Quantum Key Distribution

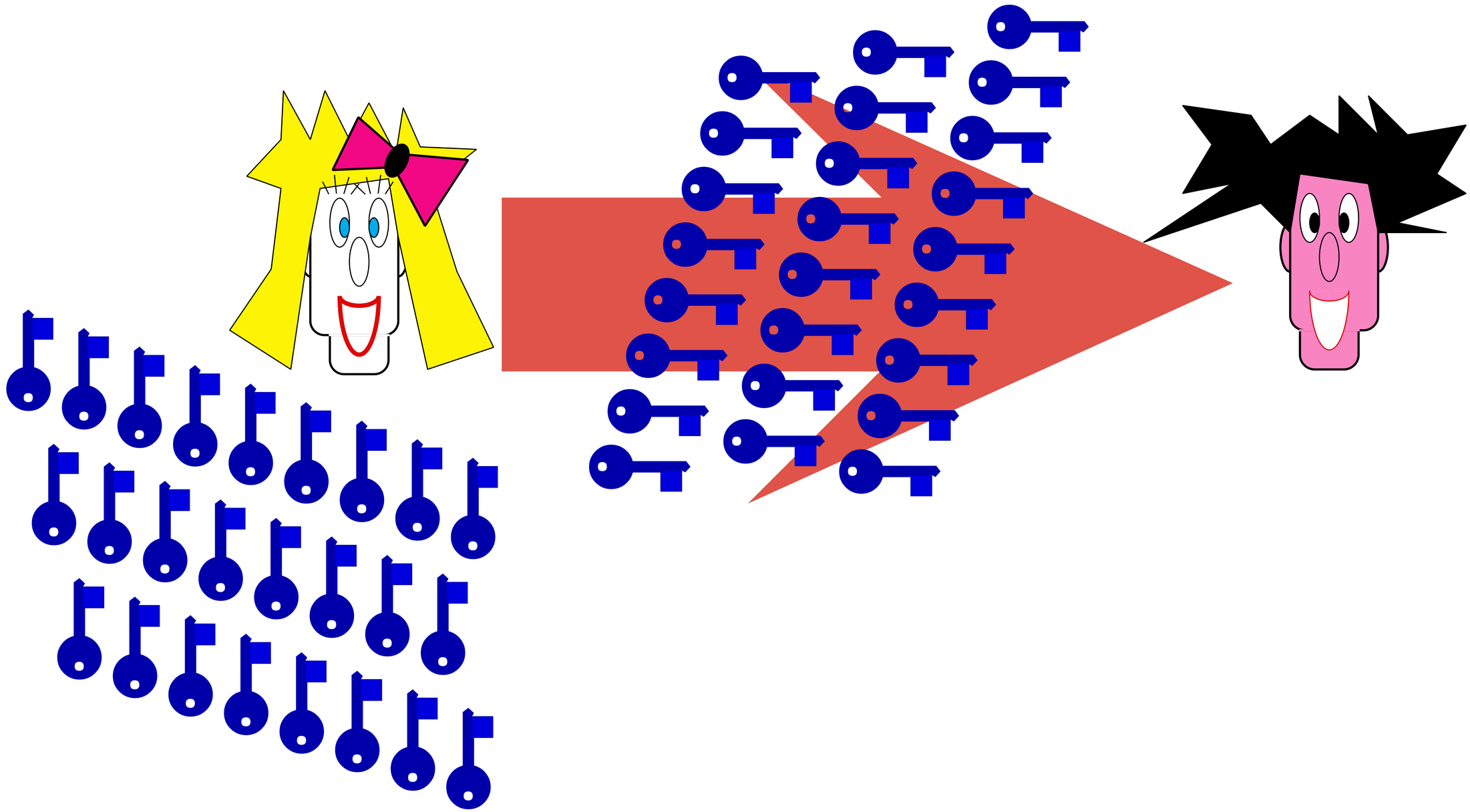
Claude Crépeau

School of Computer Science
McGill University

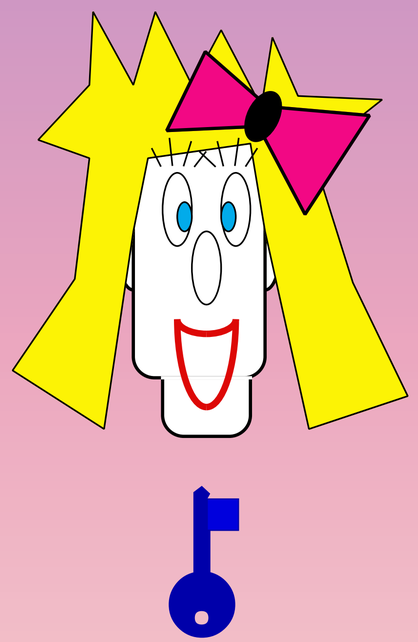
(1)

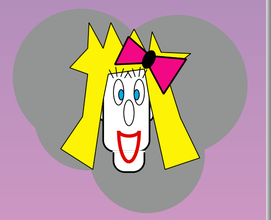
Classical Cryptography

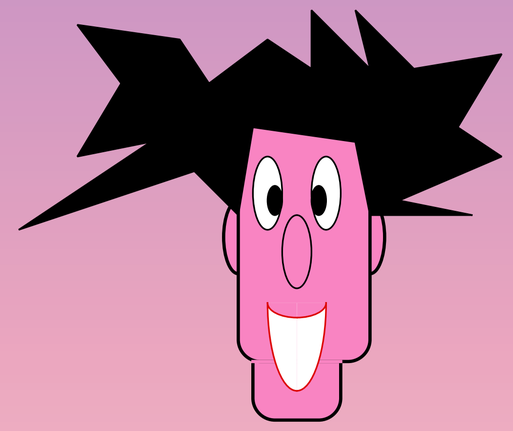
(1.1.1) key distribution PROBLEM



(1.1.3) Authentication





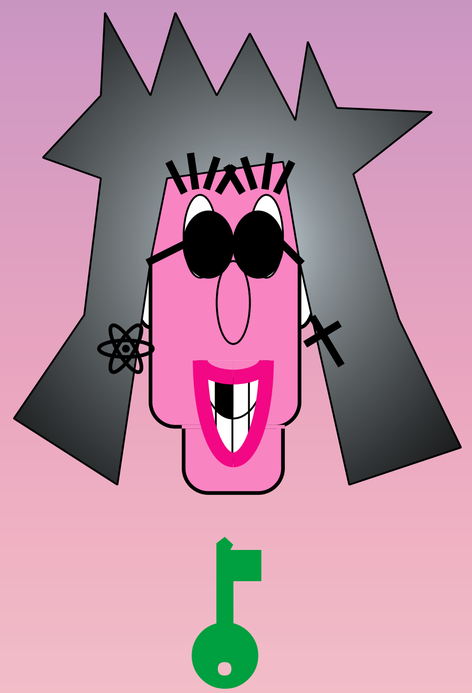


Will you marry me ?

Divorce your wife first !

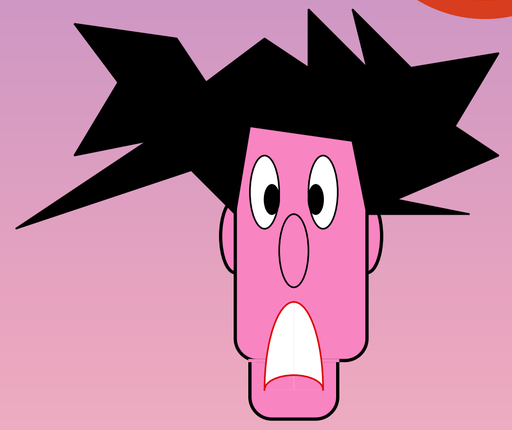
The papers are in the mail...

OK, I will !

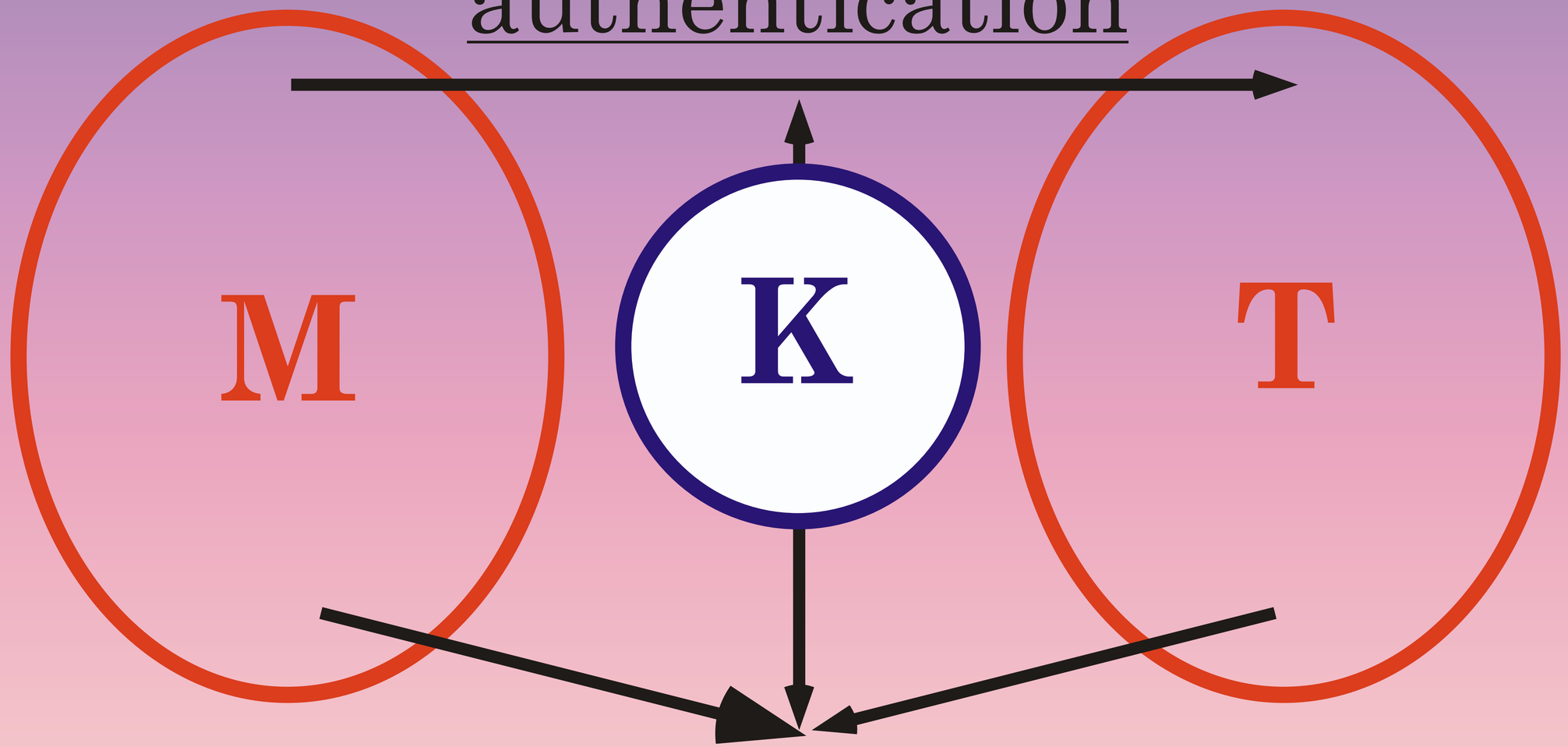


Will you marry me ?

No, I never will !

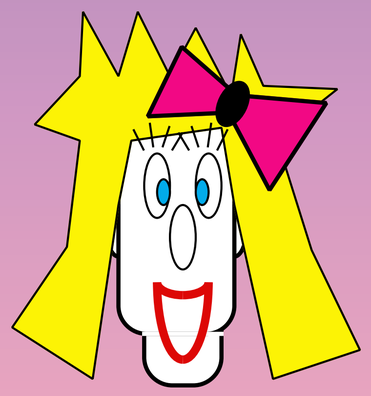


symmetric authentication

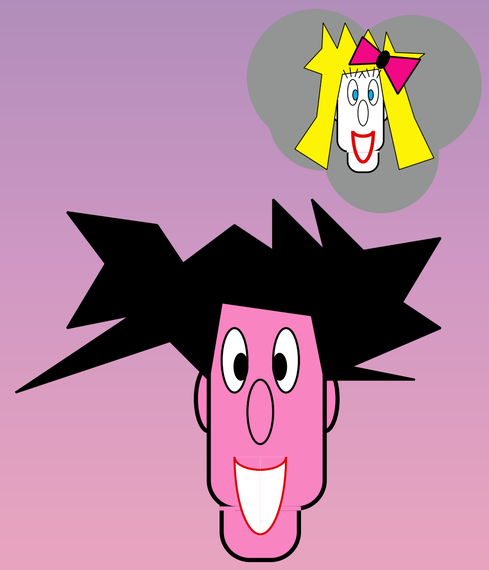


Information Theoretical Security

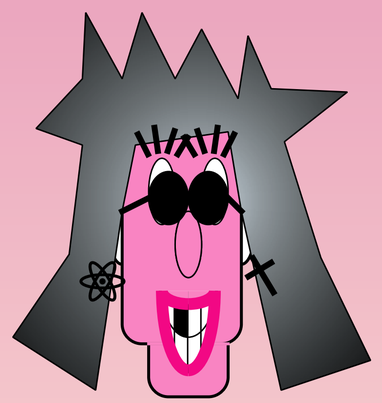
Authentication



(m,t)



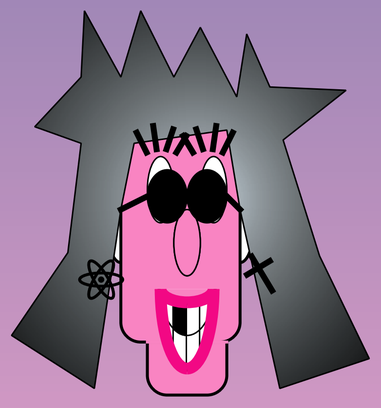
$t=auth_k(m)$



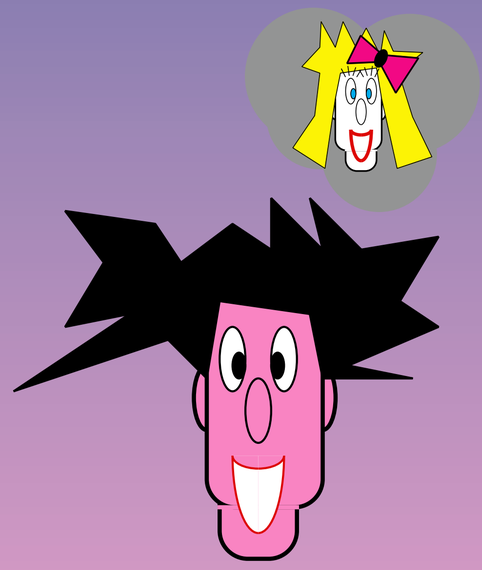
$auth_k(m)=t?$

Information Theoretical Security

Impersonation

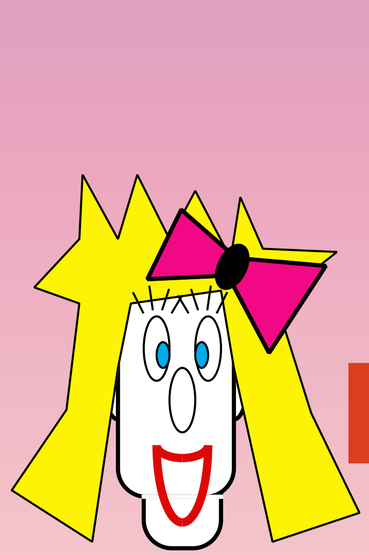


(m,t)

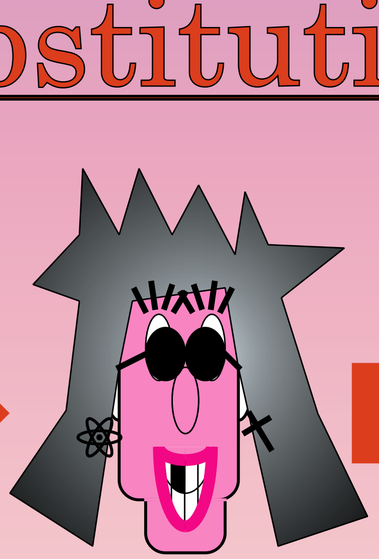


$auth_k(m)=t?$

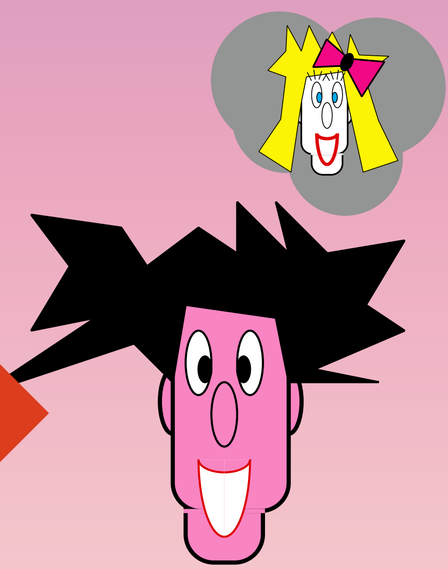
Substitution



(m,t)



(m',t')



$auth_k(m')=t'?$

Information Theoretical Security

WC One-Time-Authentication

$$\text{auth}_{\mathbf{M},b}(x) = \mathbf{M}x \oplus b$$

$$|x| = n,\ |\mathbf{M}| = n \cdot n',\ |b| = n'$$

$\forall m \in M, \forall t \in T$

$$\Pr(\text{auth}_{\mathbf{M},b}(m) = t) = 1/|T| = 1/2^{n'}$$

$\forall m \neq m' \in M, \forall t, t' \in T$

$$\Pr(\ \text{auth}_{\mathbf{M},b}(m') = t'\ \mid\ \text{auth}_{\mathbf{M},b}(m) = t\ ) = 1/|T| = 1/2^{n'}$$

WC One-Time-Authentication and (linear) error correction

$$\mathrm{auth}_{\mathbf{M},b}(x) = \mathbf{M}x \oplus b$$

$[\mathbf{I}:\mathbf{M}]m \oplus [0:b] = [m:t]$

G=[**I**:**M**] (systematic) generating matrix of error correcting code

[0:b] error pattern = one-time pad encryption of tag

[m:t] systematic form of (message,tag)

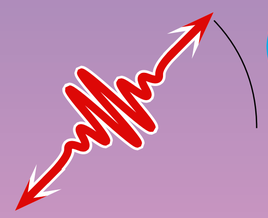
(2)

Quantum Information & Computations

Bits & QuBits

0: 

1: 

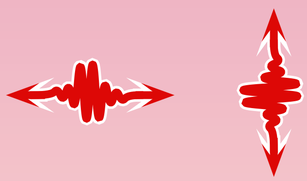


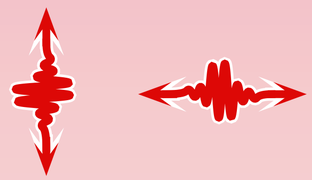
$\theta = \mathrm{Cos}_\theta$  $+ \ \mathrm{Sin}_\theta$ 

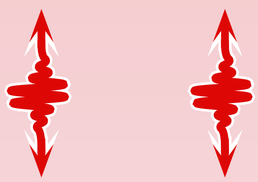
$|\Psi\rangle = C_0$  $+ \ C_1$ 

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

00: 

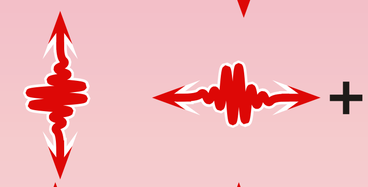
01: 

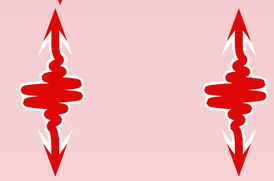
10: 

11: 

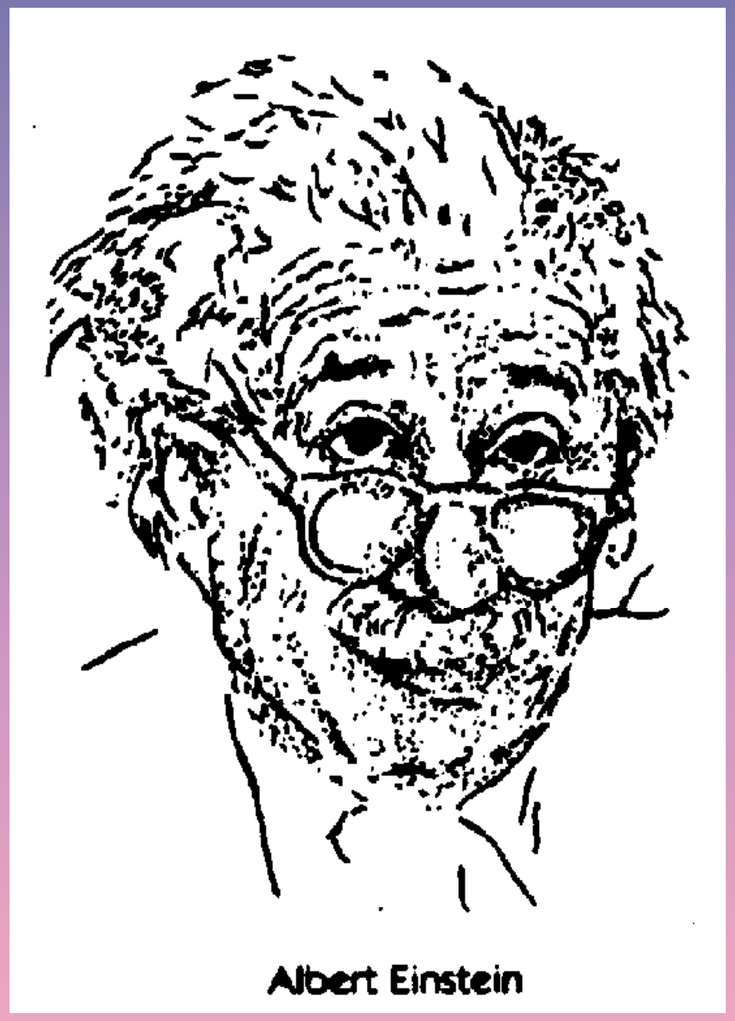
$|\Psi\rangle = C_{00}$  $+$

C_{01}  $+$

C_{10}  $+$

C_{11} 

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



Albert Einstein

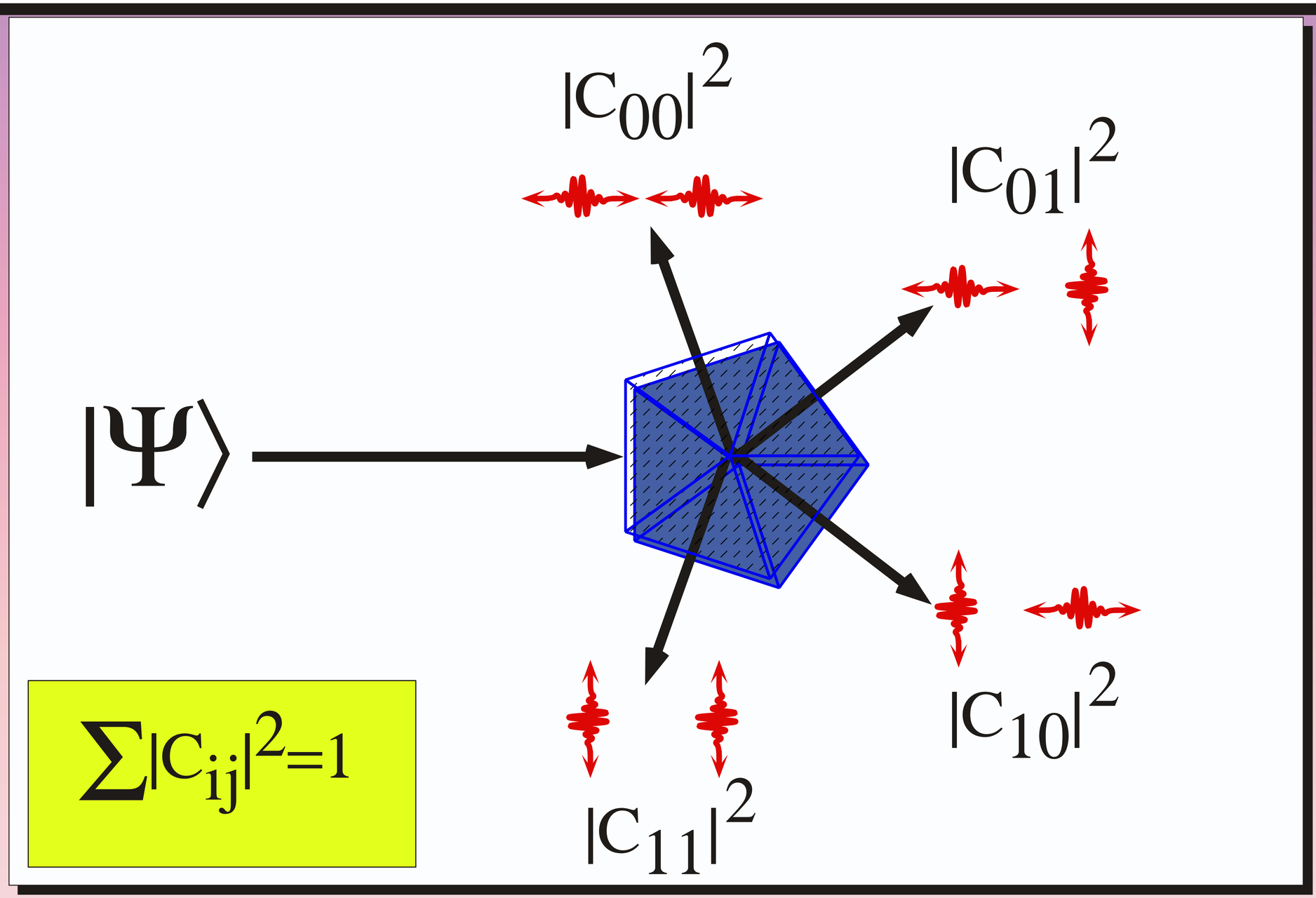
Boris Podolsky

Nathan Rosen

EPR

Quantum Measurements

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



$$\sum |C_{ij}|^2 = 1$$

Quantum Evolution: Unitary Operators

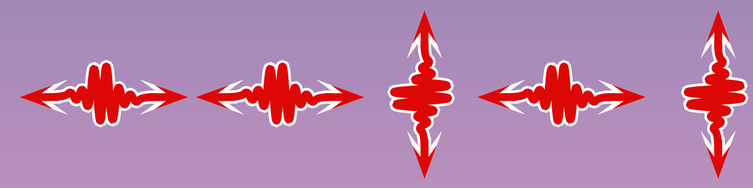
$$|\Psi\rangle \xrightarrow{U} |\Psi'\rangle$$


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


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

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

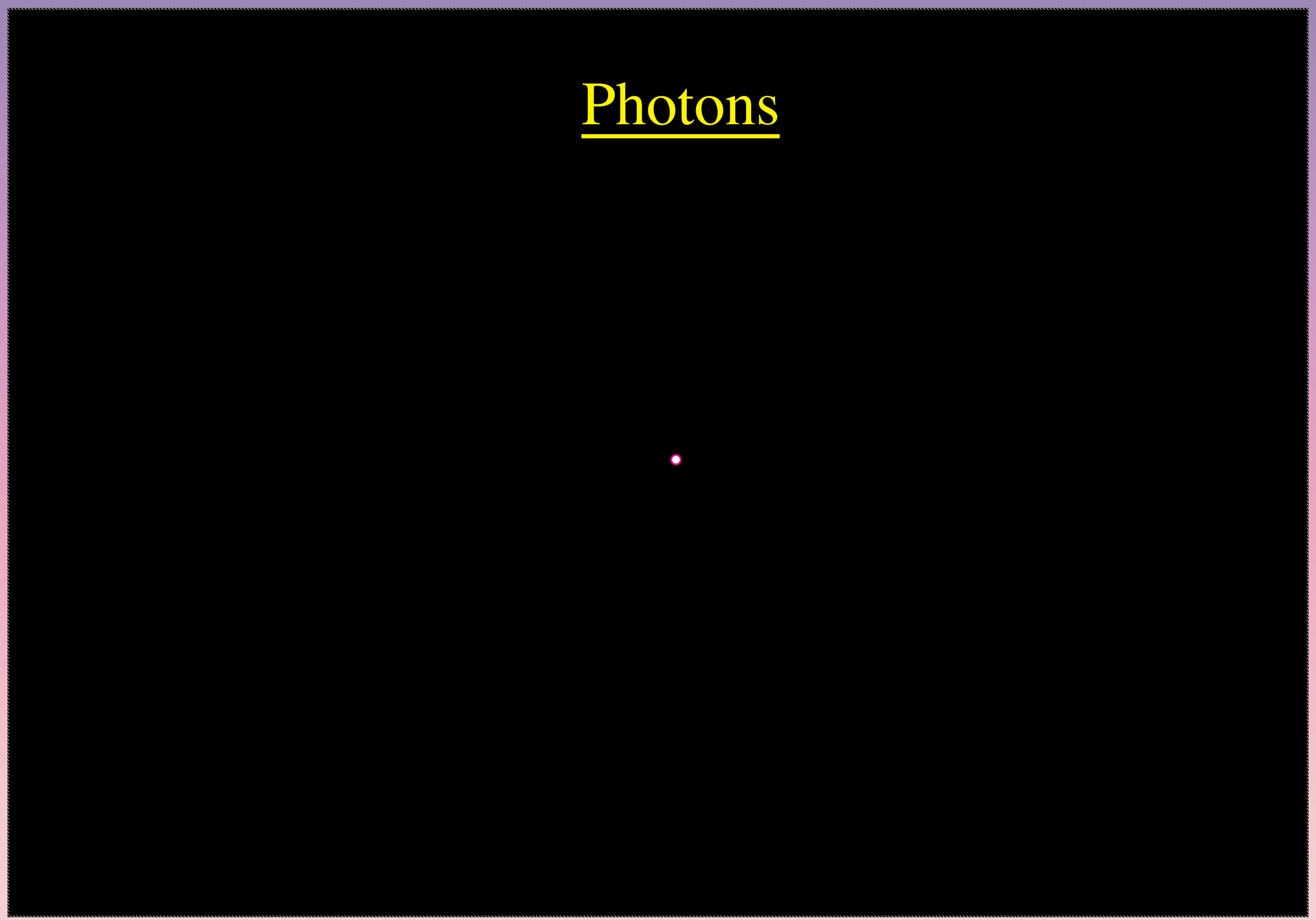
Classical & Quantum Information

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

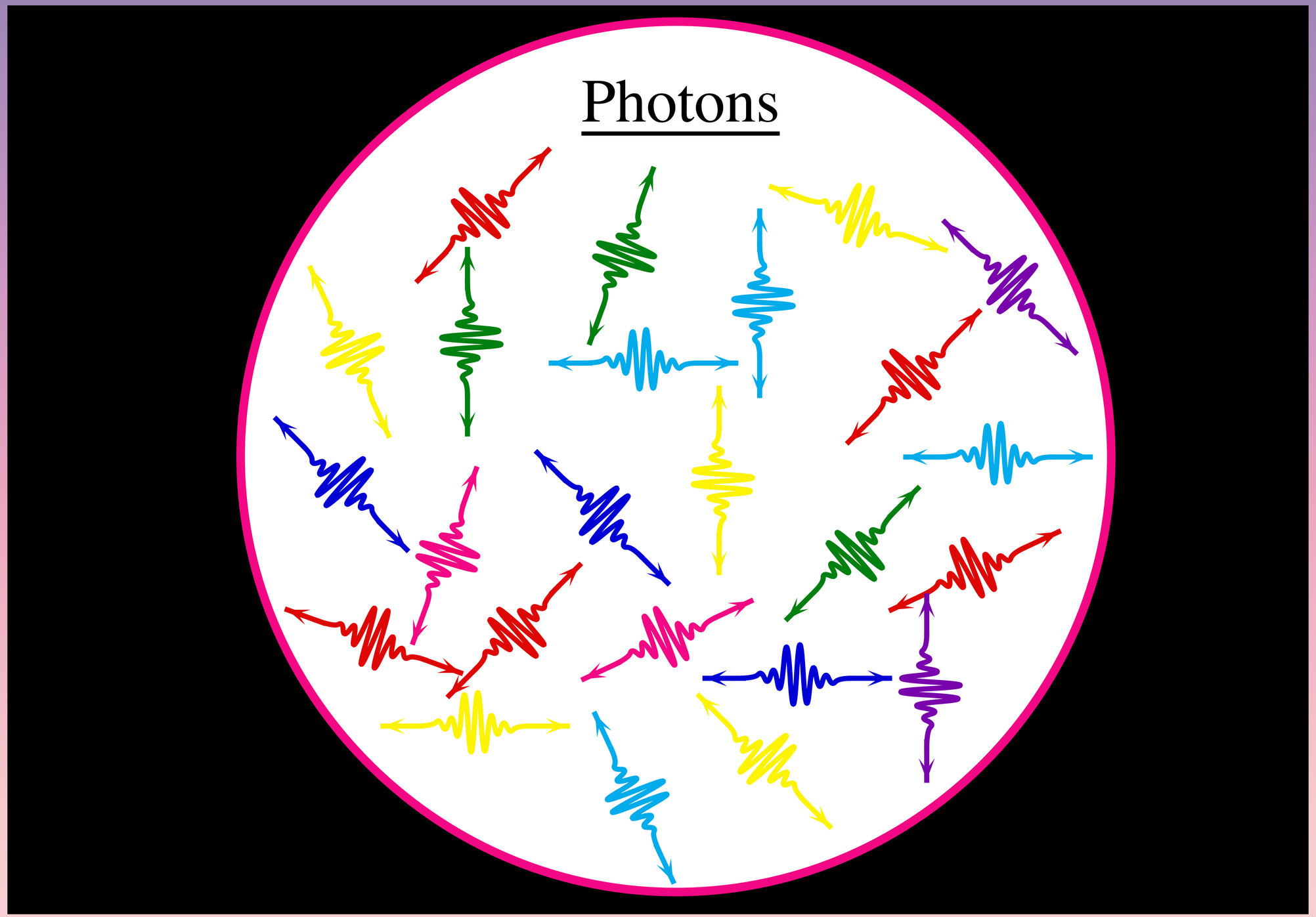
(3)

Quantum Key Distribution

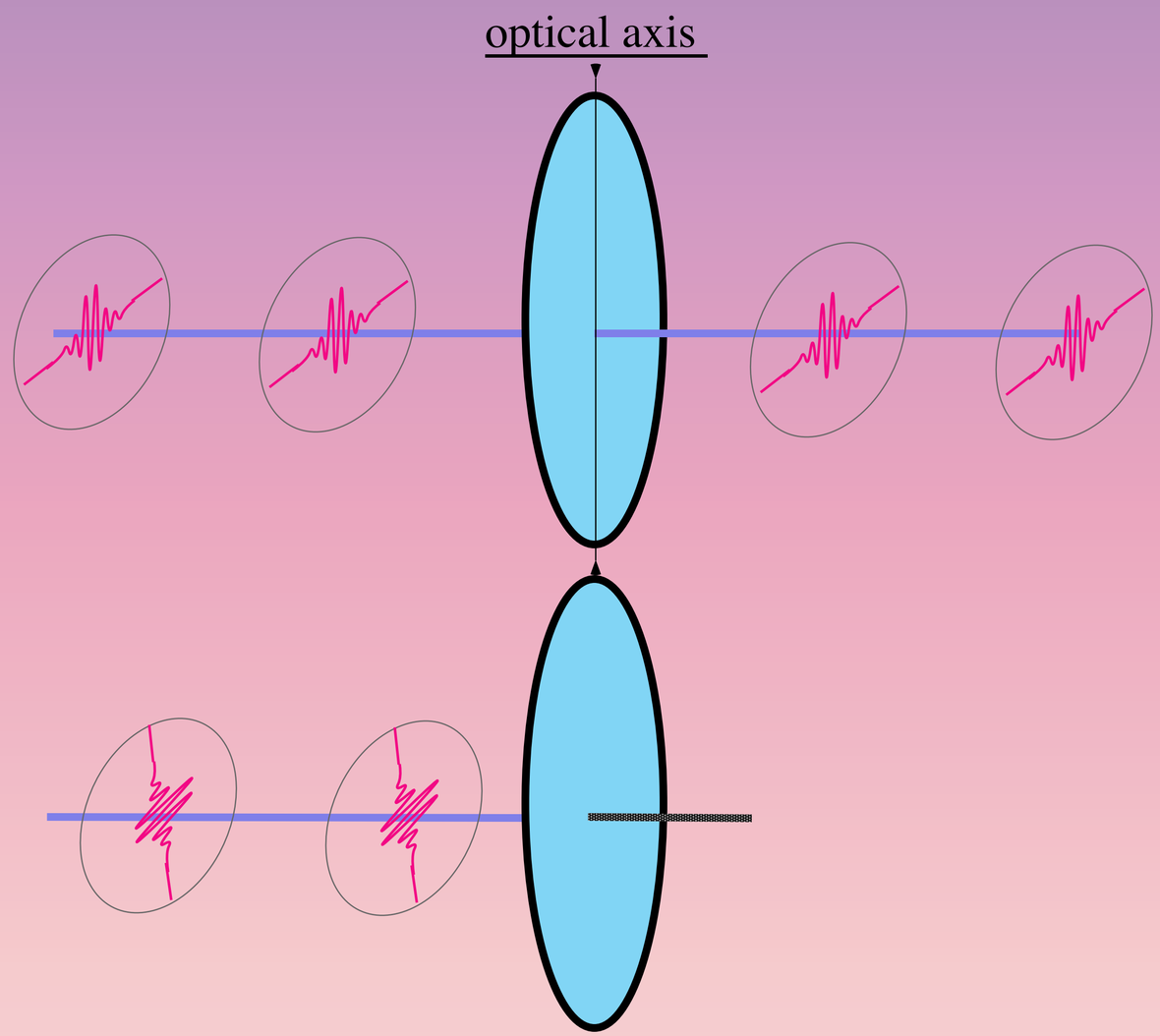
Photons



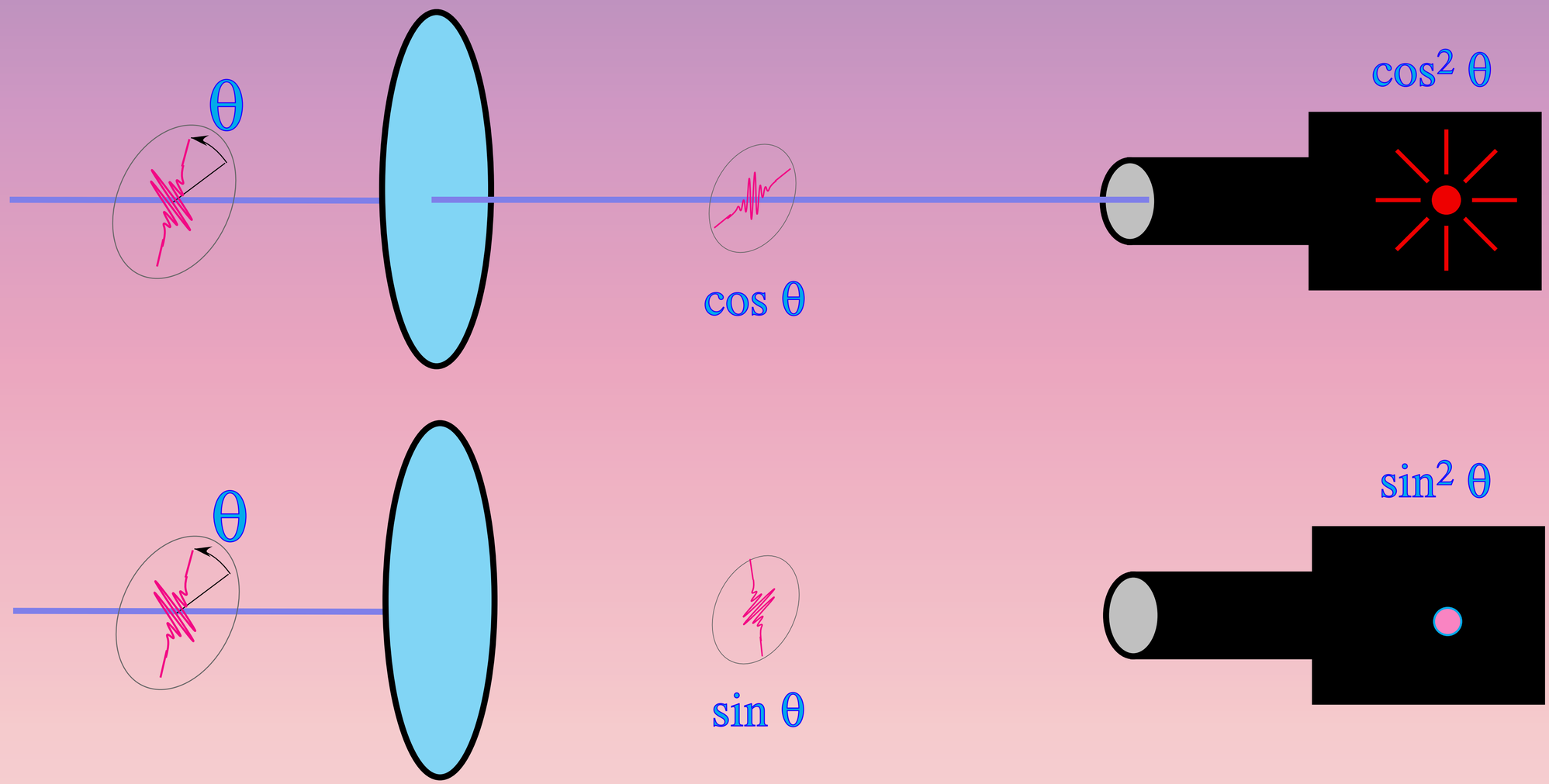
Photons



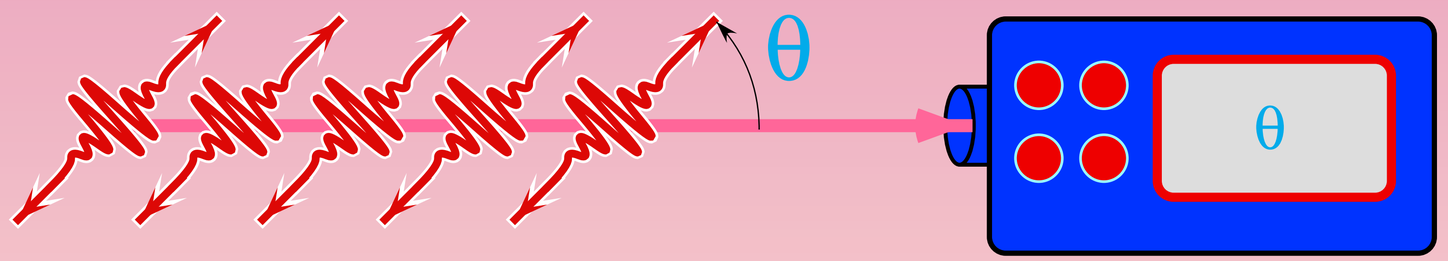
Polarizing Filter



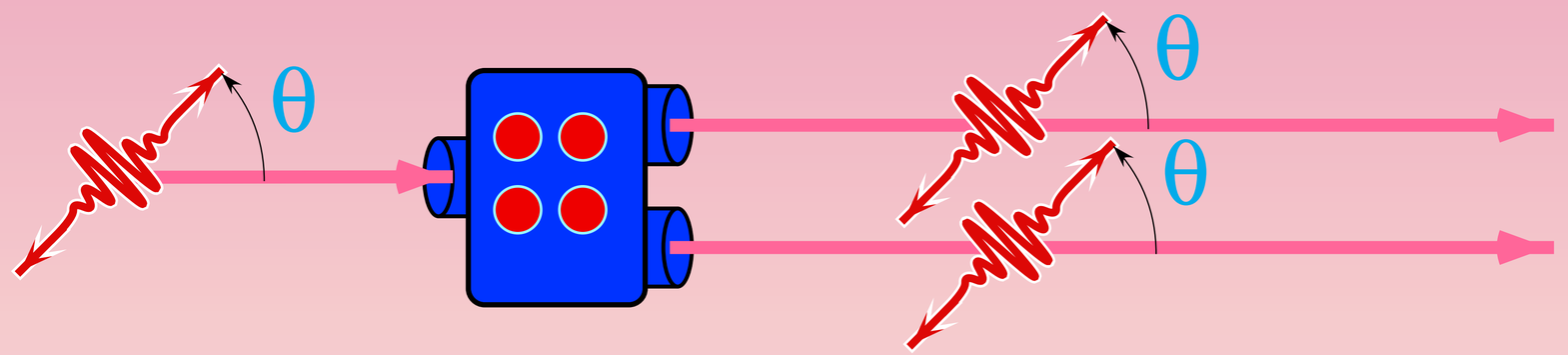
Polarizing Filter and photodetectors



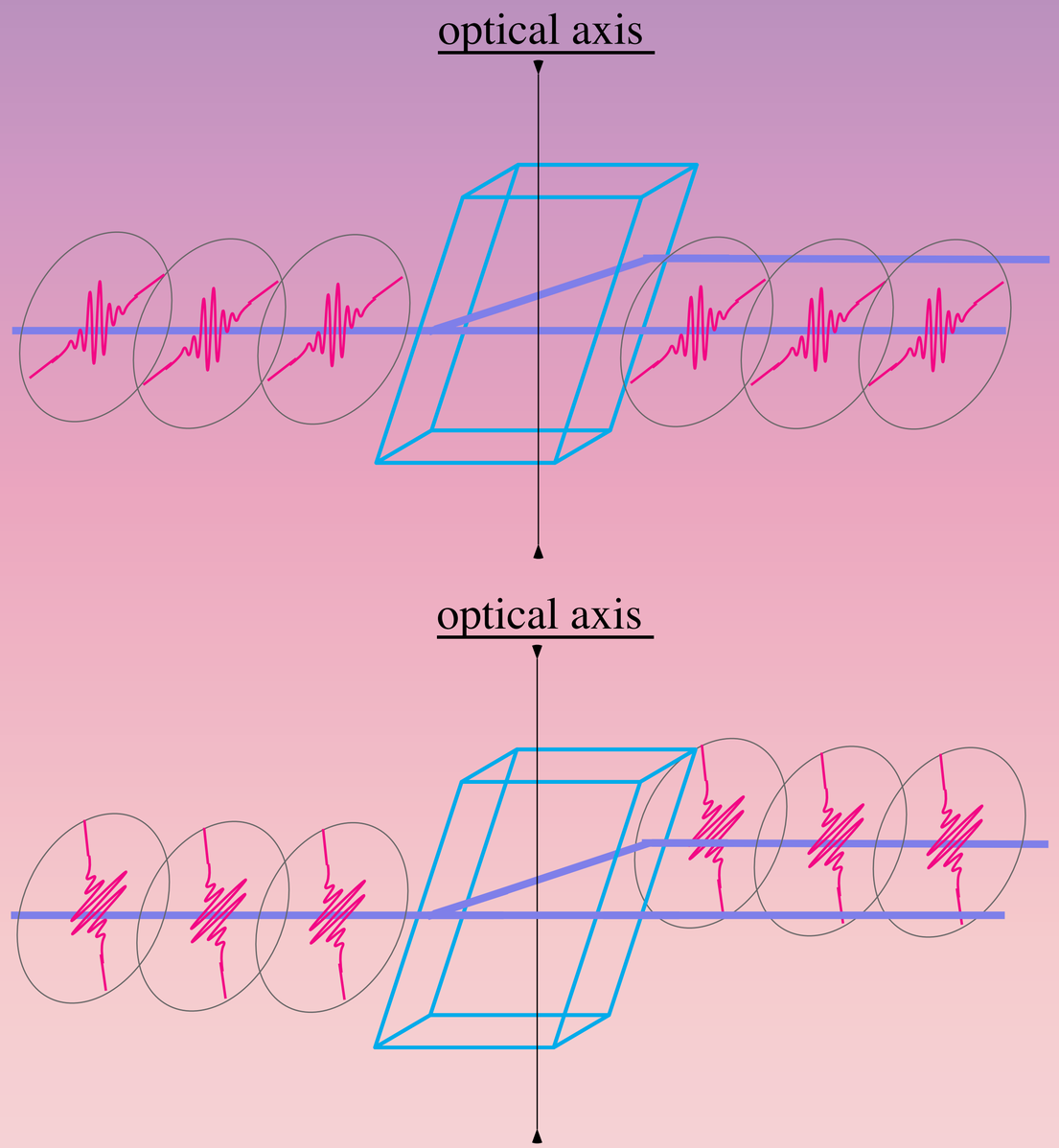
POSSIBLE!



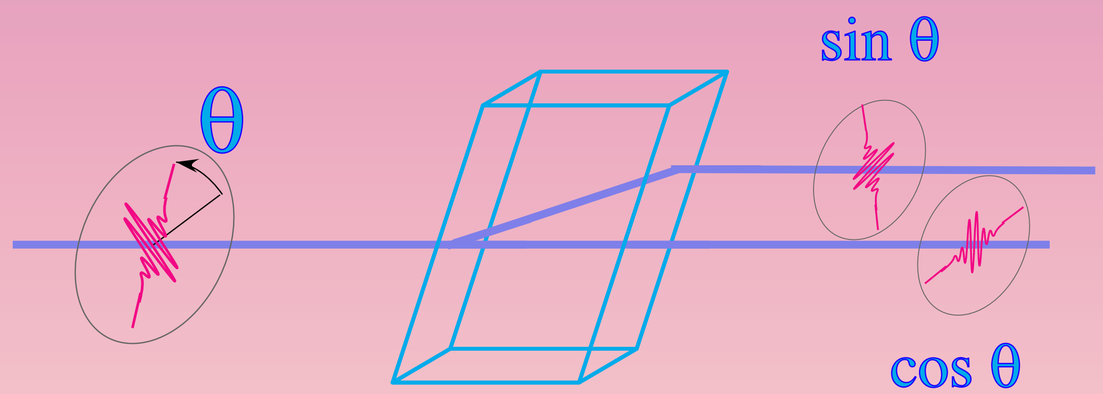
IMPOSSIBLE!



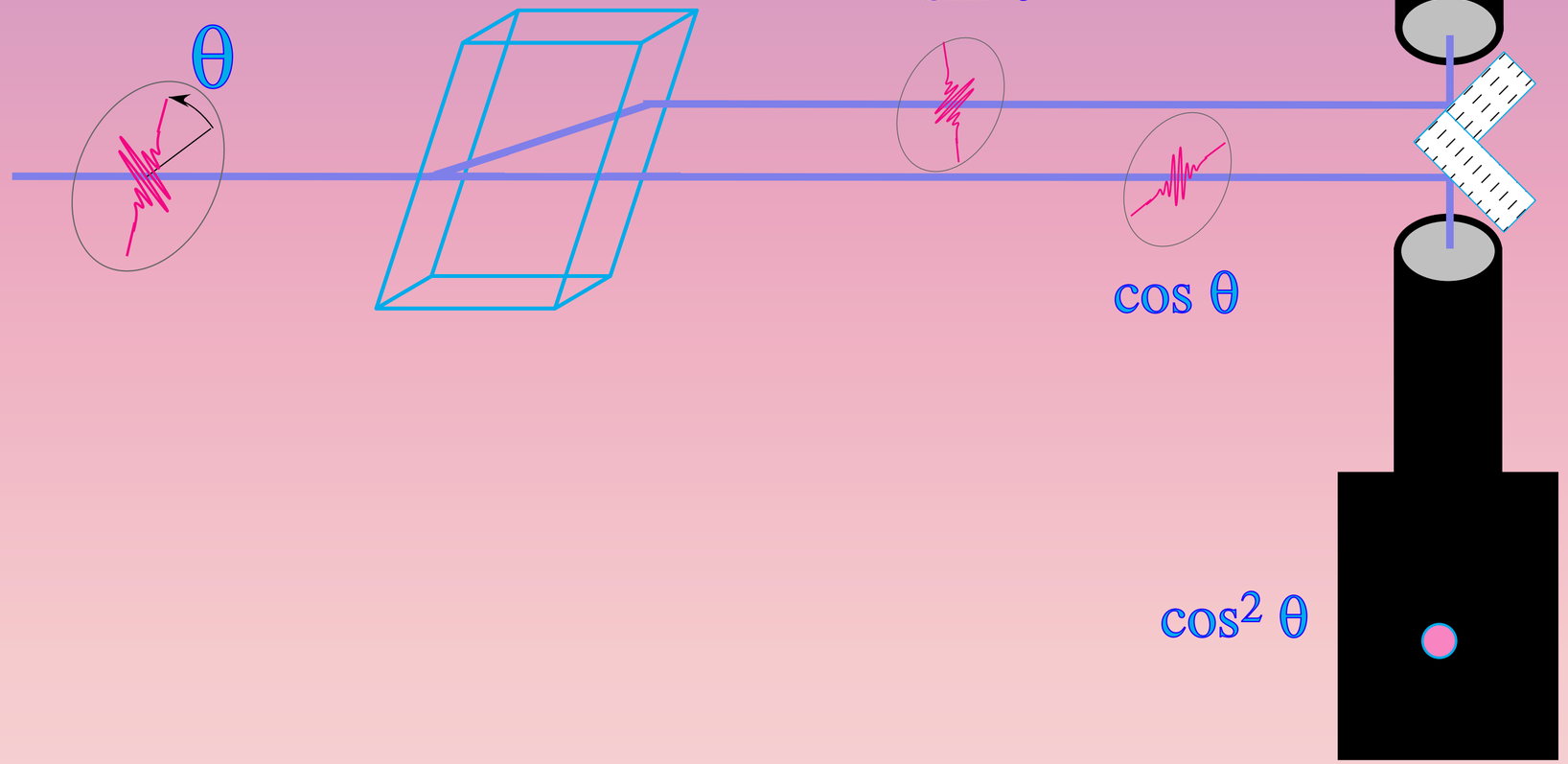
Calcite Crystal



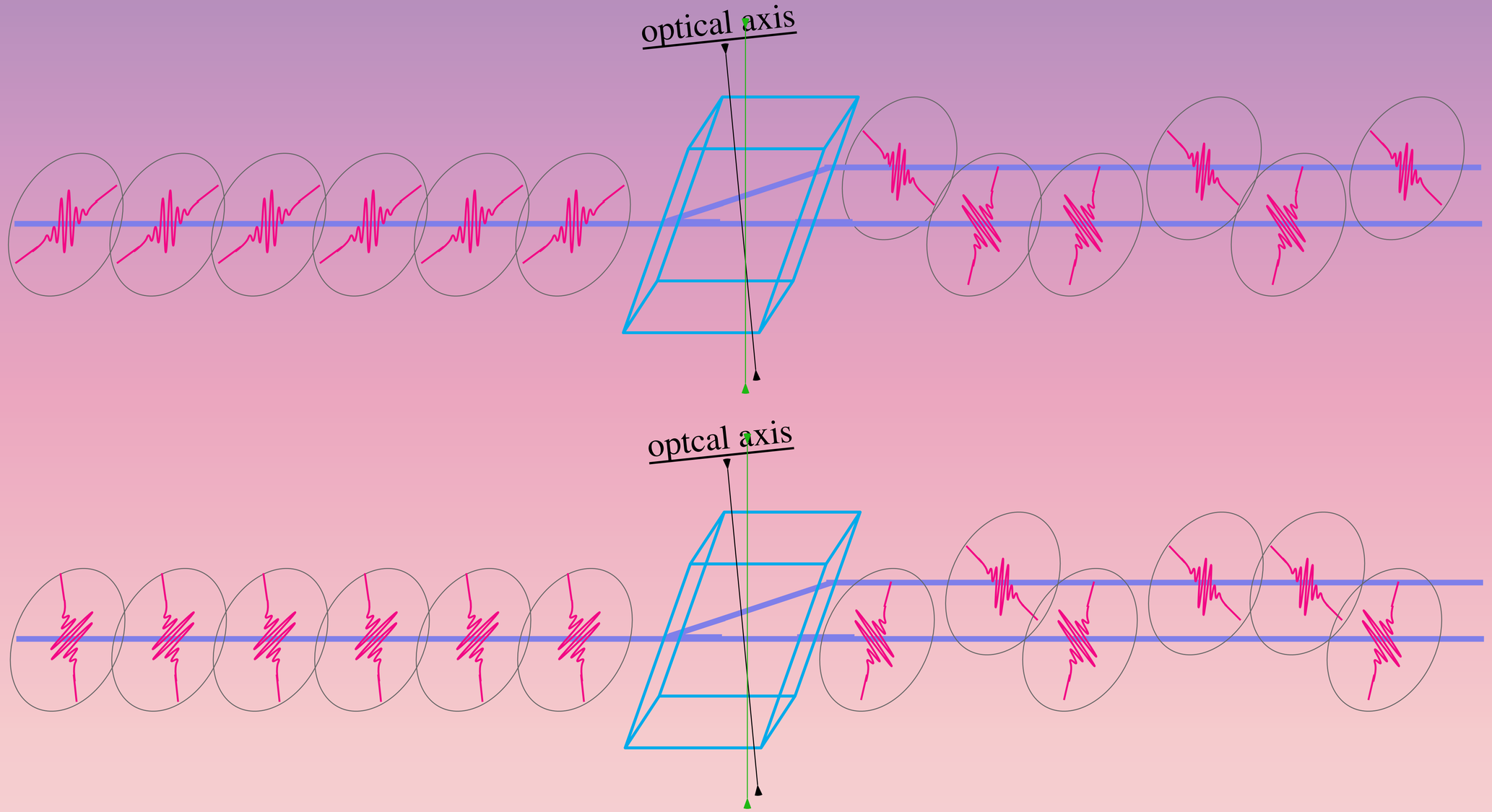
Calcite Crystal



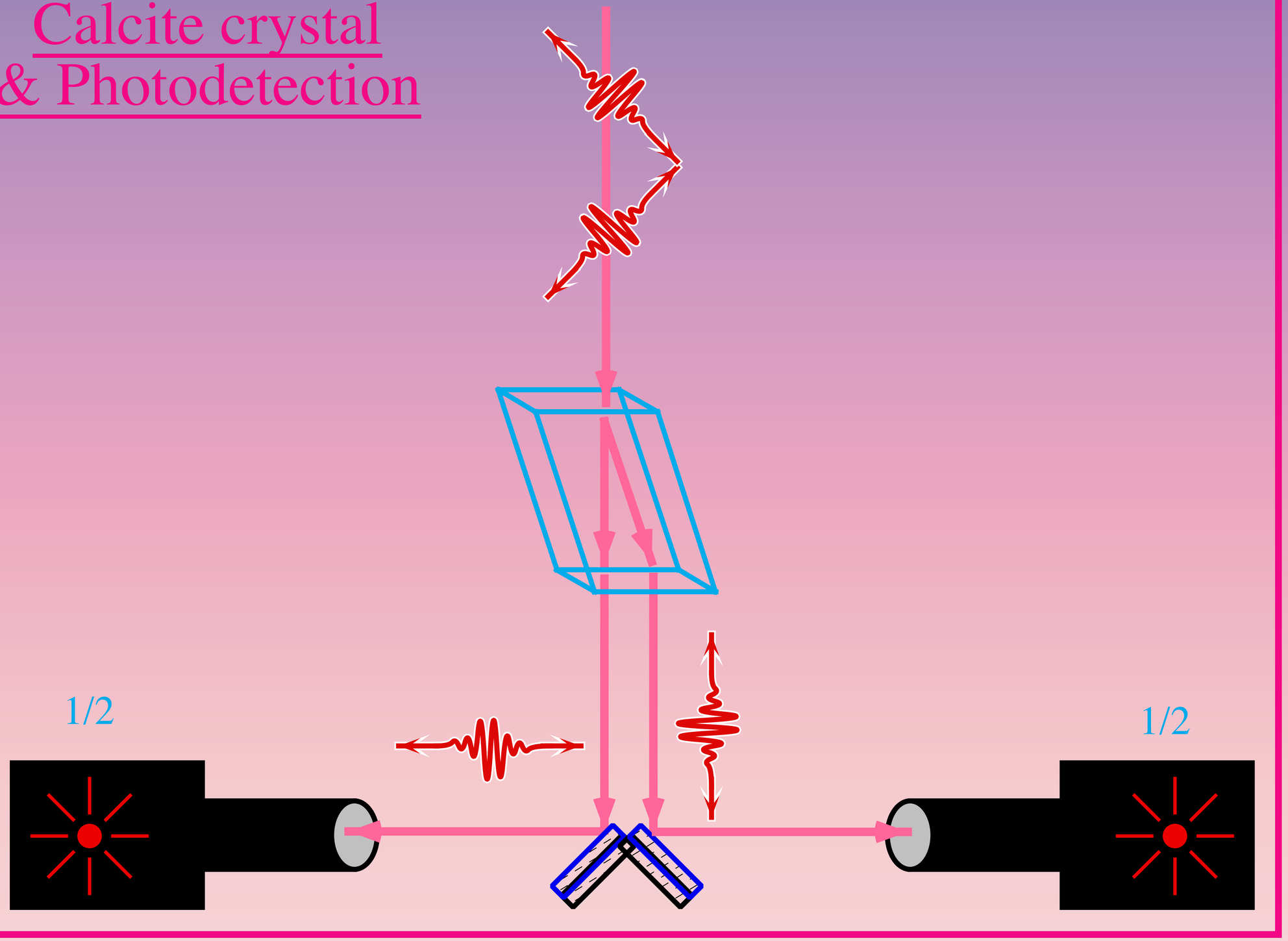
Calcite Crystal and photodétectors



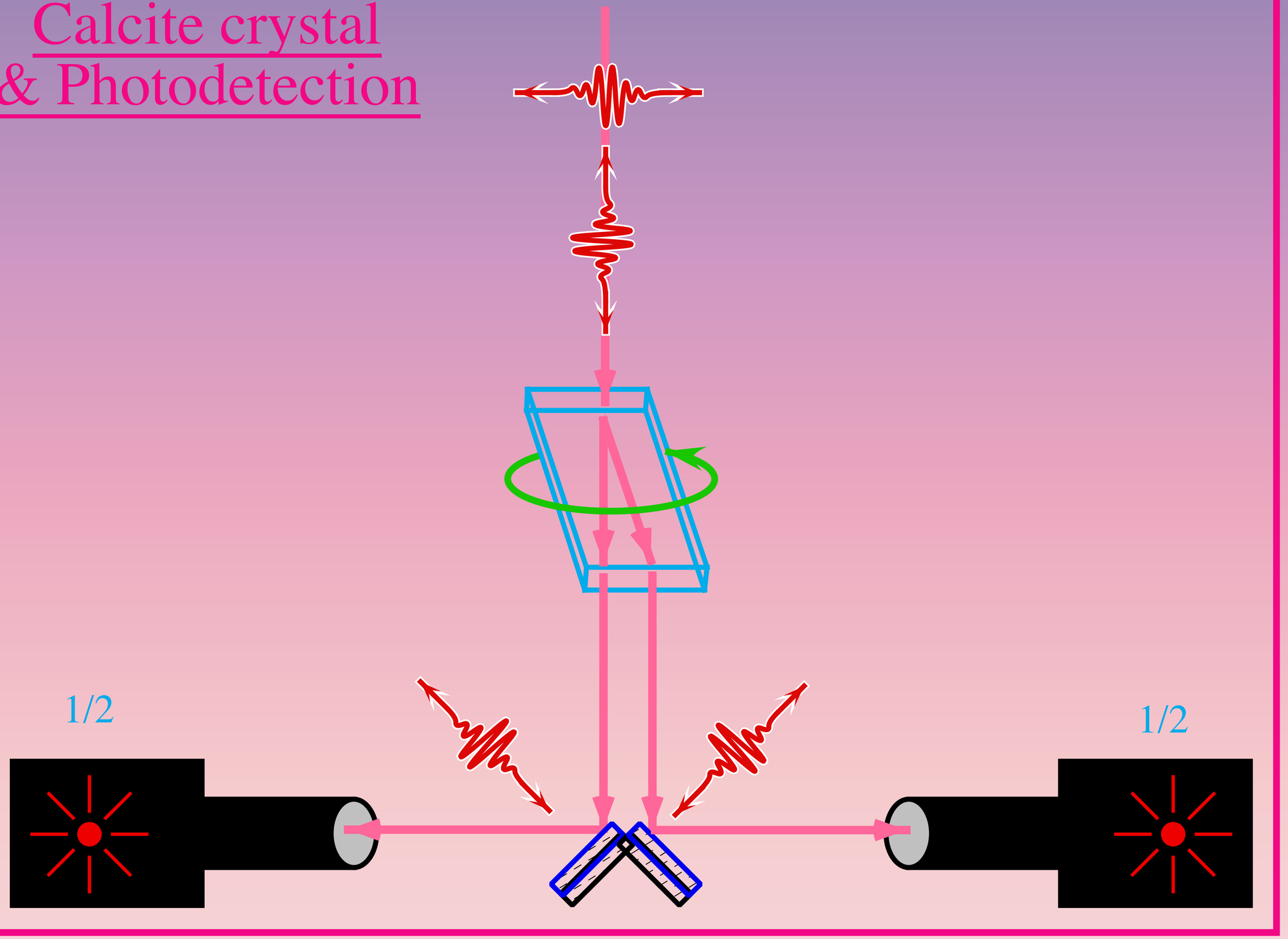
Calcite Crystal



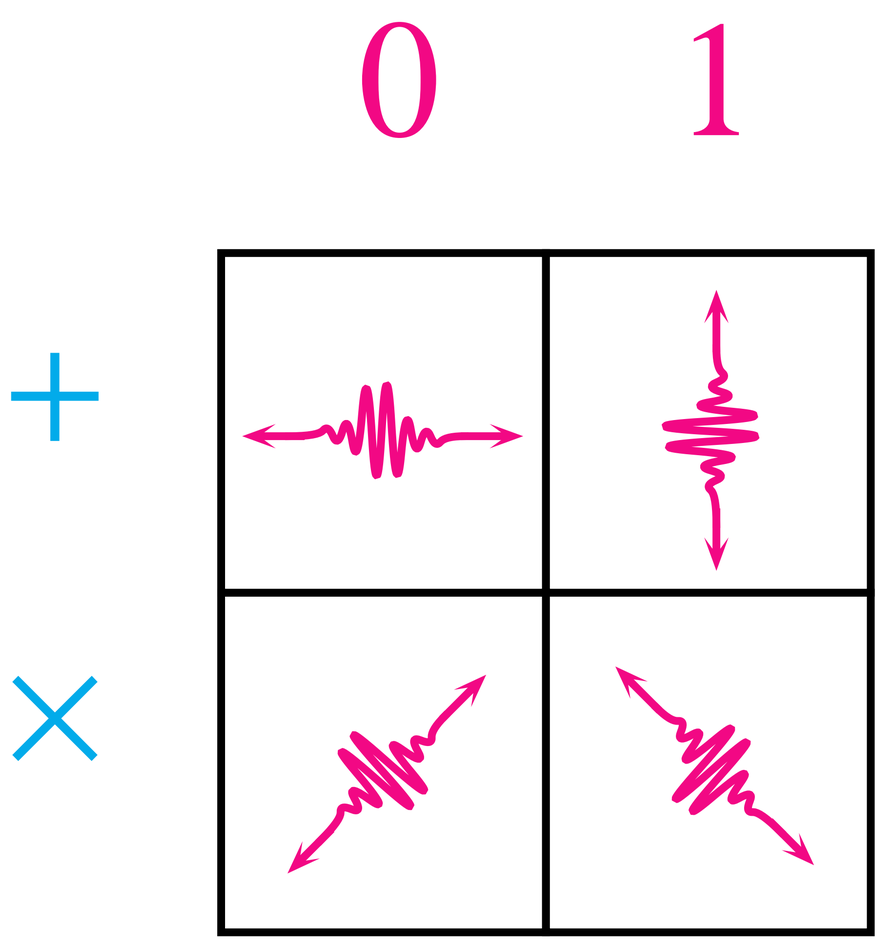
Calcite crystal & Photodetection



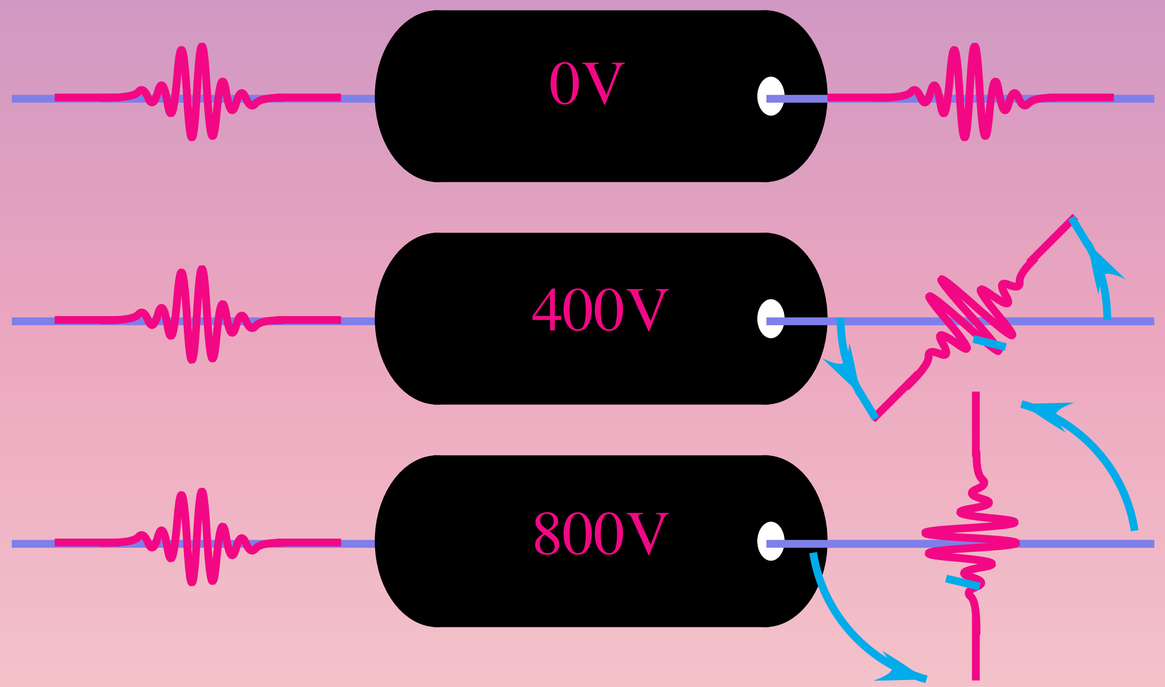
Calcite crystal & Photodetection

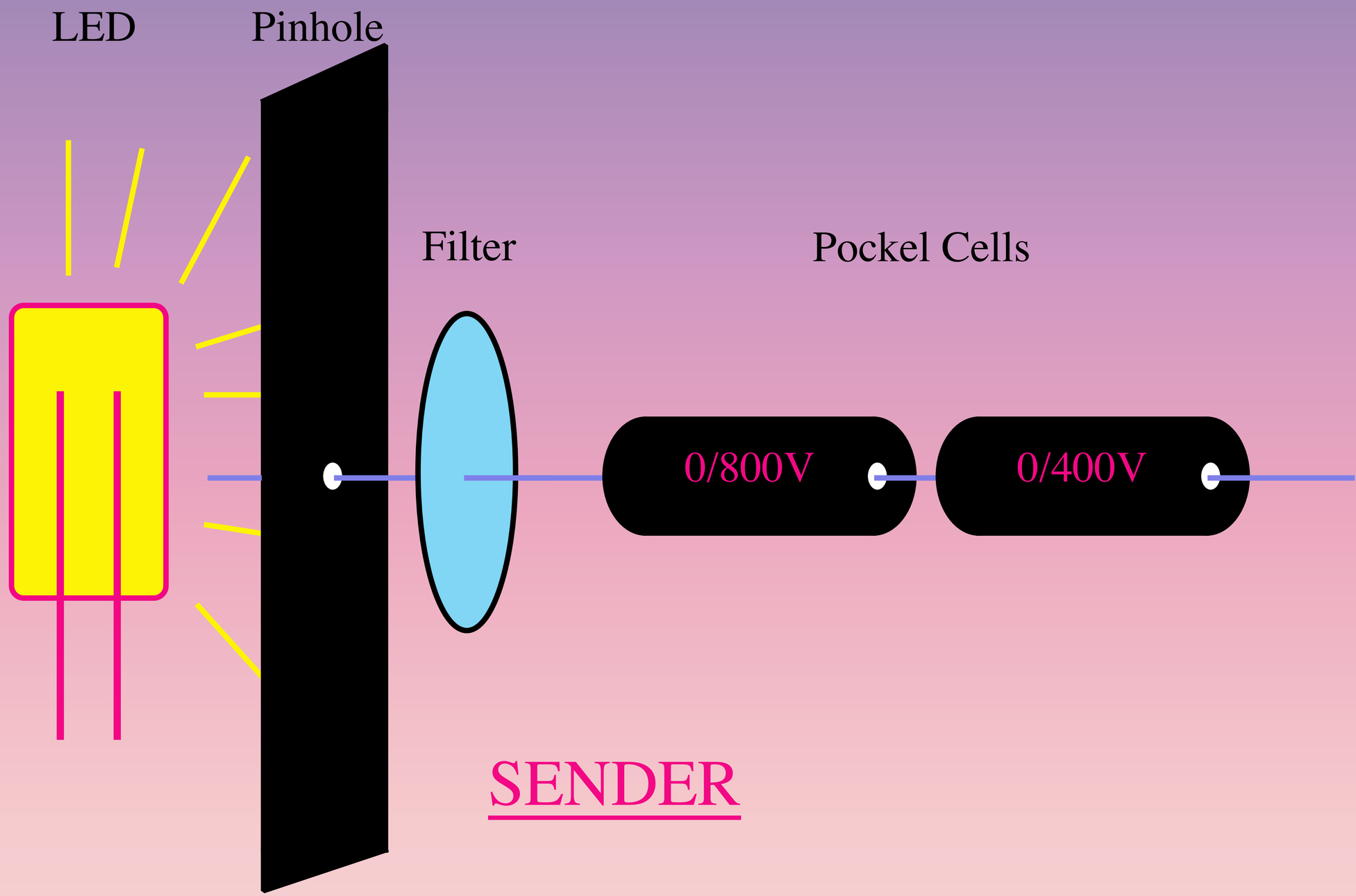


Ambiguous Coding Scheme

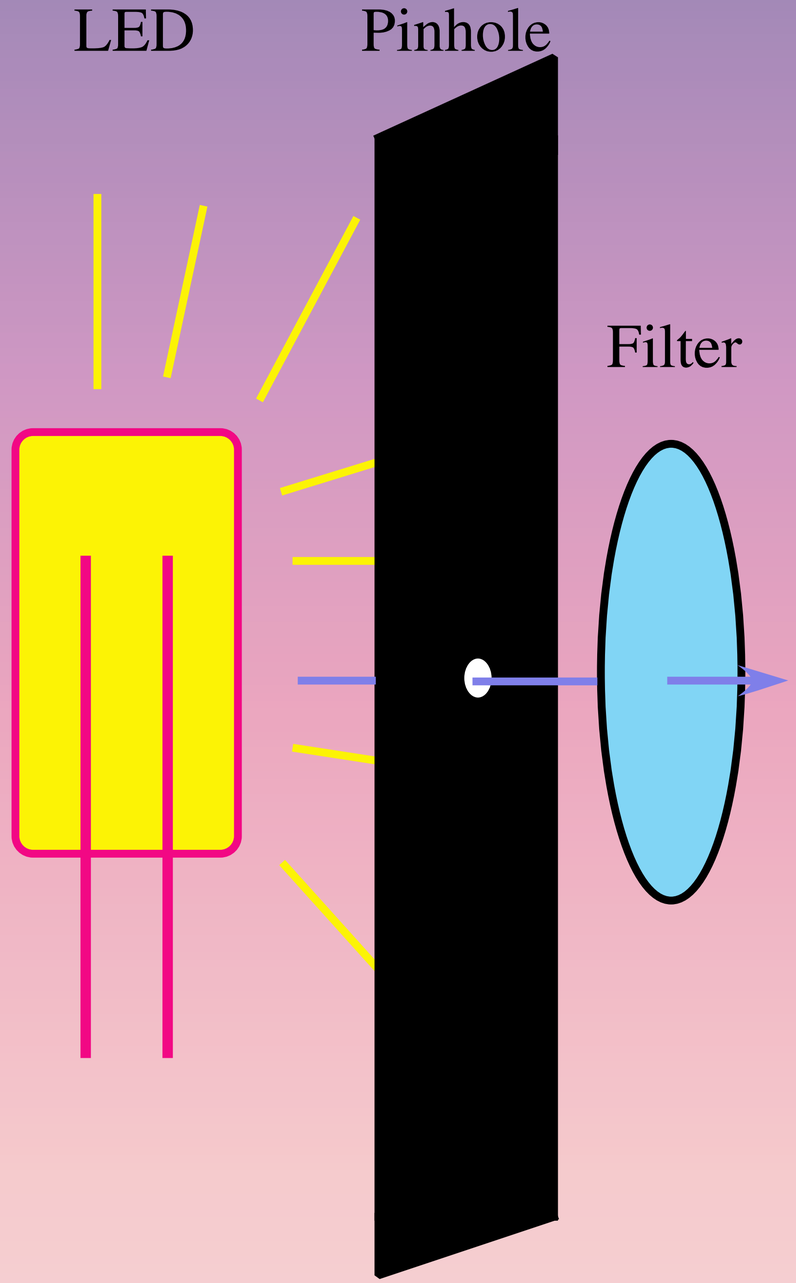


Pockel Cells





SENDER



Light source:

~ 1/10 photon per pulse

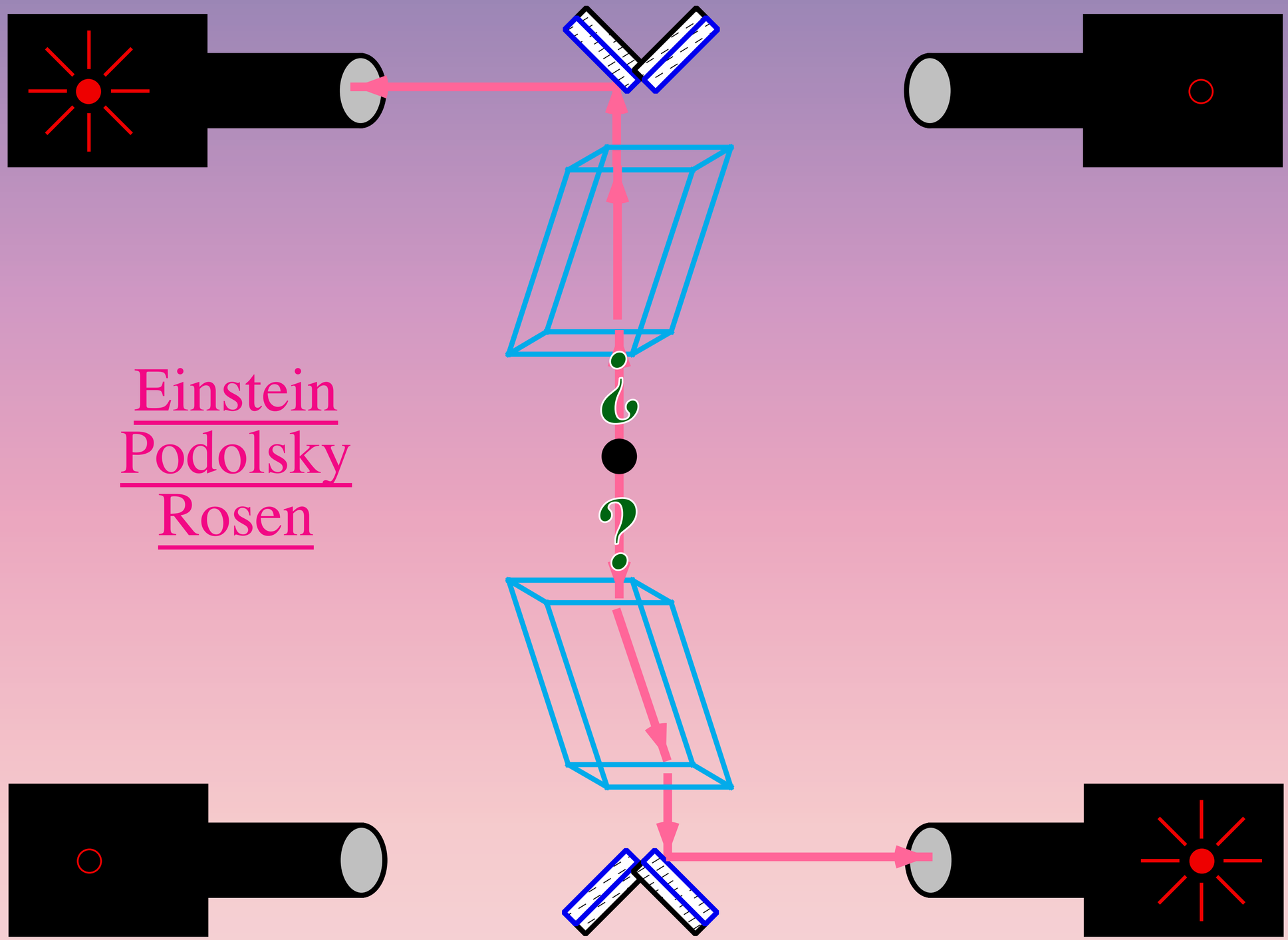
n = #photons per pulse follows
a Poisson distribution

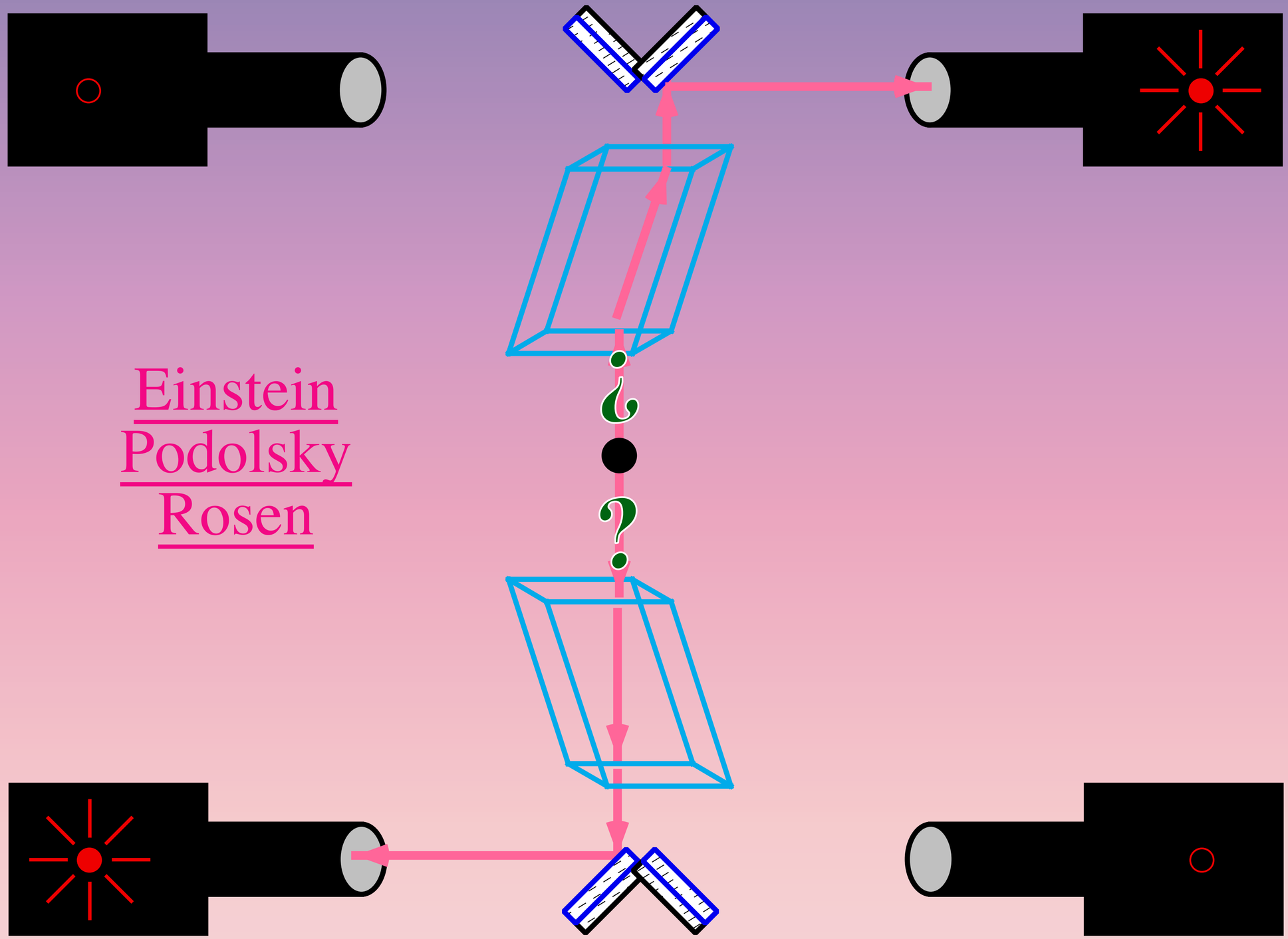
$Pr(n \leq x) = 1-e^{-x/10}$

Problem:

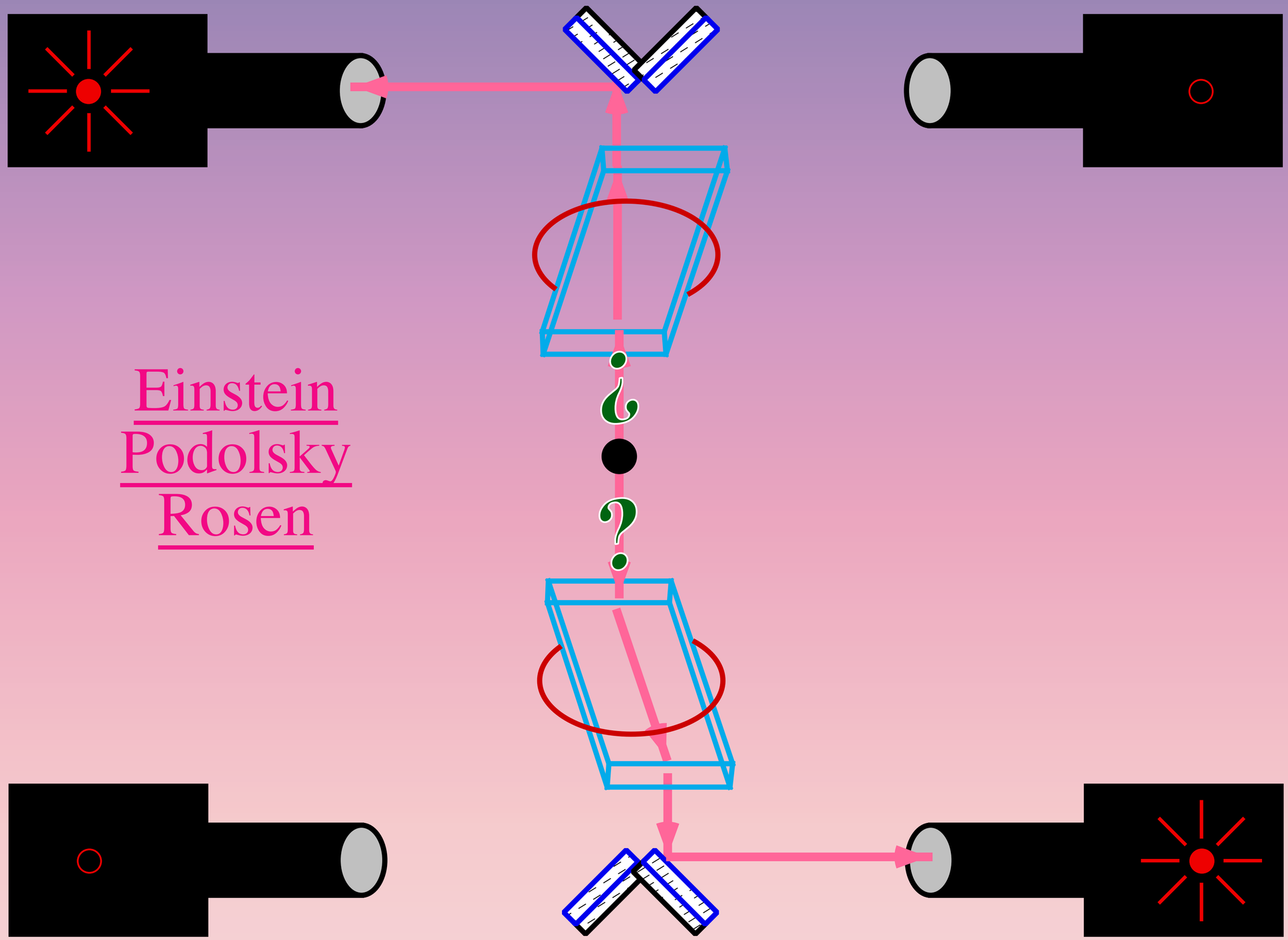
• may transmit multiple correlated polarized photons

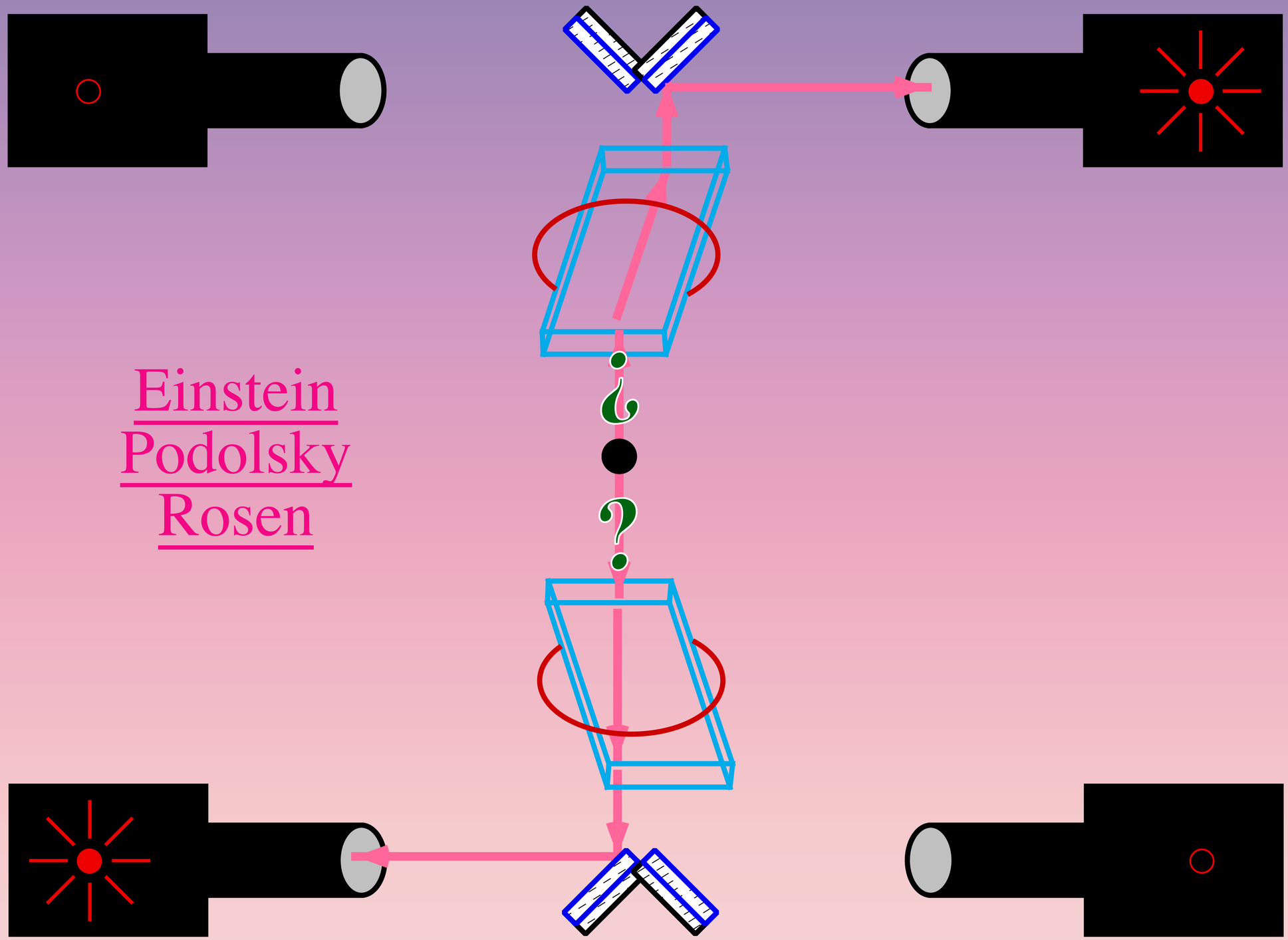
Einstein
Podolsky
Rosen





Einstein
Podolsky
Rosen





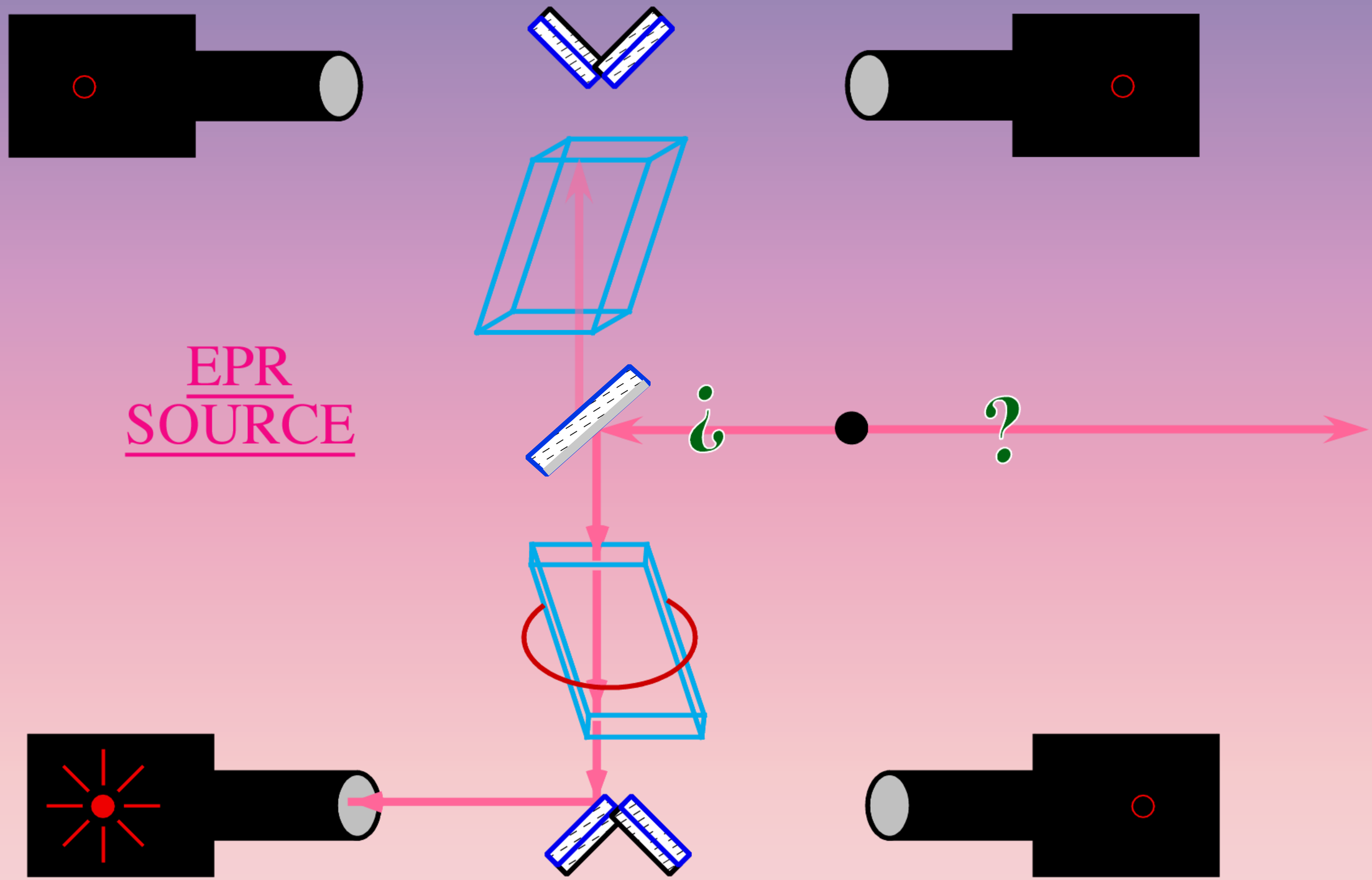


Photo Multipliers

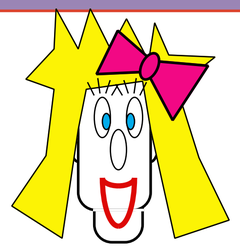
Pockel Cell

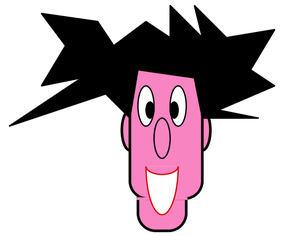
Calcite Crystal

0/400V

RECEIVER

Q-distribution of keys



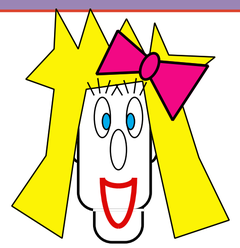


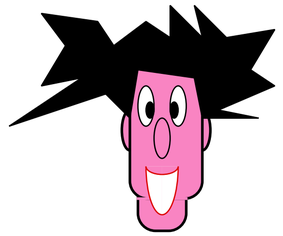
A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	×	×	+	+	×	+	+	+	×	+	+	×	×	×	+	×	×	×	+	+	×	+	×	+
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0
A:	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	0			0		1			1		0					1	0			1		0	0	0
B:	0			0		1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

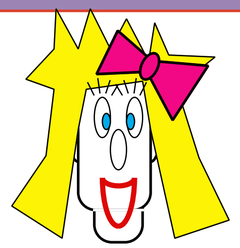
Q-distribution of keys

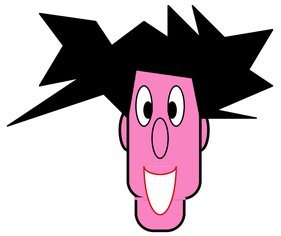




A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+

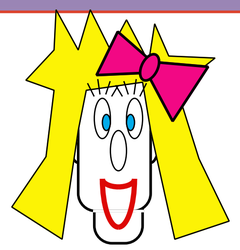
Q-distribution of keys

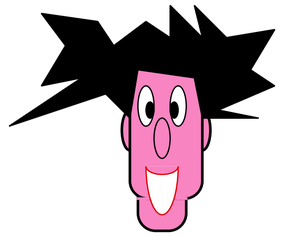




A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	×	×	+	+	×	+	+	+	×	+	+	×	×	×	+	×	×	×	+	+	×	+	×	+
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0

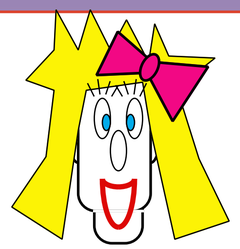
Q-distribution of keys

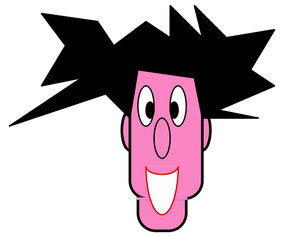




A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	×	×	+	+	×	+	+	+	×	+	+	×	×	×	+	×	×	×	+	+	×	+	×	+
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0
A:	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+

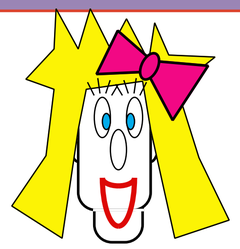
Q-distribution of keys

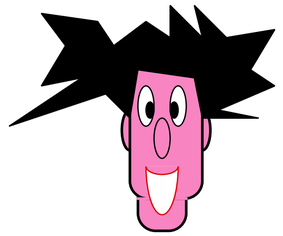




A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	×	×	+	+	×	+	+	+	×	+	+	×	×	×	+	×	×	×	+	+	×	+	×	+
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0
A:	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	0			0		1			1		0					1	0			1		0	0	0
B:	0			0		1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

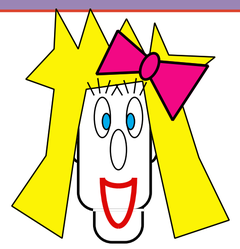
Q-distribution of keys

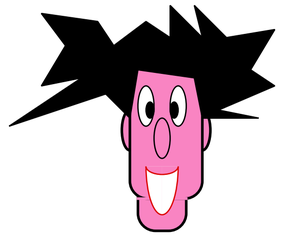




B:	0		0		1		1		0			1	0		1		0	0	0
A:	0		0		1		1		0			1	1		1		0	0	0

Q-distribution of keys

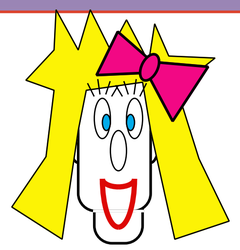


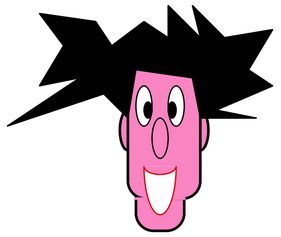


B:		0			0		1		1		0			1	0		1		0	0	0
A:		0			0		1		1		0			1	1		1		0	0	0
A:		0					1				0				1						0
B:		=					=				=				≠						=

20%

Q-distribution of keys

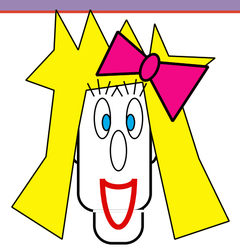


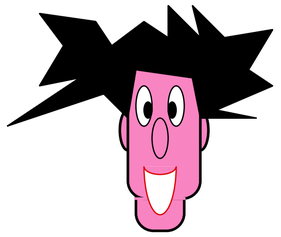


B:	=	=	=	≠	=	
B:	0	1	1	1	0	0
A:	0	1	1	1	0	0

20%

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

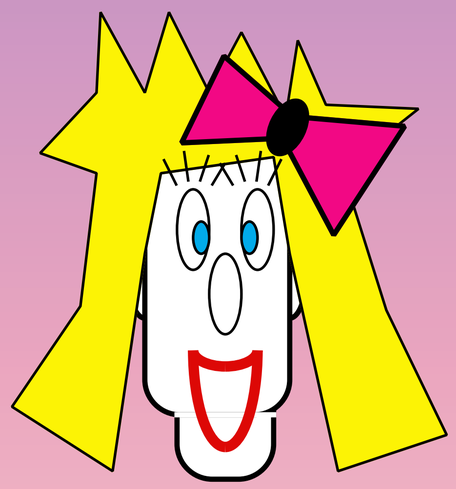
- Observed error rate indicates amount of eavesdropper information

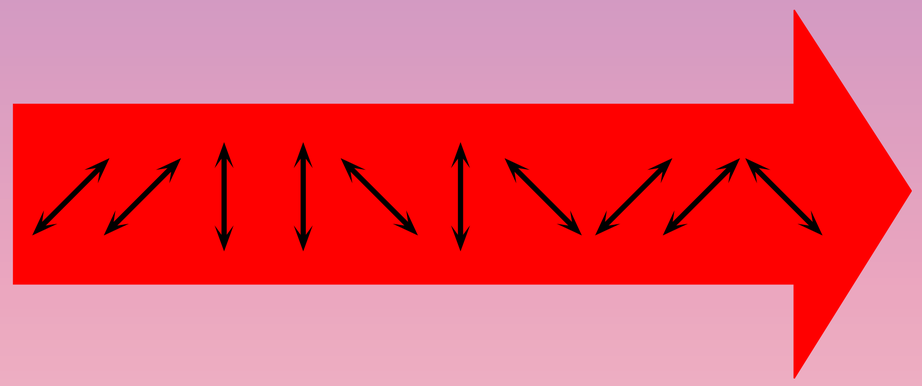
- Error-correction is used to fix errors

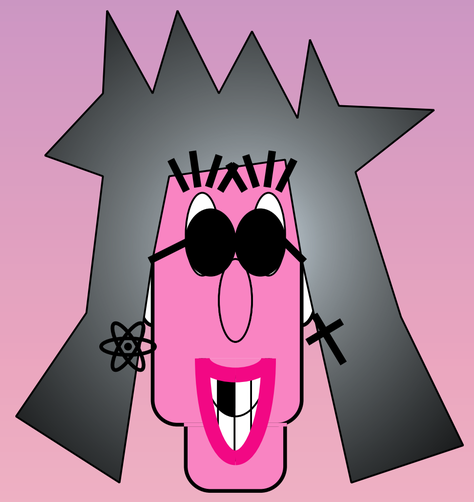
- Random hash function is used to distill a smaller secret classical key

.....

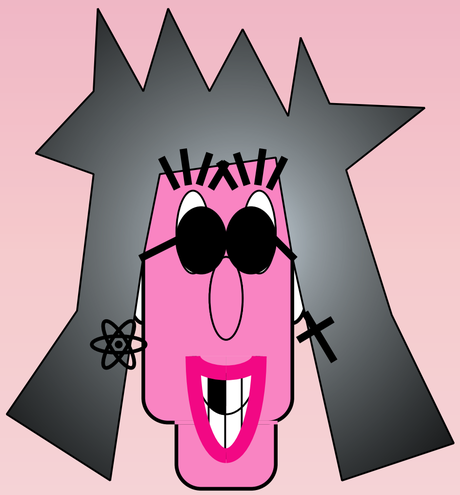
Information <--> Errors
(intercept resend)

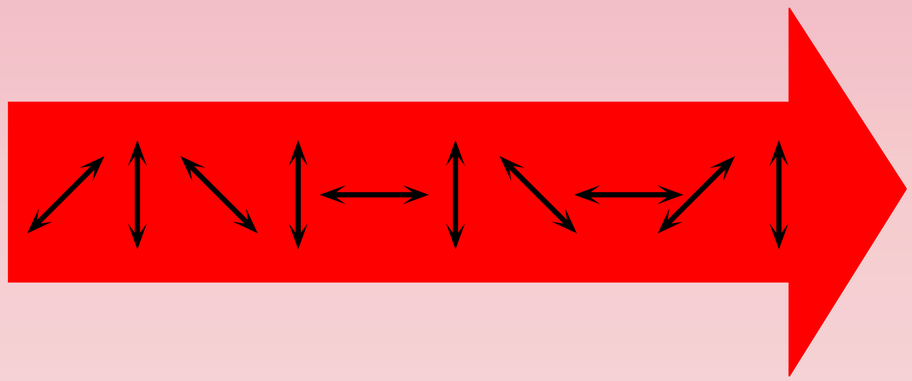


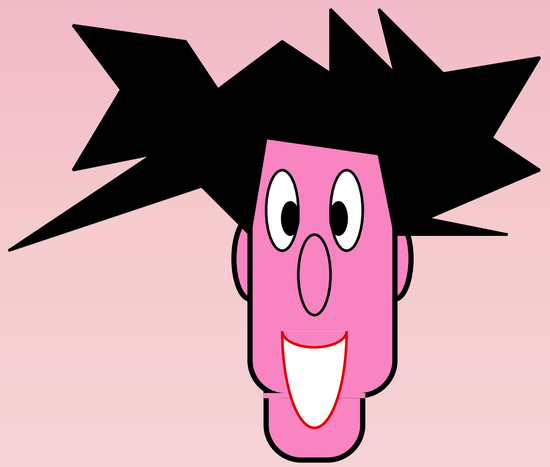




× + × + + + × + ×+

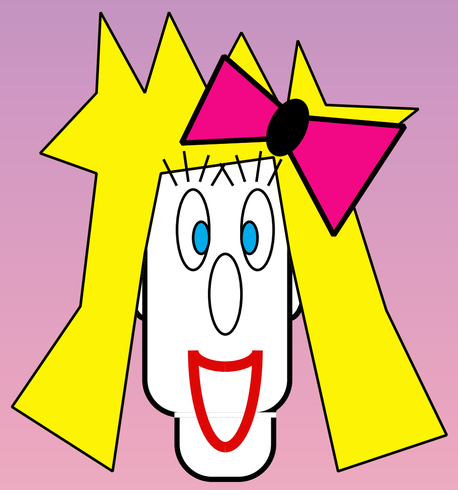


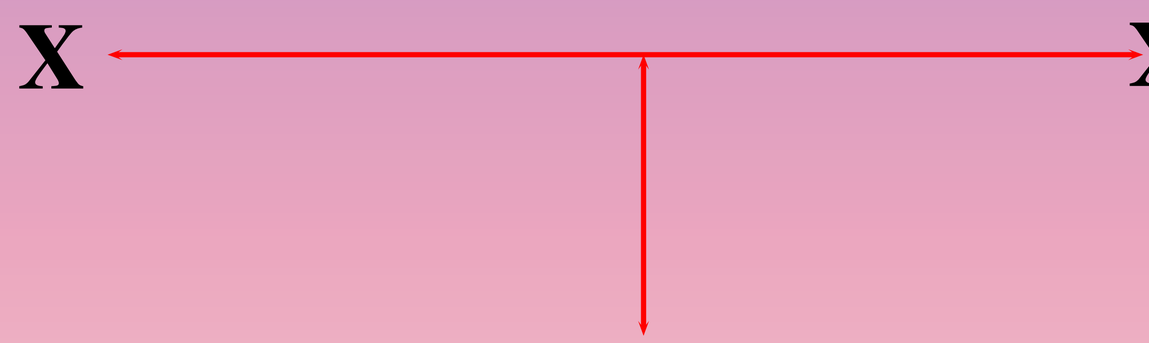


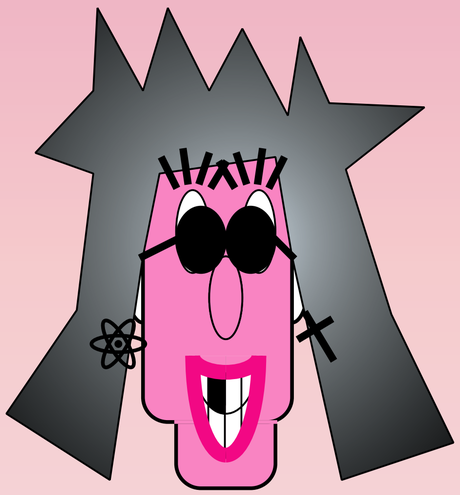


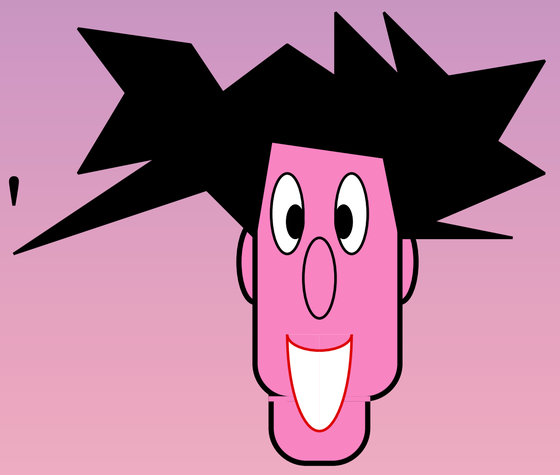
× + × + + + × + ×+

Mostly Identical Partly Secret String

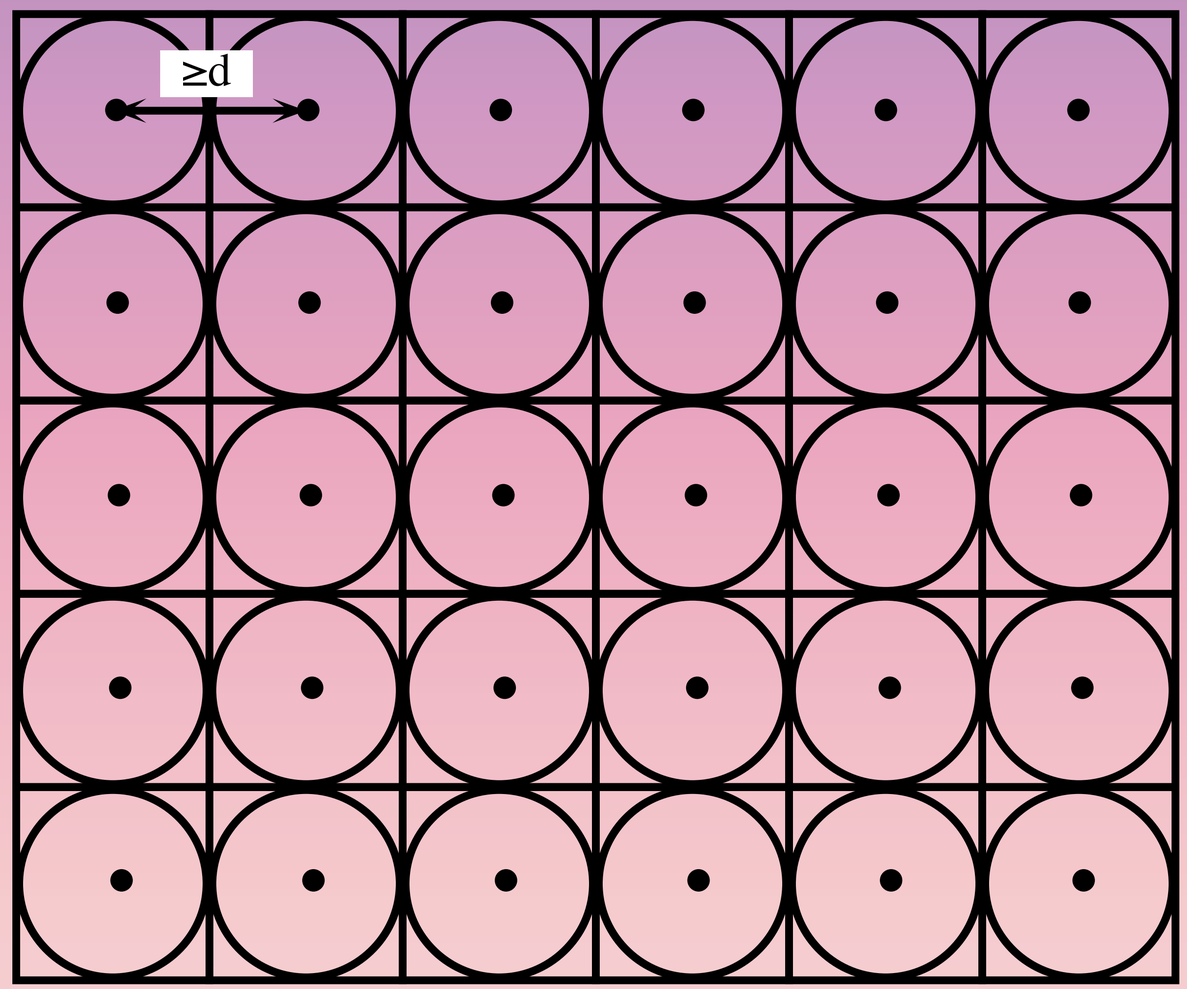




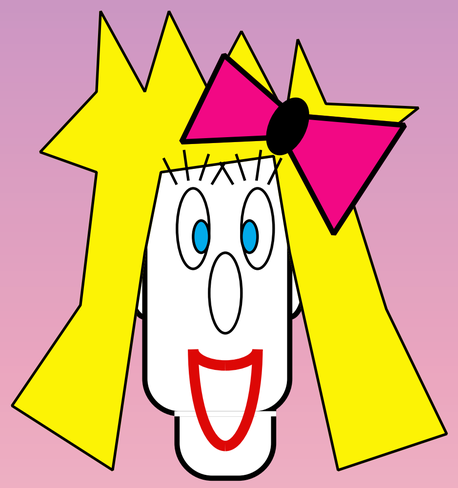




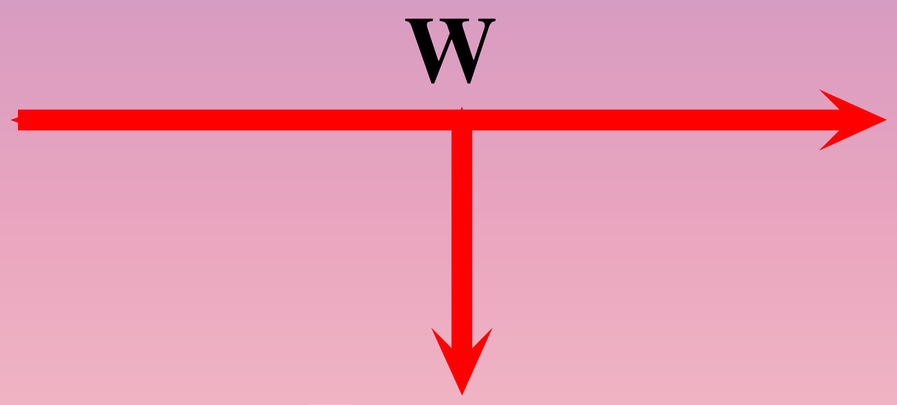
(classical) error-correcting codes



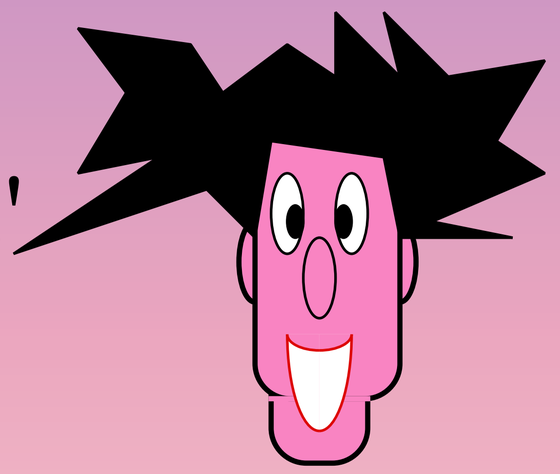
Identical Partly Secret String

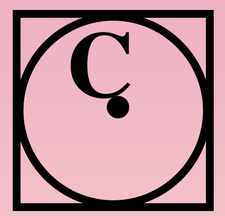


X



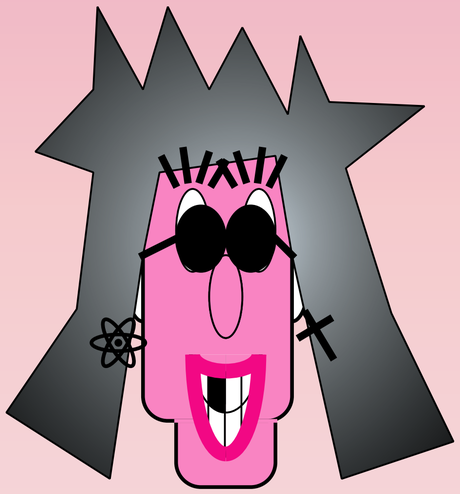
X'



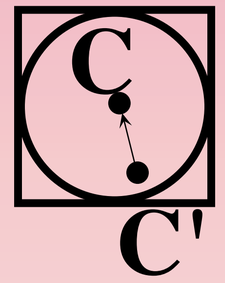


W:=C⊕X

E:=E(θ)+W

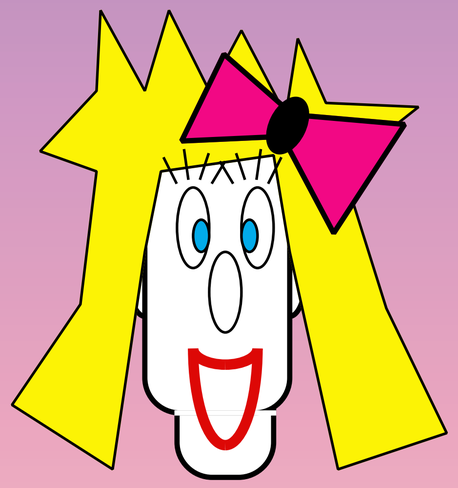


C':=W⊕X'



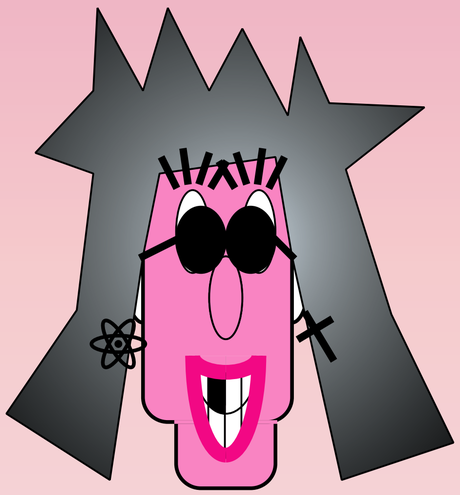
X:=C⊕W

Identical Partly Secret String

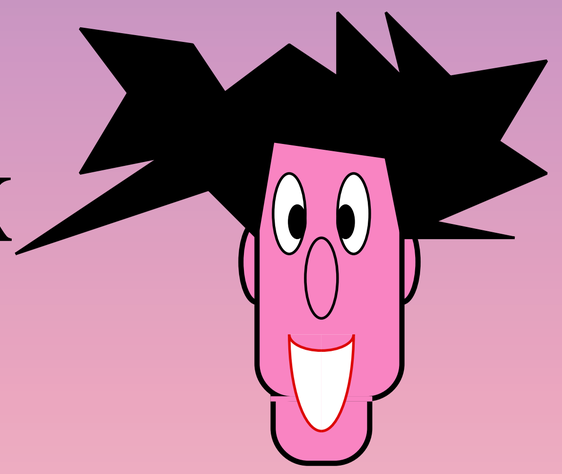


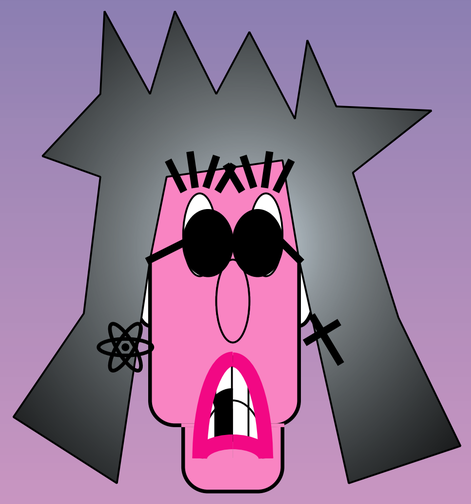
X

E



X

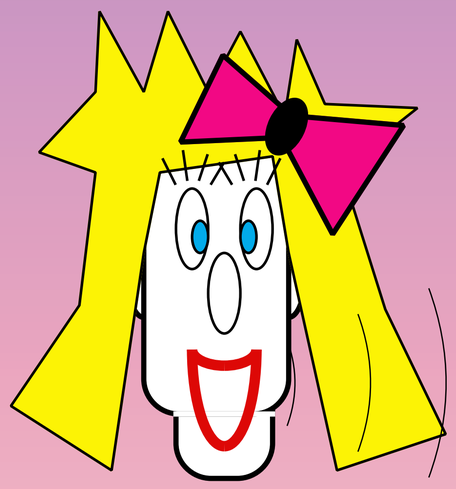




in BB84, Eve's information at this point (before privacy amplification) contains:

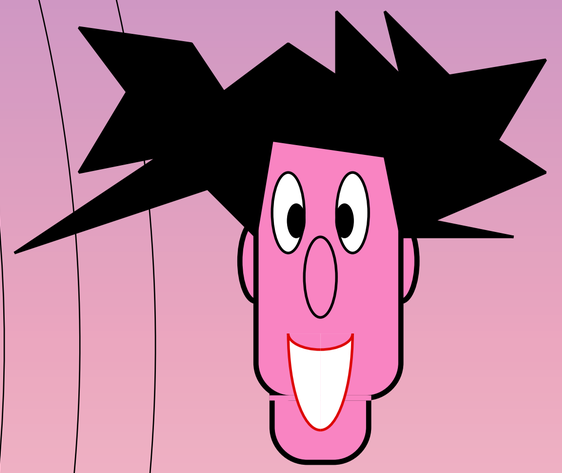
- **results of eavesdropping**
- **multi-photon pulses**
- **error correction**

Identical Secret Shorter String through Privacy Amplification

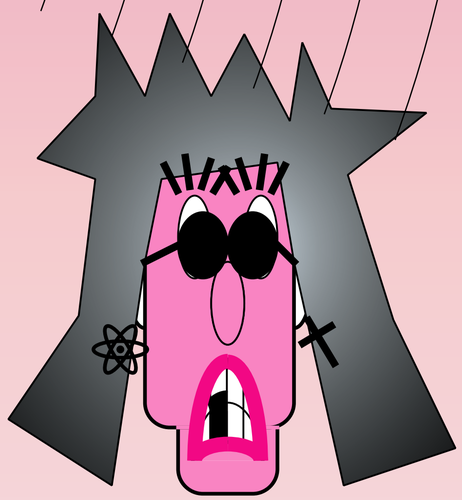


$X \rightarrow h(X)$

h



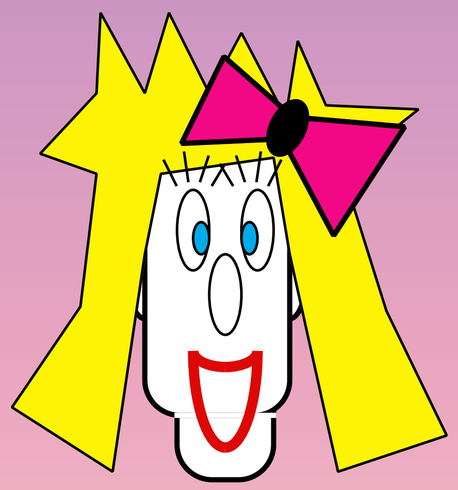
$X \rightarrow h(X)$



$E \rightarrow h(E)$

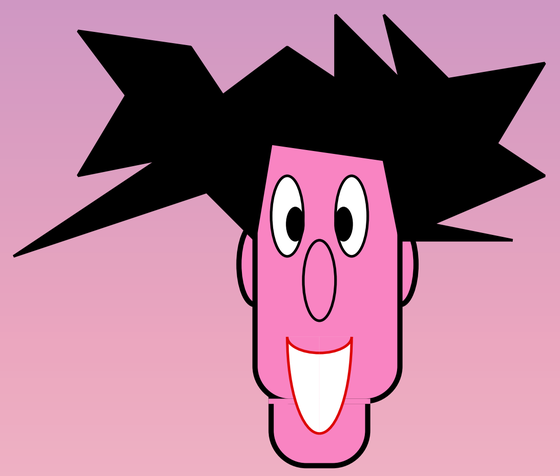
BBCM

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

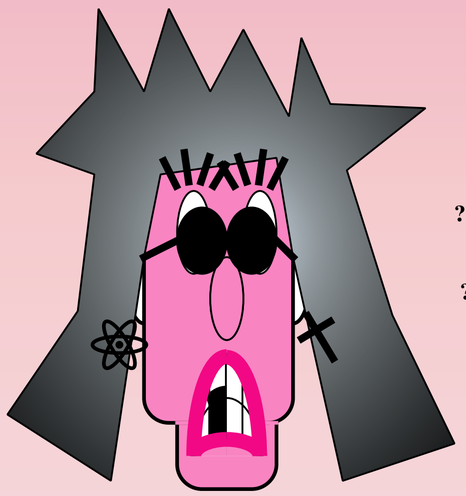


k:=g(X)

g



k:=g(X)



??????????

k':=g(E)

??????????

Quantum Key Distribution

Claude Crépeau

School of Computer Science
McGill University