Introduction to theoretical quantum CRYPTOGRAPHY

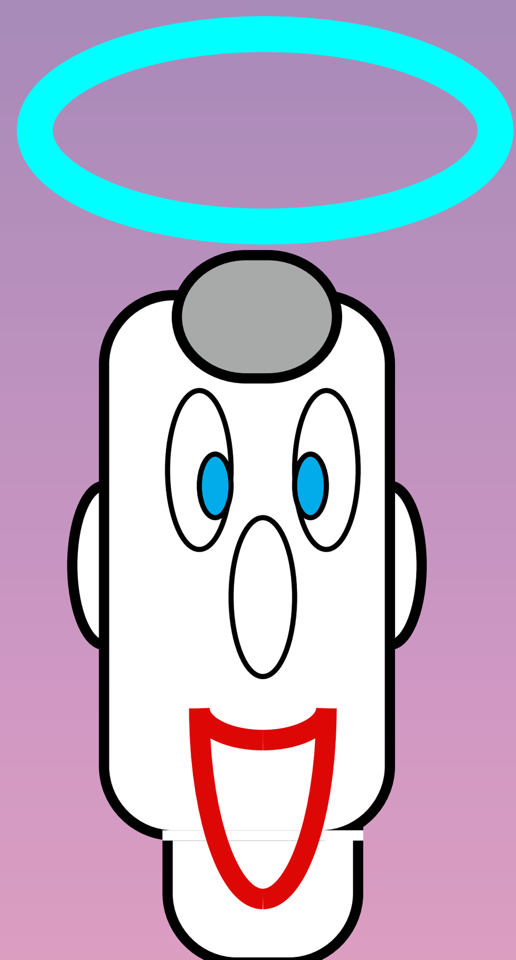
Claude Crépeau

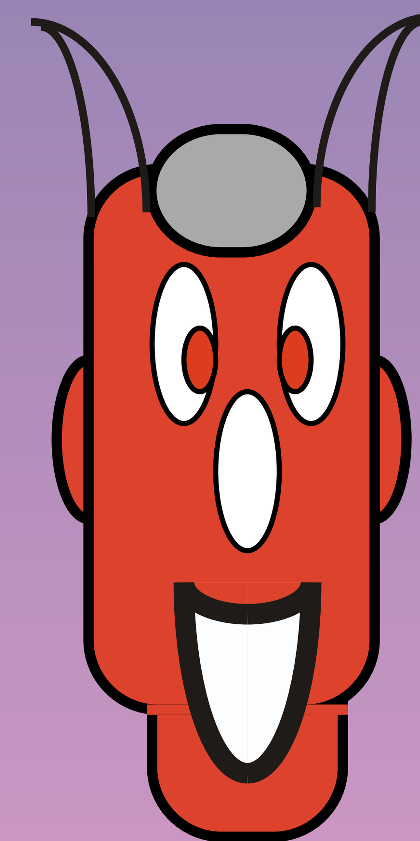
School of Computer Science
McGill University

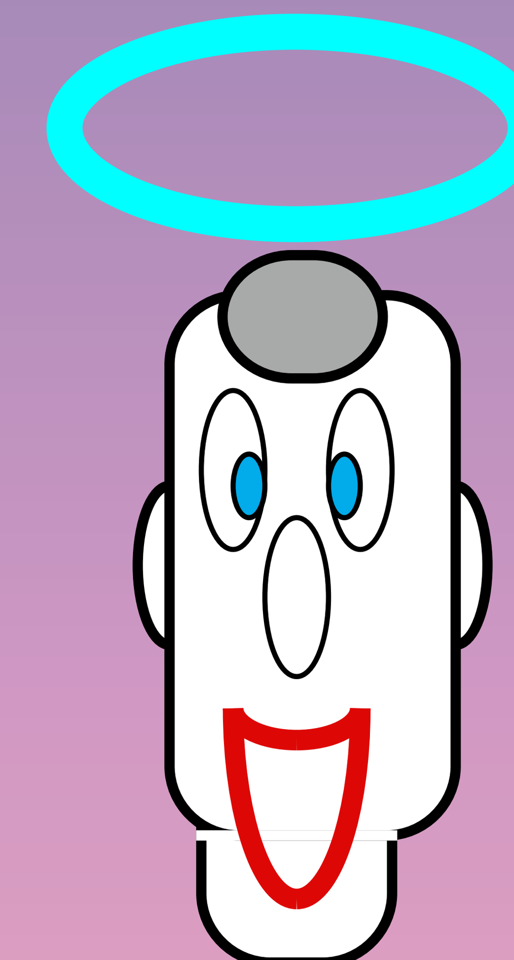
(1) Classical Cryptography

(1.1) Information Theoretical Cryptography

(1.1) Information Theoretical Cryptography







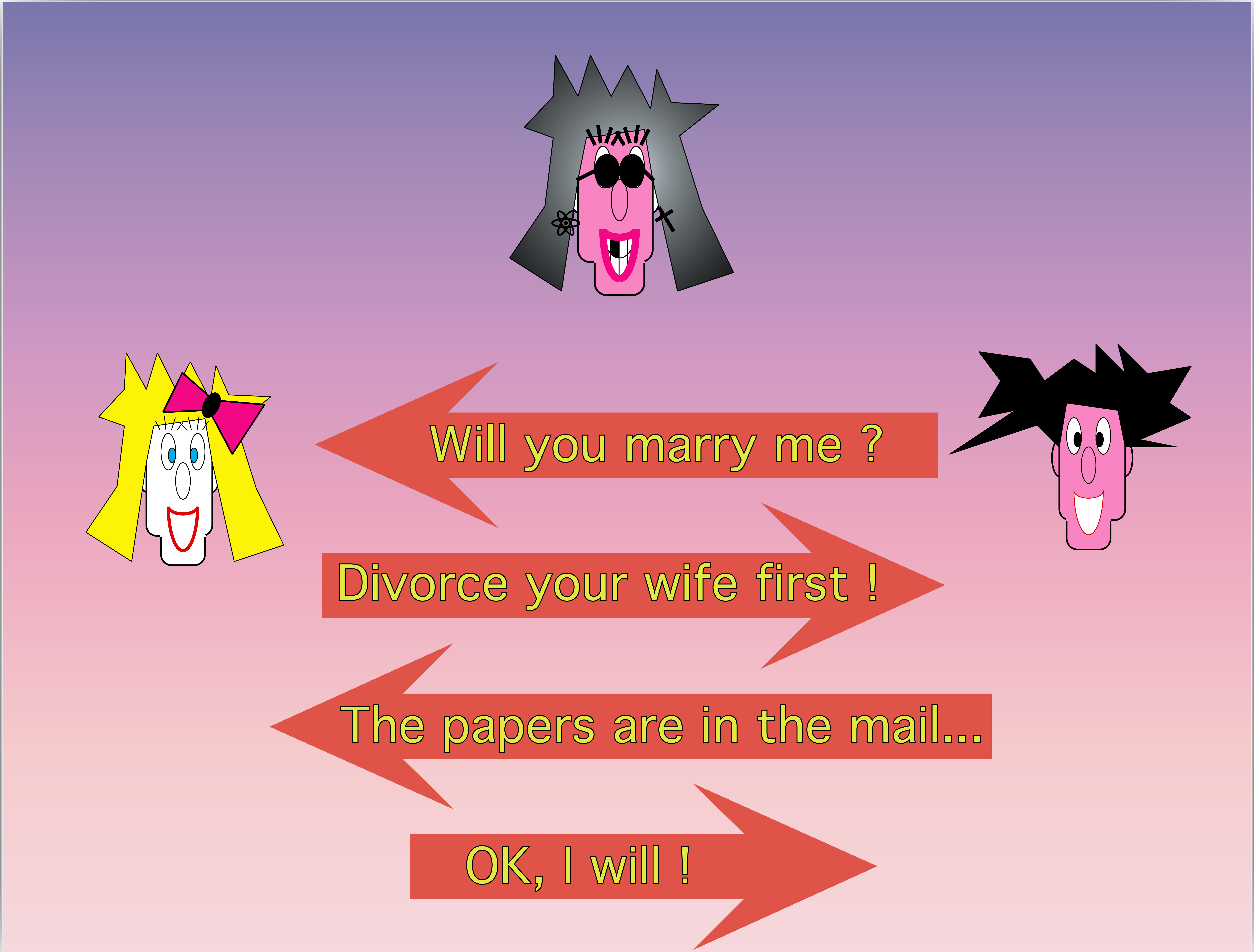
. . . . .

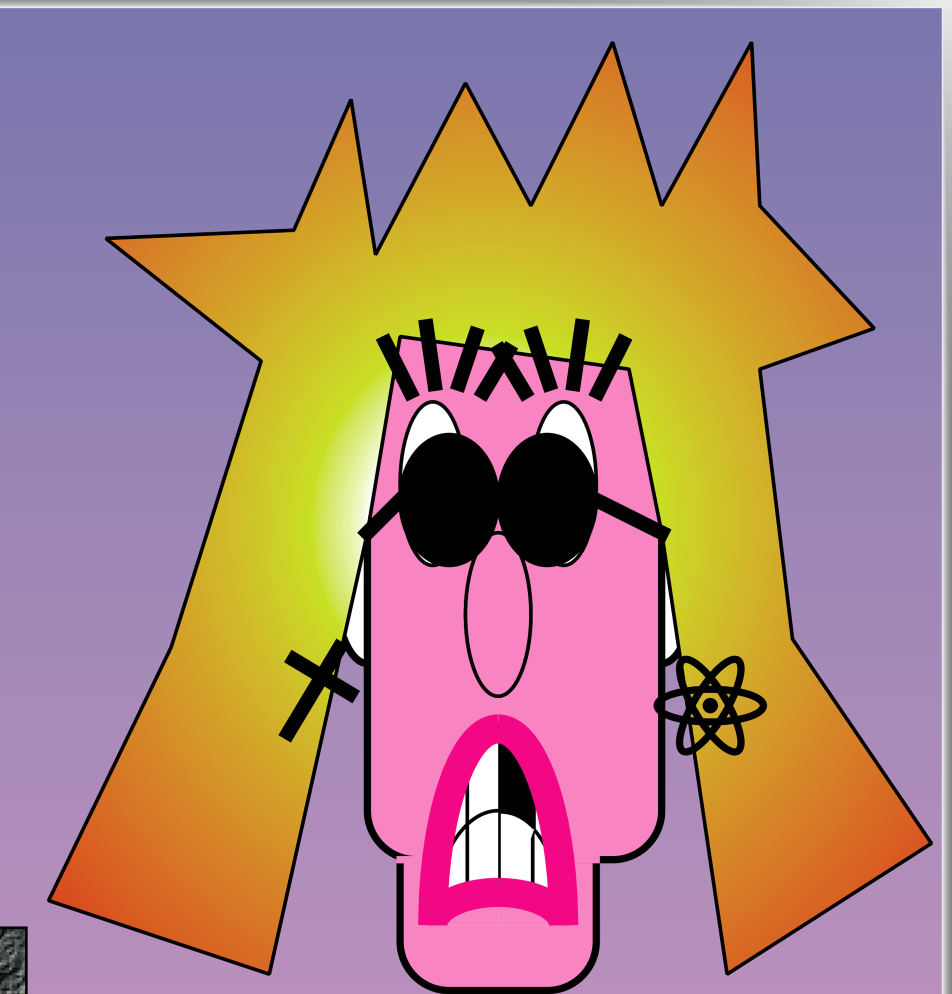
(1.1.1) key distribution

(1.1.2) Encryption

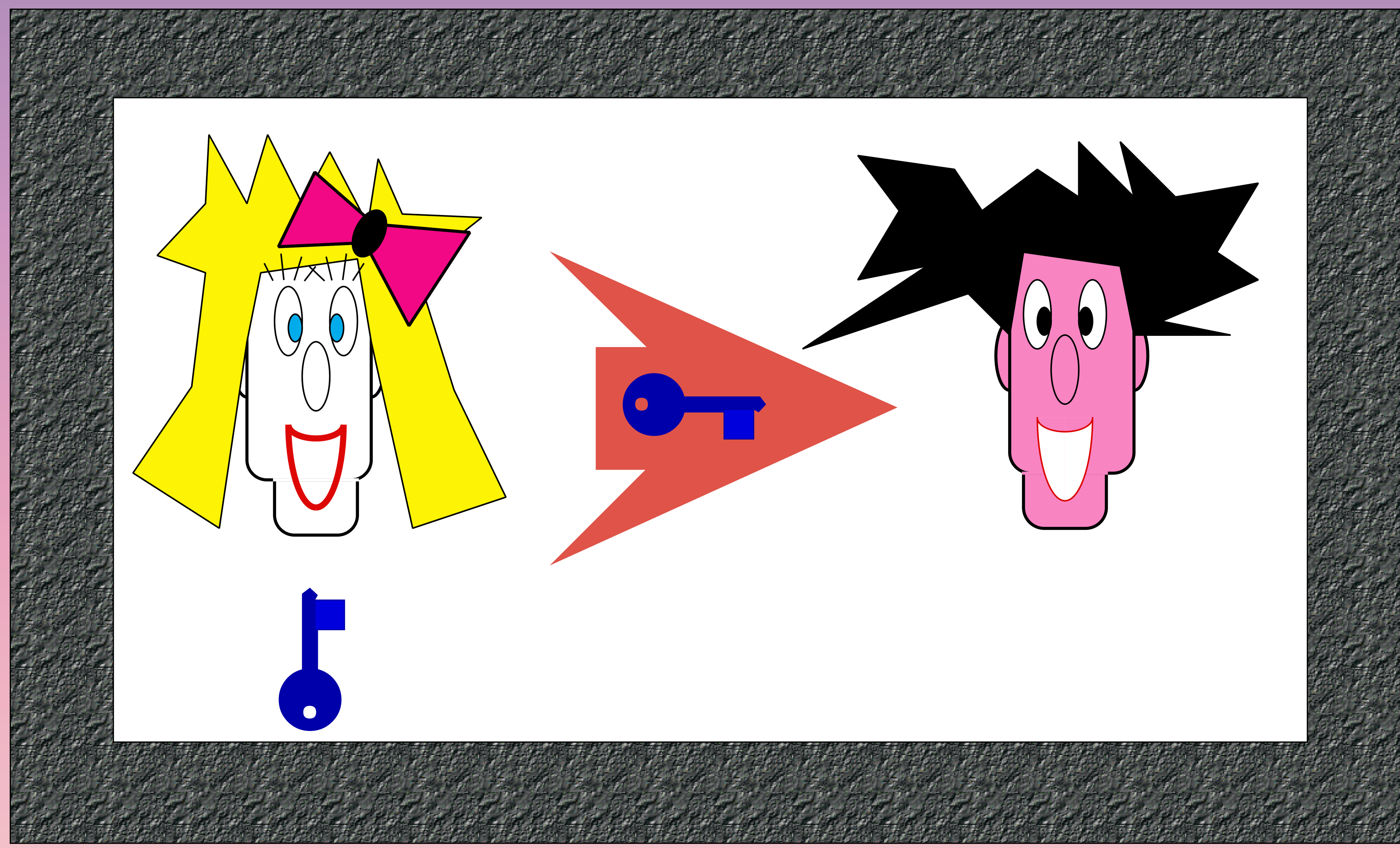
(1.1.3) Authentication

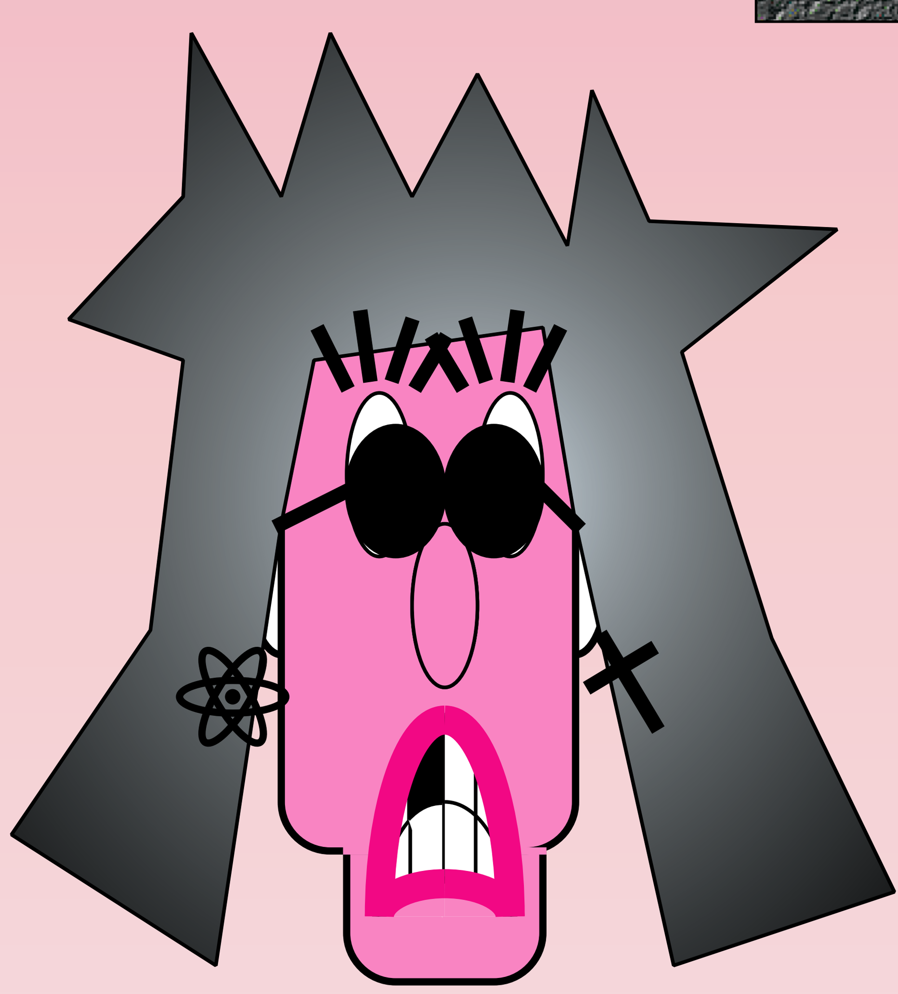
. . . . .

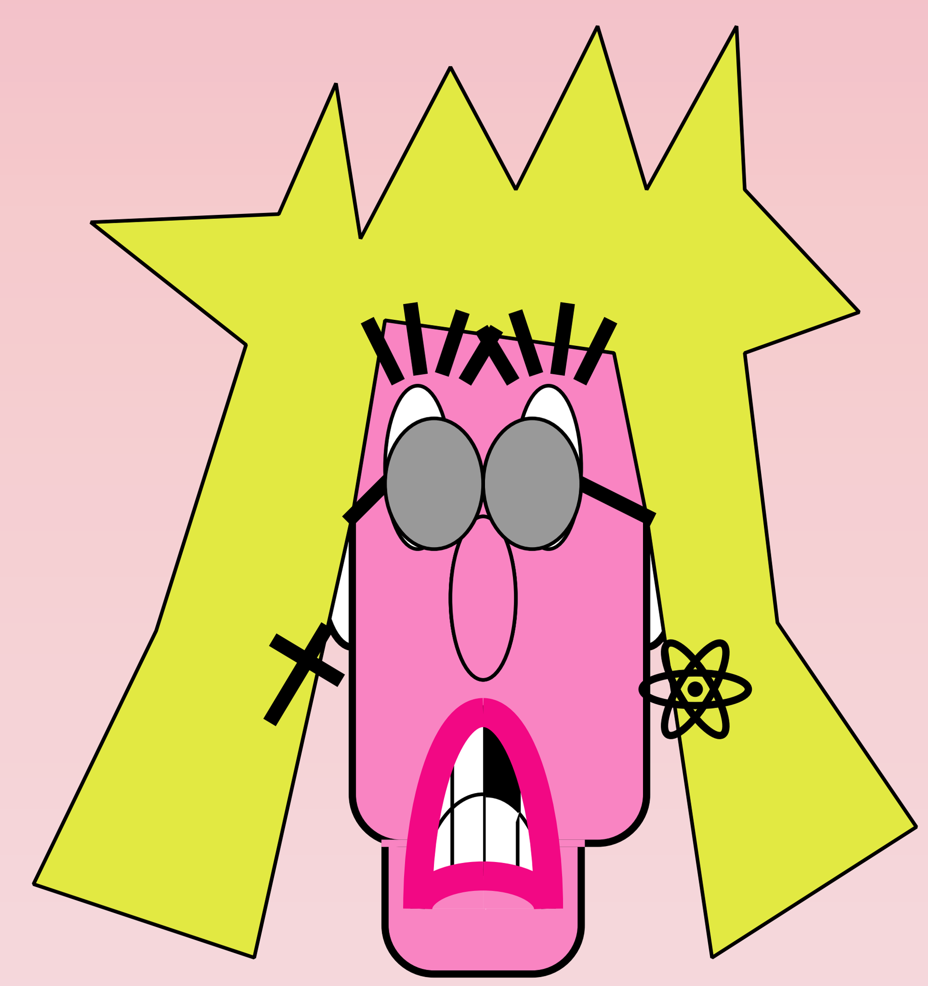

Will you marry me ?
Divorce your wife first !
The papers are in the mail...
OK, I will !



(1.1.1) key distribution

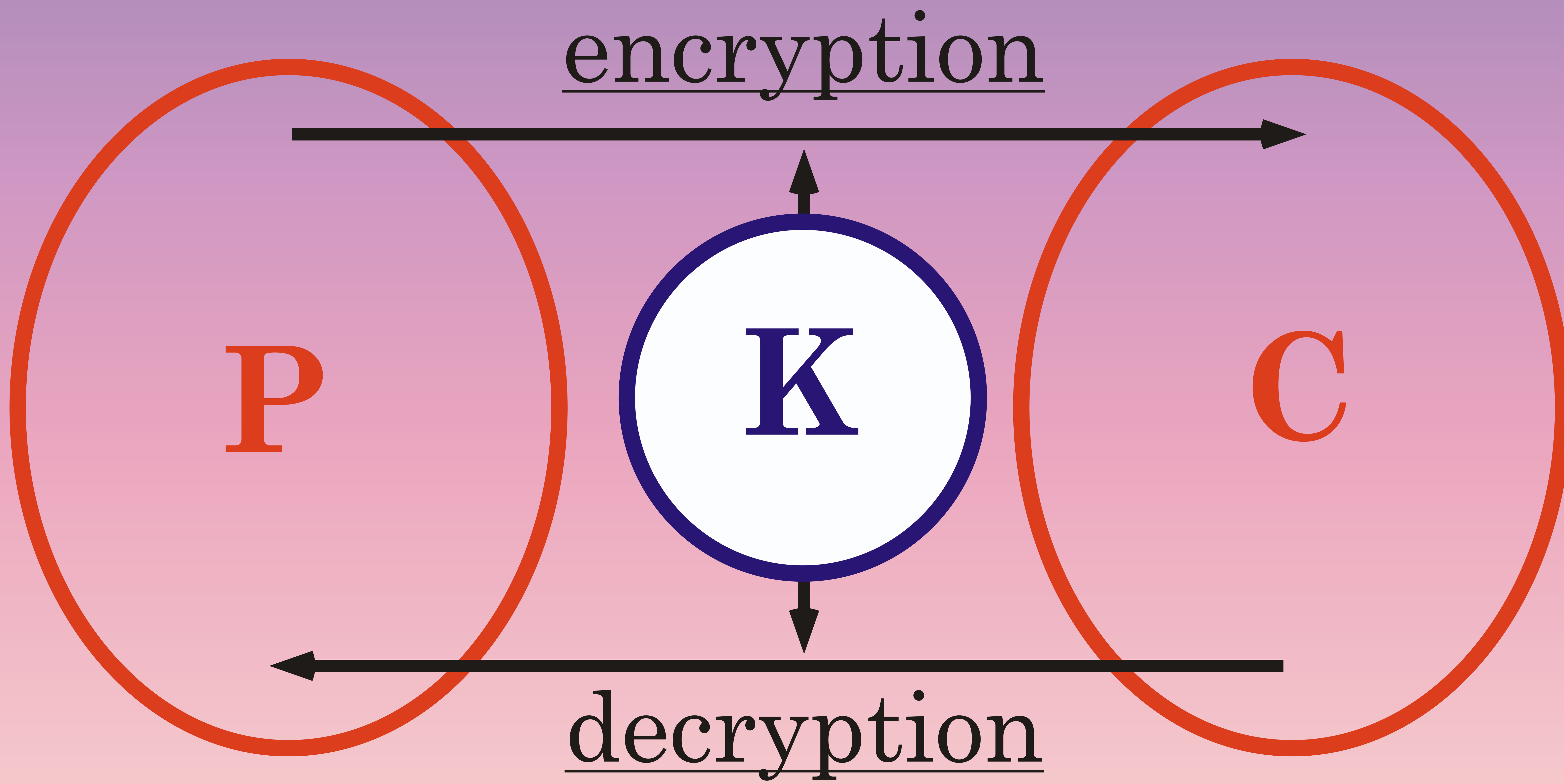






(1.1.2) Encryption

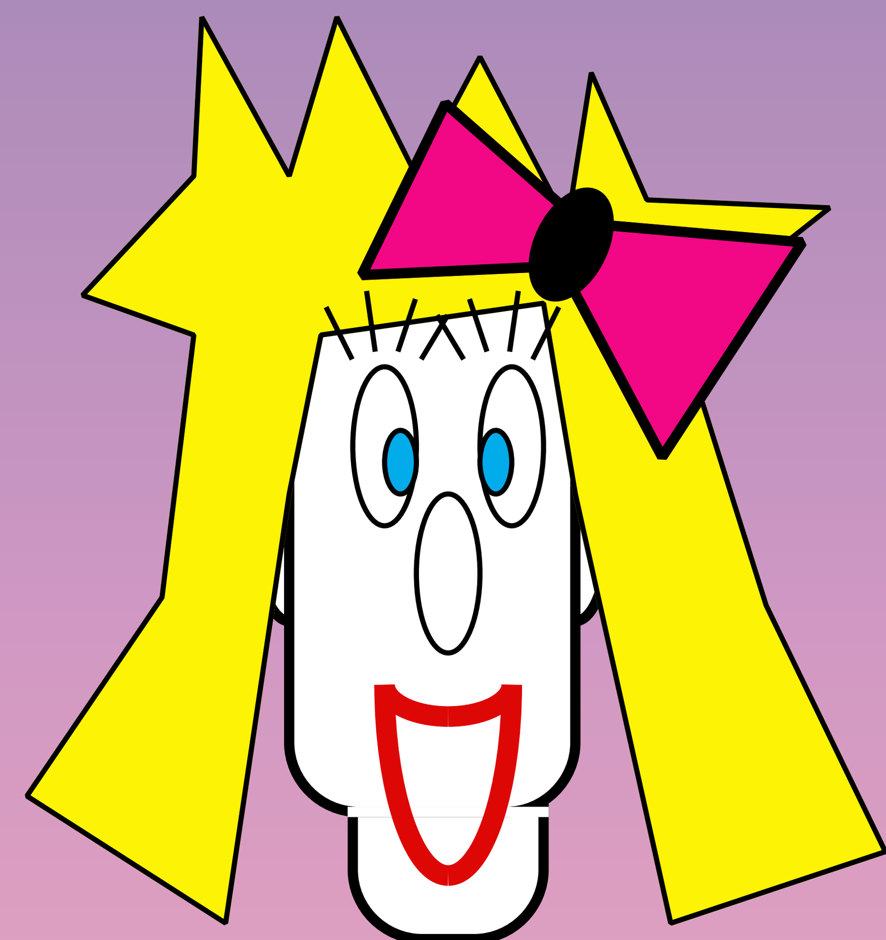
symmetric encryption

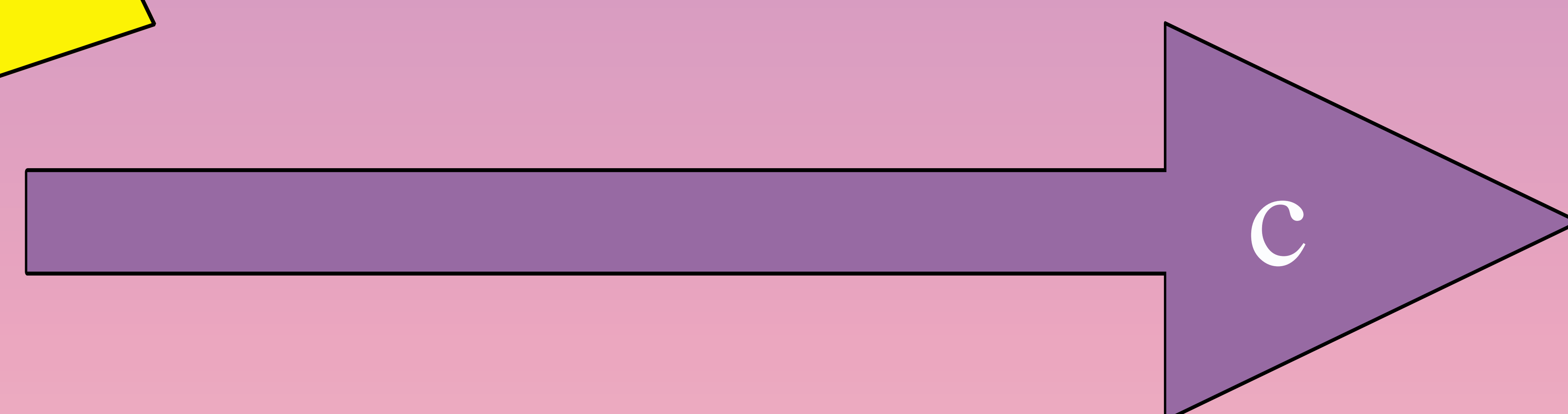


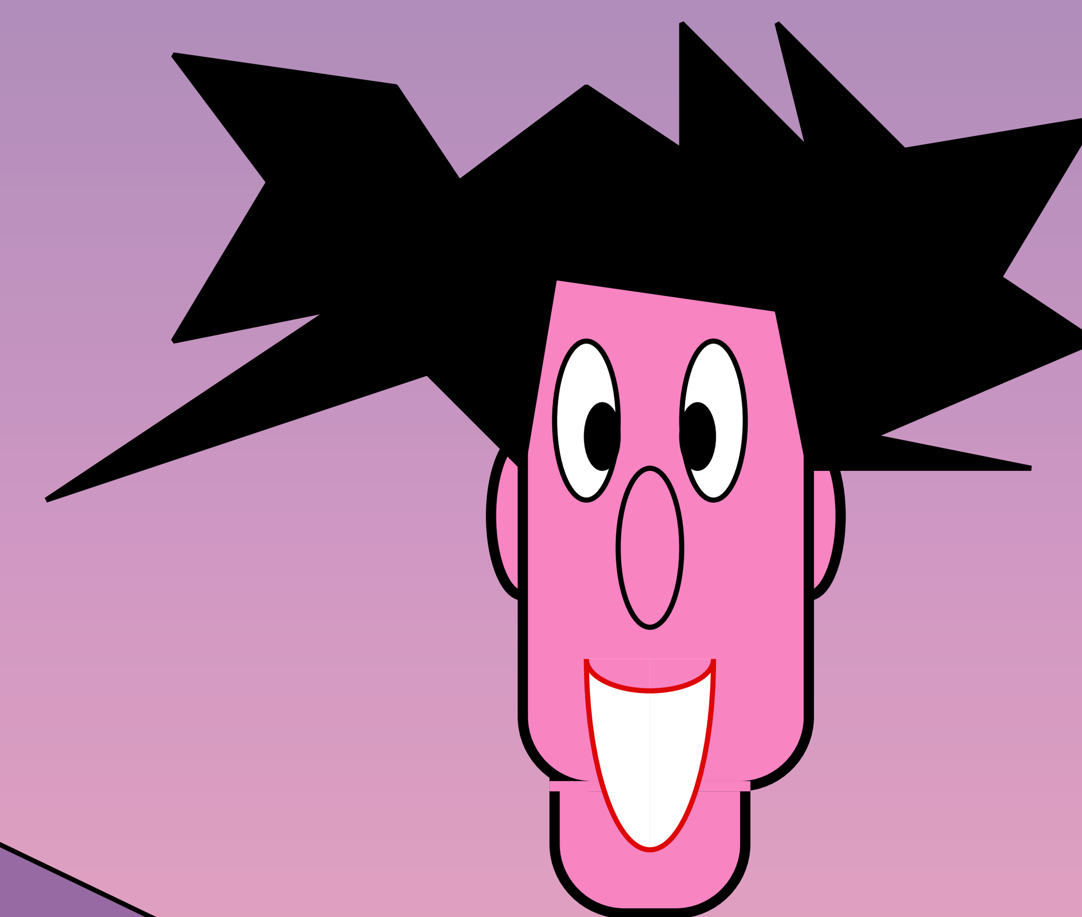
Information Theoretical Security

Vernam's One-Time-Pad

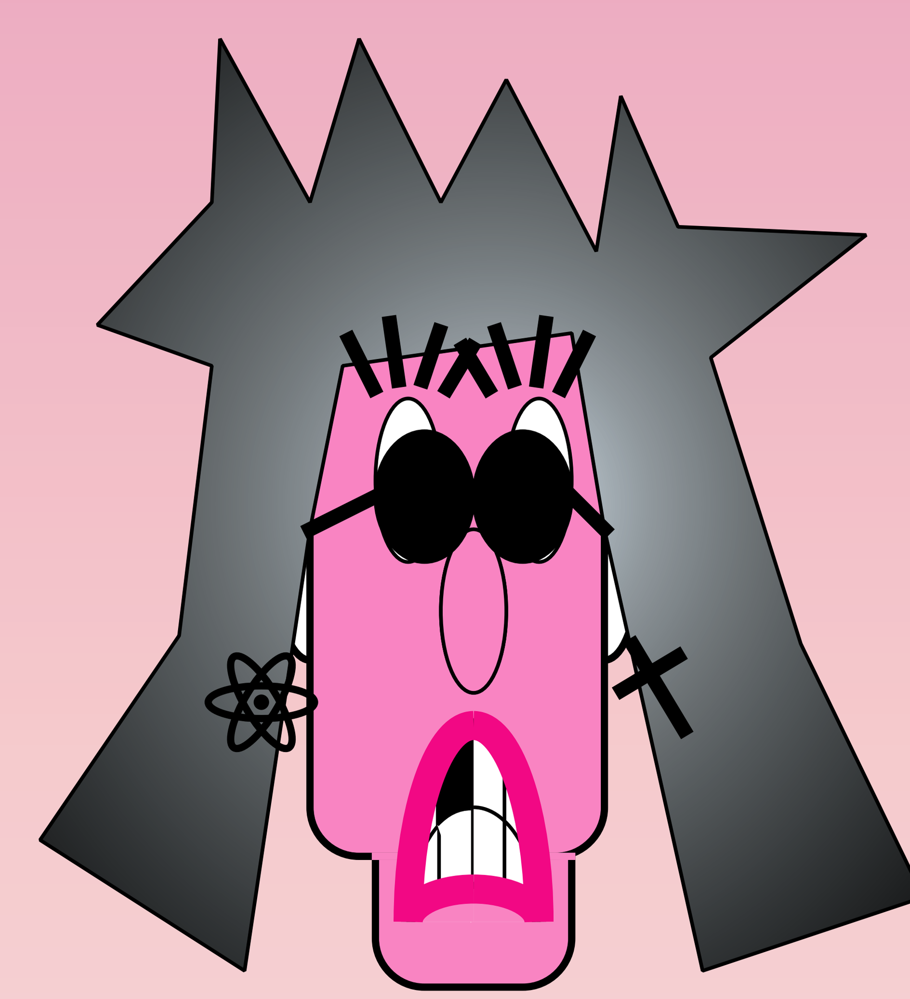
m	⊕ k	= c
1	1	0
0	1	1
1	1	0
0	0	0
0	0	0
1	1	0
0	1	1
0	0	0
1	1	0
1	1	0
1	0	1
1	1	0
1	0	1
0	1	1
0	1	1
1	1	0





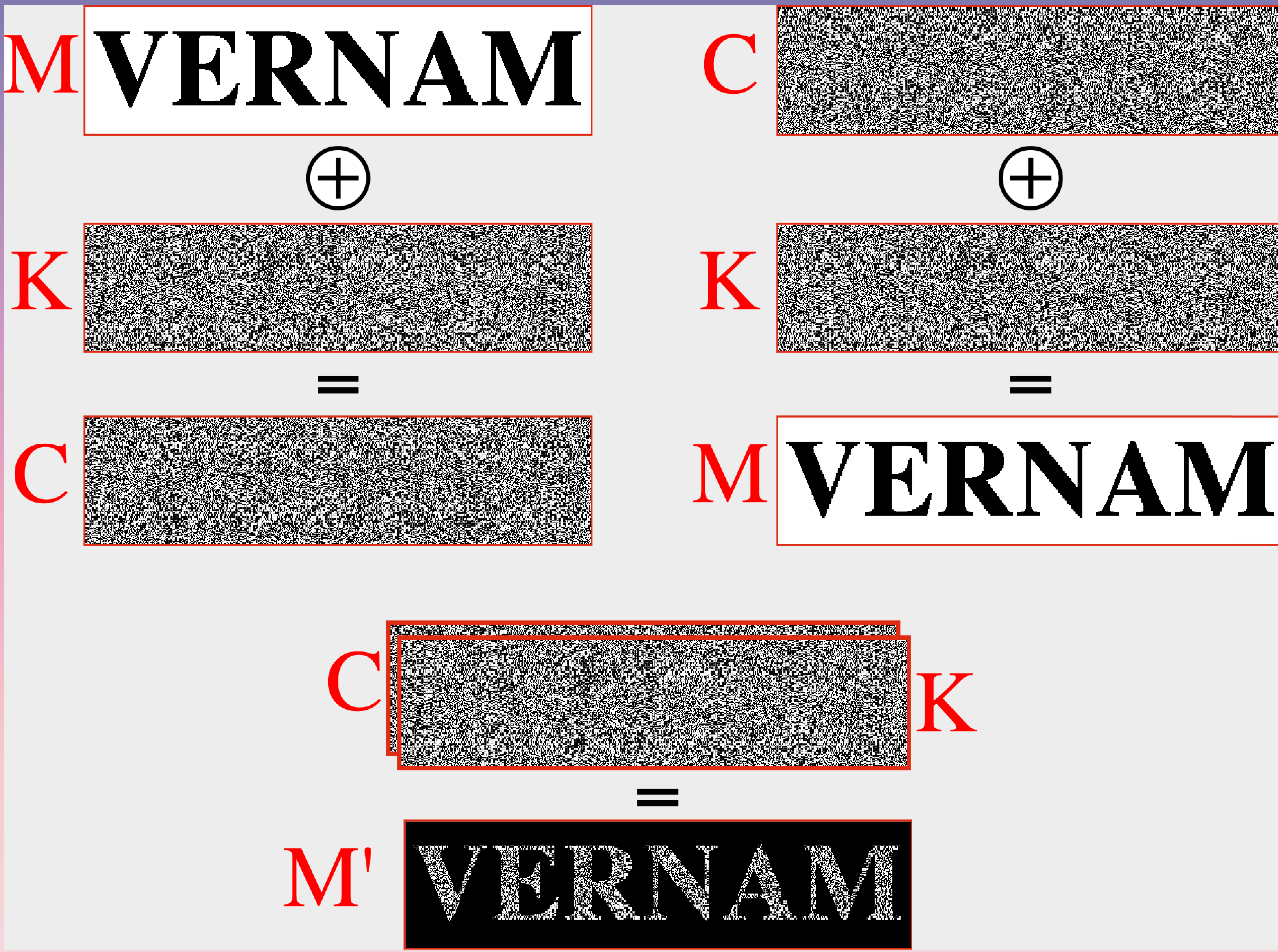


c	⊕ k	=m
0	1	1
1	1	0
0	1	1
0	0	0
0	0	0
0	1	1
1	1	0
0	0	0
0	1	1
0	1	1
1	0	1
0	1	1
1	0	1
1	1	0
1	1	0
0	1	1



Information Theoretical Security

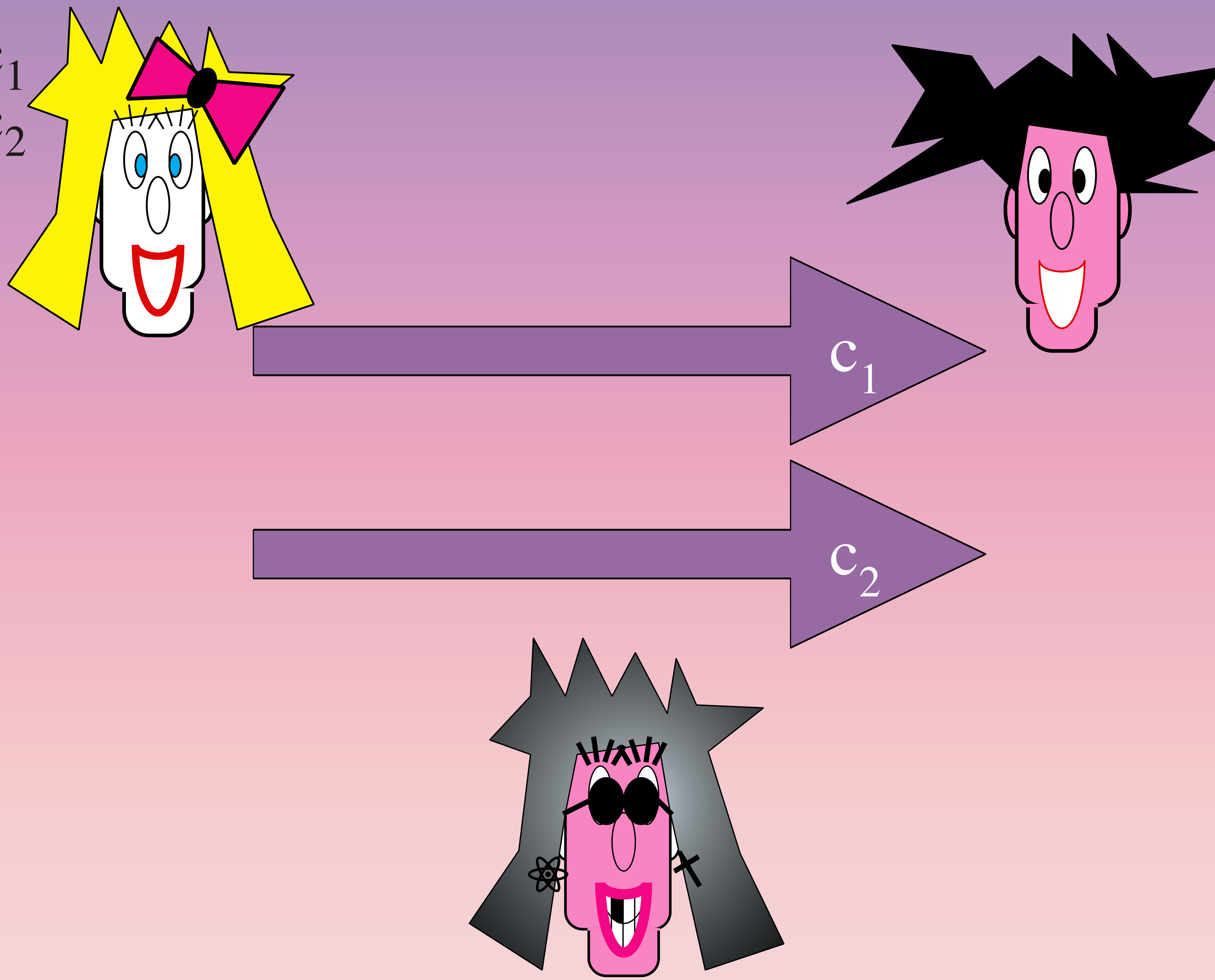
VISUAL DEMO


M
VERNAM
⊕
K
=
C
C
⊕
K
=
M
VERNAM
C
K
=
M'
VERNAM

Vernam's One-Time-Pad

$m_1 \oplus k = c_1$

$m_2 \oplus k = c_2$

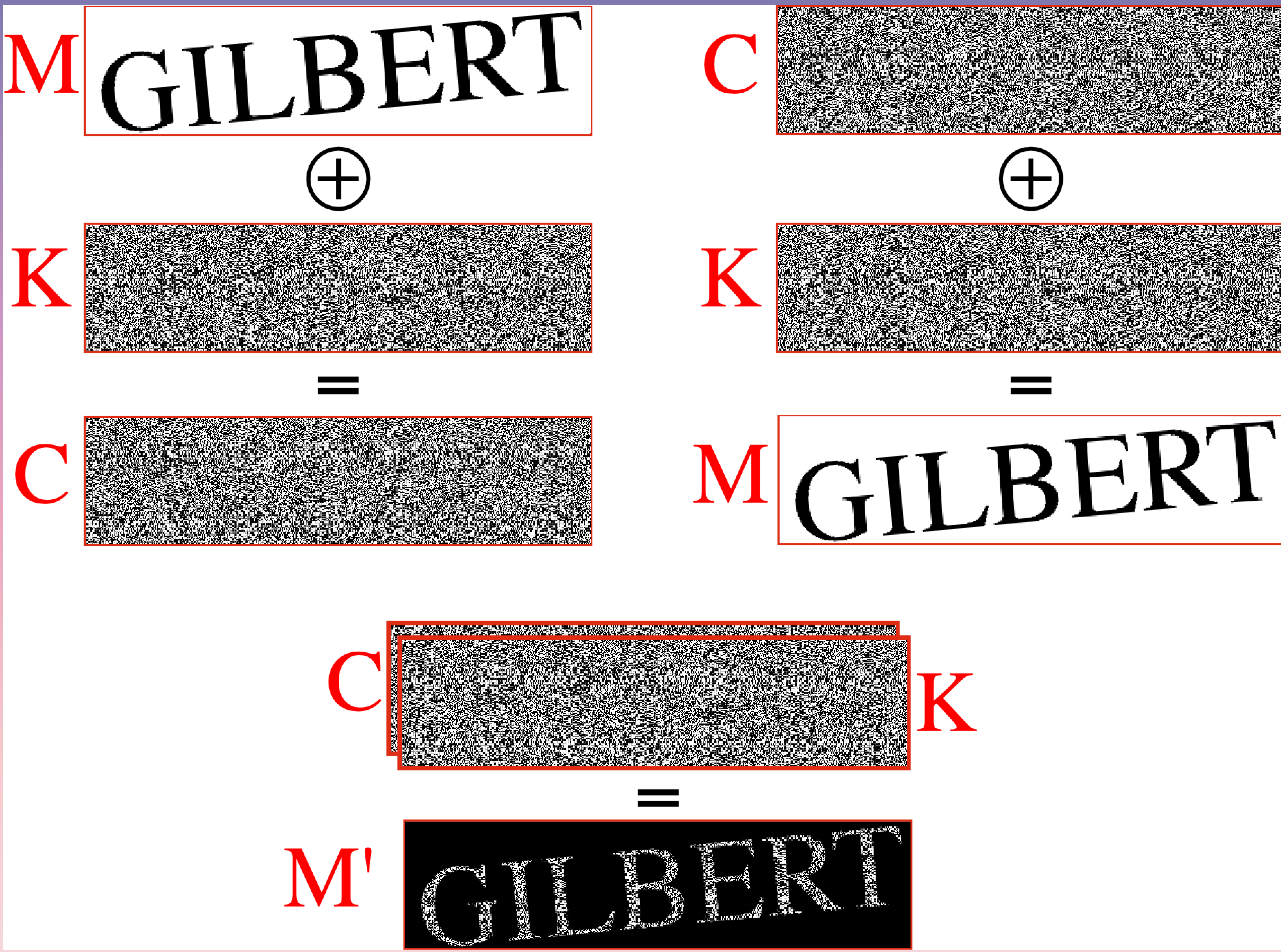


$c_1 \oplus k = m_1$

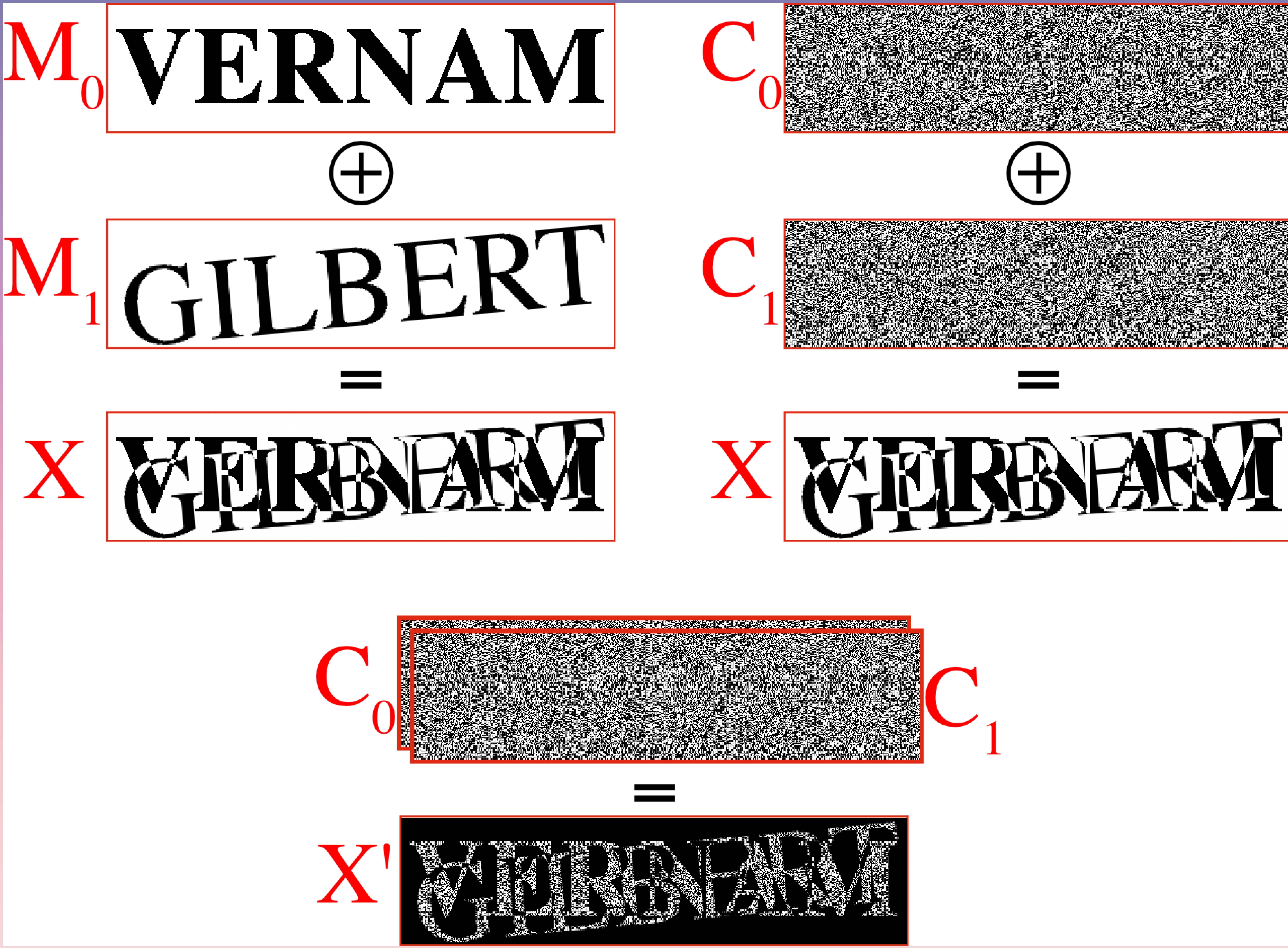
$c_2 \oplus k = m_2$

$c_1 \oplus c_2 = m_1 \oplus m_2$

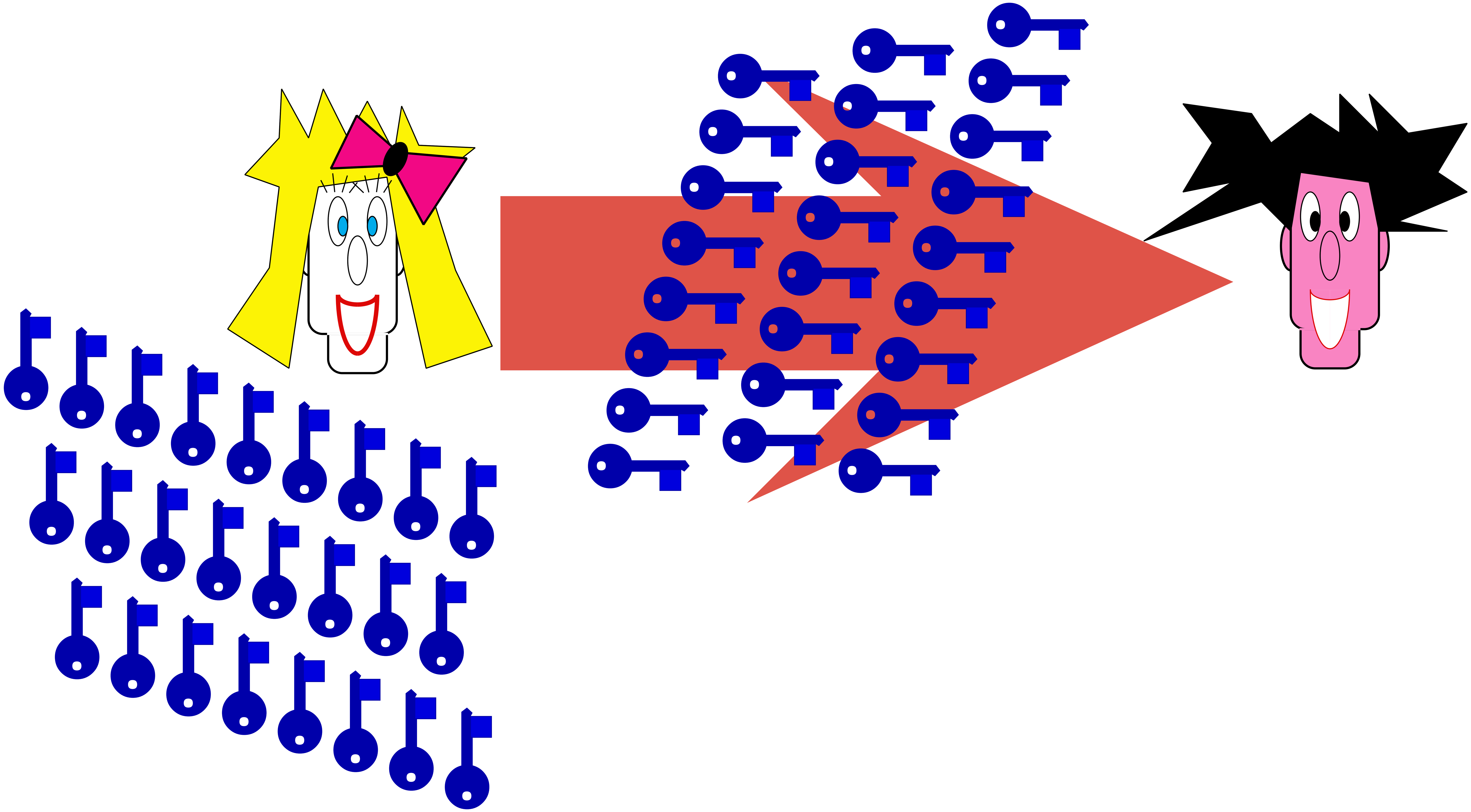
VISUAL DEMO


M
GILBERT
C
K
C
K
M
GILBERT
C
K
M'
GILBERT

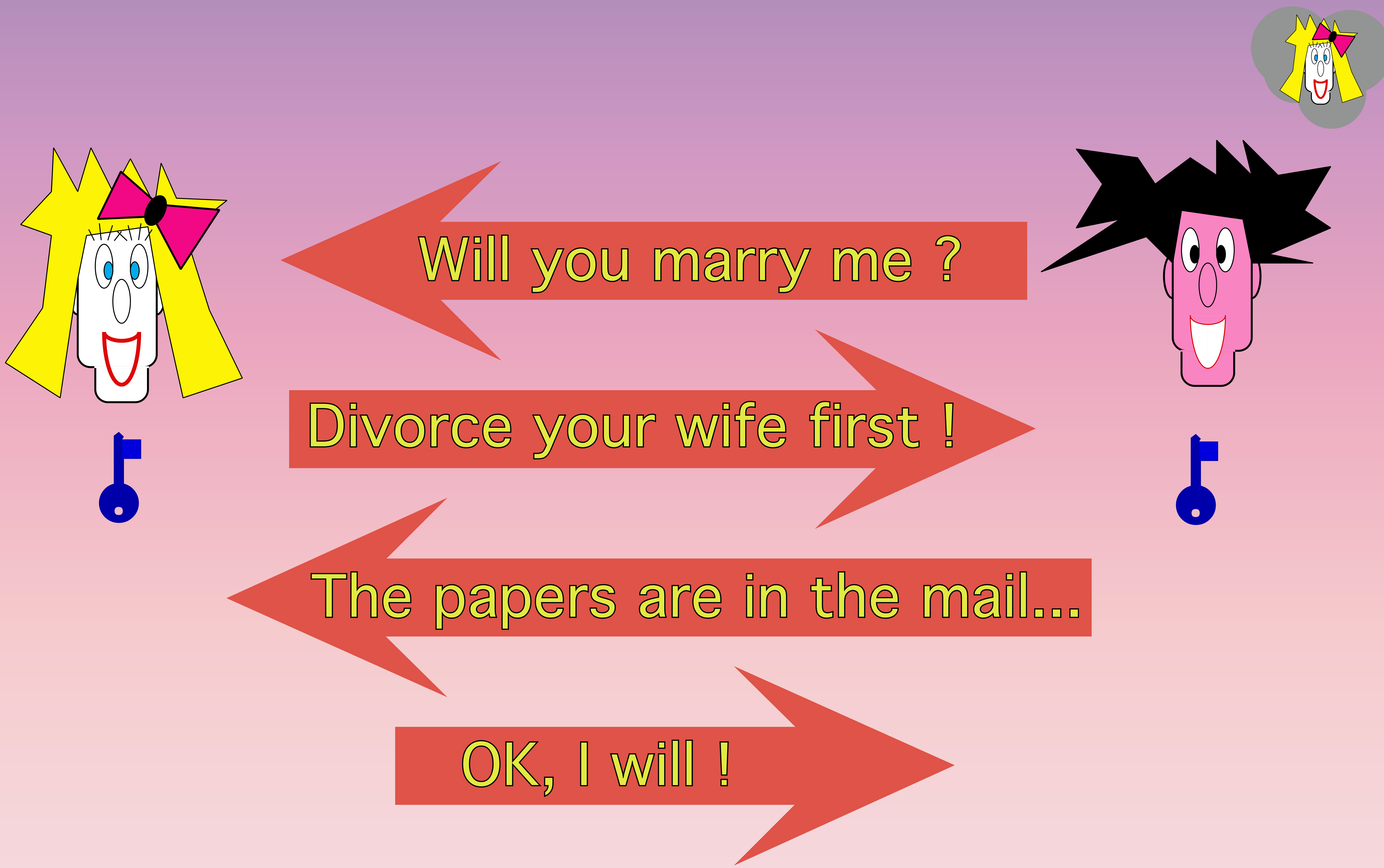
VISUAL DEMO

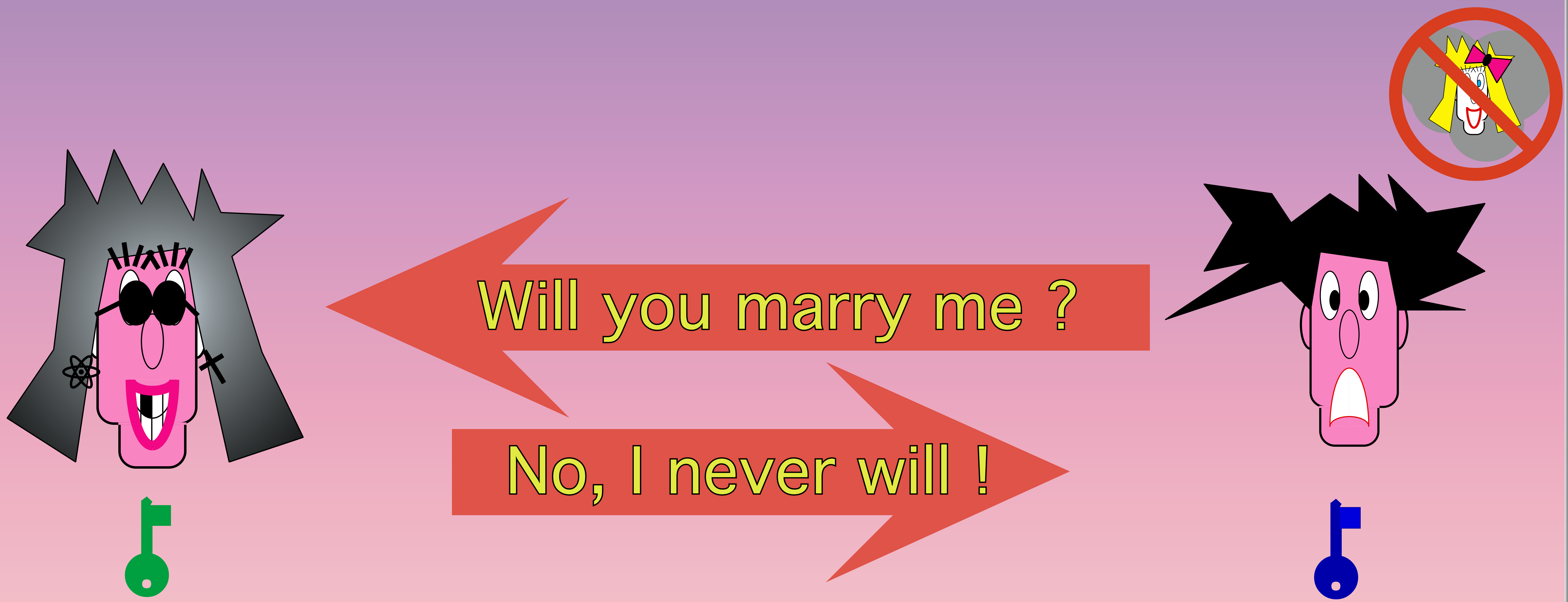

M0
VERNAM
⊕
M1
GILBERT
=
X
C0
⊕
C1
=
X
C0
C1
=
X'

(1.1.1) key distribution PROBLEM

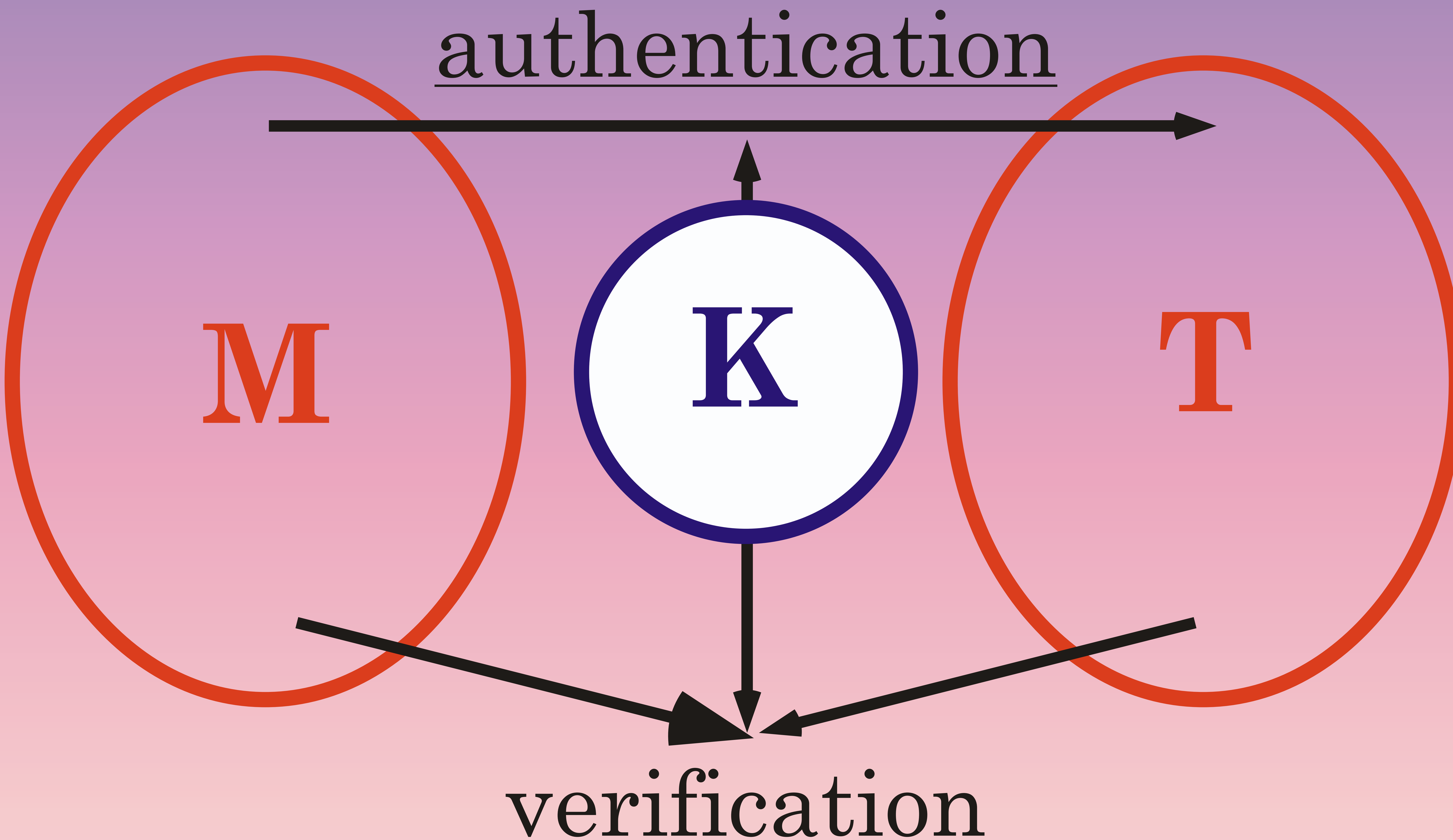


(1.1.3) Authentication



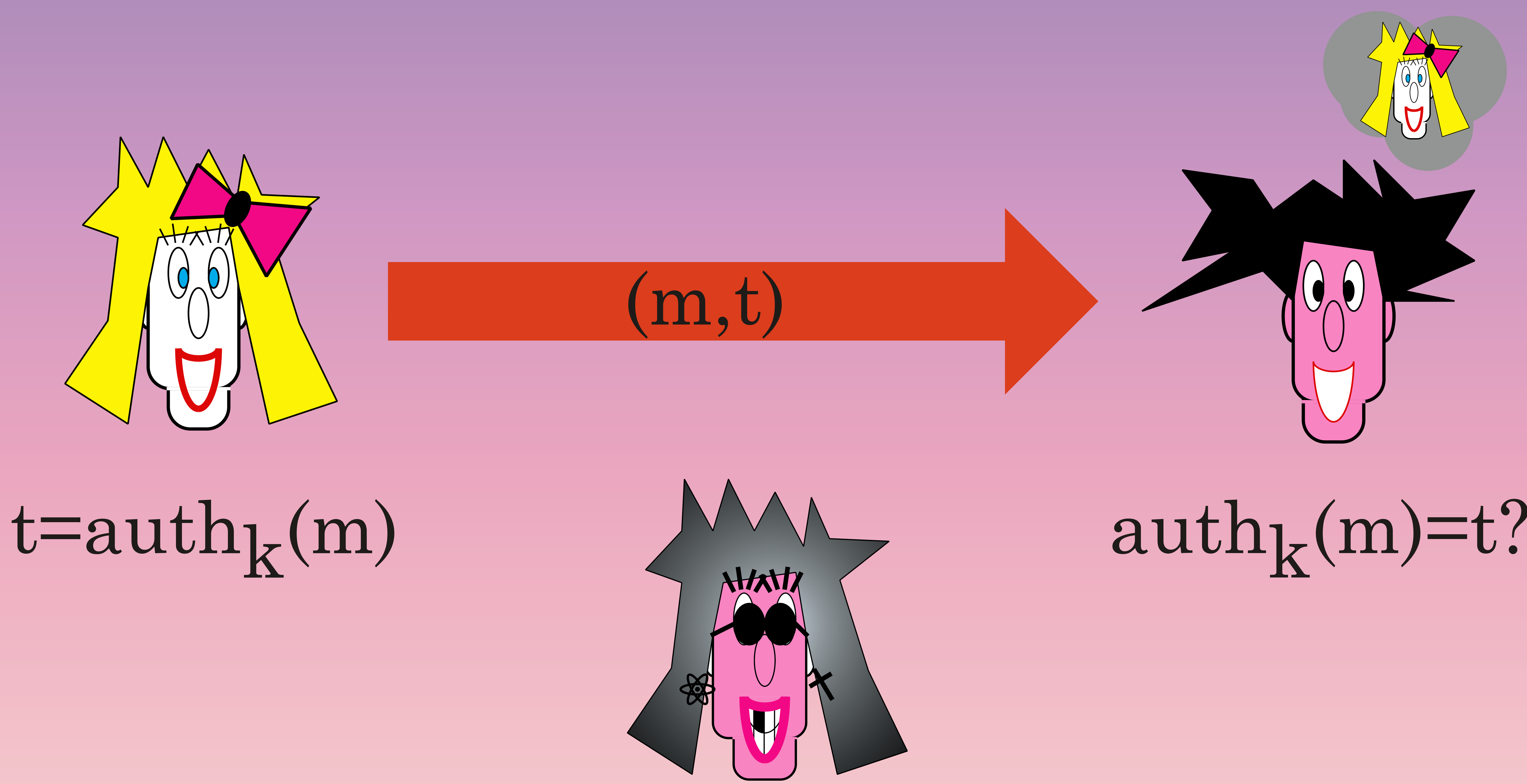

Will you marry me ?
No, I never will !

symmetric authentication



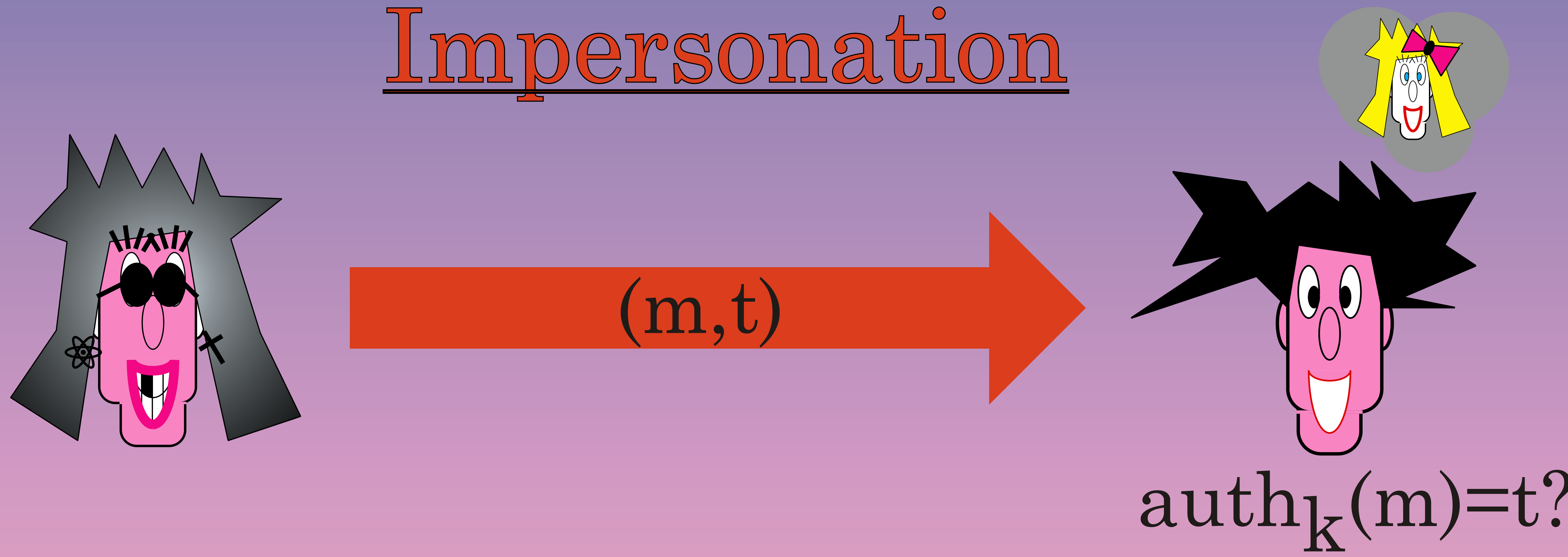
Information Theoretical Security

Authentication

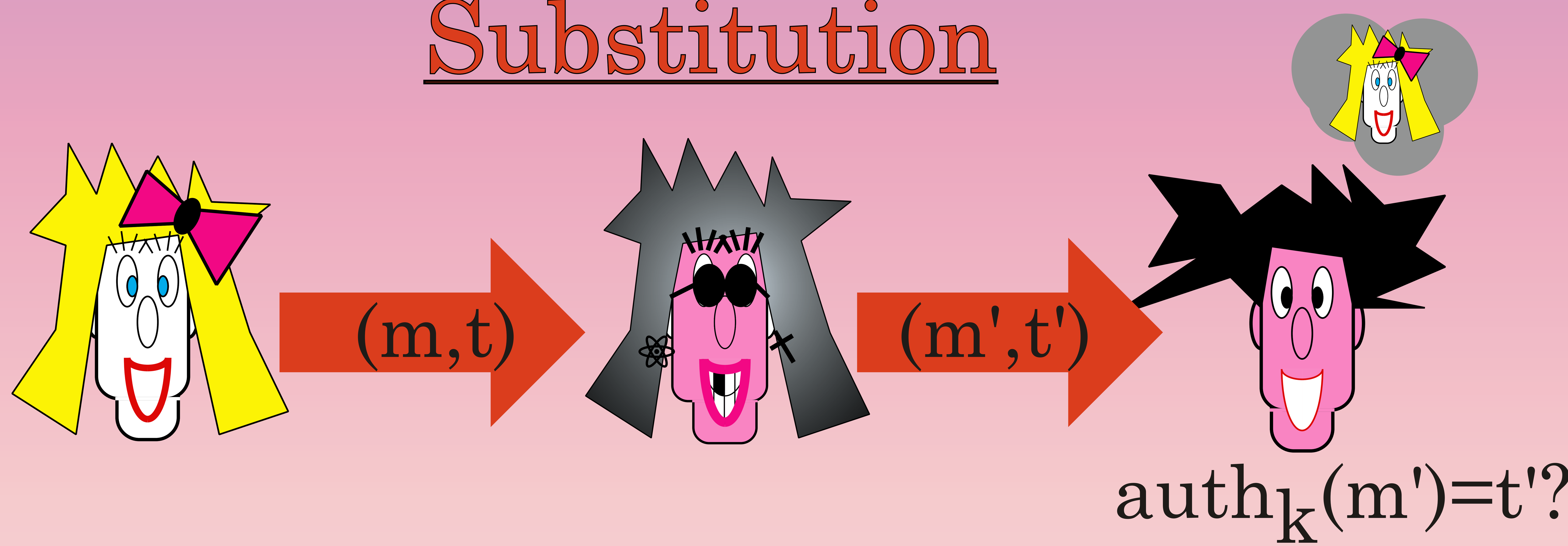


Information Theoretical Security

Impersonation



Substitution



Information Theoretical Security

WC One-Time-Authentication

$$auth_{\mathbf{M},b}(x) = \mathbf{M}x \oplus b$$

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

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

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

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

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

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

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

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

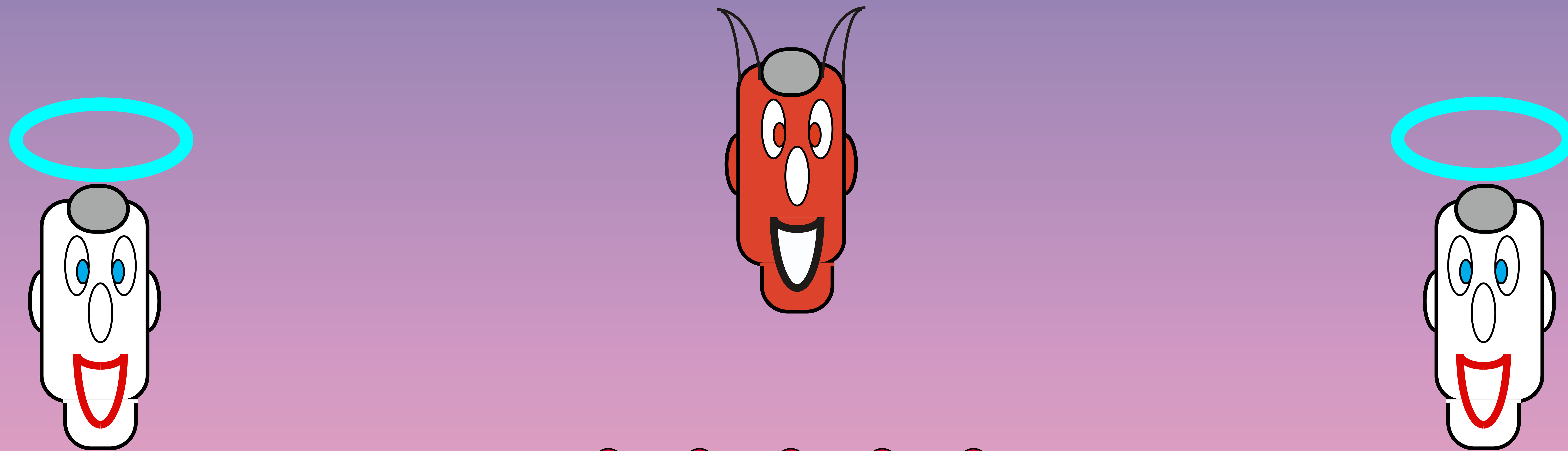
$G=[\mathbf{I}:\mathbf{M}]$ (systematic) generating matrix of error correcting code

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

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

(1.2) Complexity Theoretical Cryptography

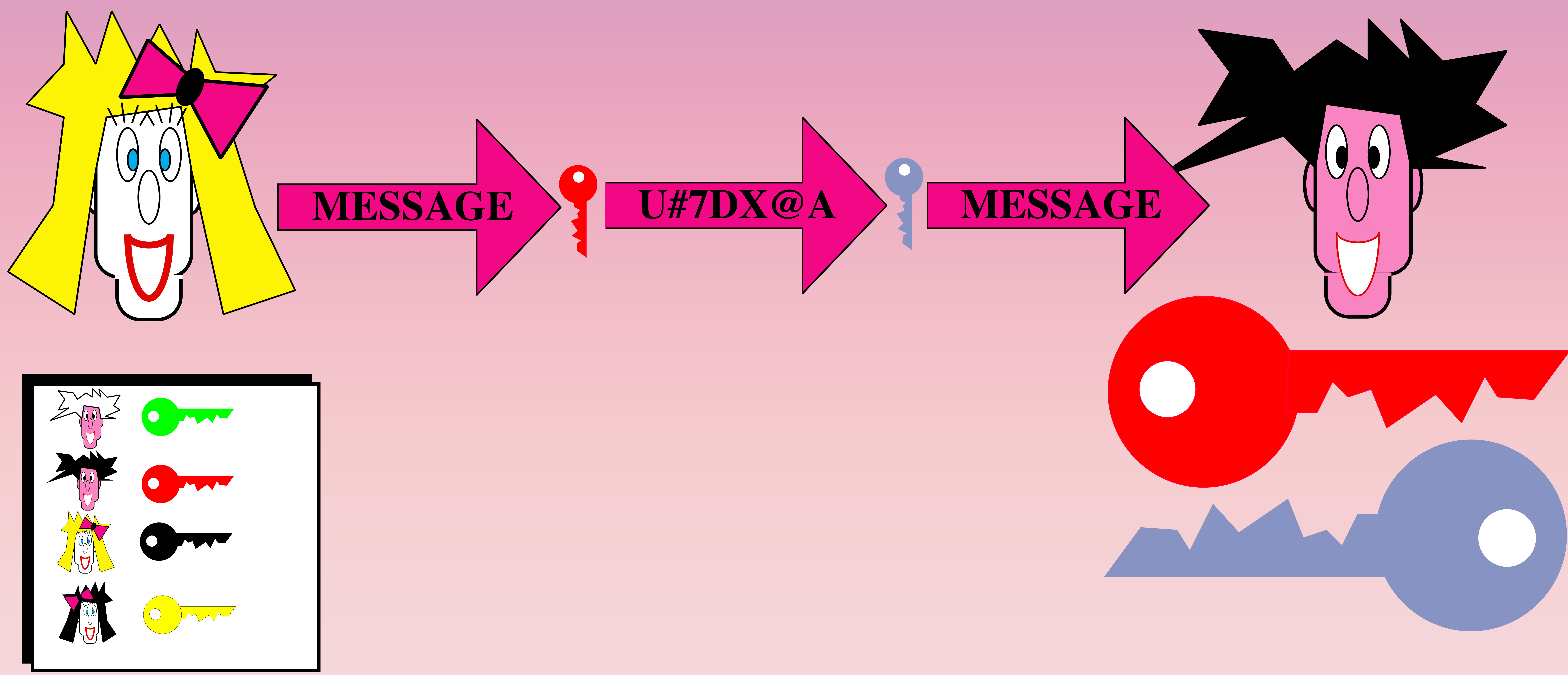
(1.2) Complexity Theoretical Cryptography



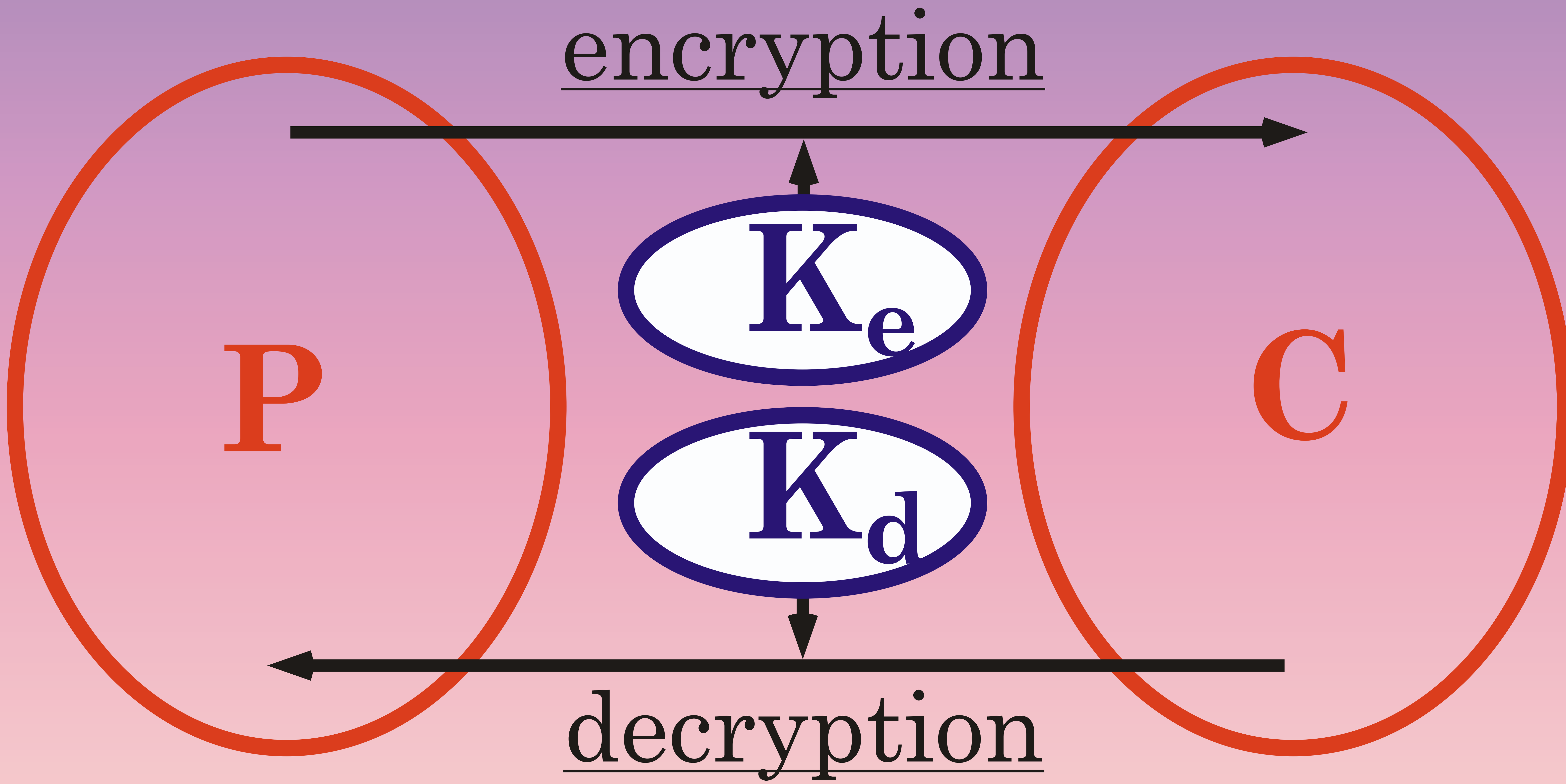
(1.2.1) Public key cryptosystem

(1.2.2) Digital signature scheme

(1.2.1) Public key cryptosystem



asymmetric encryption
(public-key cryptography)



Complexity Theoretical Security

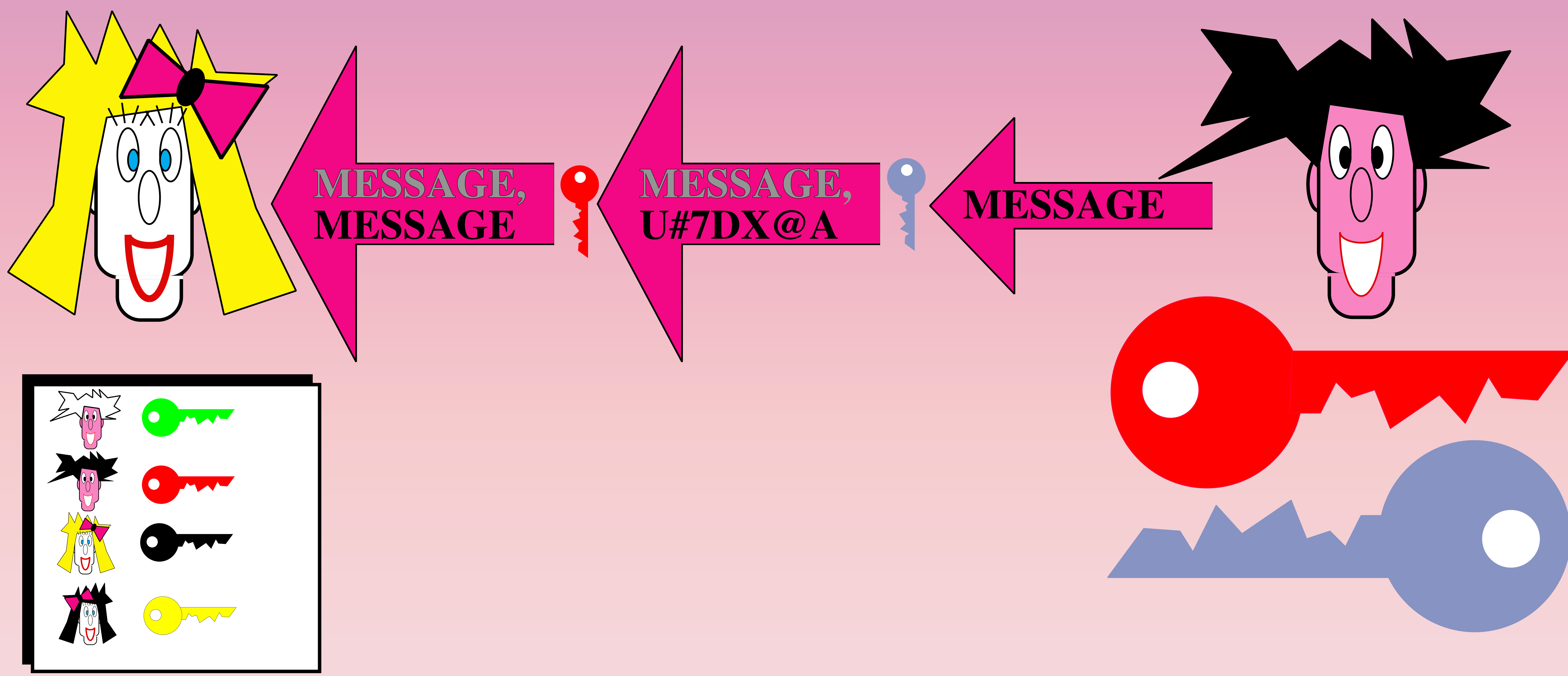
RSA public-key cryptosystem

- $n = p*q$,   two large primes
- e s.t. $\gcd(e,(p-1)(q-1))=1$
- d s.t. $e*d = 1$ **mod** $(p-1)(q-1)$

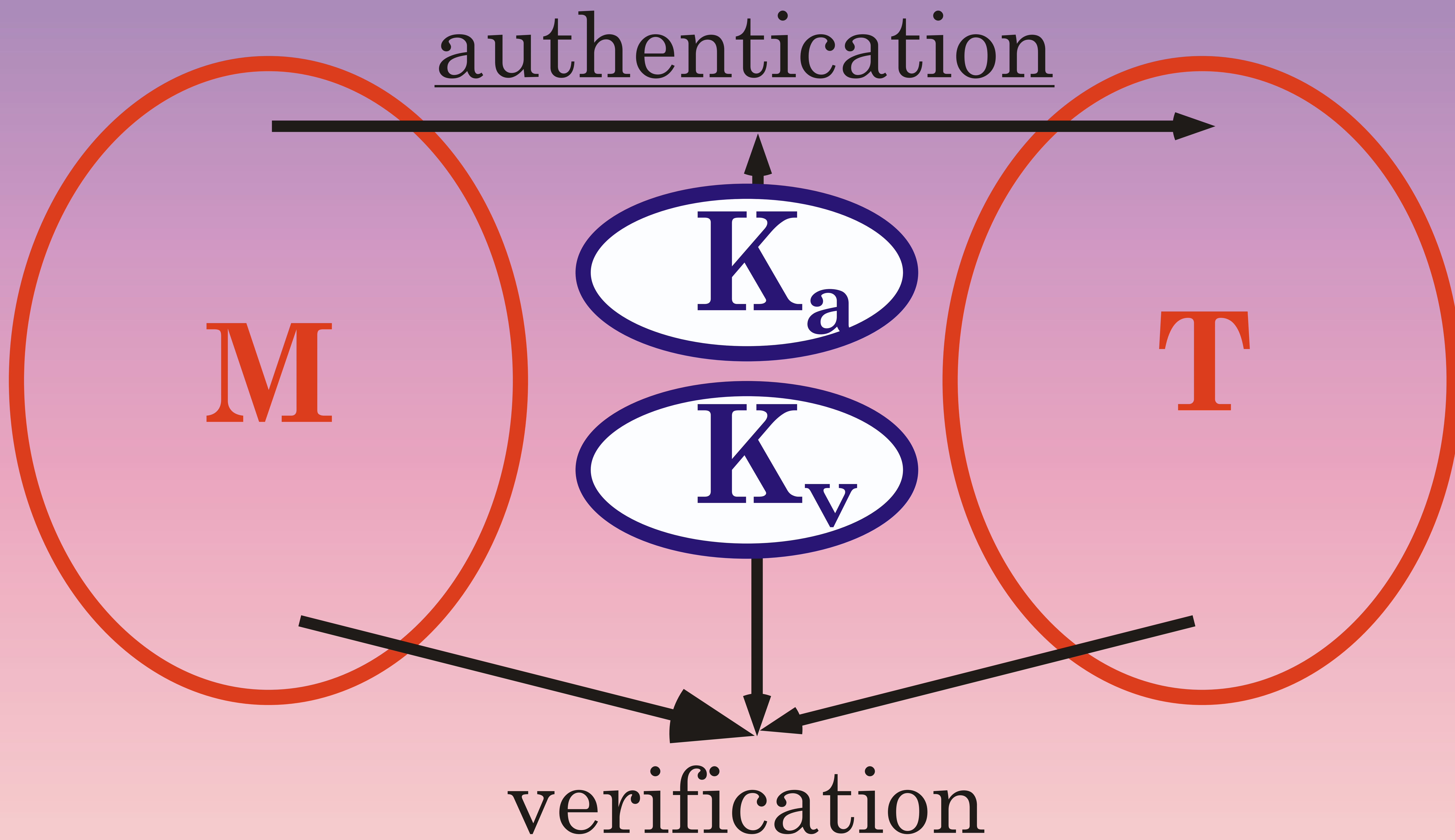
- $K_e = (n,e)$, $K_d = (n,d)$

- **encryption** $E(m)$: m^e **mod** n
- **decryption** $D(c)$: c^d **mod** n

(1.2.2) Digital signature scheme



asymmetric authentication
(digital signature schemes)



Complexity Theoretical Security

RSA digital signature

- $n = p*q$,   two large primes
- e s.t. $\gcd(e,(p-1)(q-1))=1$
- d s.t. $e*d = 1 \textbf{ mod } (p-1)(q-1)$

- $K_a = (n,d)$, $K_v = (n,e)$

- **authentication** $A(m)$: $m^d \textbf{ mod } n$
- **verification** $V(m,t)$: $t^e \stackrel{?}{\equiv} m \textbf{ mod } n$

(2) Quantum Information & Computations

Bits & QuBits

0:

1:

θ = Cos_θ + Sin_θ

$|\Psi\rangle$ = 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}

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


Albert Einstein

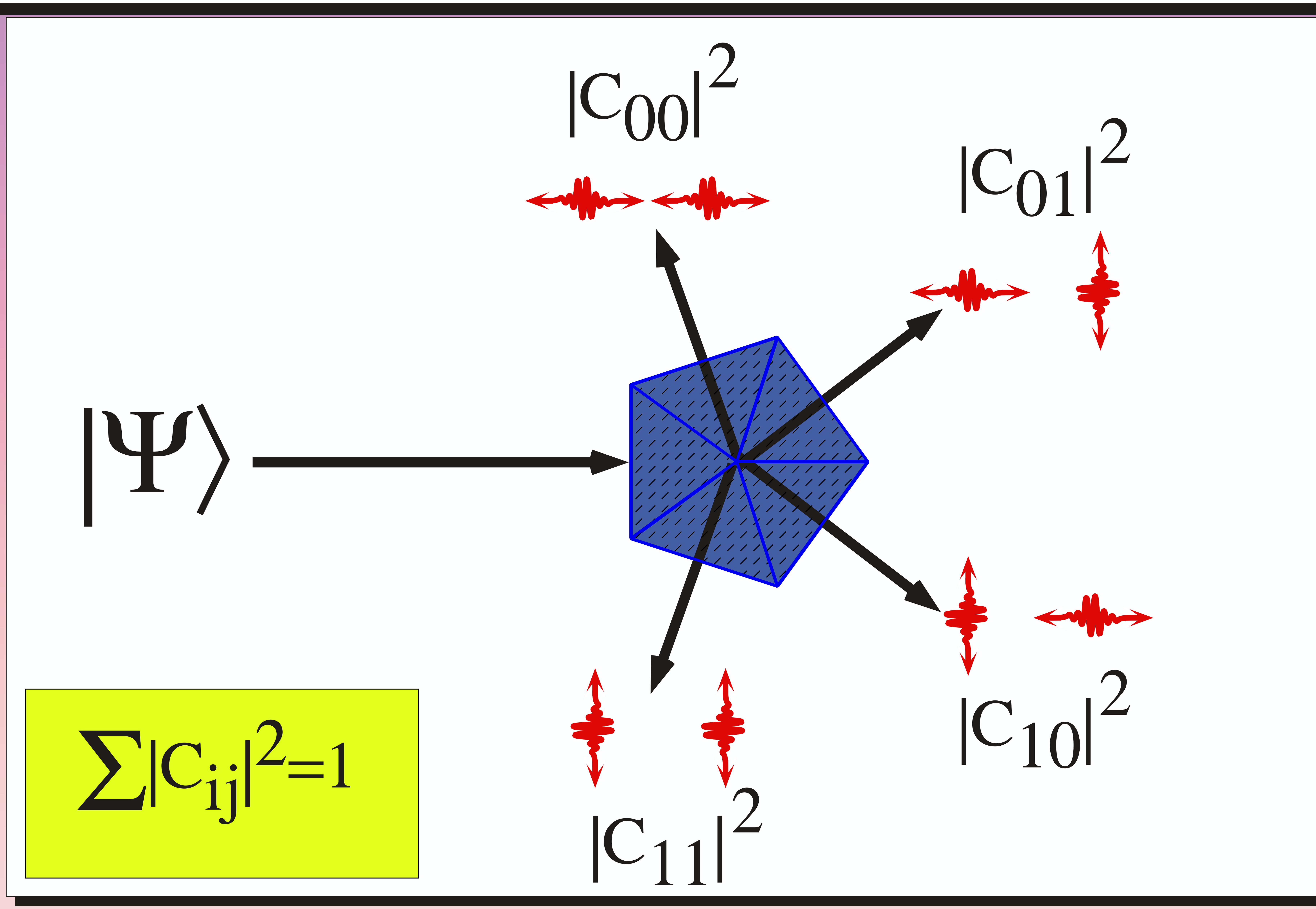

Boris Podolsky


Nathan Rosen

EPR

Quantum Measurements

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



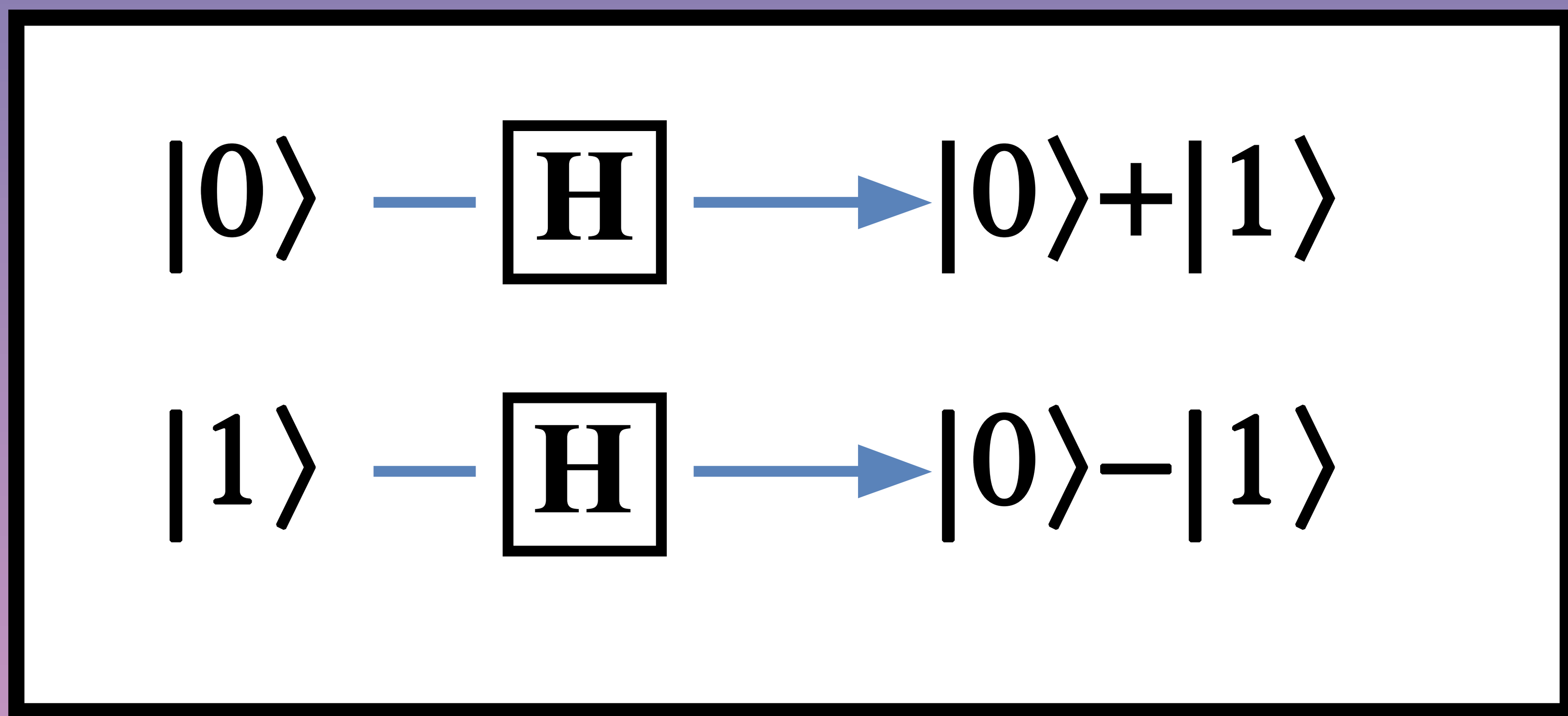
Quantum Evolution: Unitary Operators

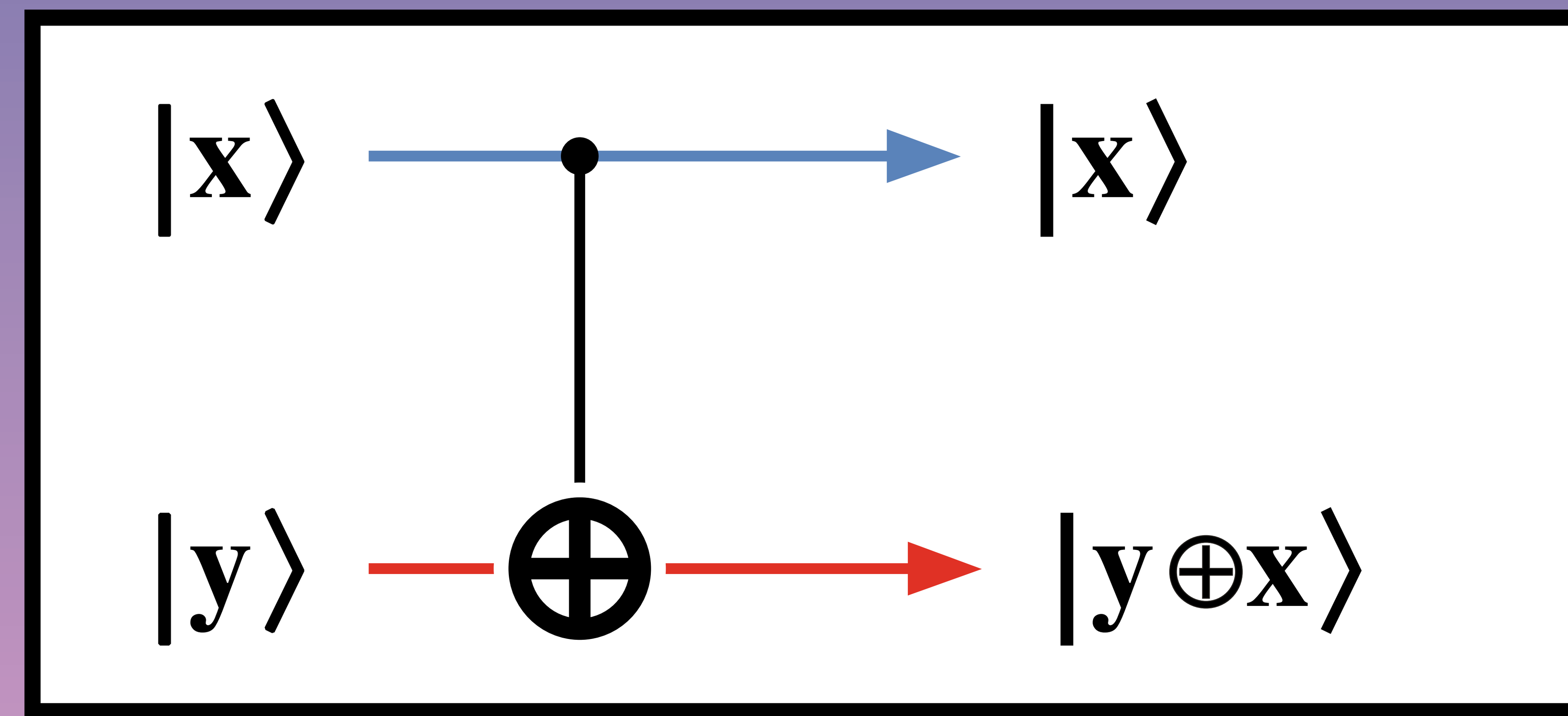
$$|\Psi\rangle \xrightarrow{\boxed{U}} |\Psi'\rangle$$

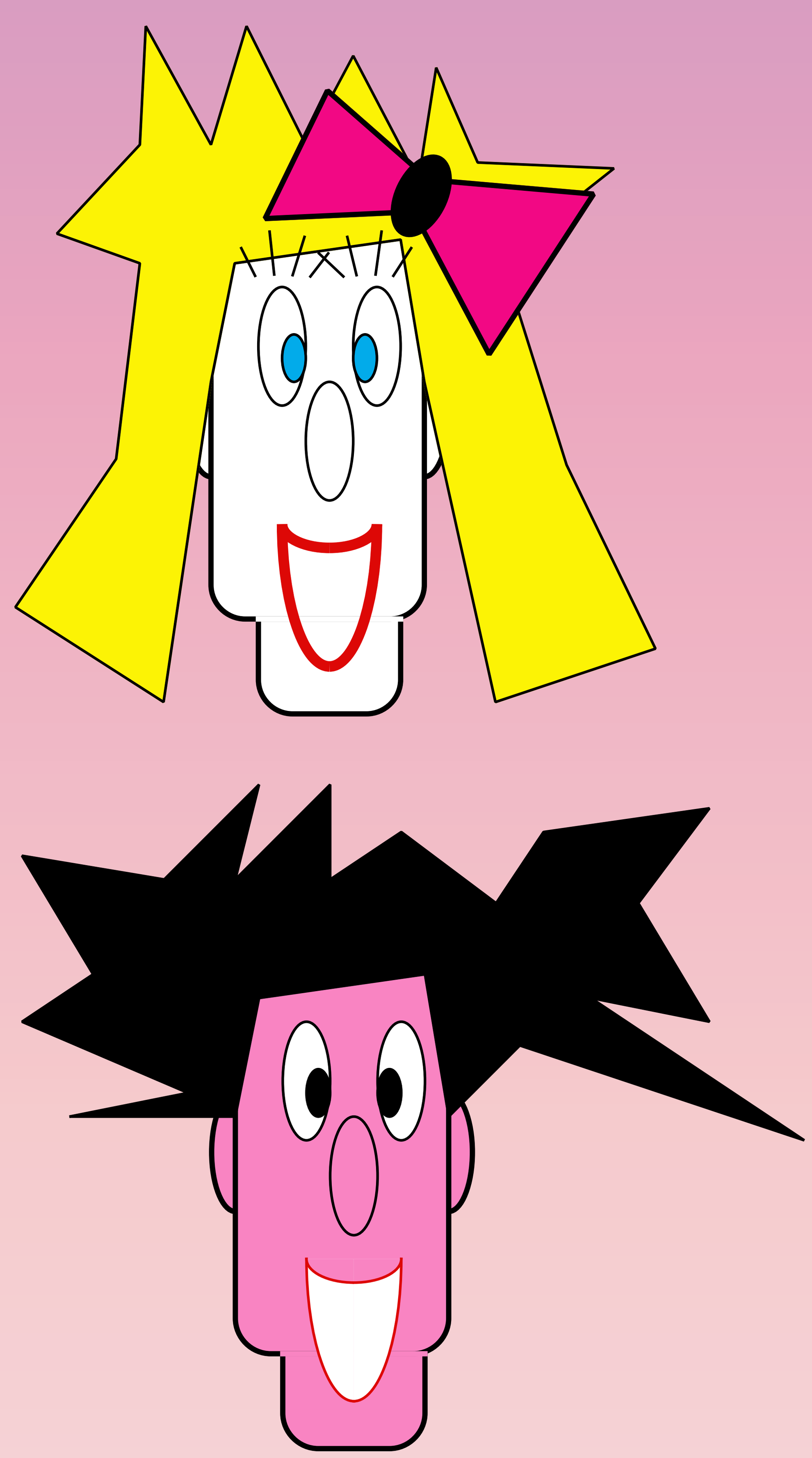
 $\xrightarrow{\boxed{U}} |\Psi_0\rangle$

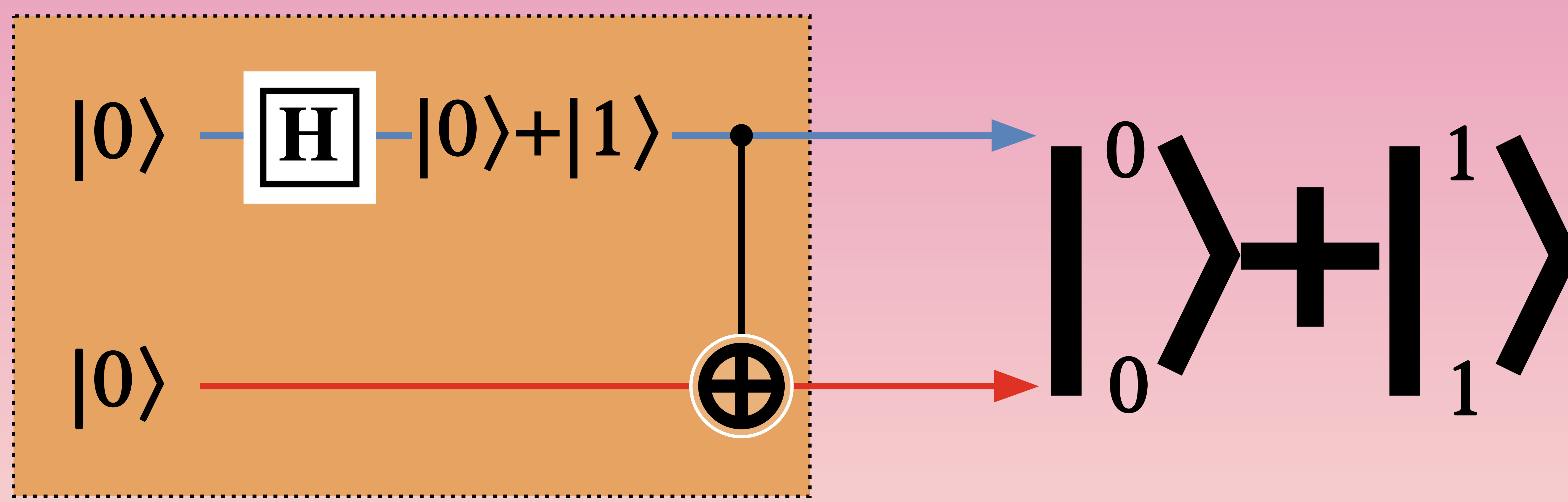
 $\xrightarrow{\boxed{U}} |\Psi_1\rangle$

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



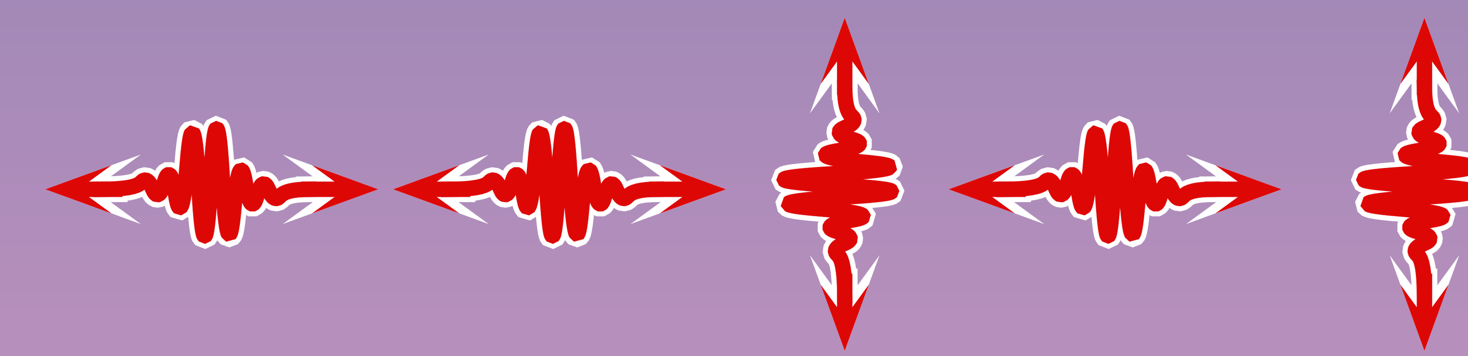






$$|??\rangle$$

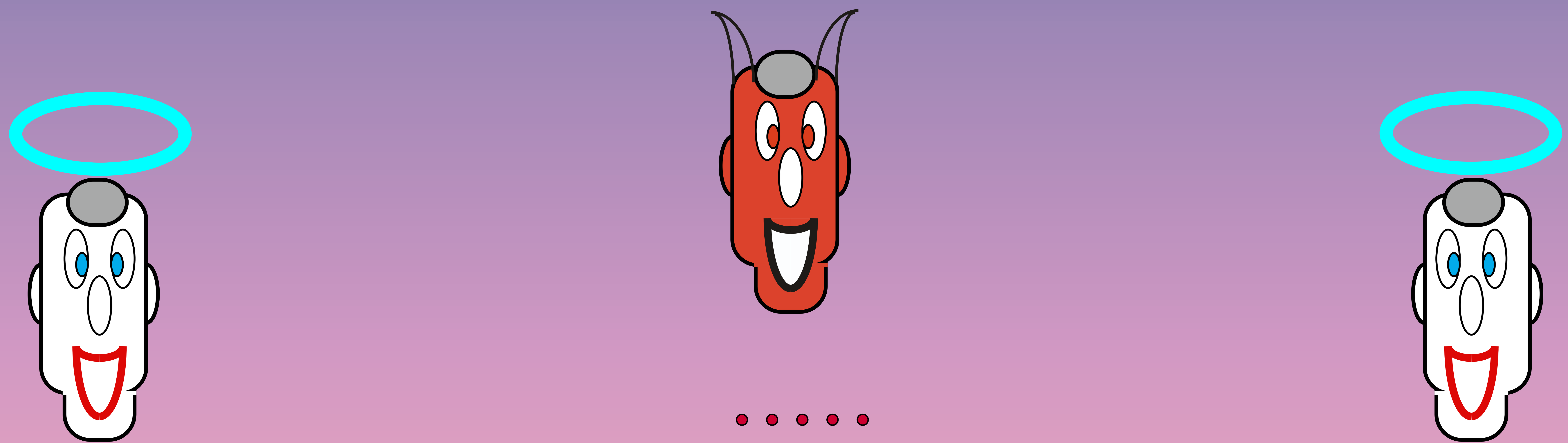
Classical & Quantum Information

00110111000110 Classical		Quantum 
Copying:	Yes	NO
Measuring:	Yes	partial
Broadcasting:	Yes	NO
Superposing:	NO	Yes
Interfering:	NO	Yes

(3)
Quantum Cryptography

(3.1) Information Theoretical Quantum Cryptography

(3.1) Information Theoretical Cryptography



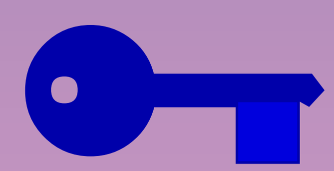
(3.1.1) Key distribution : Q-key distribution +
Q-distillation (formerly purification)

(3.1.2) One-time pad : one-time Q-pad (Q-teleportation)
Vernam Q-cipher

(3.1.3) one-time authentication : authenticated Q-teleportation +
one-time Q-authentication

(3.1.1) Key distribution

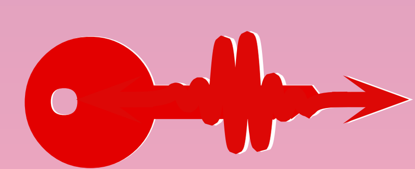
Classical key : Q-distribution of keys(BB84)



+ error-correction

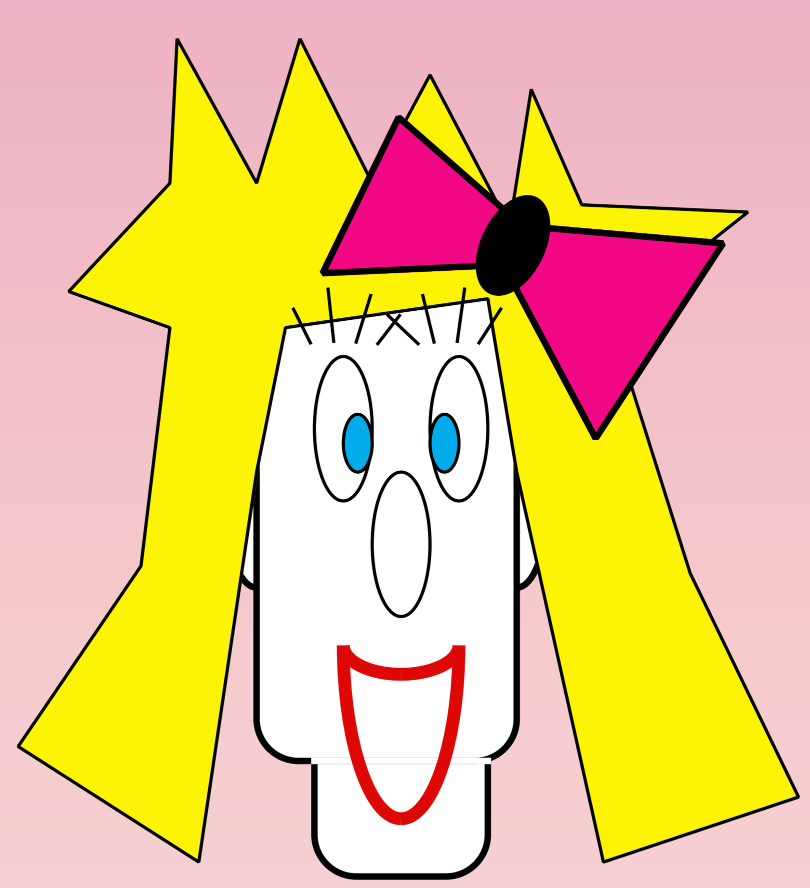
+ privacy amplification

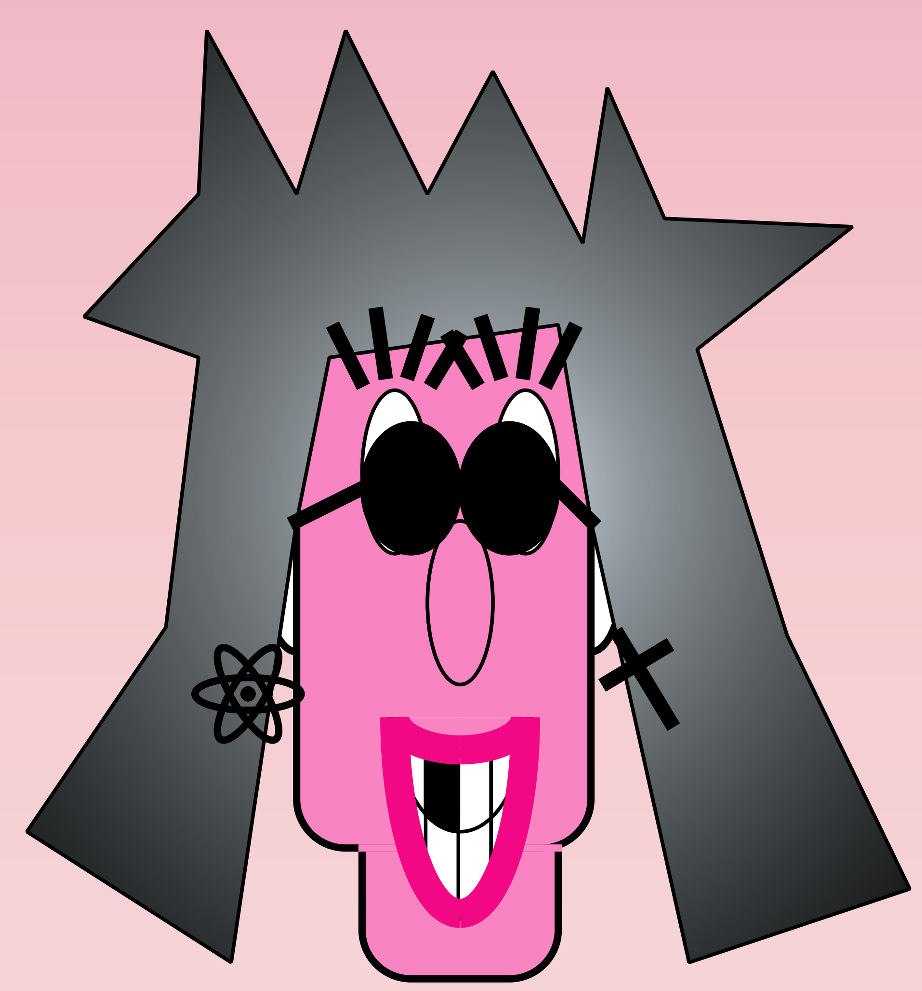
Quantum key : Q-key distribution(Ekert/Lo-Chau)

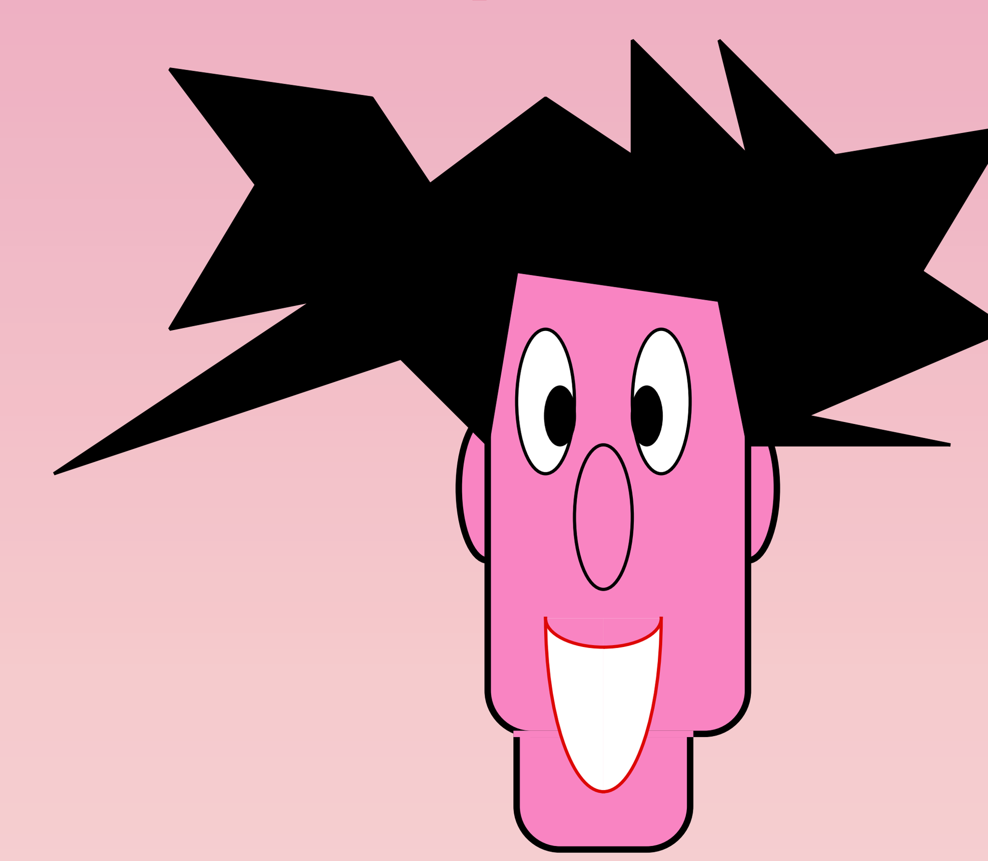


+ Q-error-correction (CSS) or

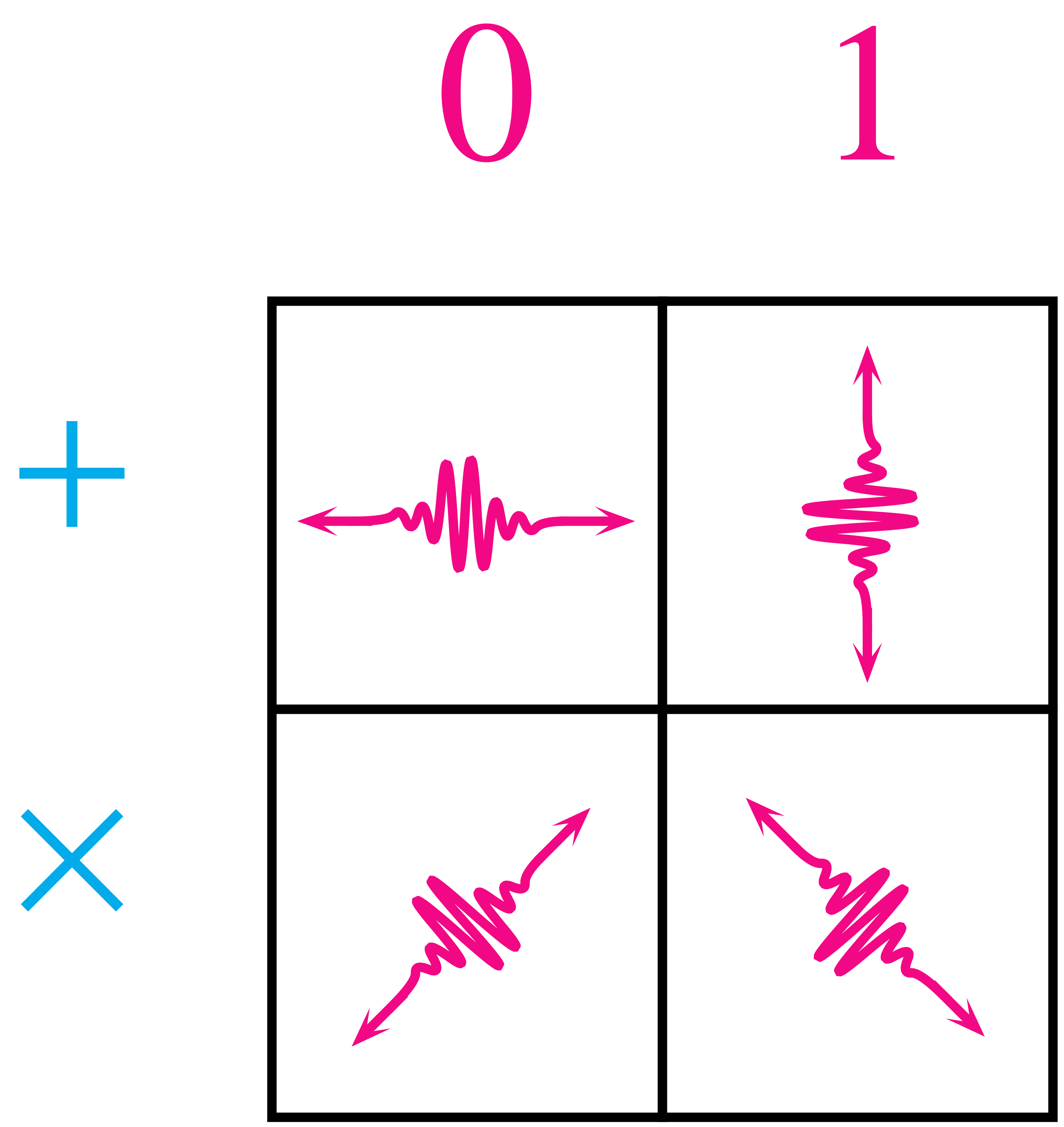
+ Q-Distillation (Purification)





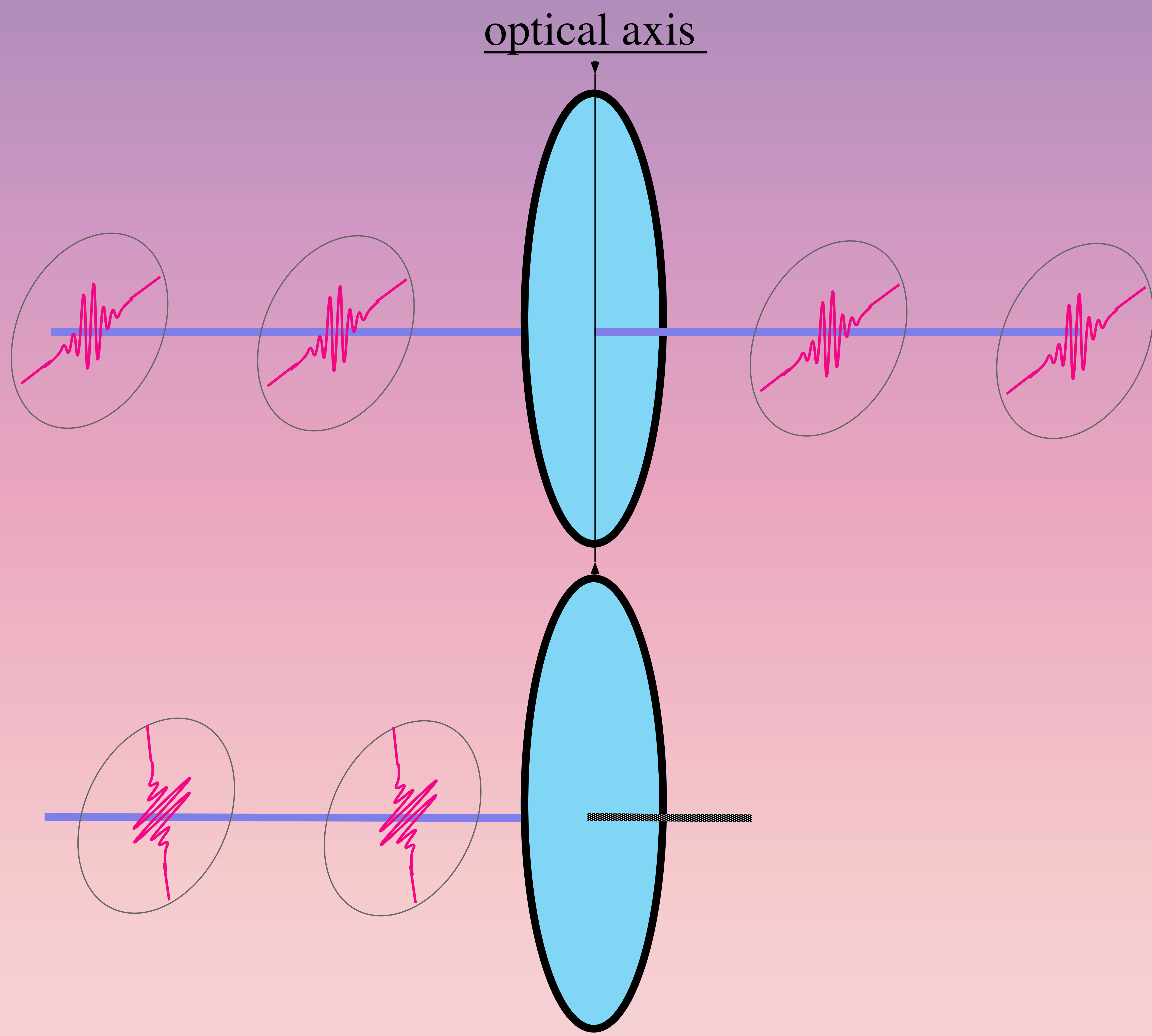


Ambiguous Coding Scheme

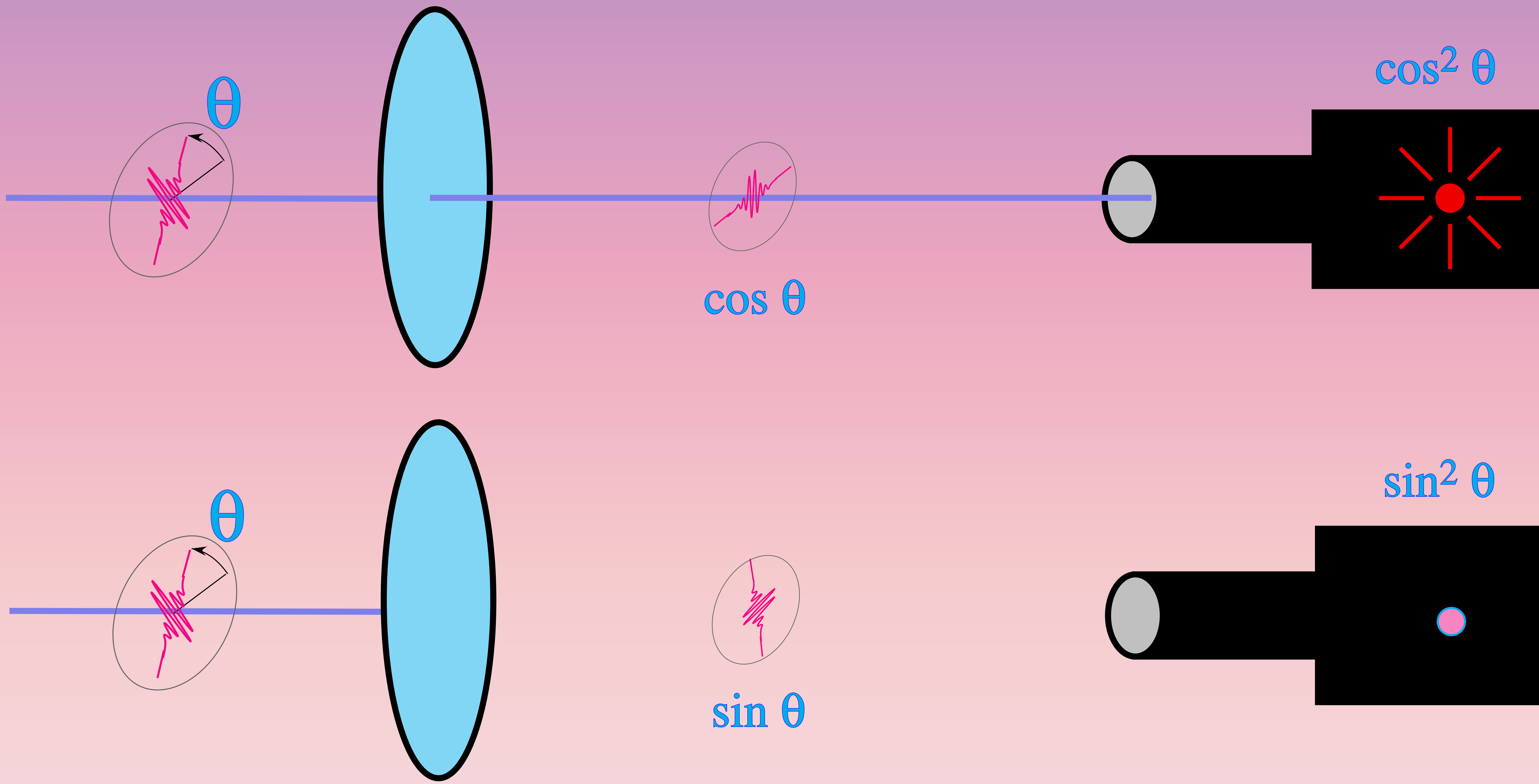


VISUAL DEMO

Polarizing Filter

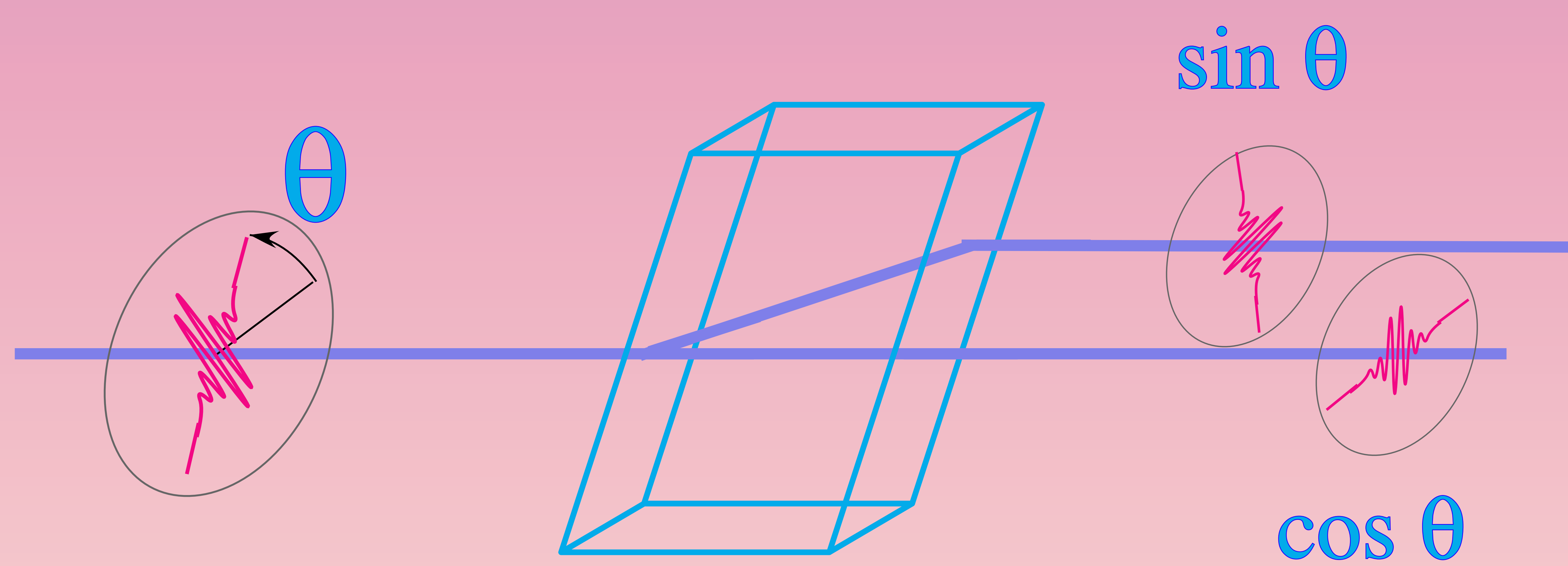


Polarizing Filter and photodetectors

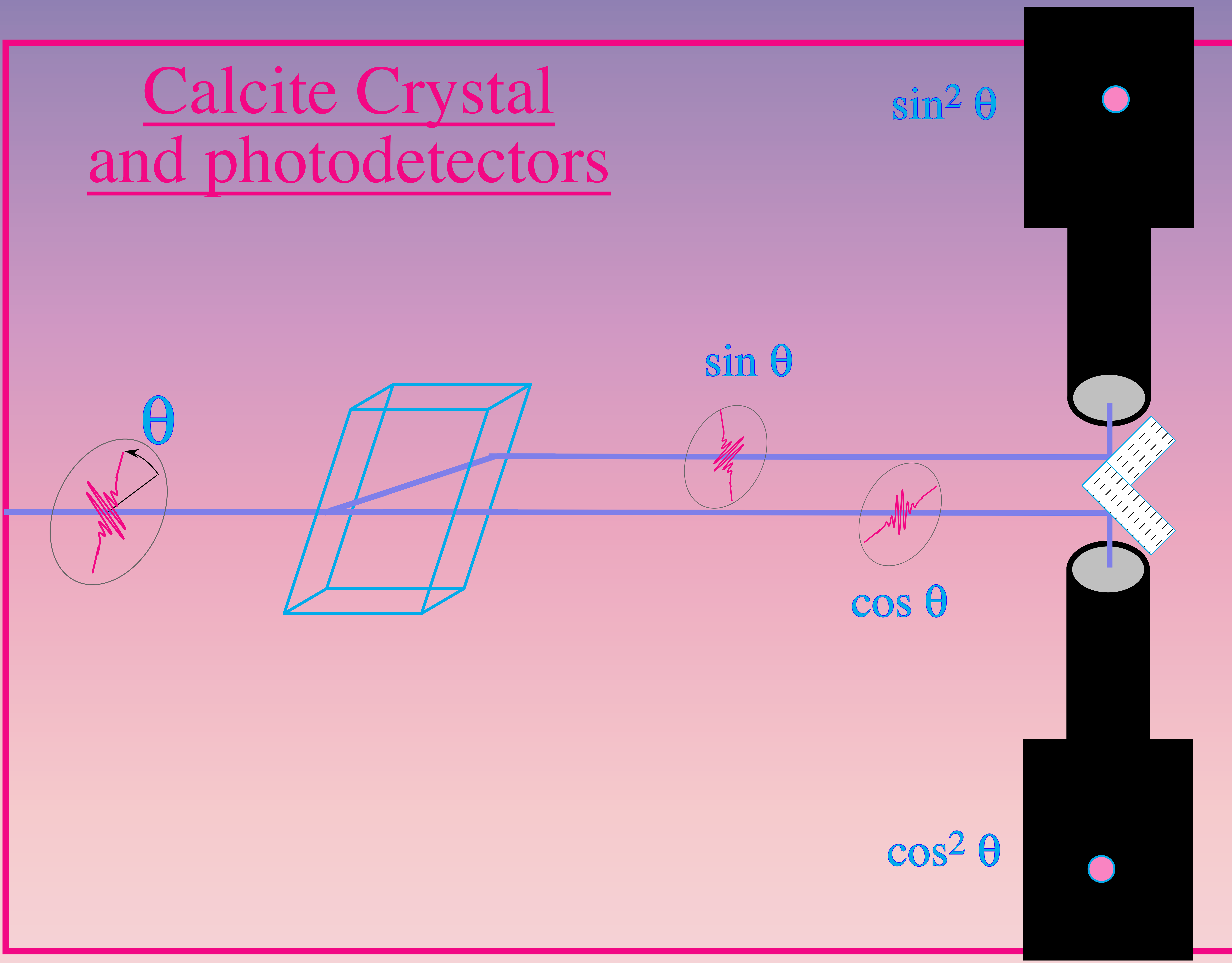


VISUAL DEMO

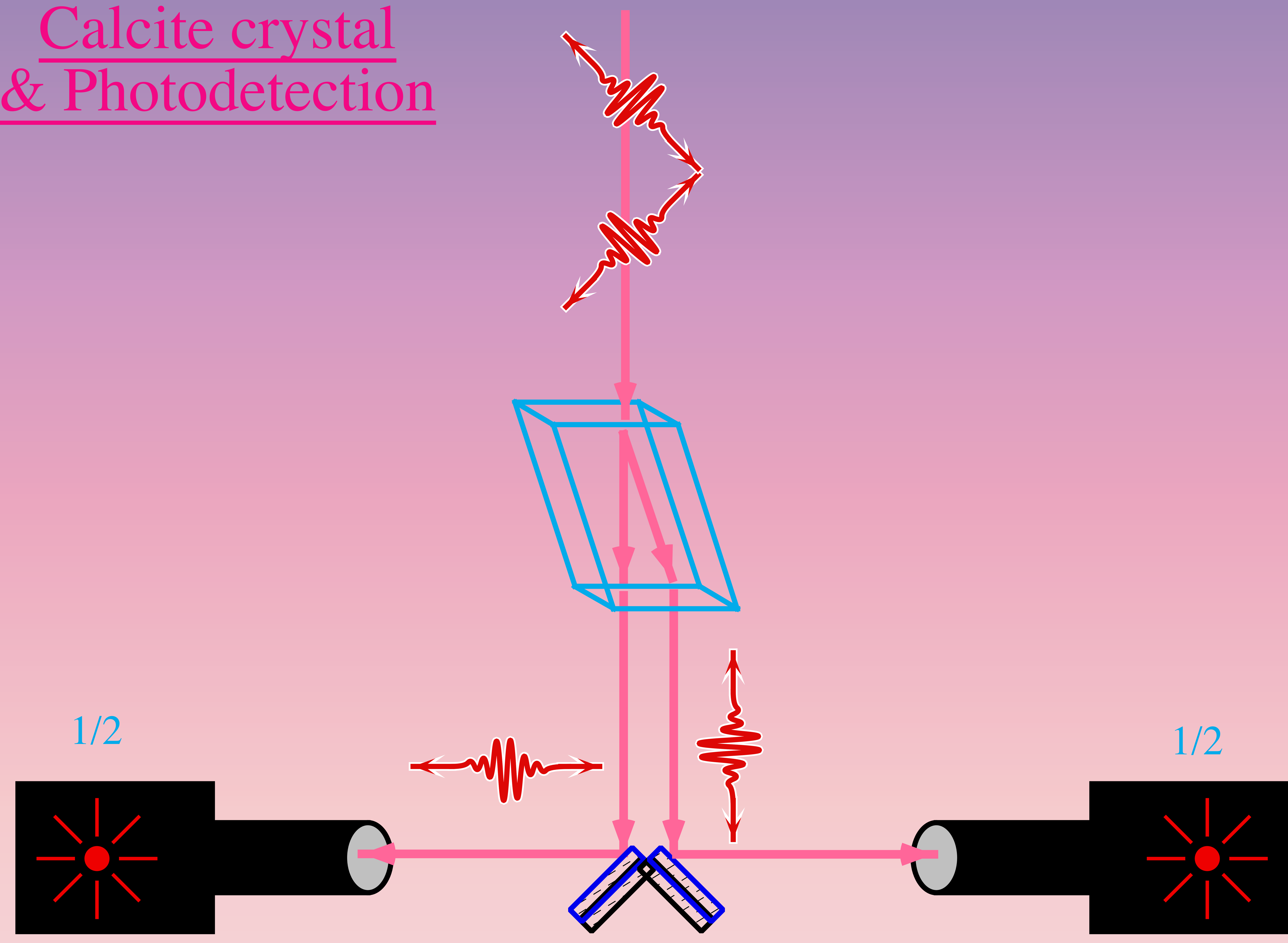
Calcite Crystal



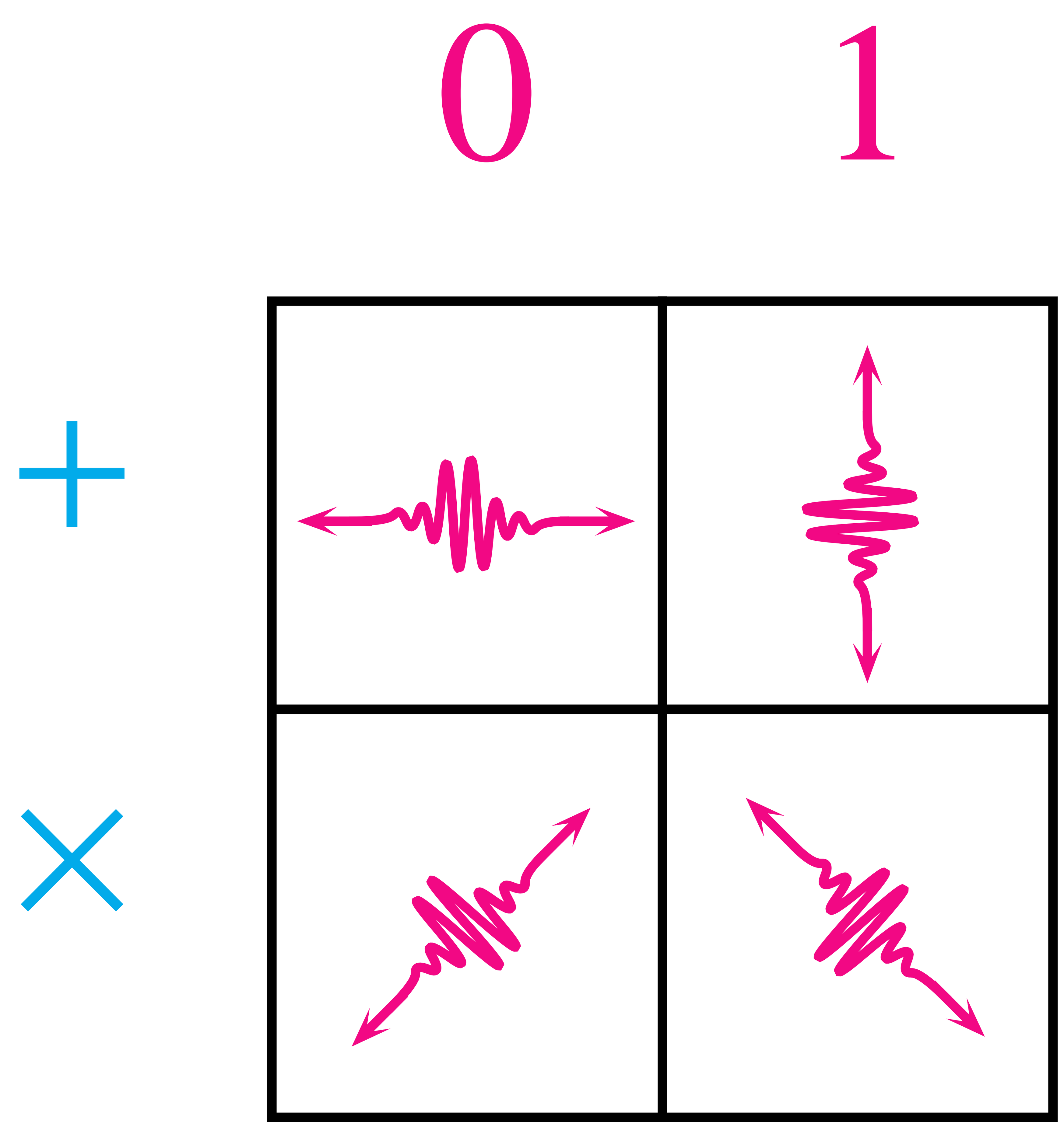
Calcite Crystal and photodetectors



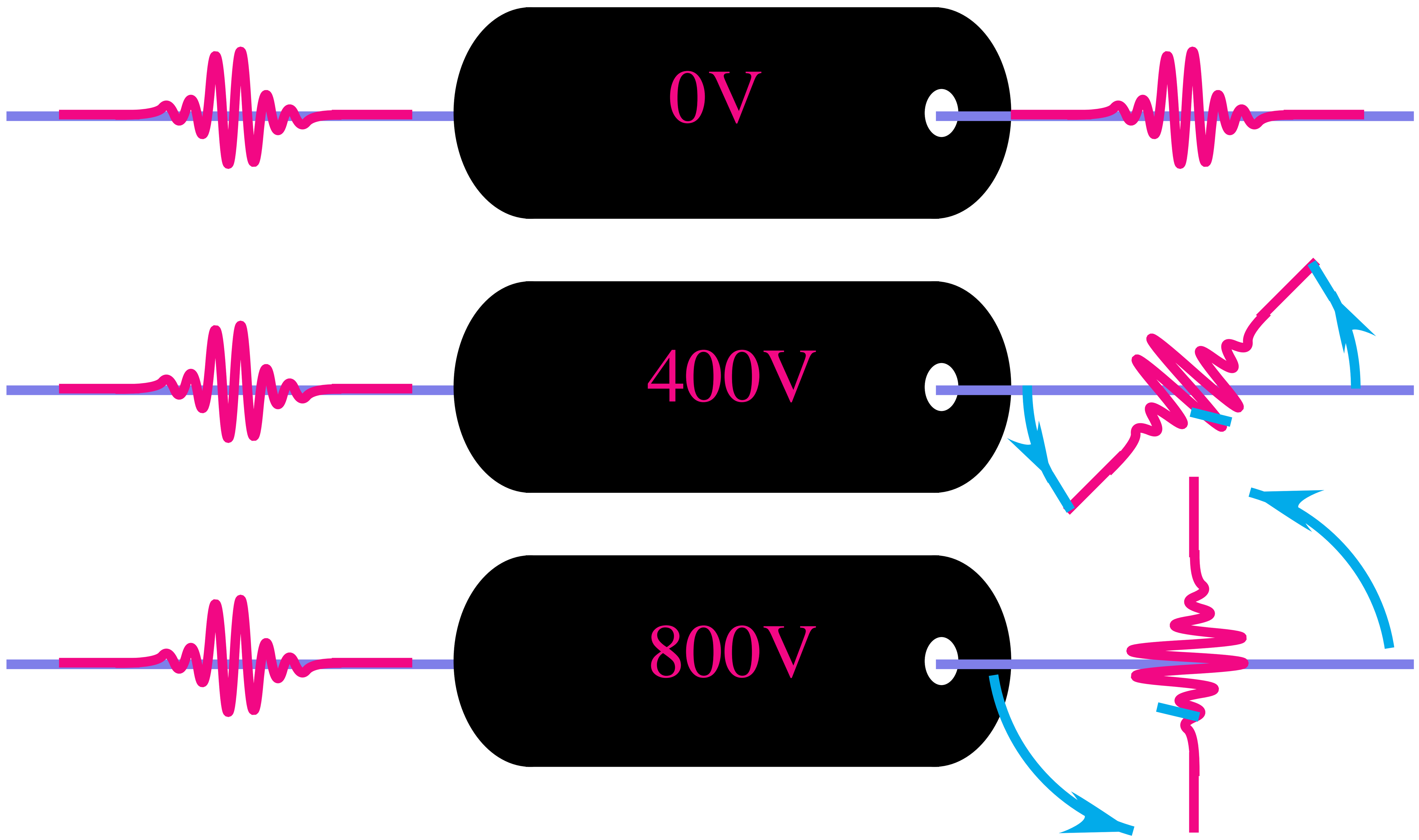
Calcite crystal & Photodetection

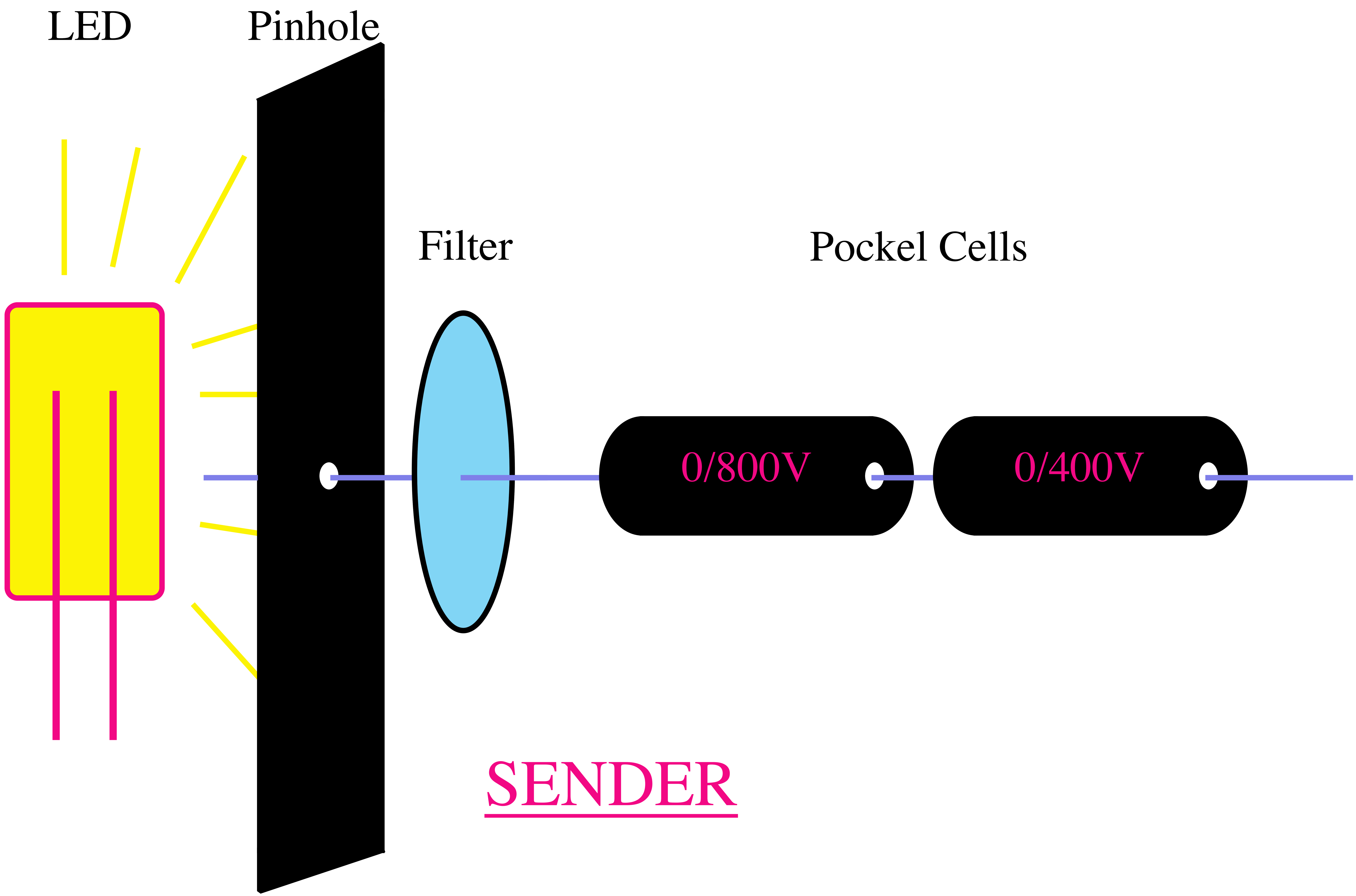


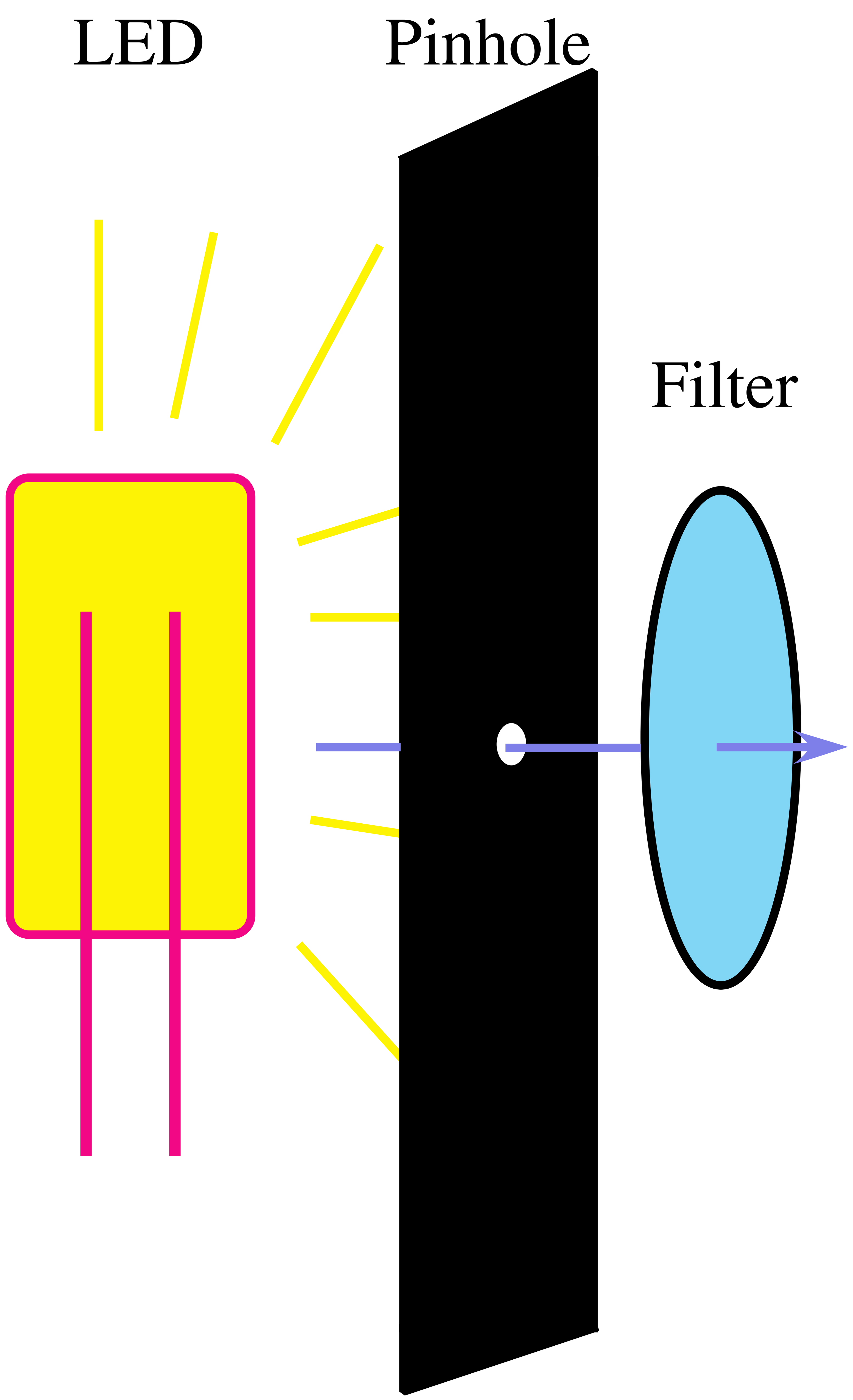
Ambiguous Coding Scheme



Pockel Cells




LED
Pinhole
Filter
Pockel Cells
0/800V
0/400V
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

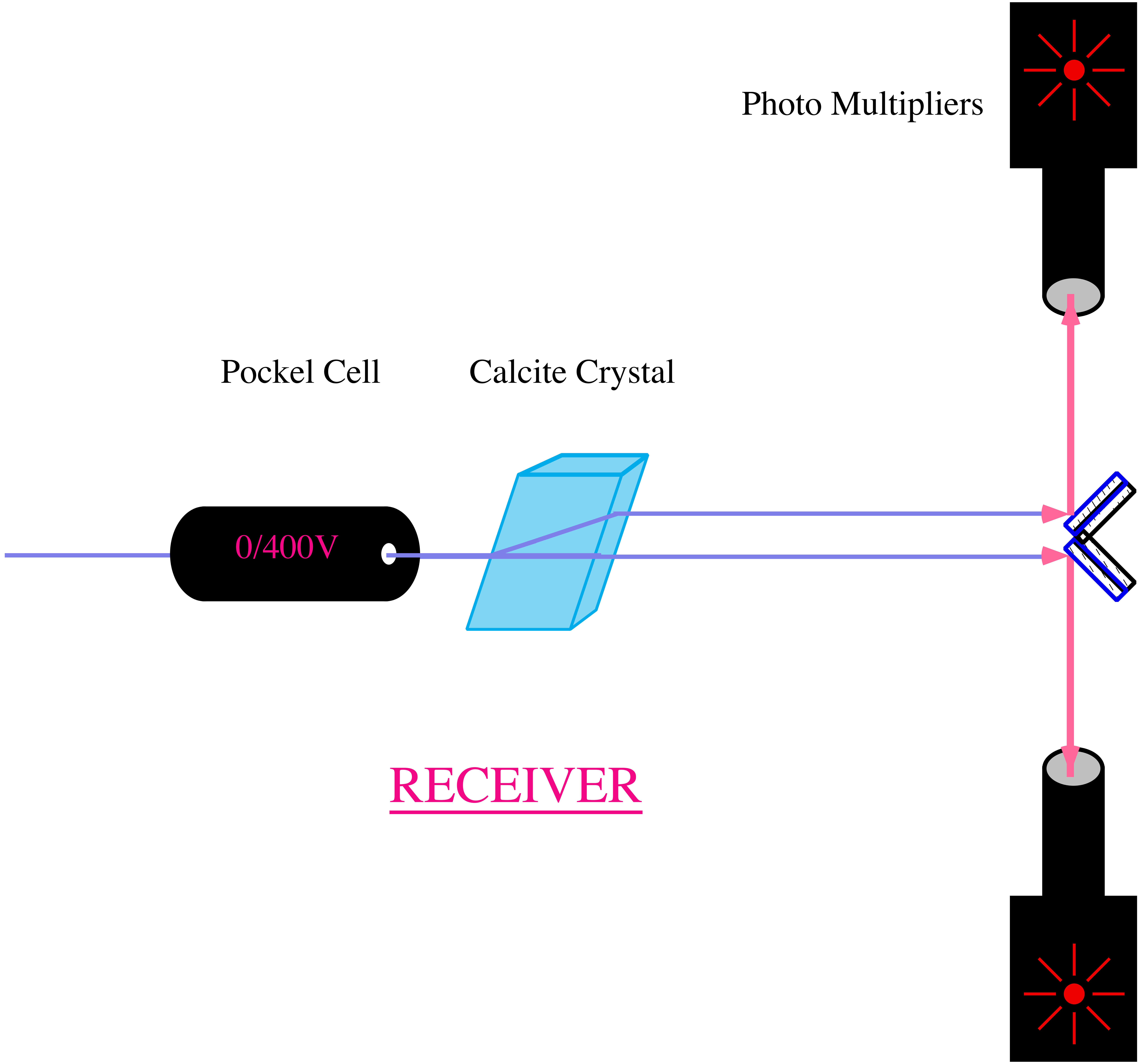
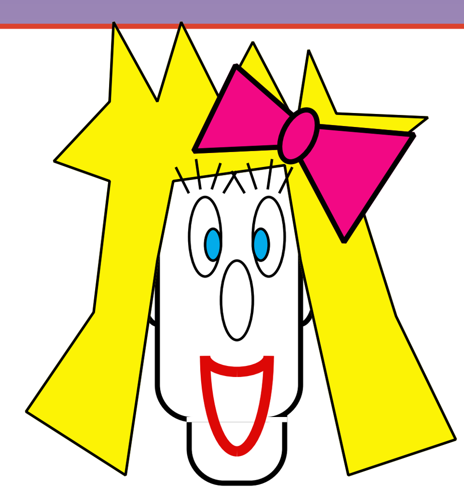
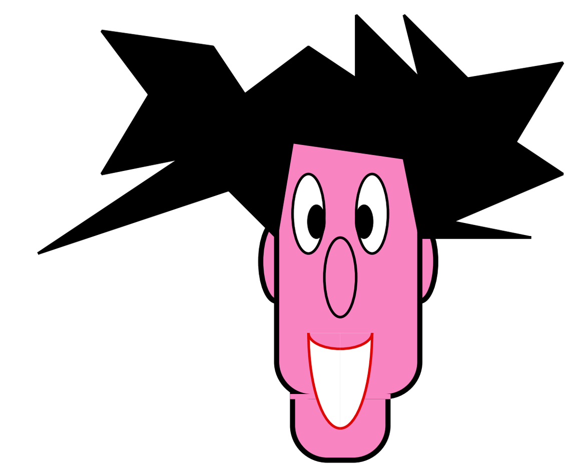


Photo Multipliers
Pockel Cell
Calcite Crystal
0/400V
RECEIVER

Q-distribution of keys

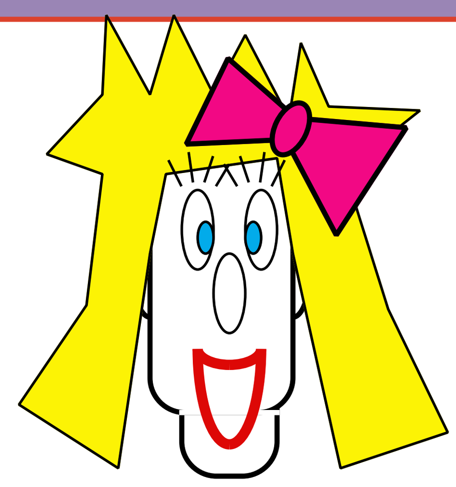


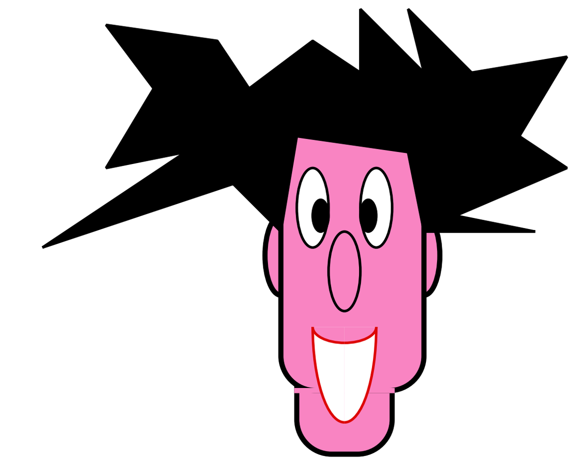


A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0	
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+	
B:	×	×	+	+	×	+	+	+	×	+	+	×	×	×	+	×	×	×	+	+	×	+	×	+	
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0	
A:	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+	
B:	0			0		1			1		0					1	0			1		0	0	0	
B:	0			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:	=					=					=						≠							=	20%
B:				0					1							1				1		0	0		
A:				0					1							1				1		0	0		

Bennett- Brassard

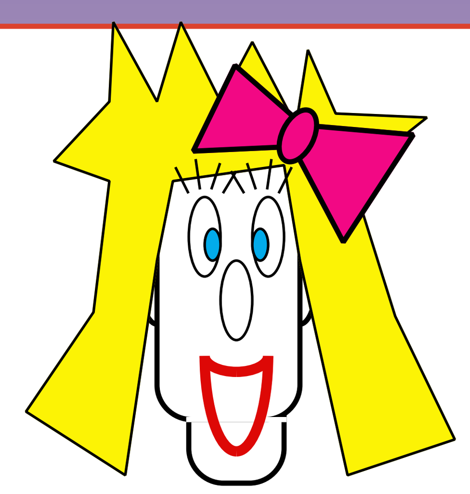
Q-distribution of keys

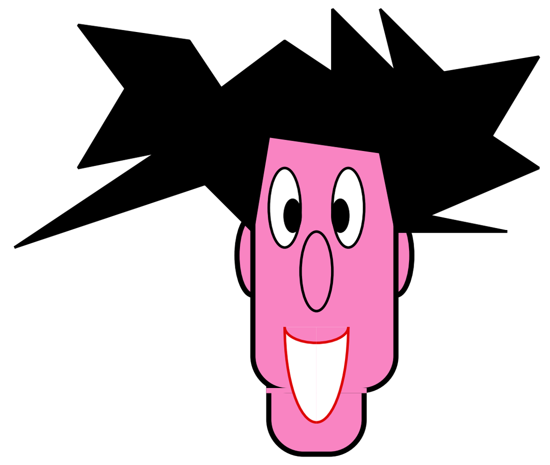




A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+

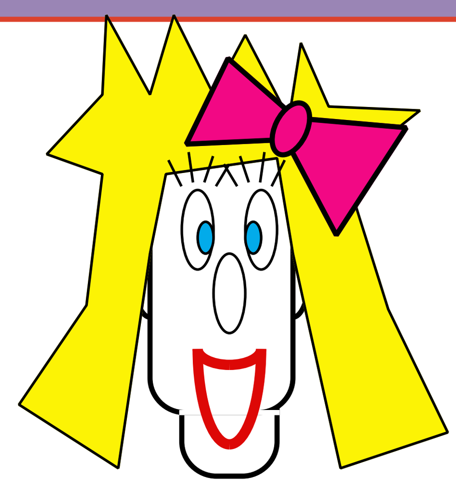
Q-distribution of keys

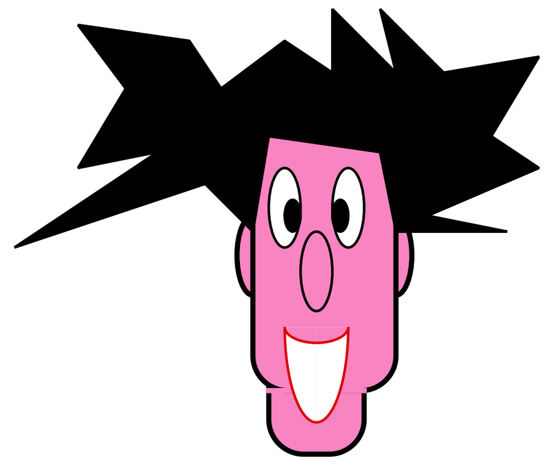




A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	×	×	+	+	×	+	+	+	×	+	+	×	×	×	+	×	×	×	+	+	×	+	×	+
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0

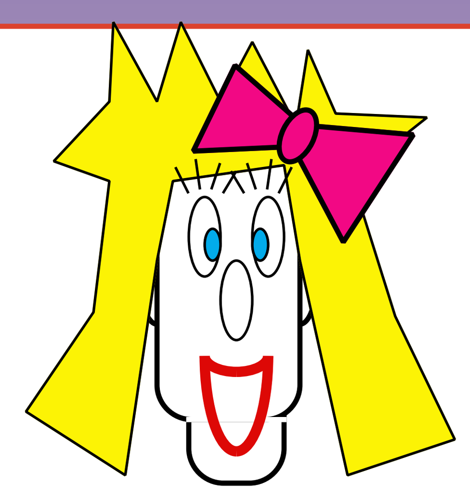
Q-distribution of keys

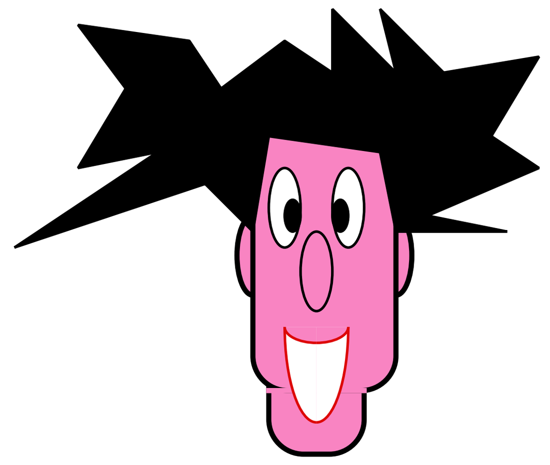




A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	×	×	+	+	×	+	+	+	×	+	+	×	×	×	+	×	×	×	+	+	×	+	×	+
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0
A:	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+

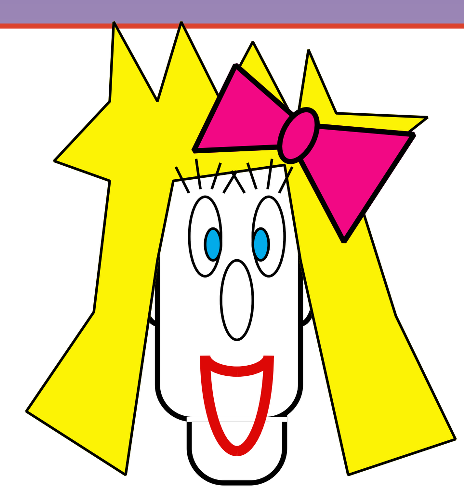
Q-distribution of keys

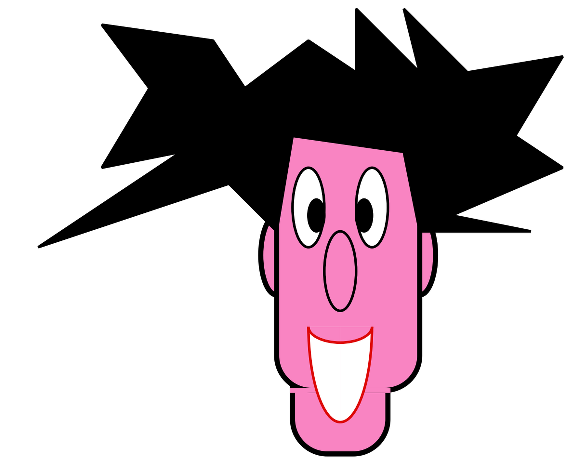




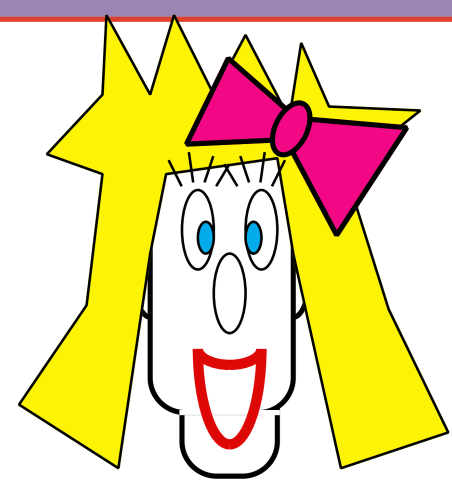
A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	×	×	+	+	×	+	+	+	×	+	+	×	×	×	+	×	×	×	+	+	×	+	×	+
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0
A:	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	0	👎	👎	0	👎	1	👎	👎	1	👎	0	👎	👎	👎	👎	1	0	👎	👎	1	👎	0	0	0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

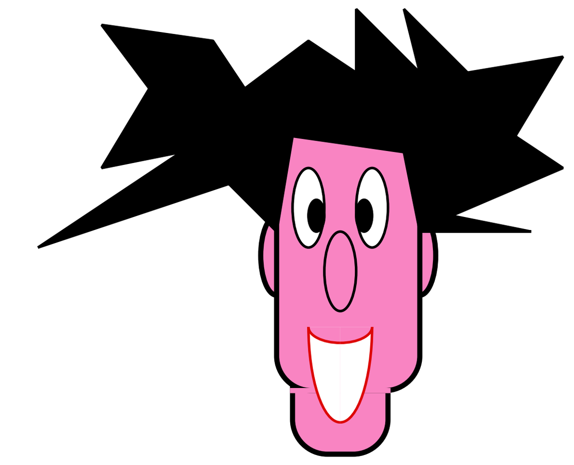




B:	0	0	1	1	0	1	0	1	0	0	0
A:	0	0	1	1	0	1	1	1	0	0	0



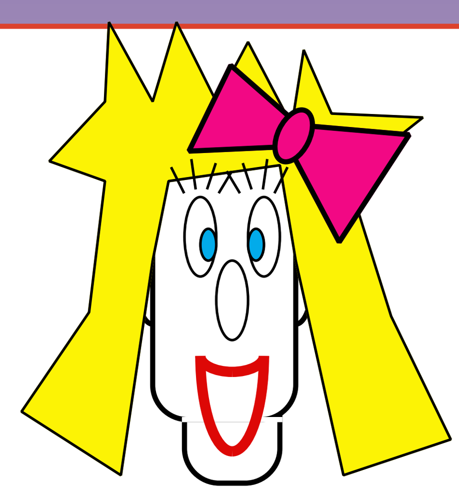
Q-distribution of keys

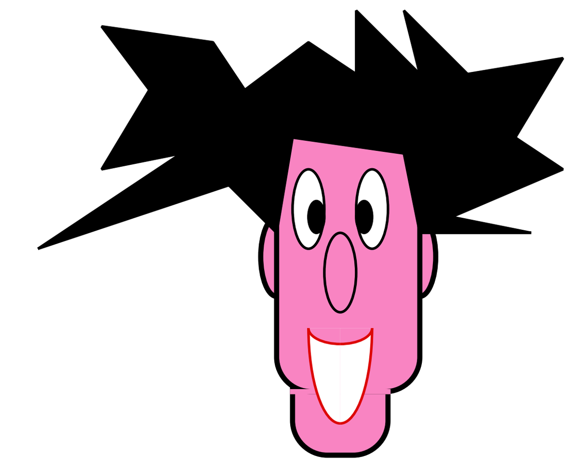


B:	0	0	1	1	0	1	0	1	0	0	0
A:	0	0	1	1	0	1	1	1	0	0	0
A:	0		1		0		1				0
B:	=		=		=		≠				=

20%

Q-distribution of keys

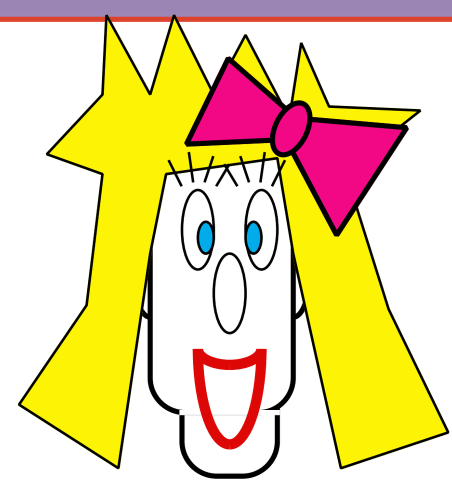




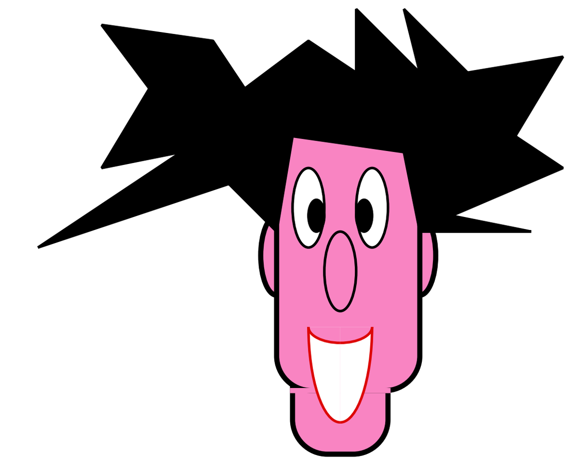
B: = = = ≠ = — 20%

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%

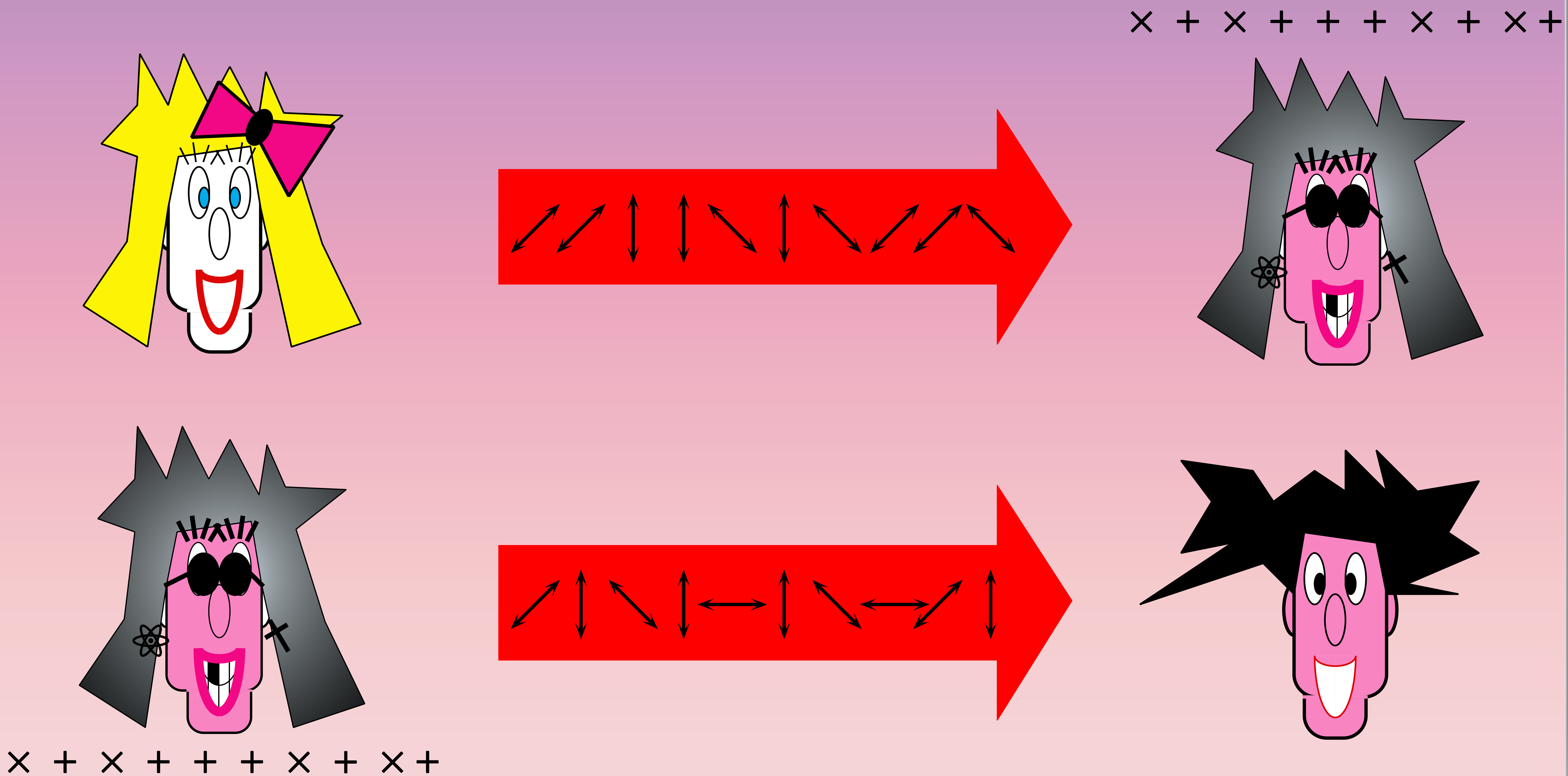
Q-distribution of keys

• • • • •

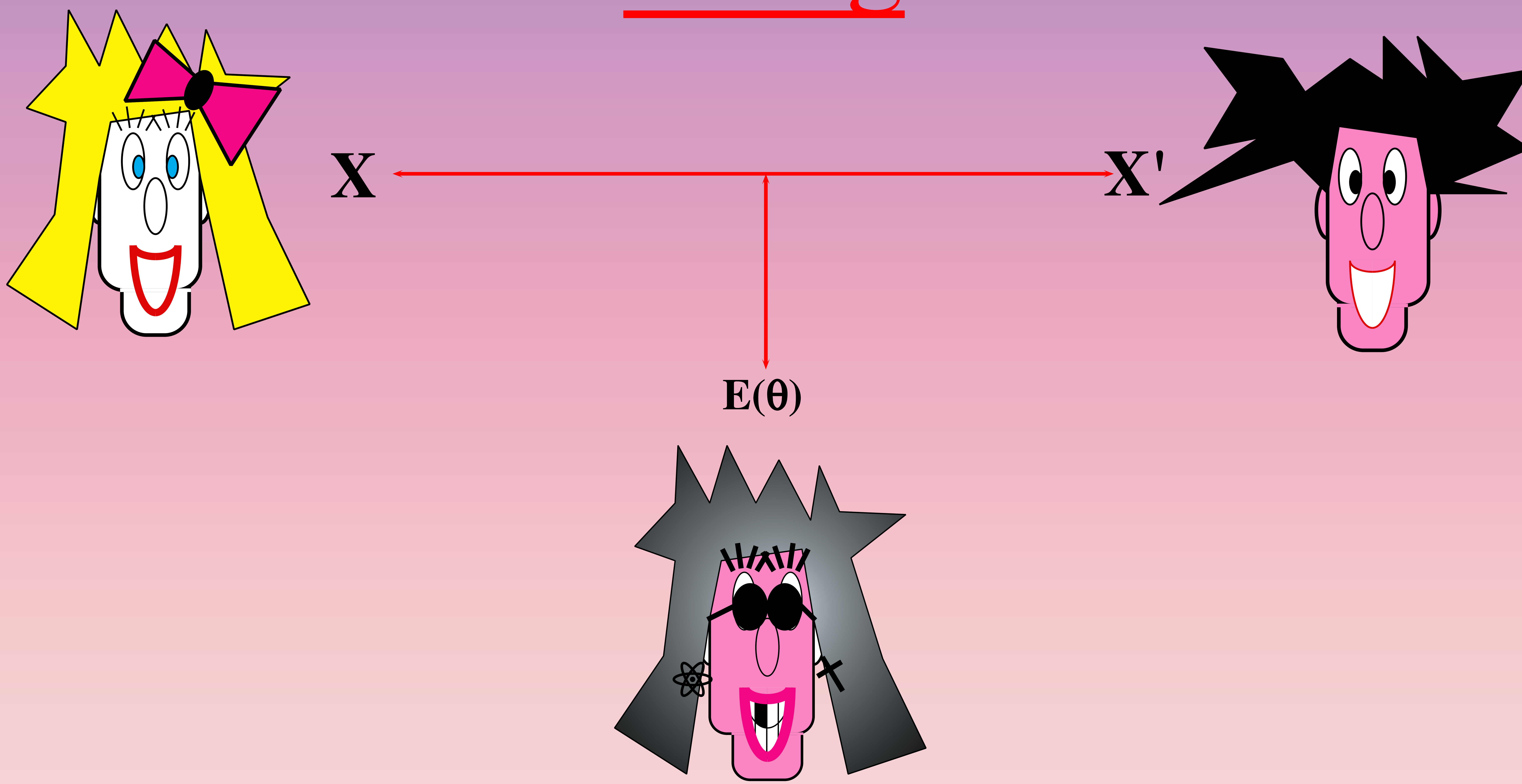
- Produces raw classical key
- Observed error rate indicates amount of eavesdropper information
- Error-correction is used to fix errors
- Random hash function is used to distill a smaller secret classical key

• • • • •

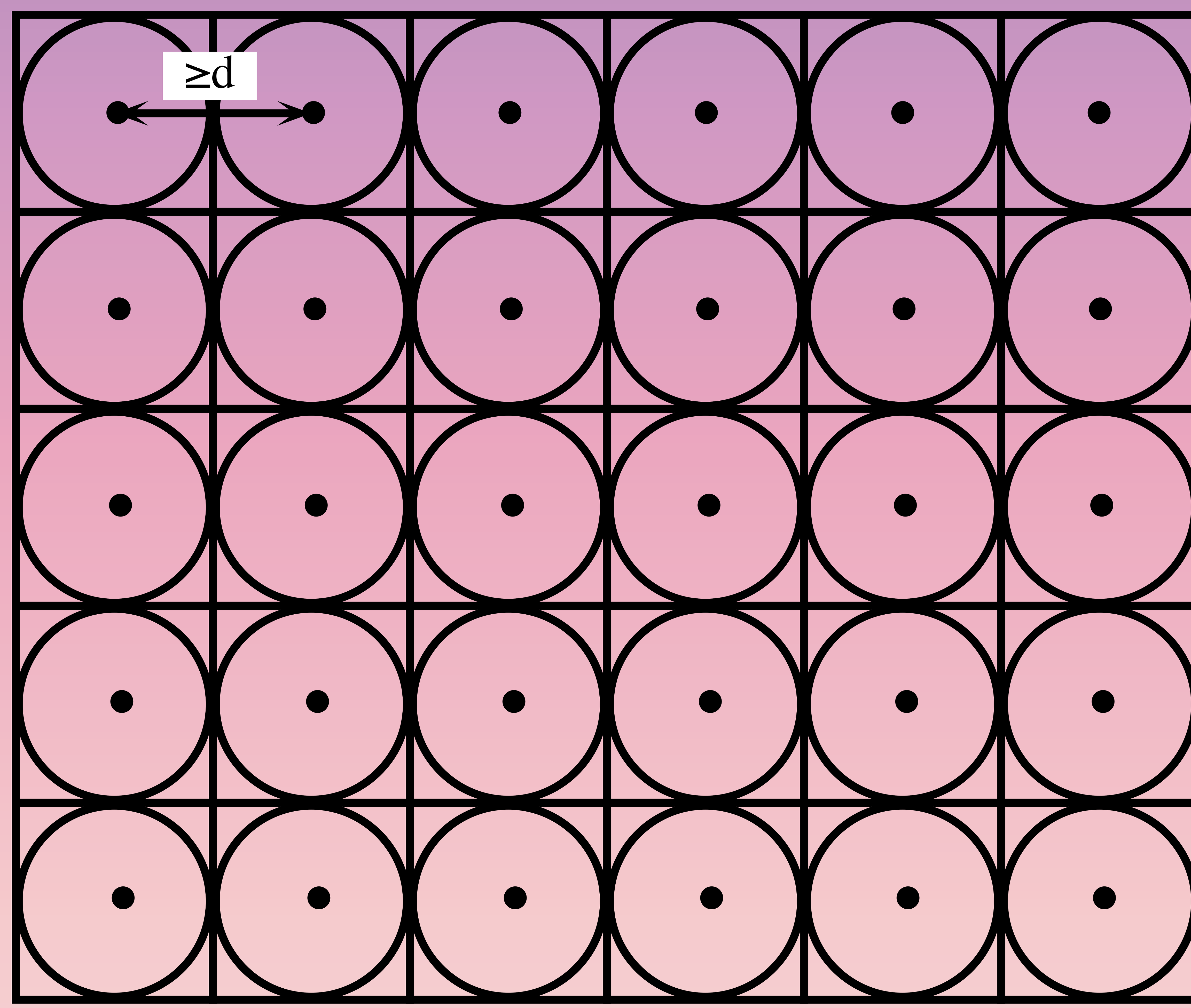
Information <--> Errors



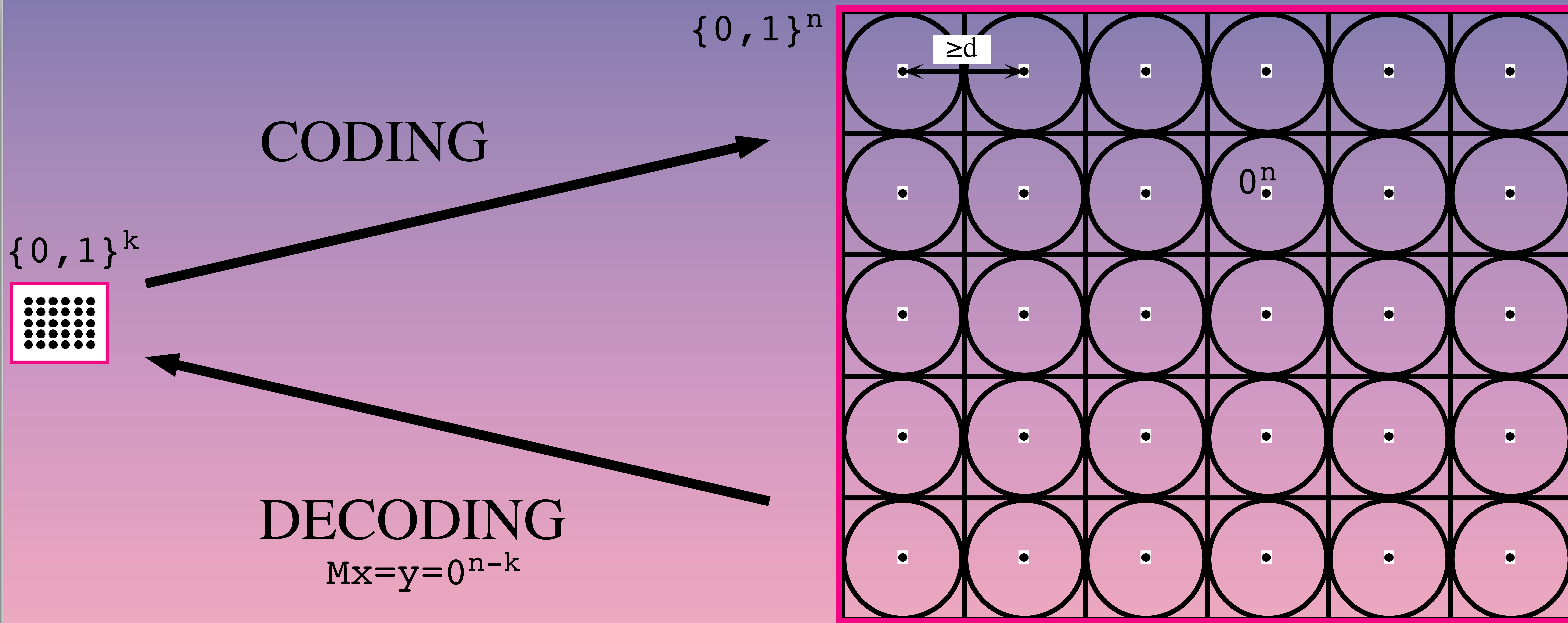
Mostly Identical Partly Secret String



(classical) error-correcting codes



(



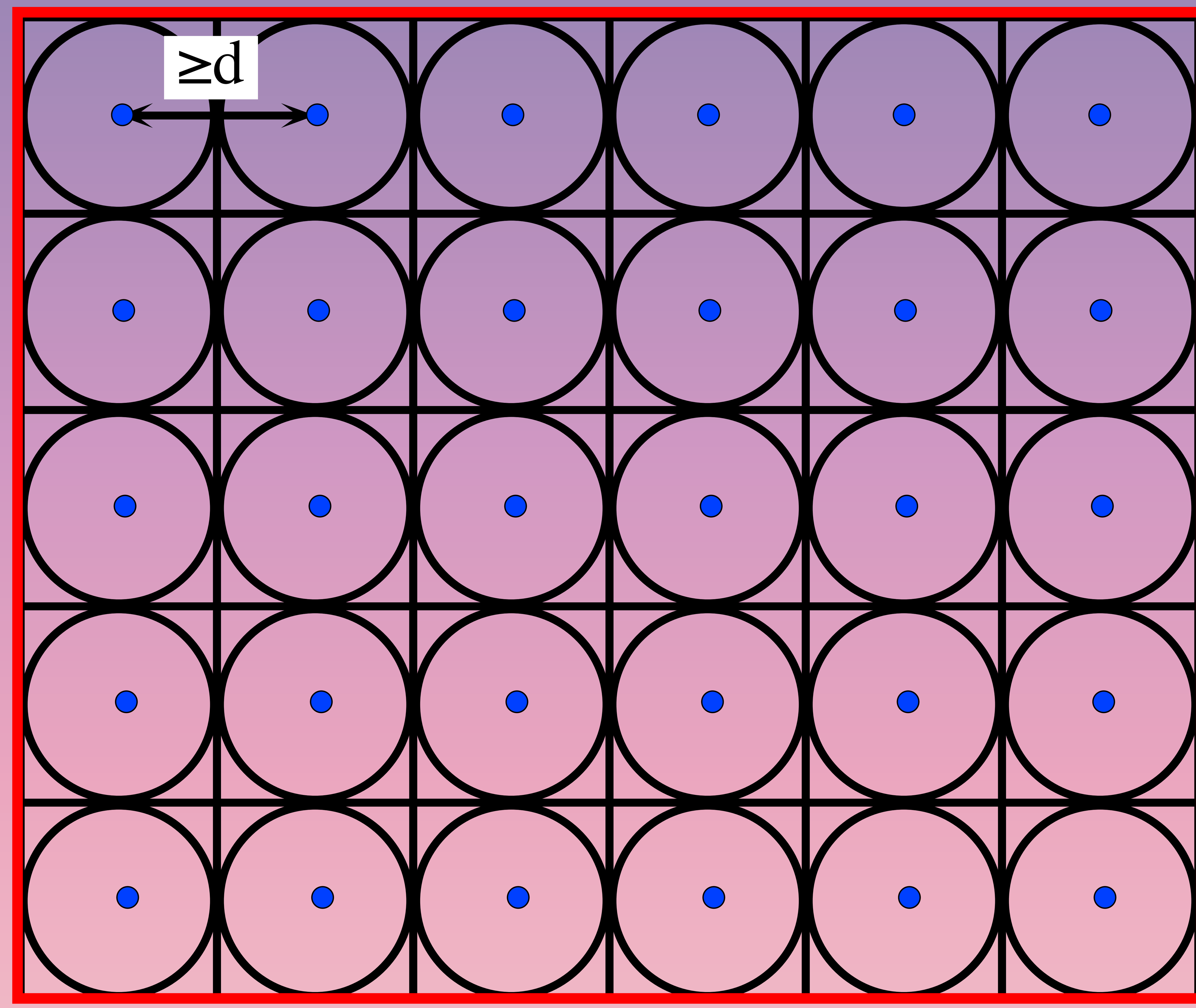
[n,k,d] linear code

$M \in \{0,1\}^{(n-k)\cdot n}$ is a Parity Check matrix

$C = \{ x \mid Mx=0^{n-k} \}$

(classical) error-correcting codes

q^n (words)

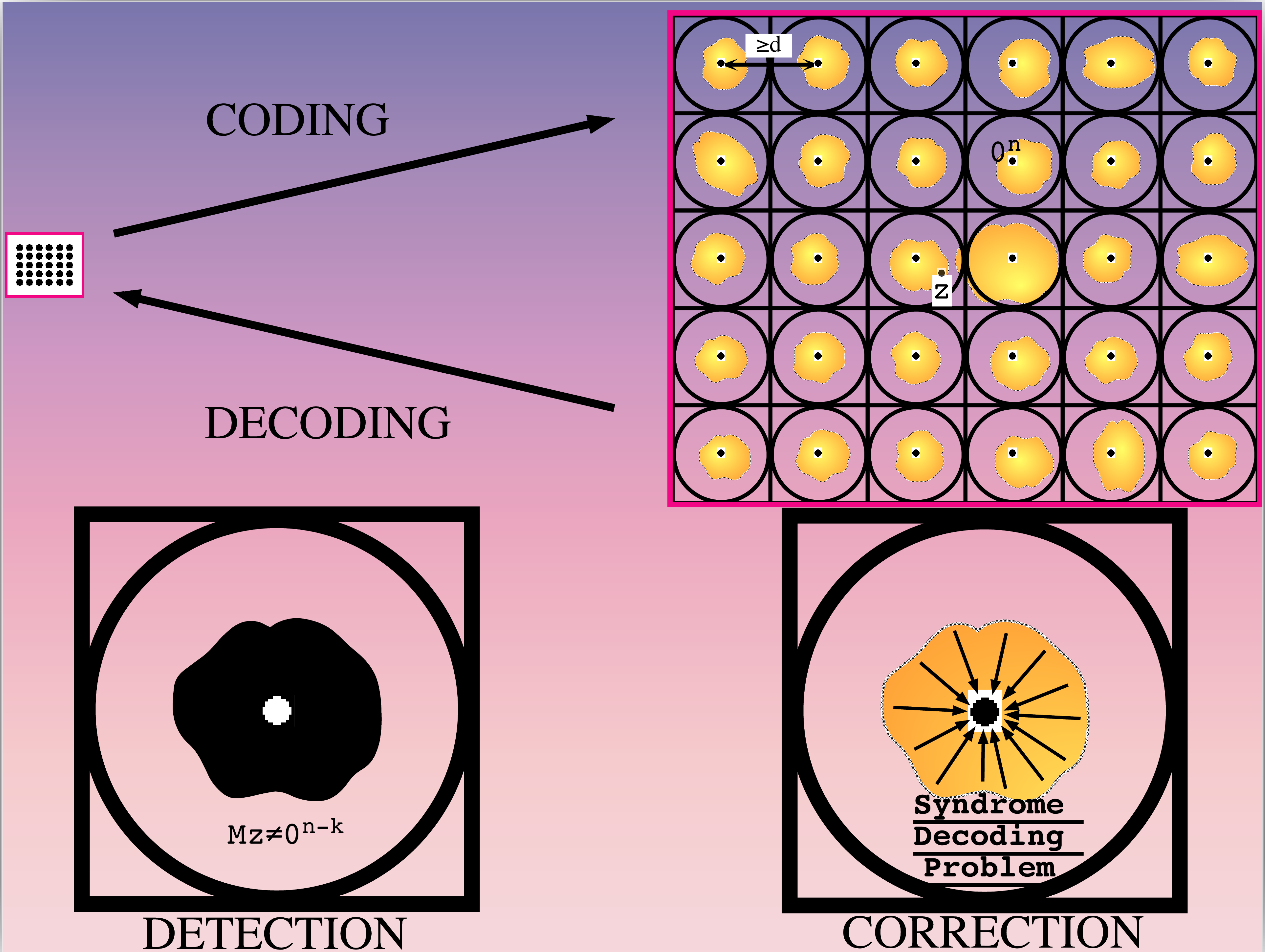


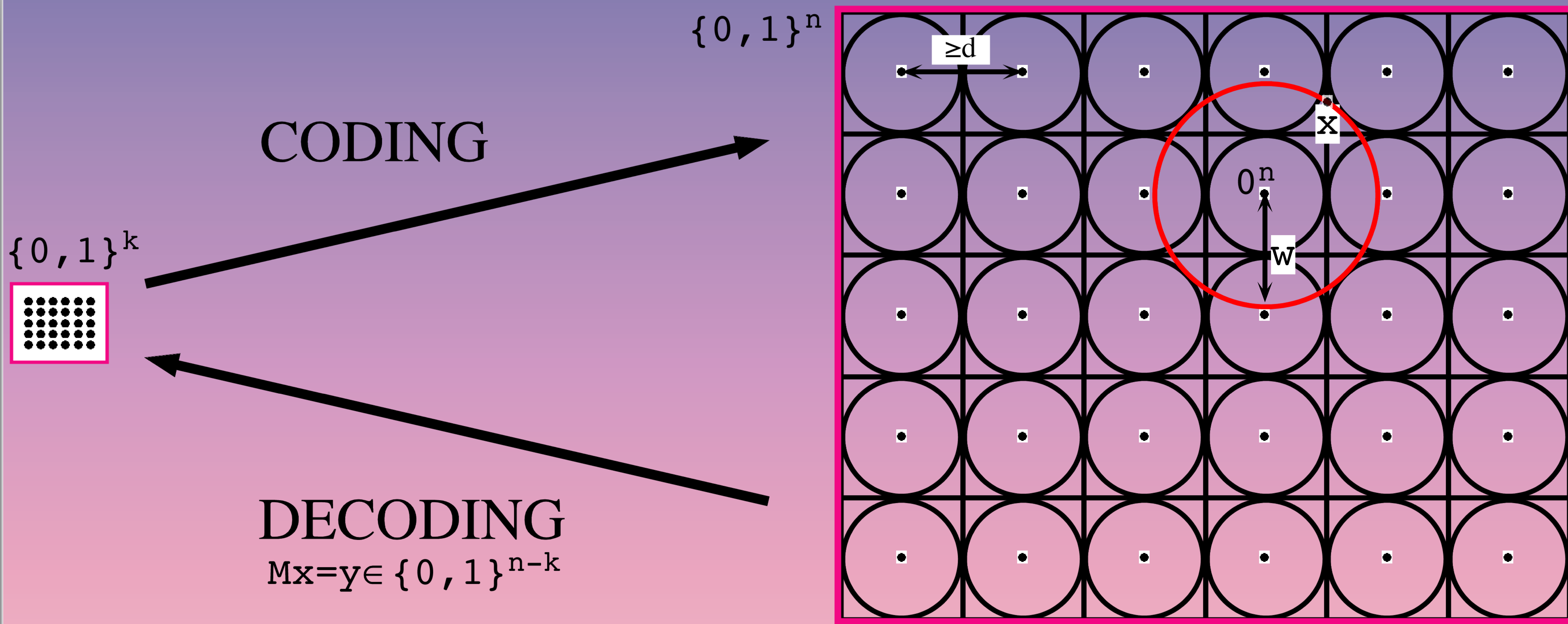
q^k (codewords)

[n,k,d] linear error-correcting code

length n, dimension k,

corrects d-1 erasures, (d-1)/2 errors

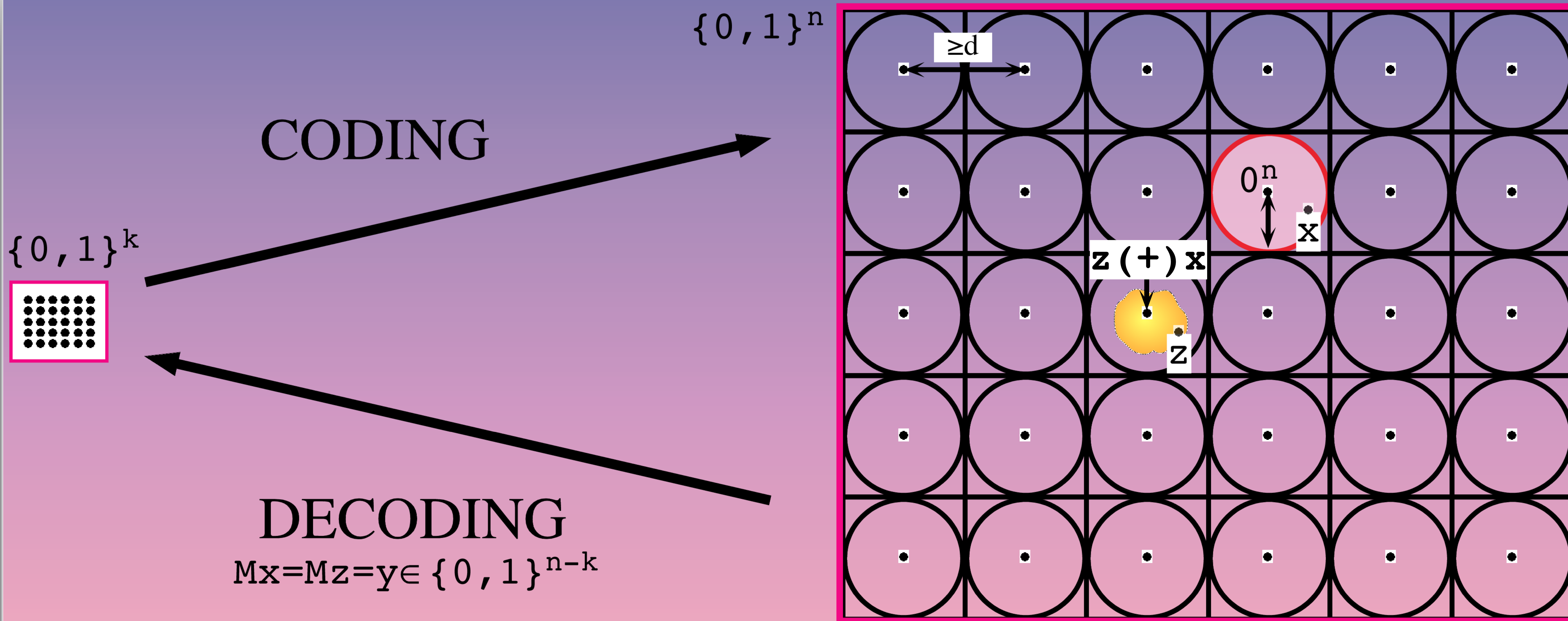

CODING
DECODING
≥d
0ⁿ
z
Mz≠0ⁿ⁻ᵏ
Syndrome
Decoding
Problem
DETECTION
CORRECTION



Syndrome Decoding Problem

Instance: PC matrix $M \in \{0,1\}^{(n-k)\cdot n}$, syndrome $y \in \{0,1\}^{n-k}$, weight $w \leq n$

Problem: is there a word $x \in \{0,1\}^n$, $|x| \leq w$ s.t. $Mx=y$?



CORRECTING(M,z) <= Syndrome Decoding Problem (M, w=(d-1)/2, y=Mz)

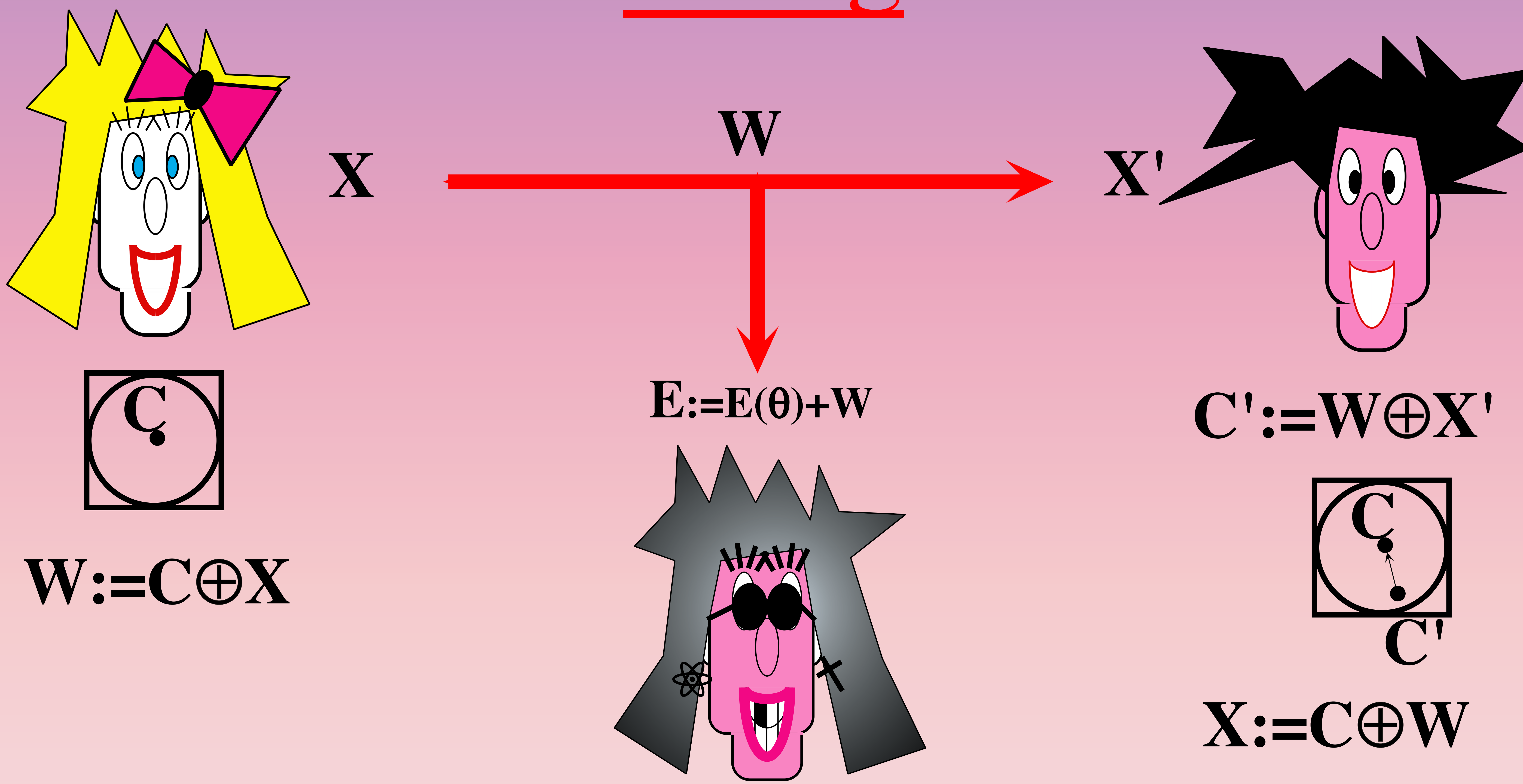
Instance: PC matrix $M\in\{0,1\}^{(n-k)\cdot n}$, $y=Mz\in\{0,1\}^{n-k}$, $w=(d-1)/2$

Problem: is there a word $x\in\{0,1\}^n$, $|x|\leq w$ s.t. $Mx=y$?

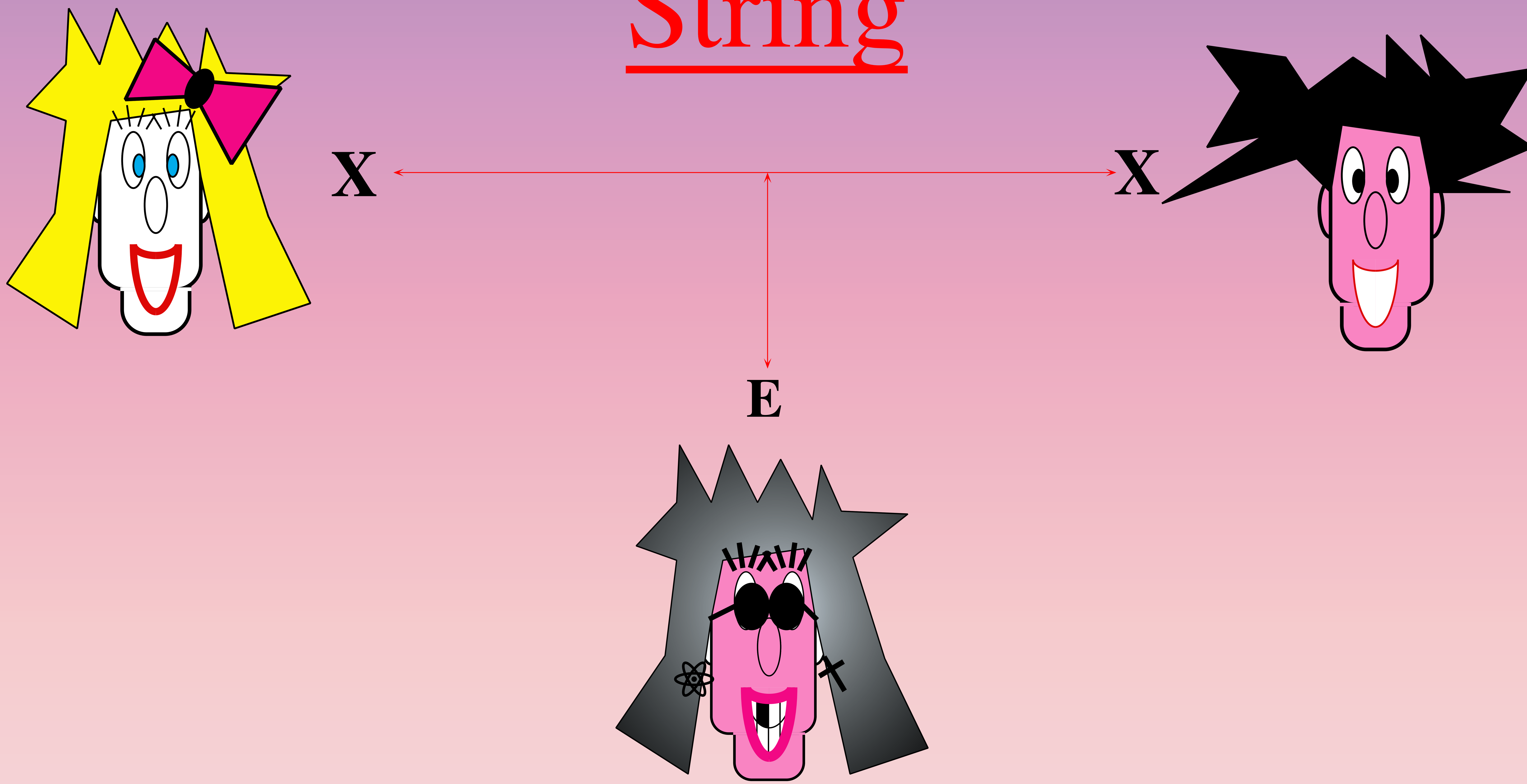
CORRECTING(M,z) = z(+)x

)

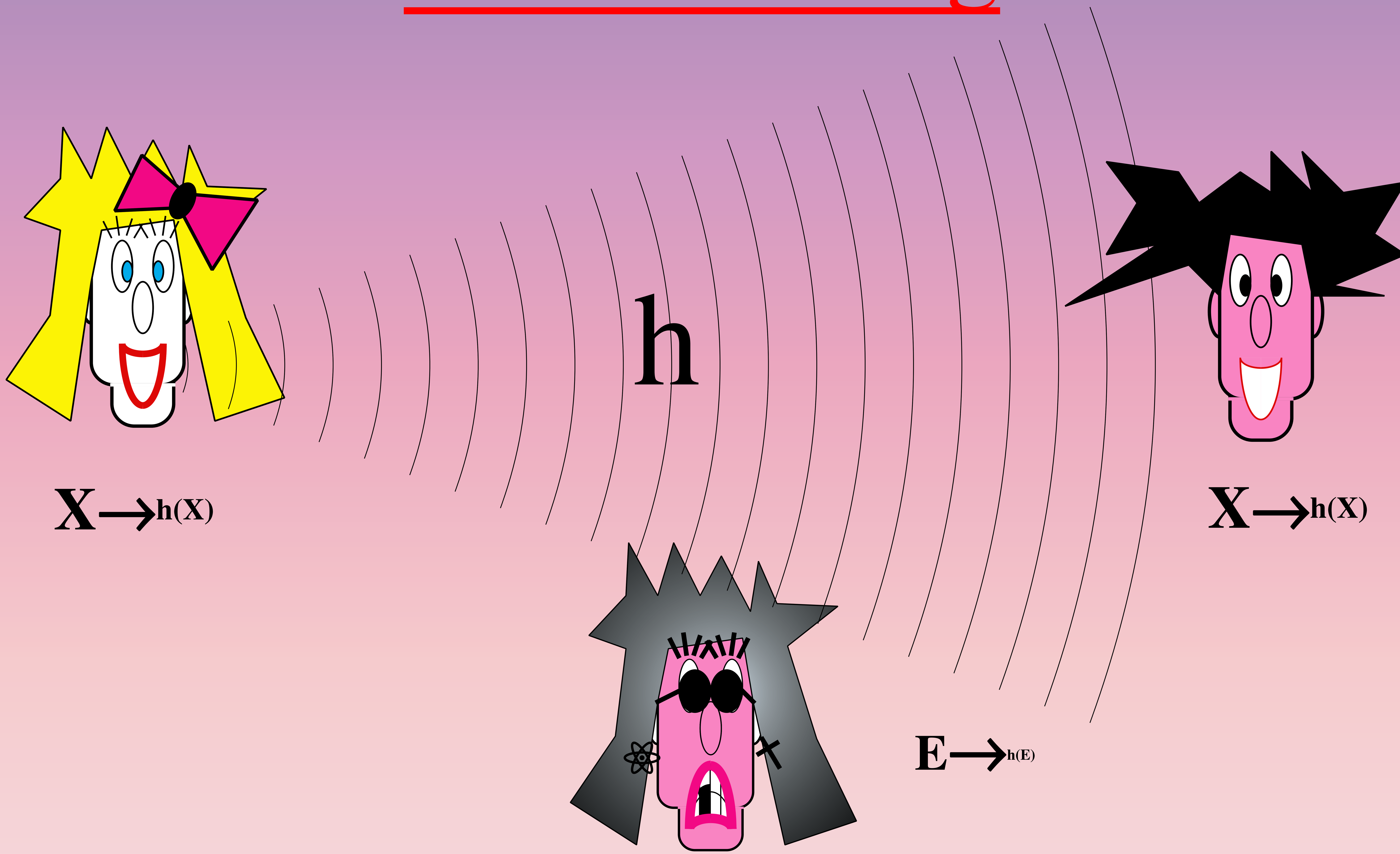
Identical Partly Secret String



Identical
Partly Secret
String

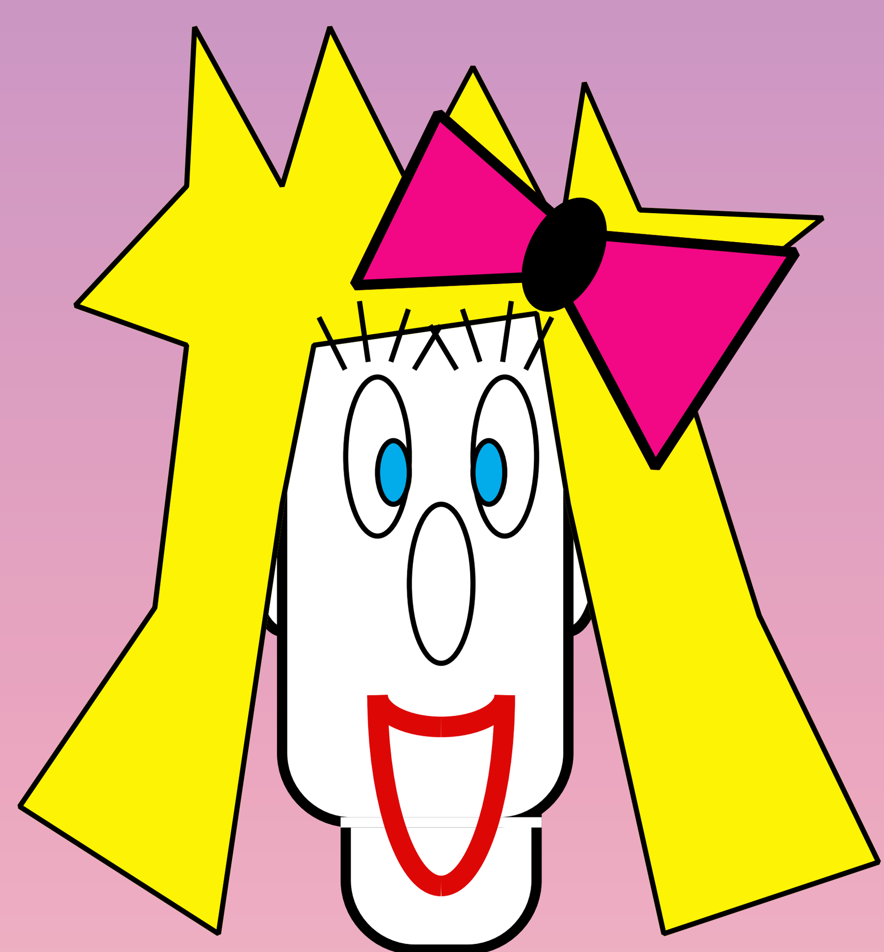


Identical Secret
Shorter String



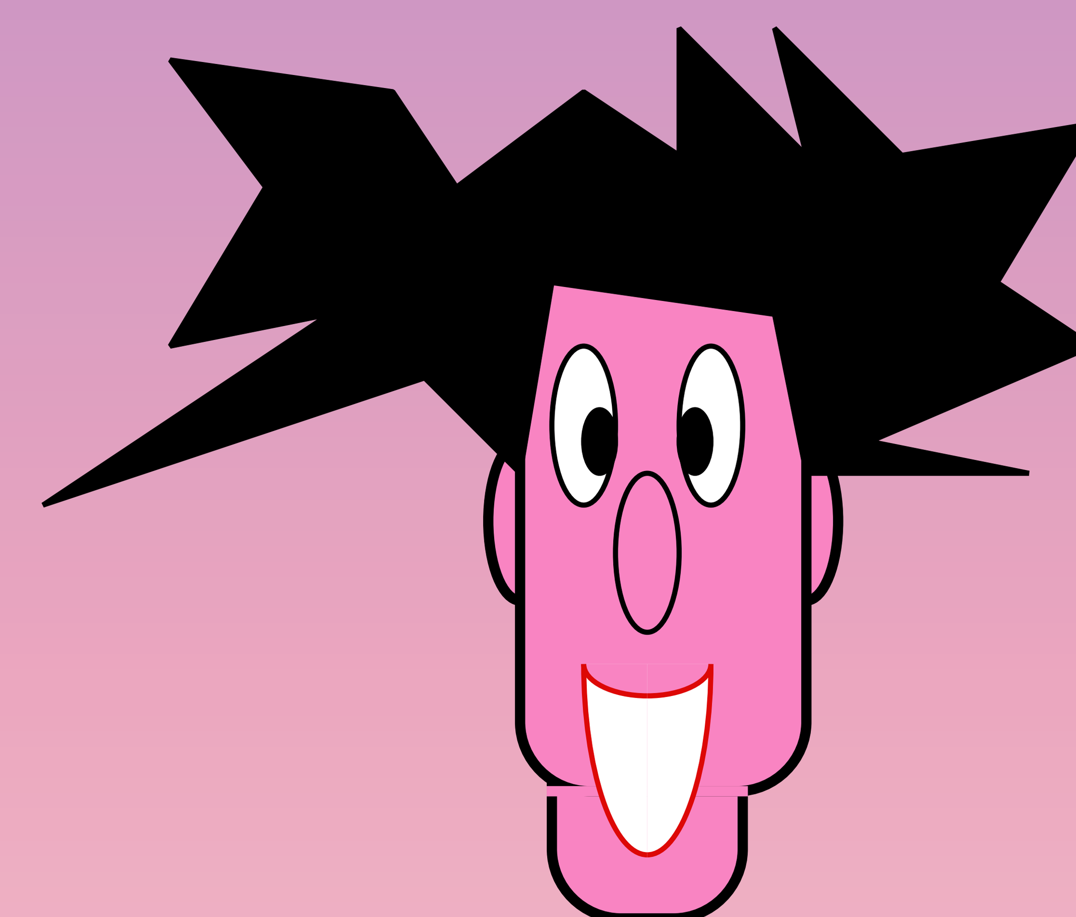
BBCM

$$H(h(X) \mid E,h) > |h(X)| - 2^{(|h(X)|-H_\infty(X))}$$

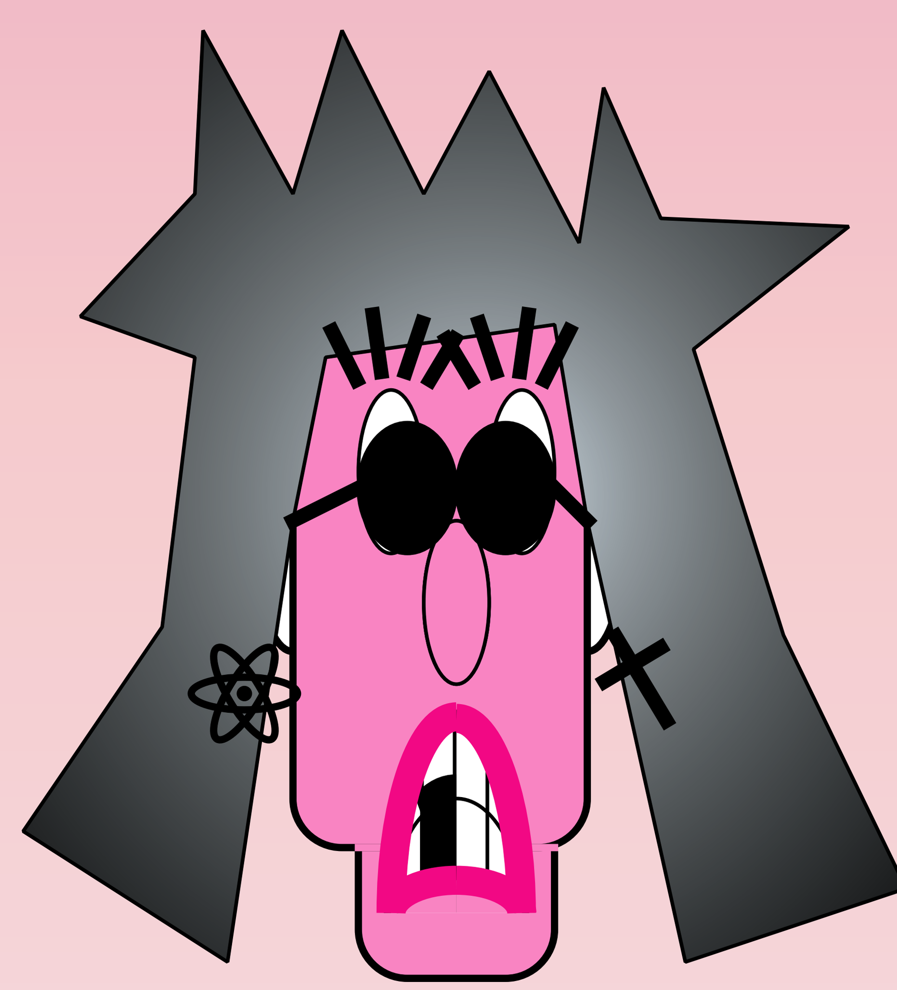


k:=h(X)

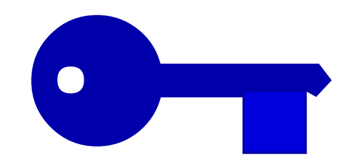
h

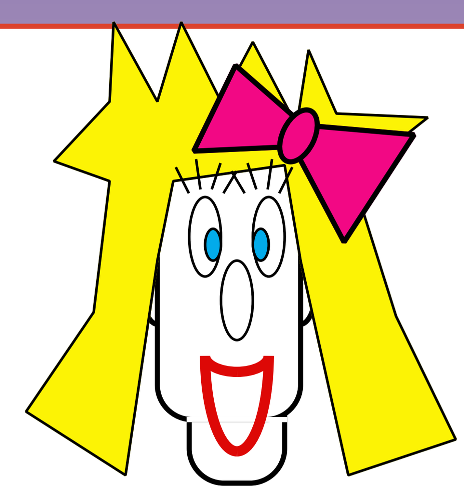


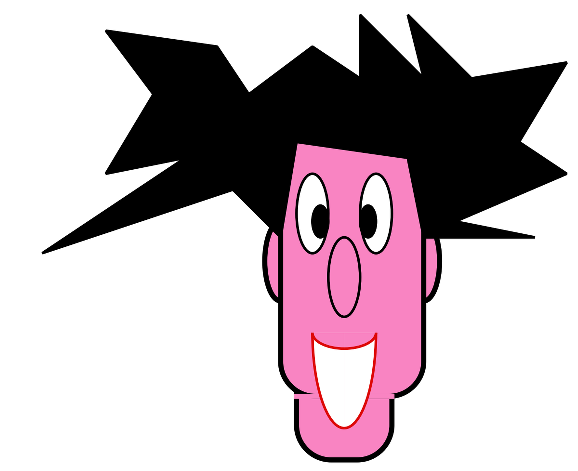
k:=h(X)



???????????
k':=h(E)
??????????

Q-distribution of keys 





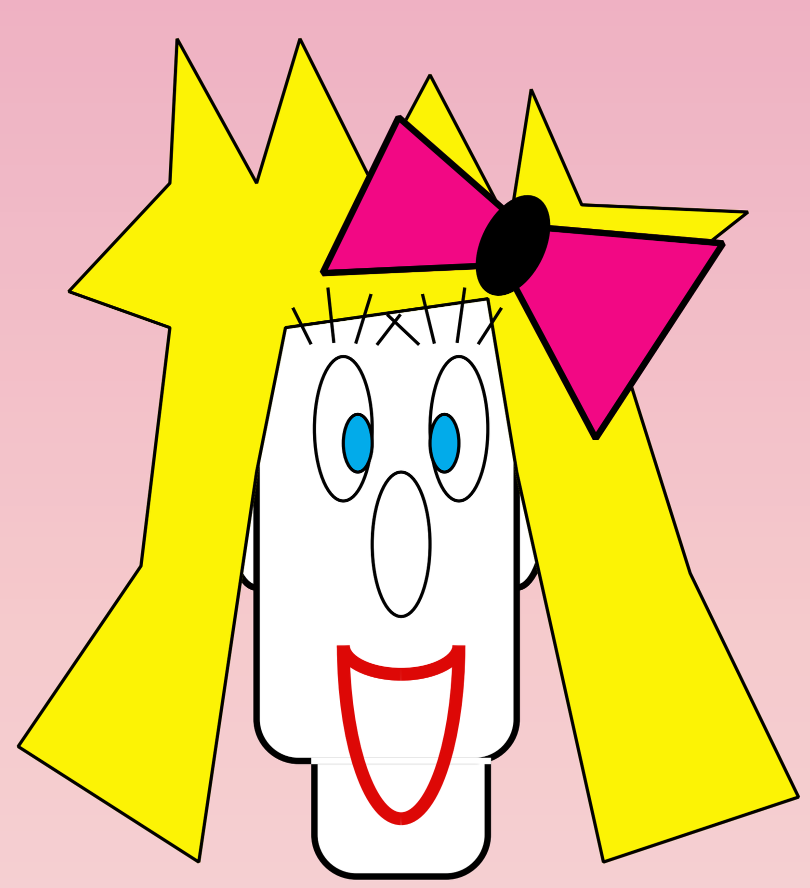
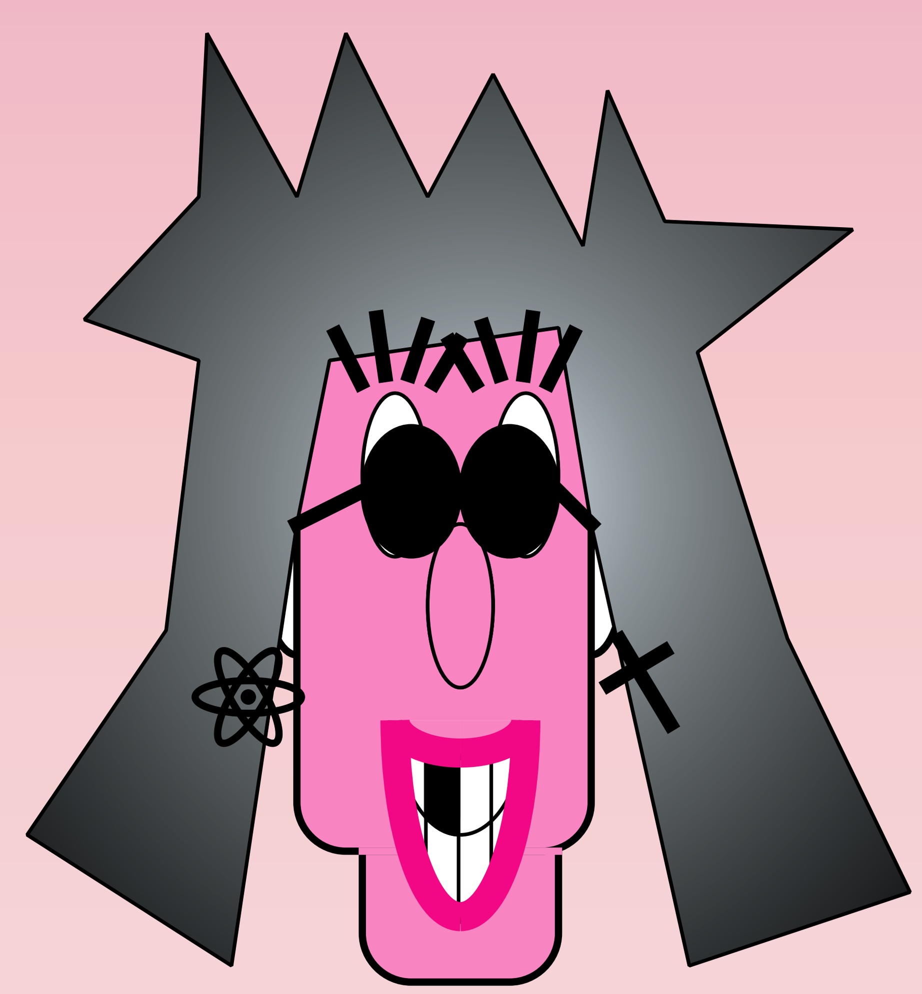
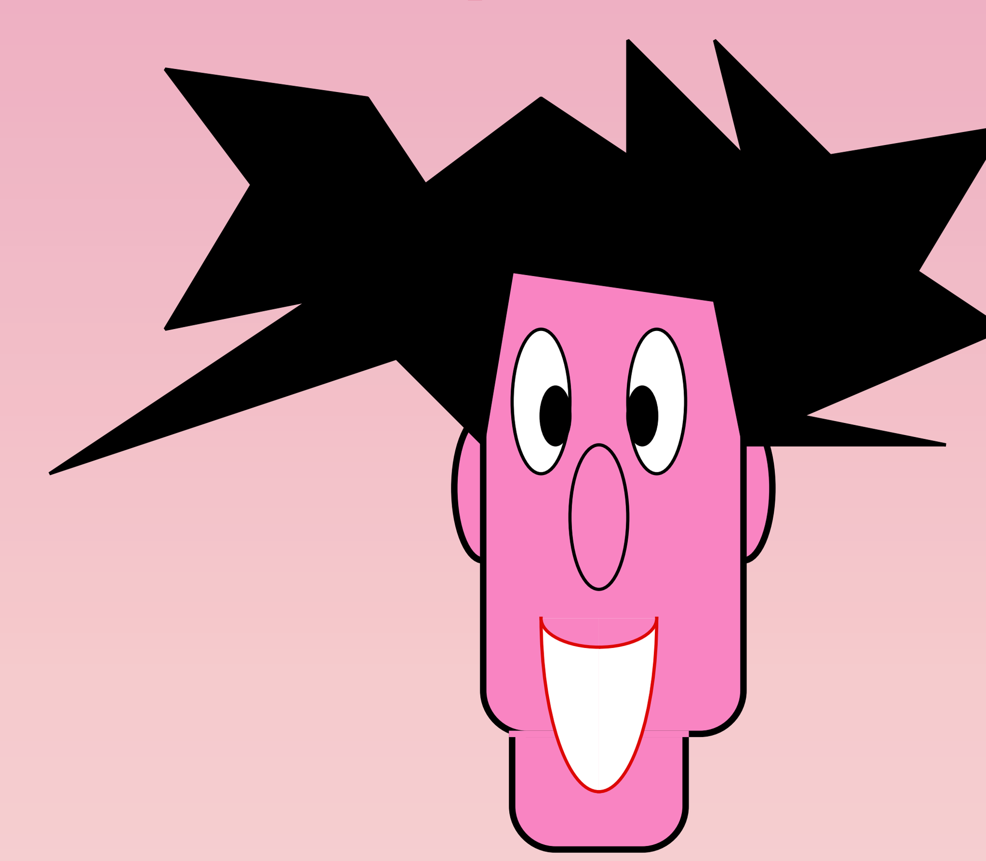
A:	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+	
B:	¿	¿	¿	¿	¿	¿	?	¿	¿	¿	¿	¿	¿	¿	¿	¿	?	¿	¿	¿	¿	¿	¿	¿	
	×	×	+	+	×	+	+	+	×	+	+	×	×	×	+	×	×	×	+	+	×	+	×	+	
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0	
A:	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+	
B:	0	👎	👎	0	👎	1	👎	👎	1	👎	0	👎	👎	👎	👎	1	0	👎	👎	1	👎	0	0	0	
A:	1			1		0			0		1					0	0			0		1	1	1	
A:	1					0					1						0							1	
B:	≠					≠					≠					≠	=							≠	20%
B:				0					1							1				1		0	0		
A:				1					0							0				0		1	1		

Ekert

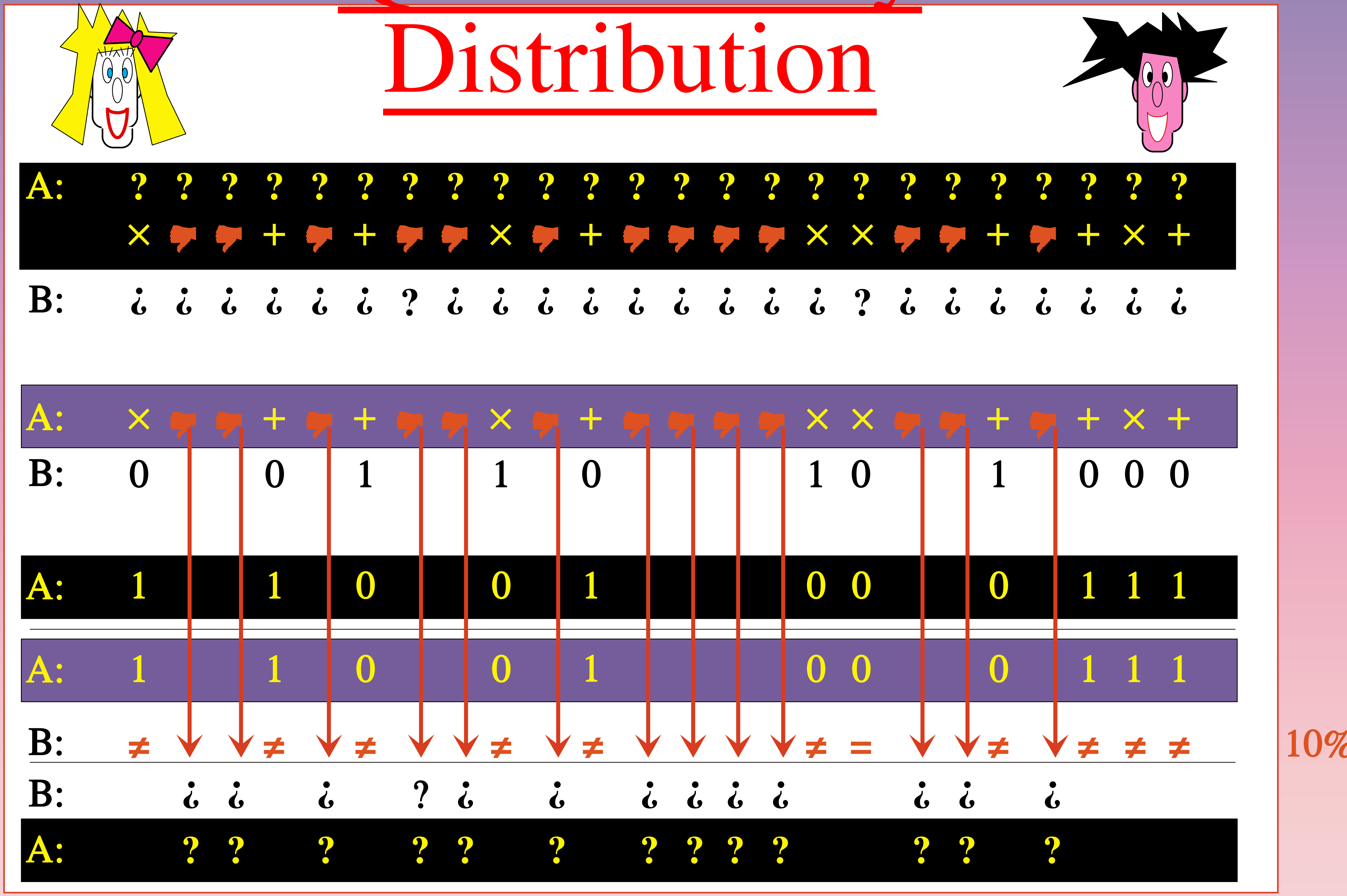
(3.1.1) Key distribution

Classical key : Q-distribution of keys(BB84)
+ error-correction
+ privacy amplification

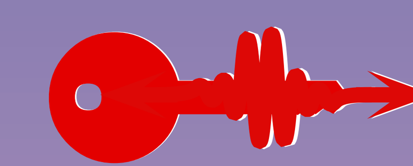
Quantum key : Q-key distribution(Ekert/Lo-Chau)
+ Q-error-correction (CSS) or
Q-Distillation (Purification)

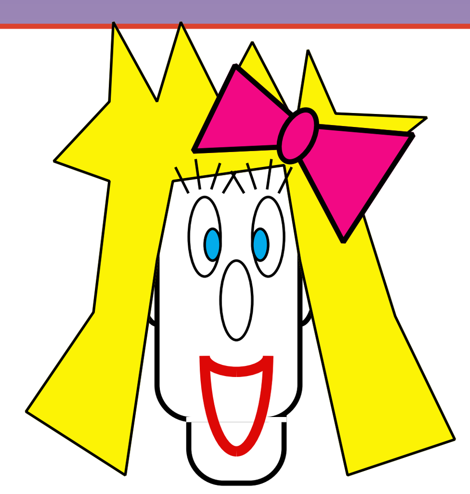
Quantum-Key Distribution

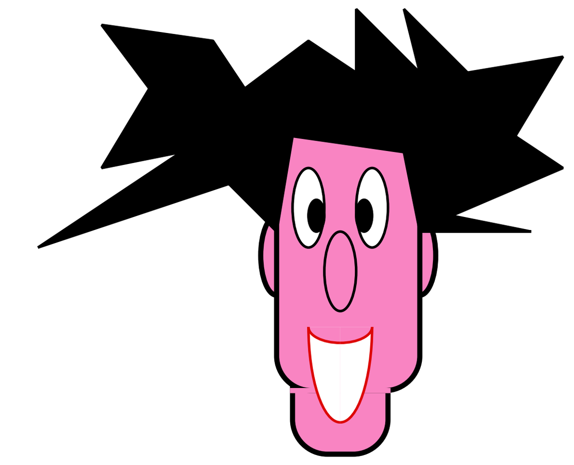


Ekert + Lo-Chau

Quantum-Key 

Distribution





A:	1	?	?	1	?	0	?	?	0	?	1	?	?	?	?	0	0	?	?	0	?	1	1	1
	×	👎	👎	+	👎	+	👎	👎	×	👎	+	👎	👎	👎	👎	×	×	👎	👎	+	👎	+	×	+
B:	\	¿	¿	|	¿	—	?	¿	/	¿	|	¿	¿	¿	¿	/	/	¿	¿	—	¿	|	\	|
A:	×	👎	👎	+	👎	+	👎	👎	×	👎	+	👎	👎	👎	👎	×	×	👎	👎	+	👎	+	×	+
B:	1			1		0			0		1					0	1			0		1	1	1
A:	1			1		0			0		1					0	0			0		1	1	1
A:	1			1		0			0		1					0	0			0		1	1	1
B:	=	↓	↓	=	↓	=	↓	↓	=	↓	=	↓	↓	↓	↓	=	≠	↓	↓	=	↓	=	=	=
B:		¿	¿		¿		?	¿		¿		¿	¿	¿	¿			¿	¿		¿			
A:		?	?		?		?	?		?		?	?	?	?			?	?		?			

10%

Shor-Preskill

Quantum-Key Distribution

• • • • •

• Produces raw quantum key (EPR states)

• Observed error rate indicates amount of impurity of EPR states

• Quantum error-correction (CSS) is used to purify raw EPR states into a smaller pure set

• • • • •

(

Q: (over GF(3))

$$|0\rangle \rightarrow |000\rangle + |111\rangle + |222\rangle$$
$$|1\rangle \rightarrow |012\rangle + |120\rangle + |201\rangle$$
$$|2\rangle \rightarrow |021\rangle + |102\rangle + |210\rangle$$

$$Q|\psi\rangle = H_1 \otimes H_2 \otimes H_3$$

$Q=[[3,1,2]]$ corrects 2-1=1 erasure.

$$|0\rangle \otimes H_2 \otimes H_3 \rightarrow (-H_2 - H_3 \bmod 3) \otimes H_2 \otimes H_3$$
$$H_1 \otimes |0\rangle \otimes H_3 \rightarrow H_1 \otimes (-H_3 - H_1 \bmod 3) \otimes H_3$$
$$H_1 \otimes H_2 \otimes |0\rangle \rightarrow H_1 \otimes H_2 \otimes (-H_1 - H_2 \bmod 3)$$

Calderbank-Shor-Steane Q-ECCs

Let C_1, C_2 be two linear codes such that

$$\{0\} \subseteq C_2 \subseteq C_1 \subseteq F^n$$

$$\{0\} \subseteq C_1^\perp \subseteq C_2^\perp \subseteq F^n$$

For $v \in C_1$ define

$$v \rightarrow \frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} |v + w\rangle$$

$$Q = \left\{ \frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} |w + v\rangle : v \in C_1 \right\}$$

For $v \in C_2^\perp$ define

$$v \rightarrow \frac{1}{\sqrt{|C_1^\perp|}} \sum_{w \in C_1^\perp} |v + w\rangle$$

$$Q^* = \left\{ \frac{1}{\sqrt{|C_1^\perp|}} \sum_{w \in C_1^\perp} |w + v\rangle : v \in C_2^\perp \right\}$$

CSS *Q*-ECCs

Let $C_1=[n,k_1,d_1]$, $C_2^{\perp}=[n,n\text{–}k_2,d_2]$ be two linear codes

$$\dim(Q) = \dim(C_1)\text{-}\dim(C_2^{\perp})$$
$$= k_1 - k_2$$
$$= \dim(C_2)\text{-}\dim(C_1^{\perp}) = \dim(Q^*)$$

$$d(Q) = d(Q^*) = \min\{d(C_1),d(C_2^{\perp})\} = \min\{d_1,d_2\}$$

$$Q = [[\ n,\ k_1\text{–}k_2,\ \min\{d_1,d_2\}\ ]] = Q^*$$

CSS *Q*-ECCs

EXAMPLE: Quantum Reed-Solomon codes (Aharonov-BenOr)

Let $q=4t$

$C_1 = [4t,2t+1,2t]$ ERS-code over GF(q)

$C_2 = [4t,2t,2t+1]$ ERS-code over GF(q)

$\dim(Q) = \dim(Q^*) = 1$

$d(Q) = d(Q^*) = 2t$

$Q,Q^* = [[4t, 1, 2t]]$ QRS-code over GF(q)

$Q,Q^* = [[n, 1, n/2]]$ QRS-code over GF(q), $q=n$

)