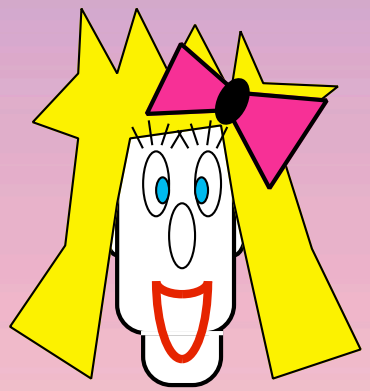
- **results of eavesdropping**
- **multi-photon pulses**
- **error correction**

Identical Secret Shorter String through Privacy Amplification



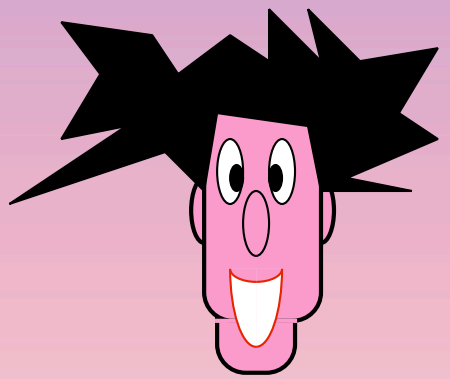
BBCM

$$H(G(X) \mid E=e, G) > |G(X)| - 2^{(|G(X)|-R(X|E=e))}$$

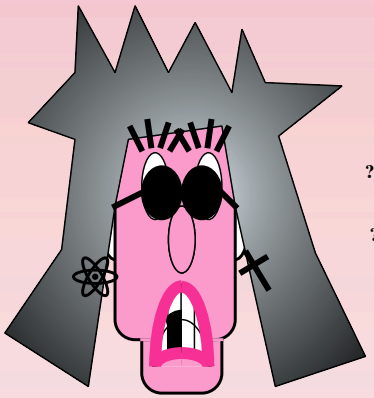


k:=g(X)

g



k:=g(X)



???????????

k':=g(E)

??????????