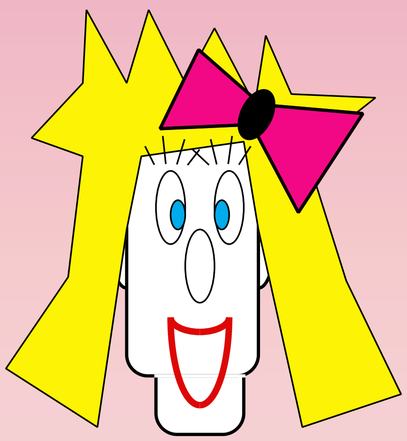
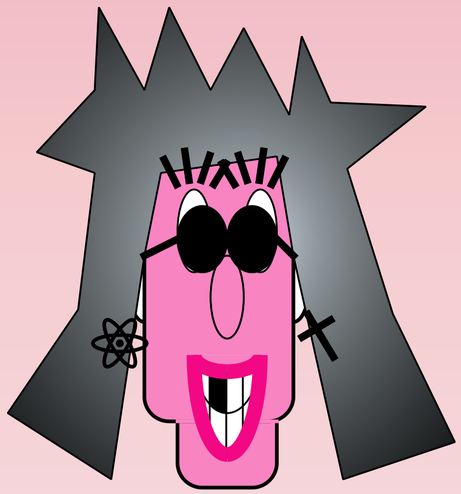
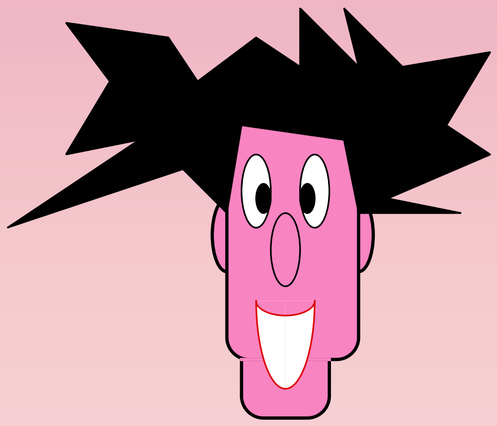
(3.1.2) One-time pad

Classical key : Vernam Q-cipher (various sources)
Quantum Ciphertext

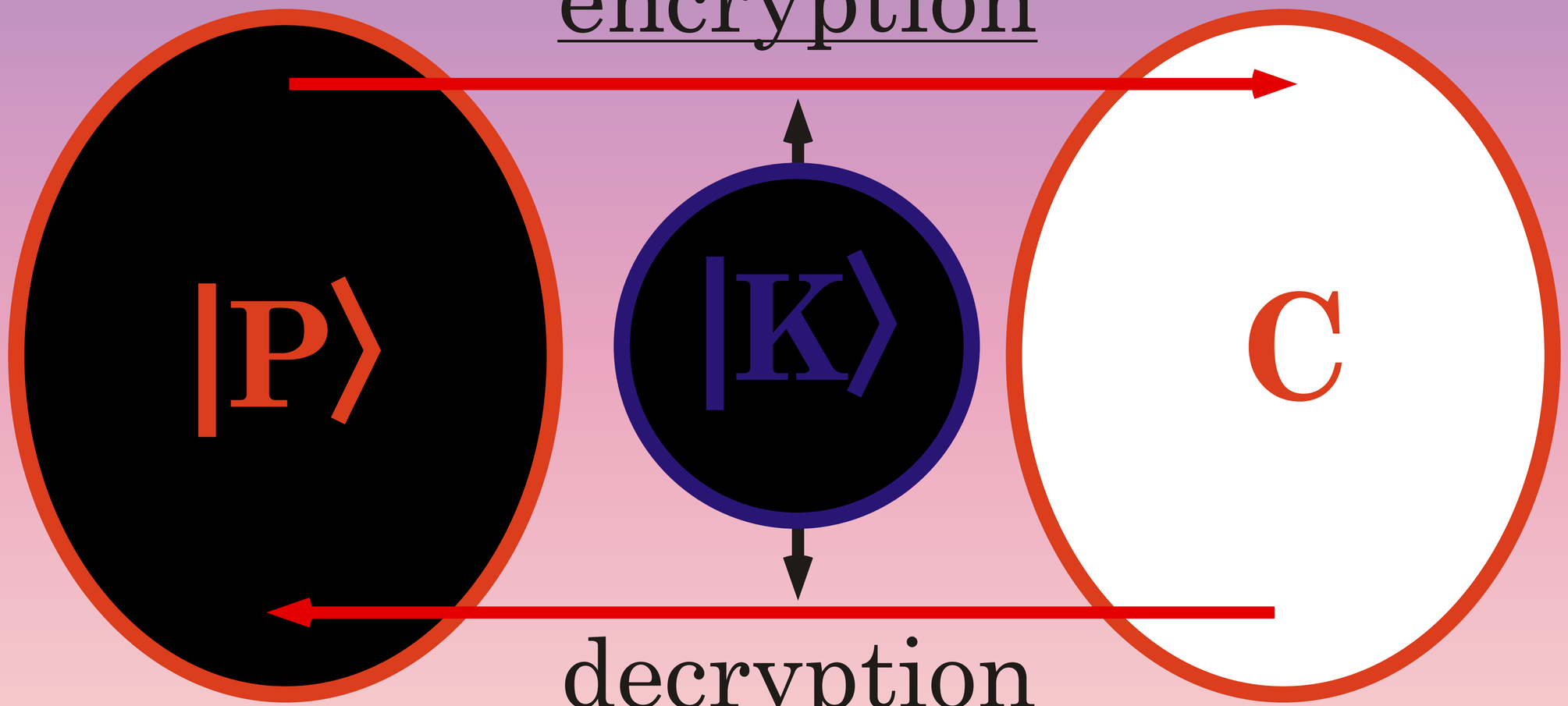
Quantum key : one-time Q-pad (Q-teleportation)
Classical Ciphertext (BBCJPW)





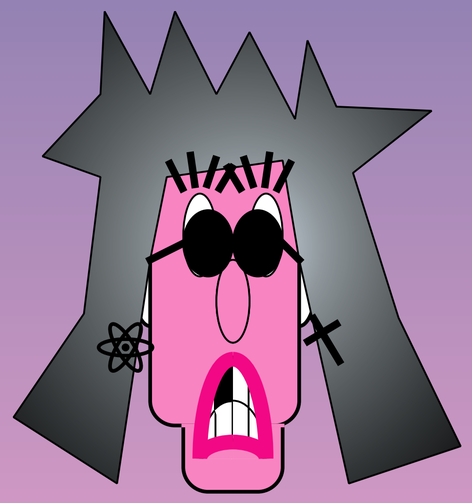


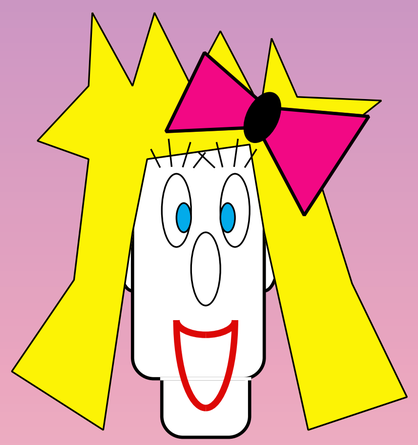
symmetric encryption of Quantum messages

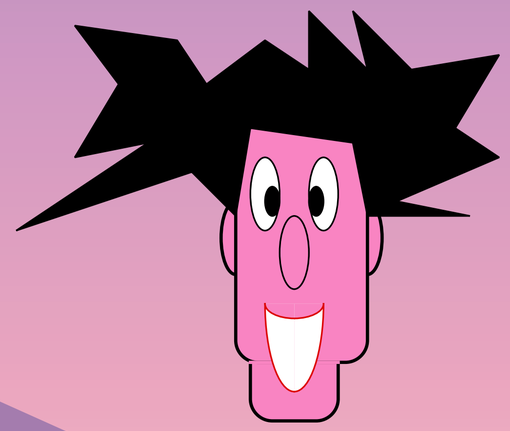


Information Theoretical Security

One-time Q-pad







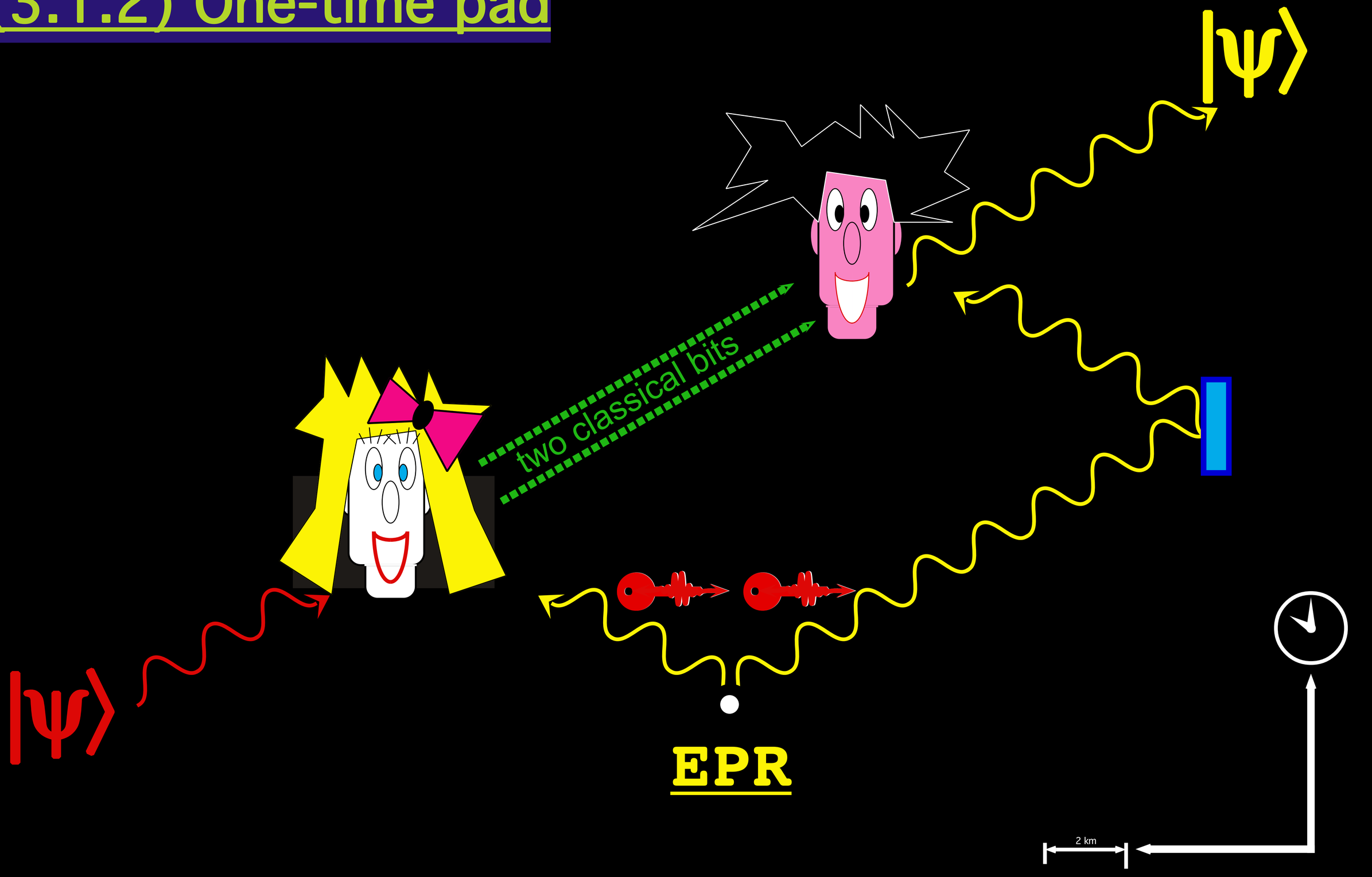
8RdewtU5qkLa$es!T9@

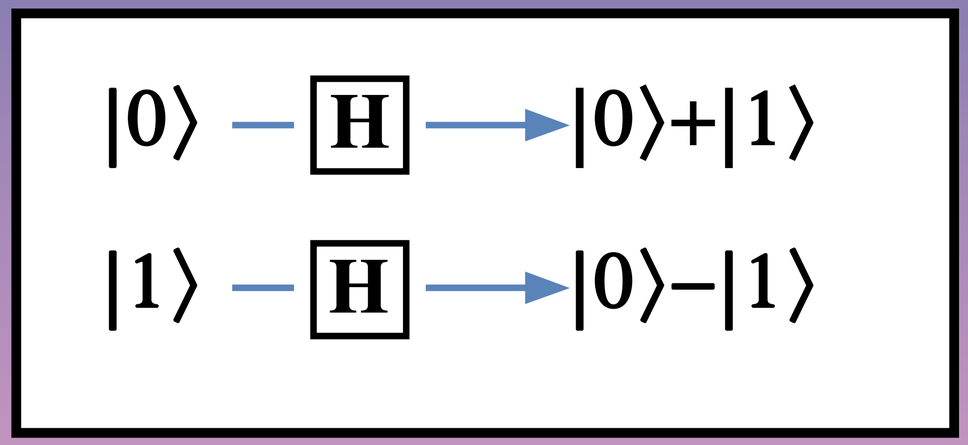
I(D%eXhDqliykl#2cV7dEwnMs

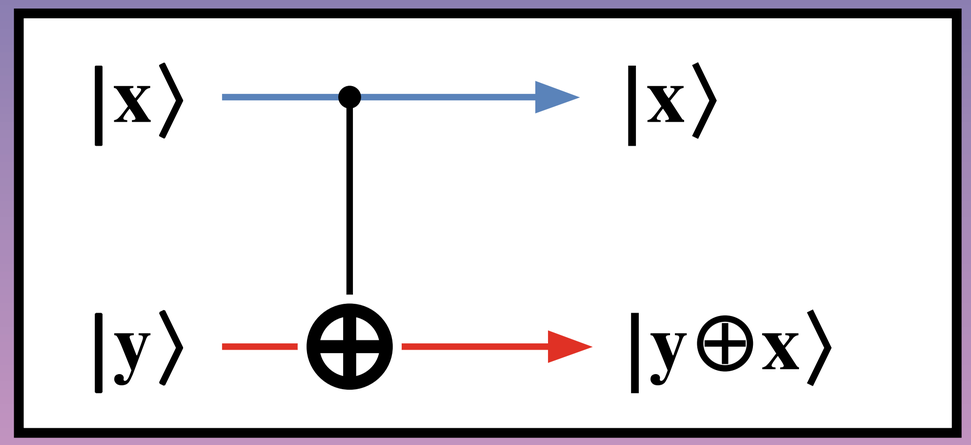
H&fs@tyHvFGhaOKpTrGbl.Z/rUih*

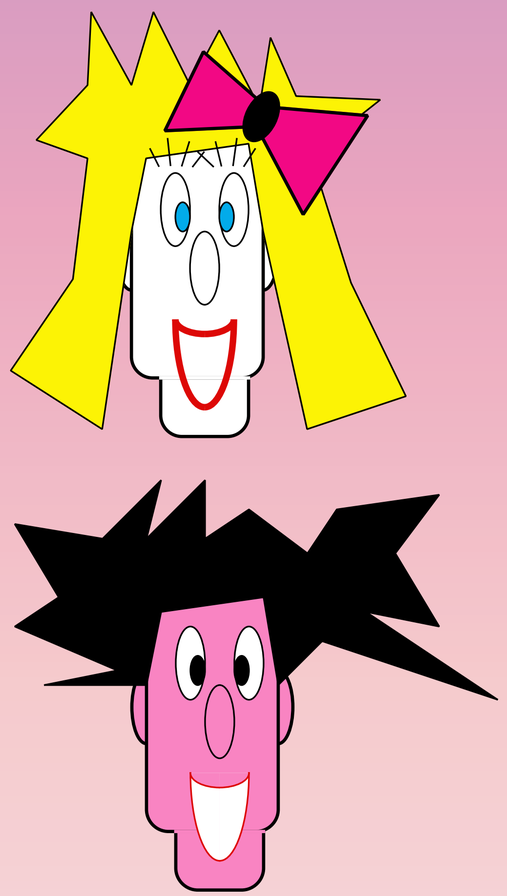
B7B3tdsjUila

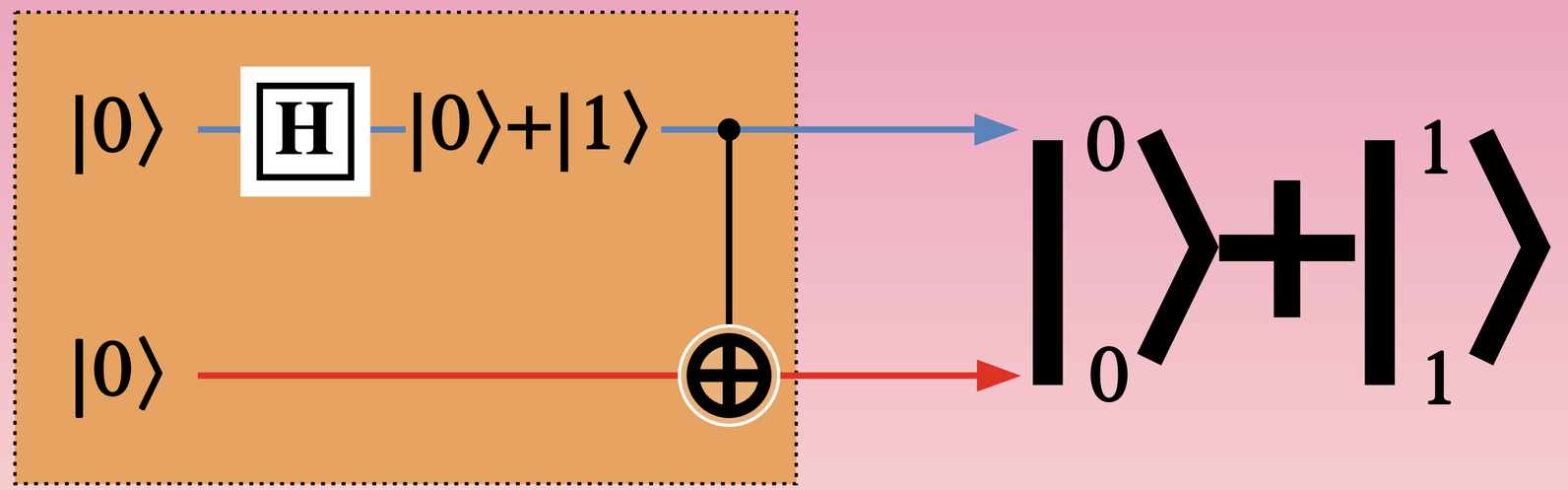
(3.1.2) One-time pad



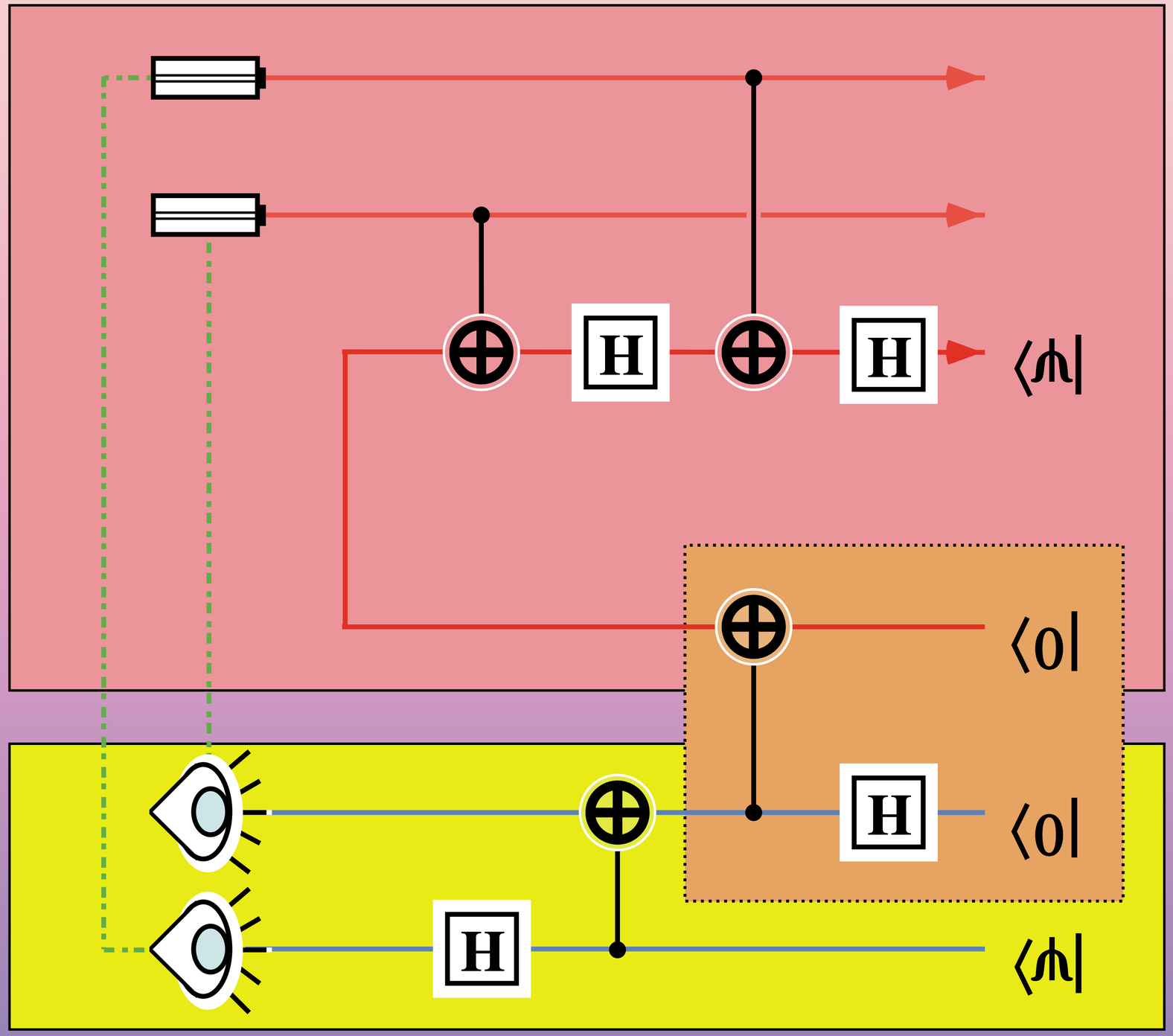


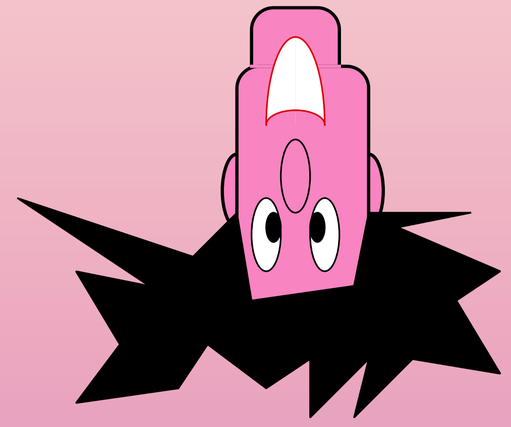


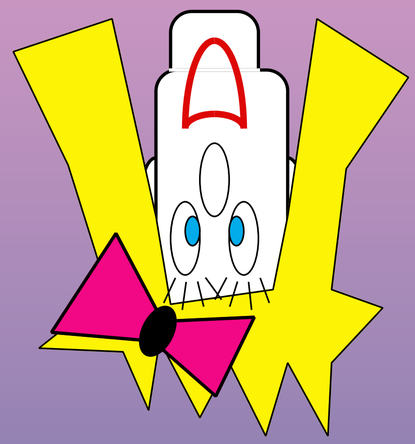


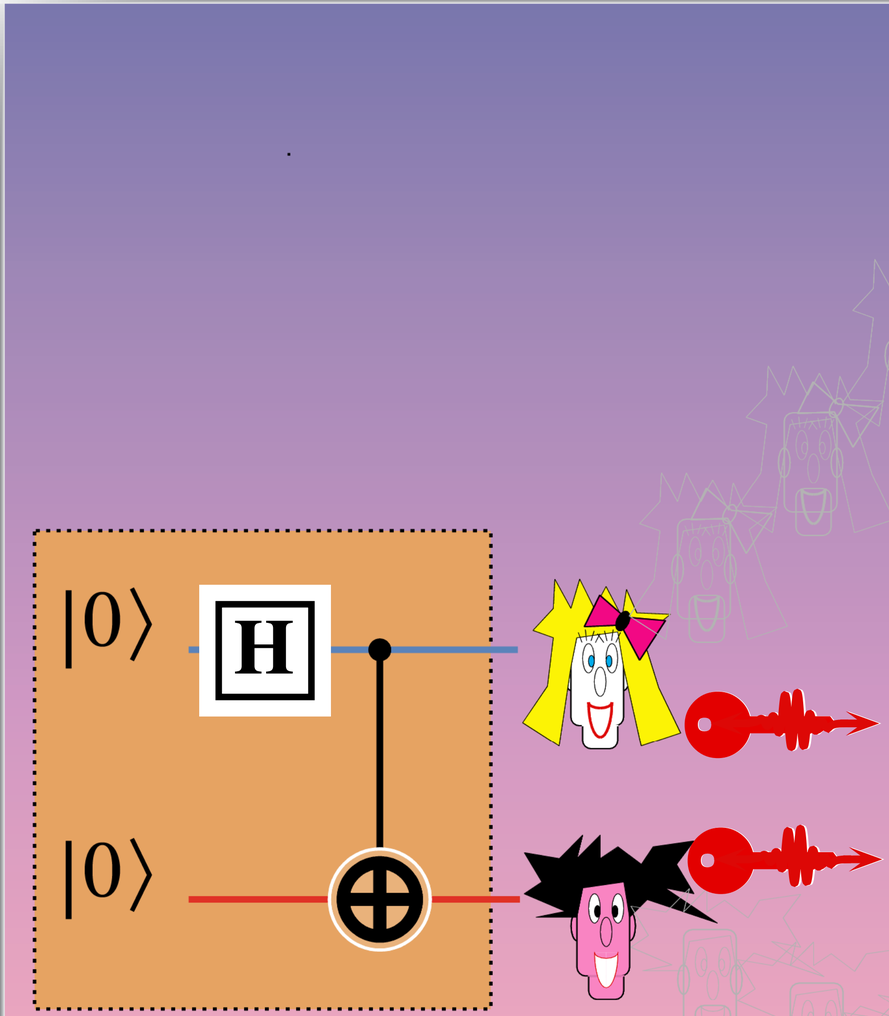


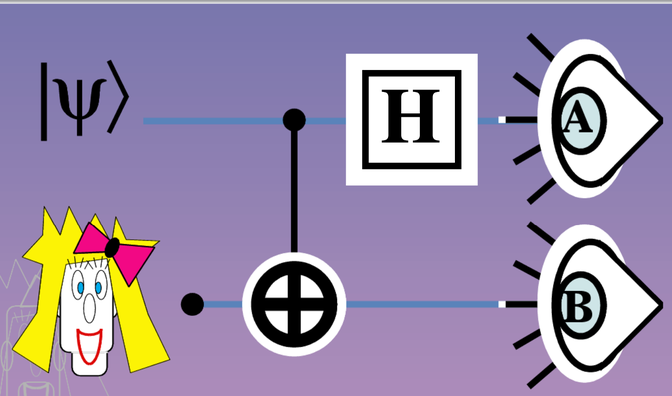
|??⟩

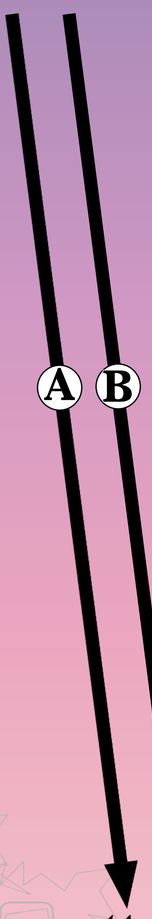


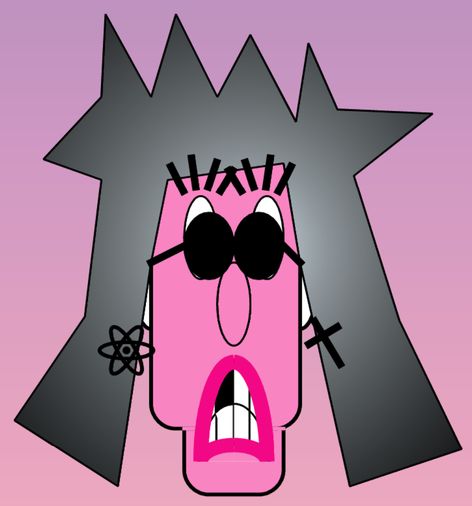




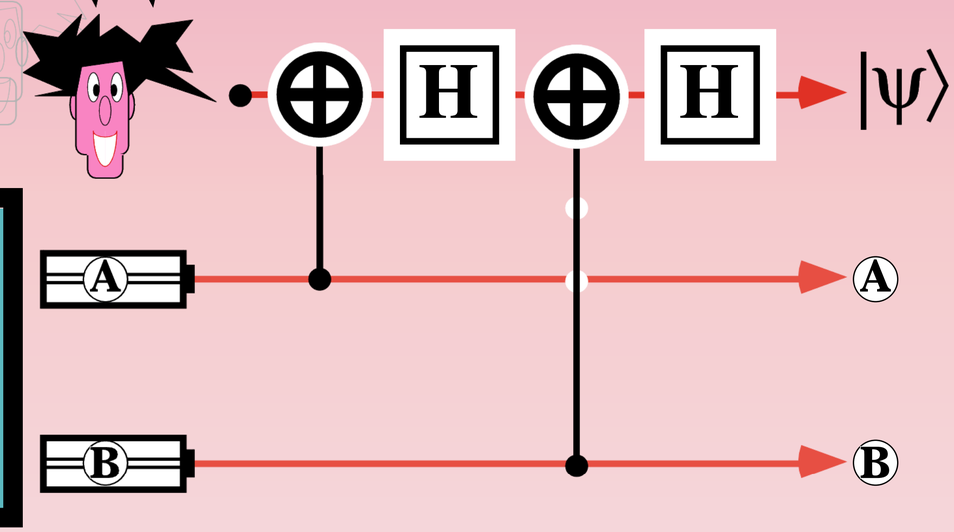








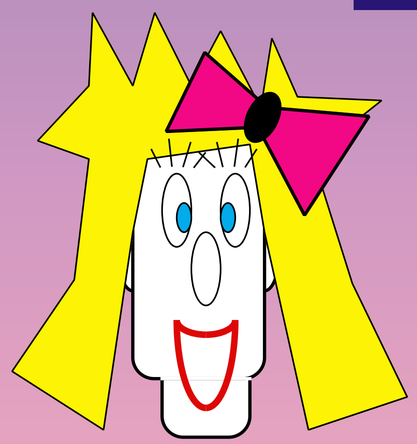
$$\sigma_x=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},\sigma_z=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$$



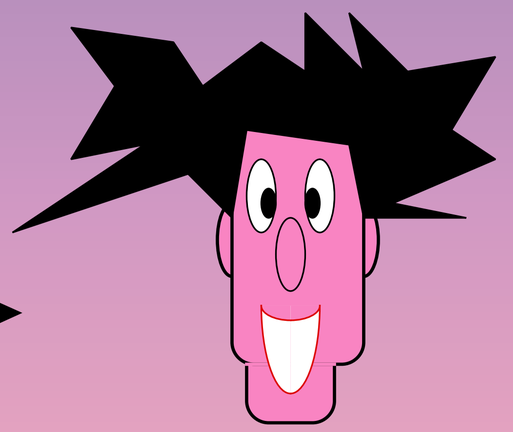
$$\begin{aligned}1/4 &: |\Psi\rangle\\ 1/4 &: \sigma_x|\Psi\rangle\\ 1/4 &: \sigma_z|\Psi\rangle\\ 1/4 &: \sigma_x\sigma_z|\Psi\rangle\end{aligned}$$

(3.1.2b) one-time pad

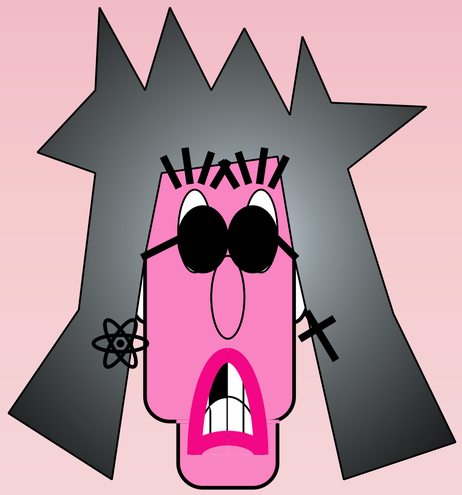
Quantum key : one-time Q-pad
Classical Ciphertext



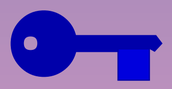
two random bits



$|\Psi\rangle$

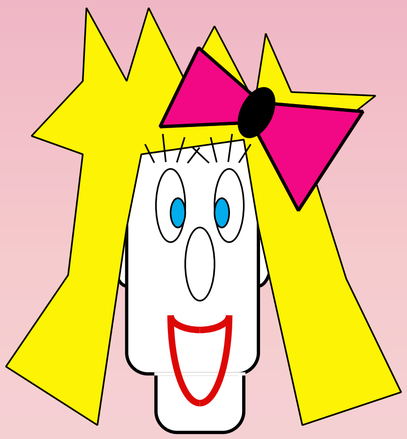


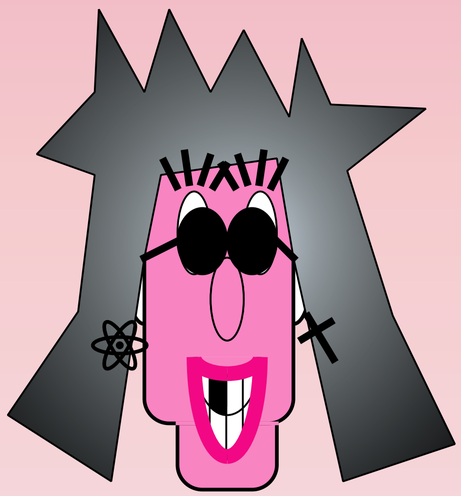
(3.1.2a) One-time pad

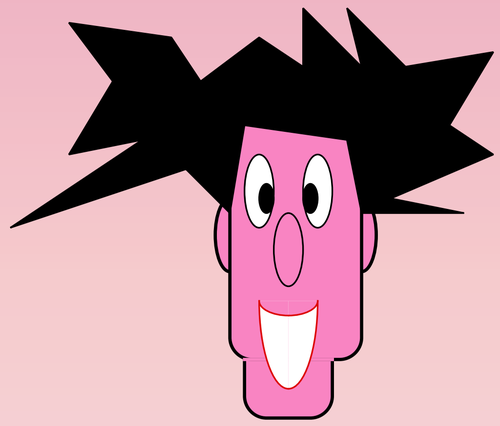


Classical key : Vernam Q-cipher (various sources)
Quantum Ciphertext

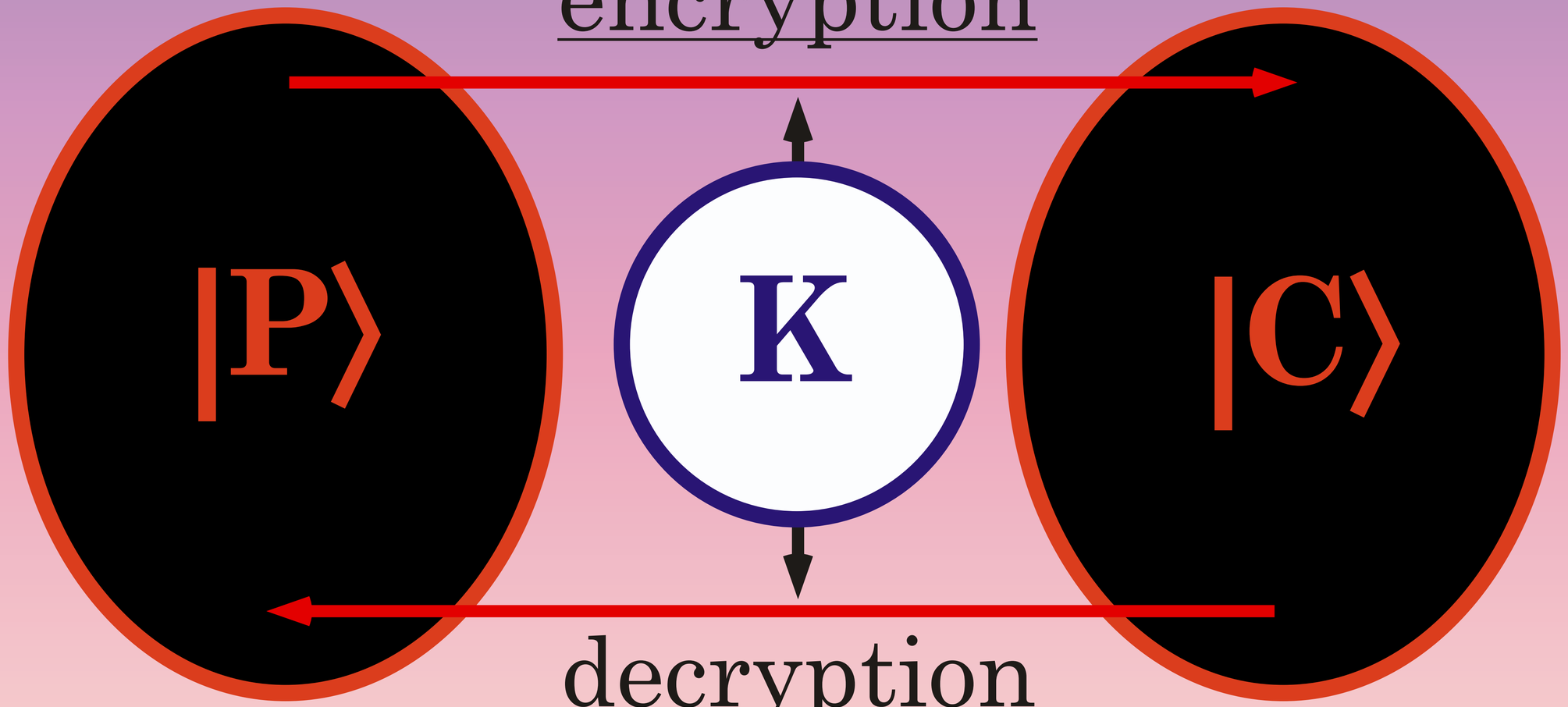
Quantum key : one-time Q-pad (BBCJPW)
Classical Ciphertext





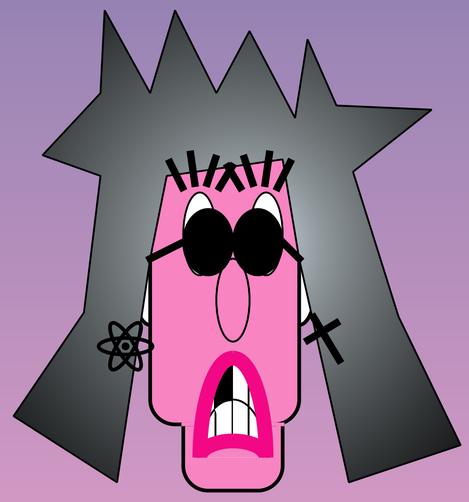


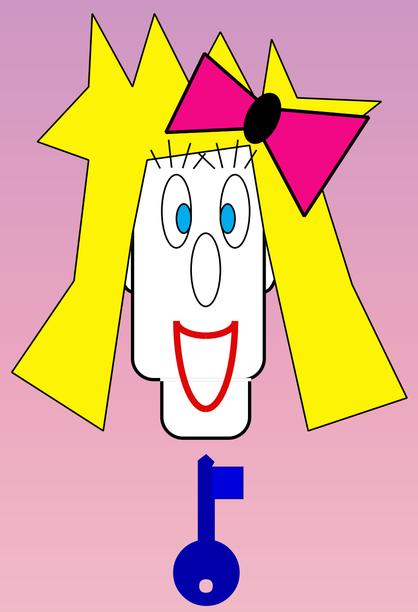
symmetric encryption of Quantum messages



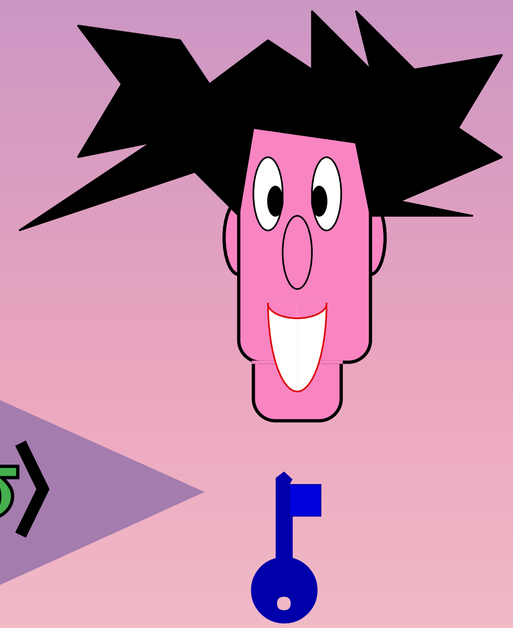
Information Theoretical Security

Vernam Q-cipher





|8PδεωτY5θκΛαΞεσ!T9≅⟩



|I(Δ%εΞηΔθIιψκλ#2χς7δEωνMσ⟩

|H&φσ≅τψϖΦηαOKπTρΓβλ.Z/ρYιη*⟩

|B7B3τδσφYιλα⟩

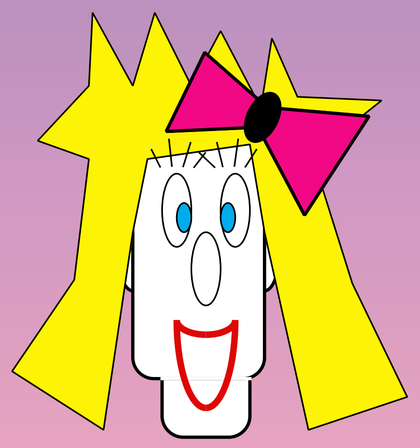
(3.1.2a) one-time pad

Classical key : Vernam Q-cipher

Quantum Ciphertext

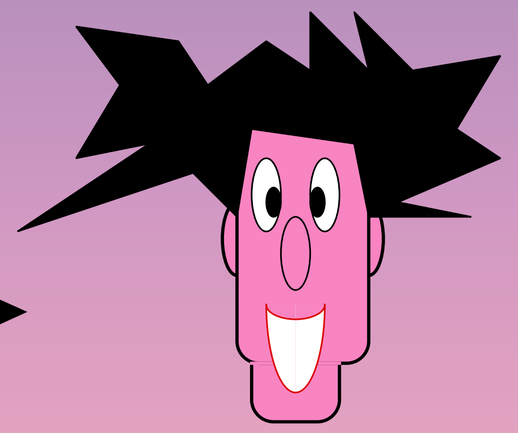
Quantum key : one-time Q-pad

Classical Ciphertext



$|\Psi\rangle$

$|\Psi'\rangle$



a,b random bit key

$|\Psi'\rangle = \sigma_x^a \sigma_z^b |\Psi\rangle$

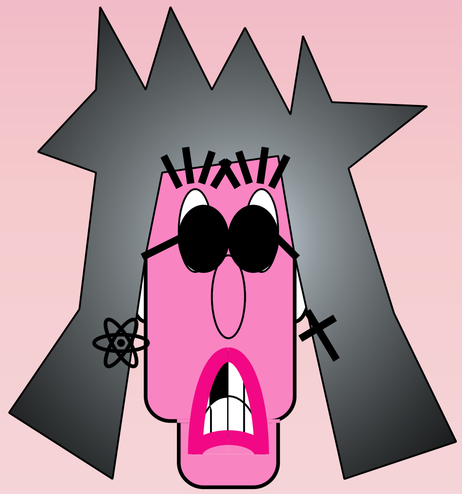
$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

¼ : $|\Psi\rangle$

¼ : $\sigma_x|\Psi\rangle$

¼ : $\sigma_z|\Psi\rangle$

¼ : $\sigma_x\sigma_z|\Psi\rangle$

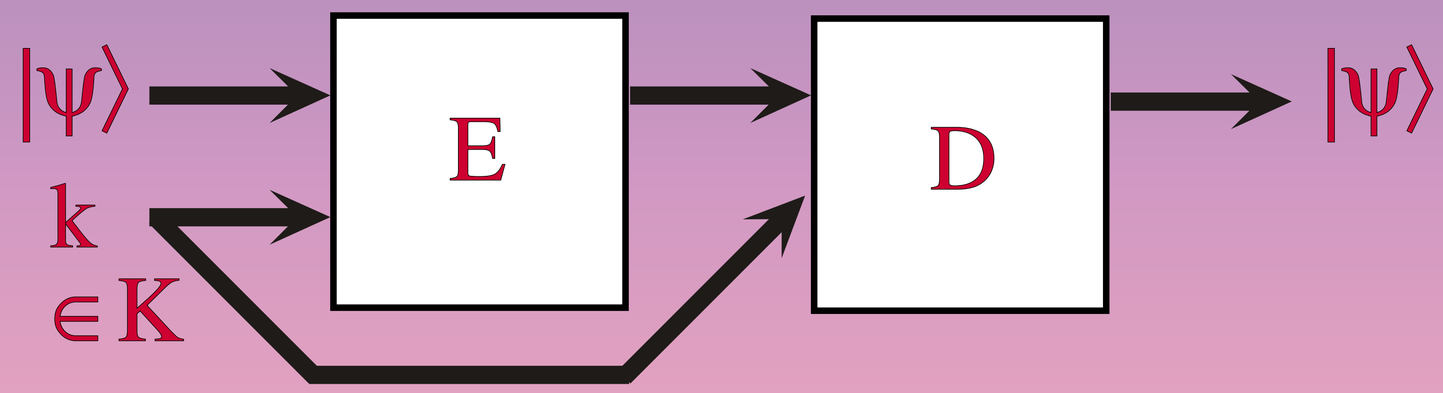


a,b random bit key

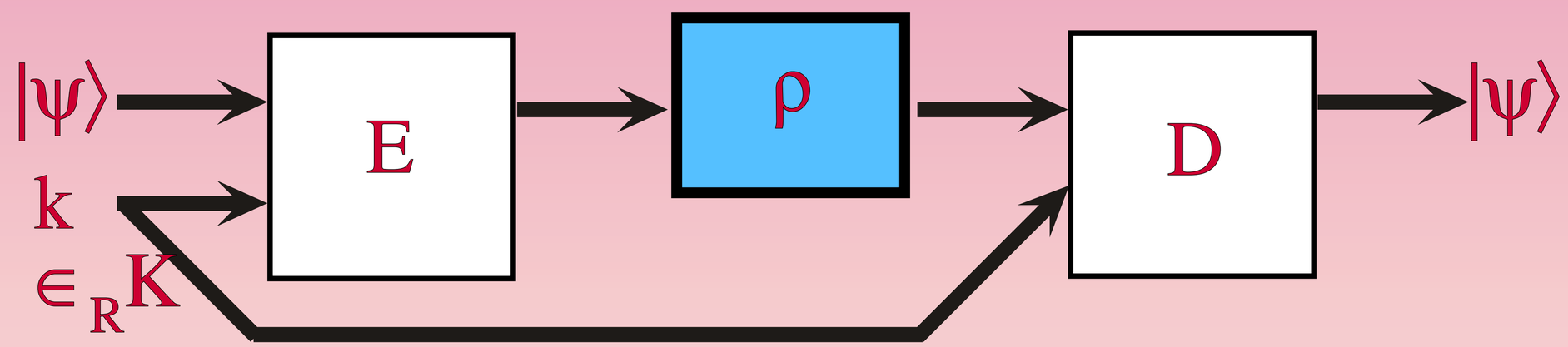
$|\Psi\rangle = \sigma_z^b \sigma_x^a |\Psi'\rangle$

One-time Q-encryption with error ε

Completeness:



Secrecy:



$$\forall |\psi_0\rangle, |\psi_1\rangle \quad D(\rho_0,\rho_1)=Tr(|\rho_0-\rho_1|)<\varepsilon$$

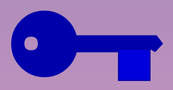
One-time Q-encryption with error ε>0

Lower bounds:

[MTW00]
Arbitrary quantum state = 2 bits / qubit

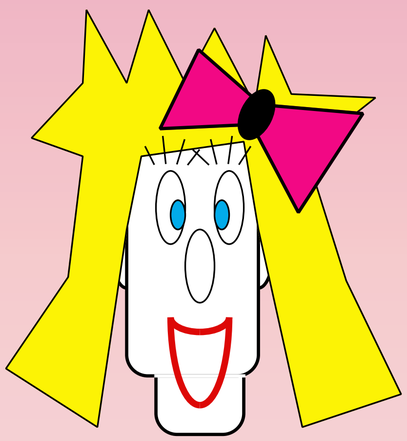
[HLSW03]
Arbitrary quantum state but not entangled with eavesdropper ~ 1 bit / qubit

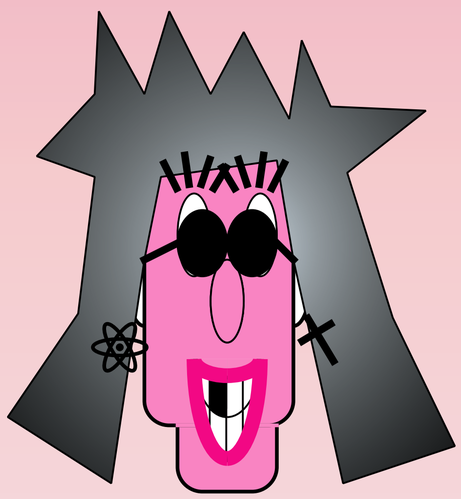
(3.1.3) One-time Q-Authentication

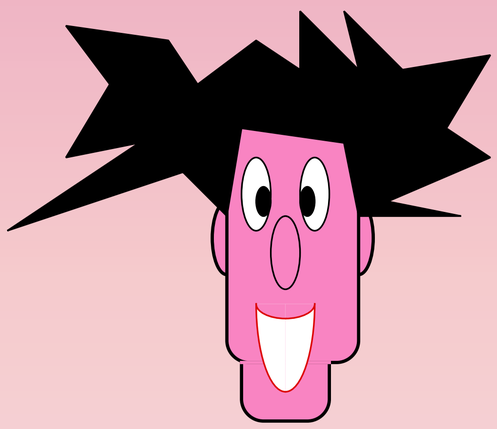


Classical key : Q-Authentication (BCGST)
Quantum message+tag

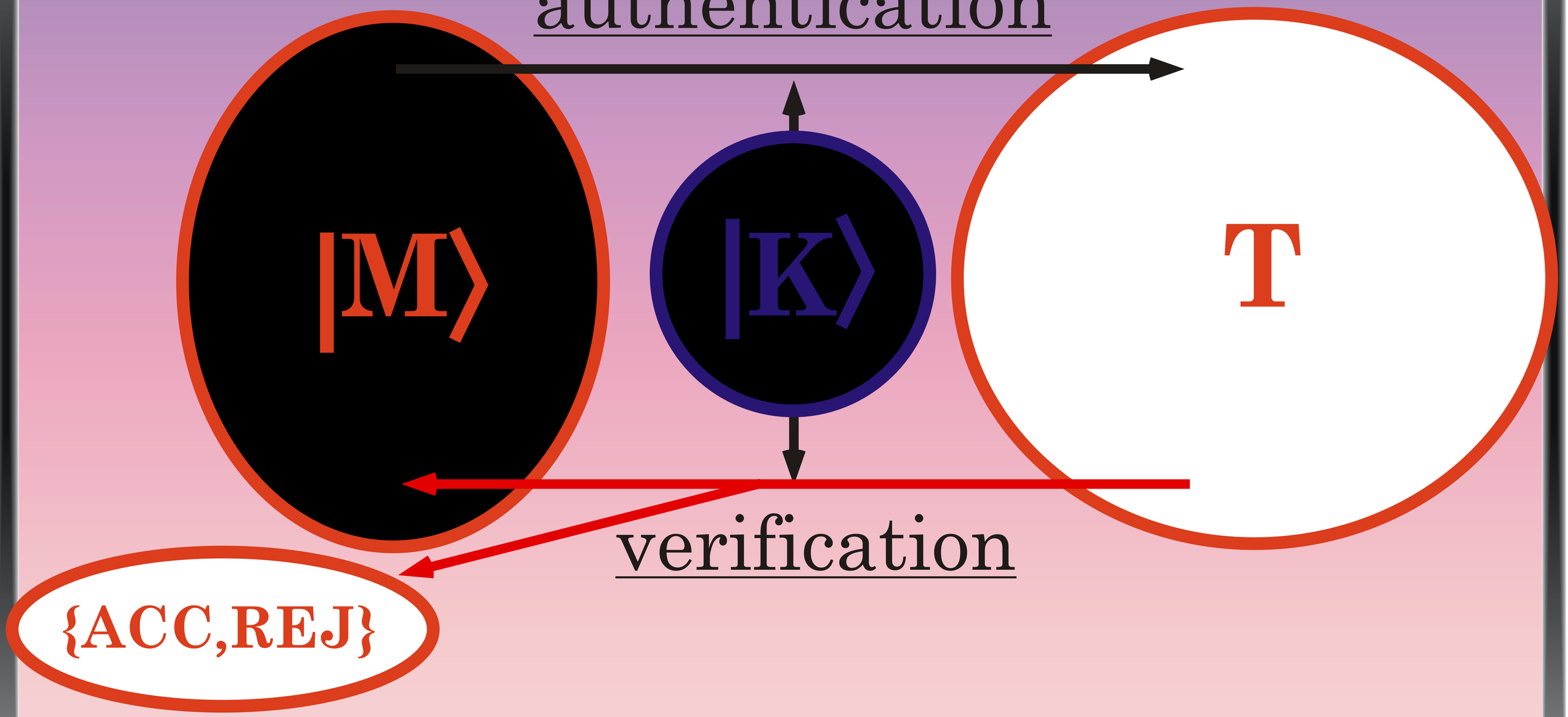
Quantum key : Authenticated Q-teleportation (BBCJPW)
Classical message+tag





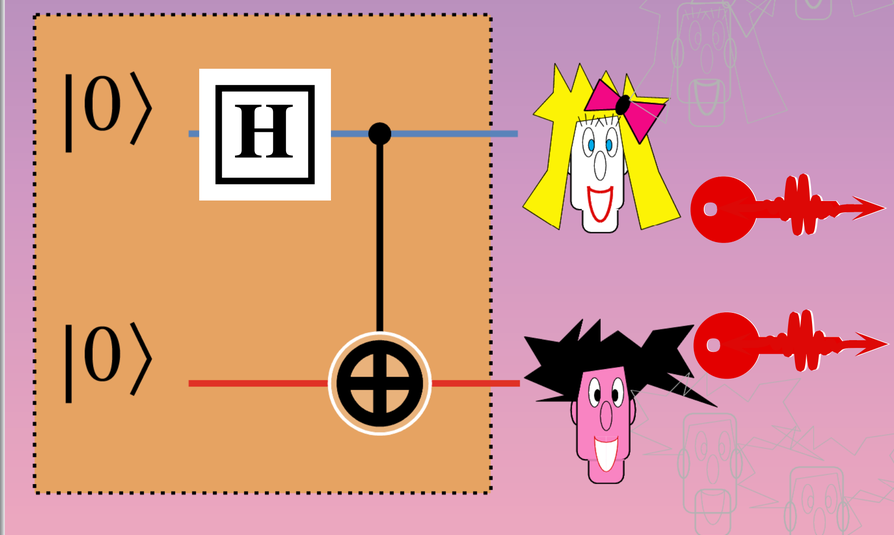


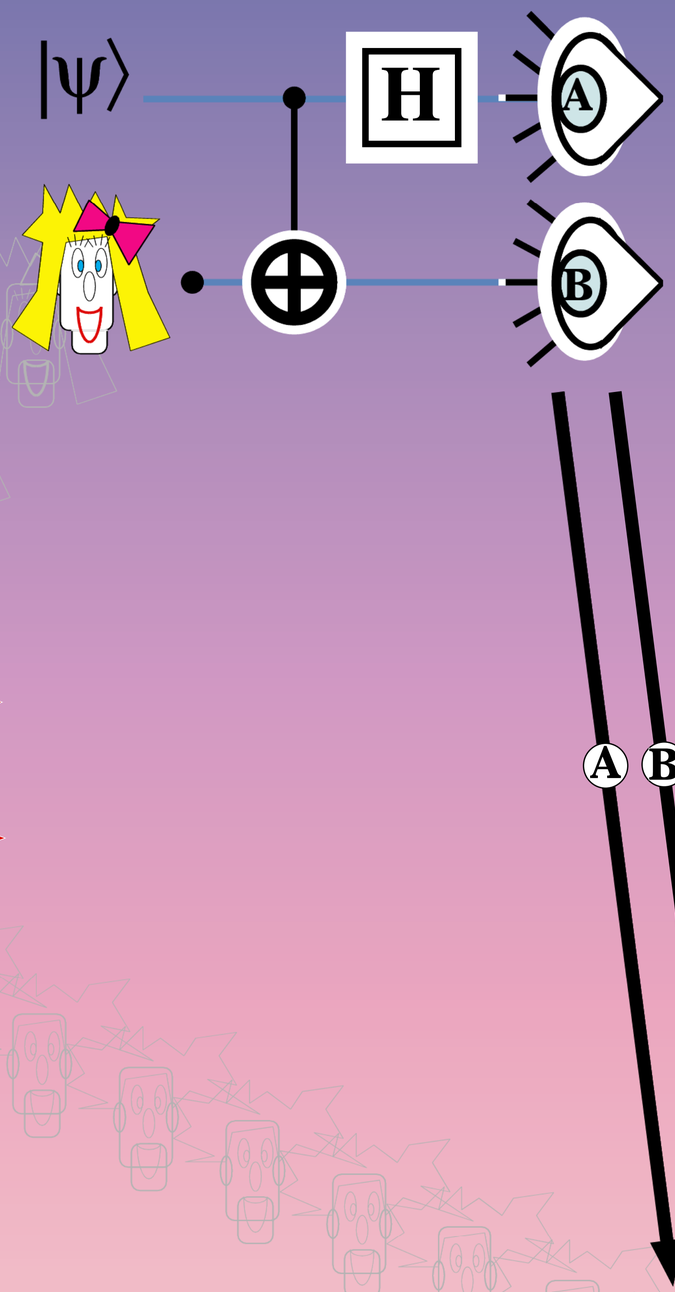
symmetric authentication

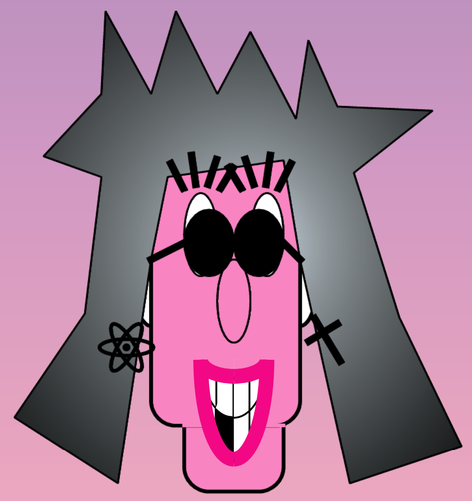


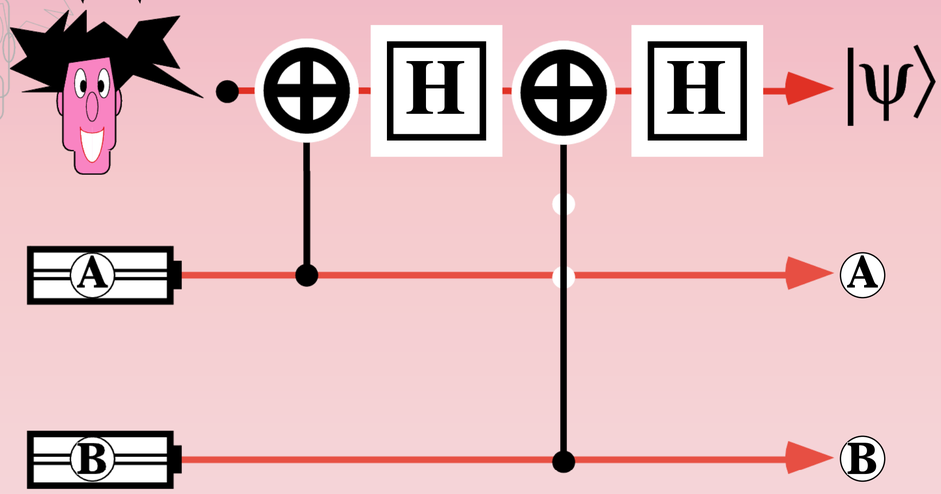
Information Theoretical Security

(3.1.3) One-time Q-Authentication

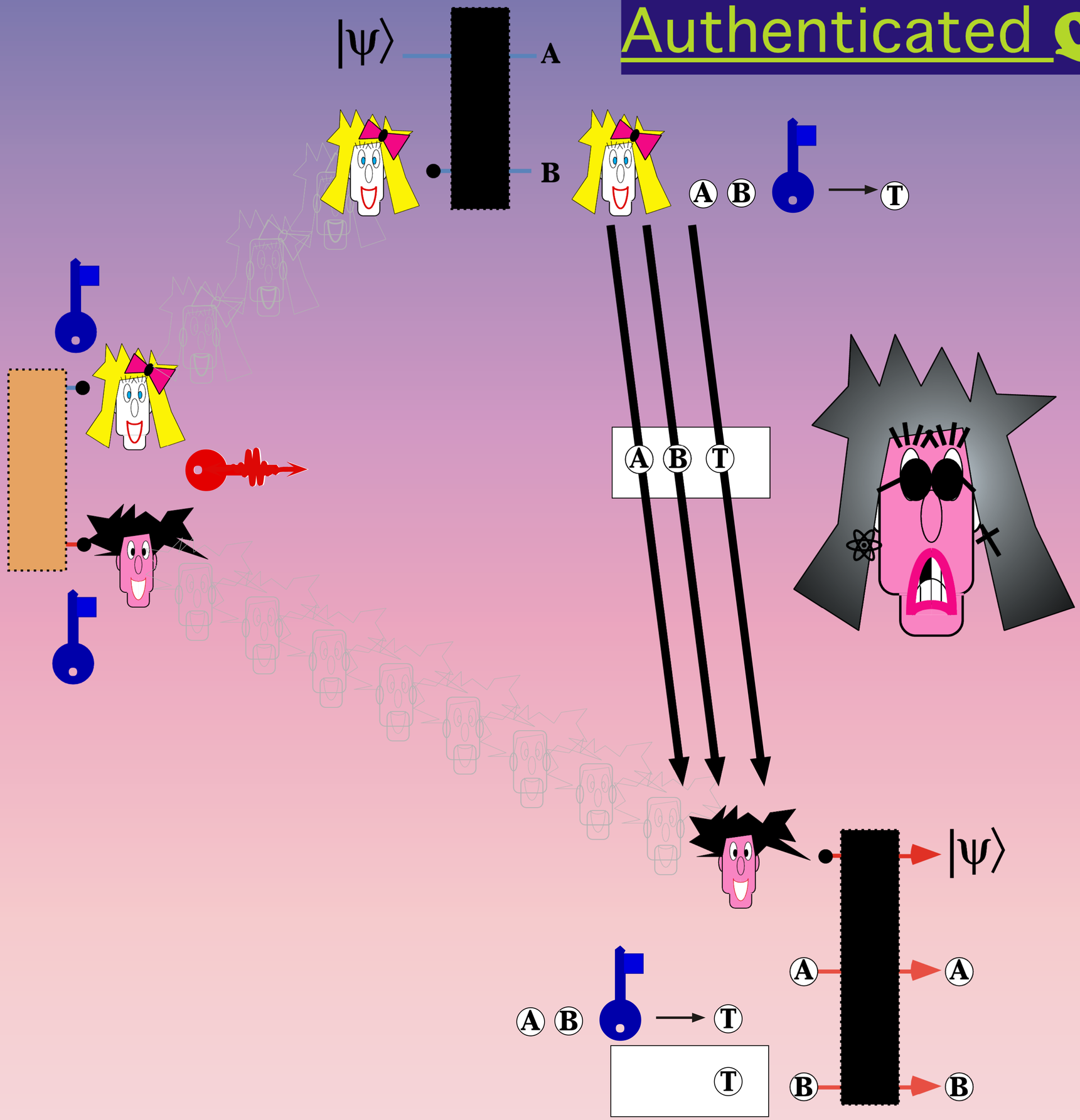




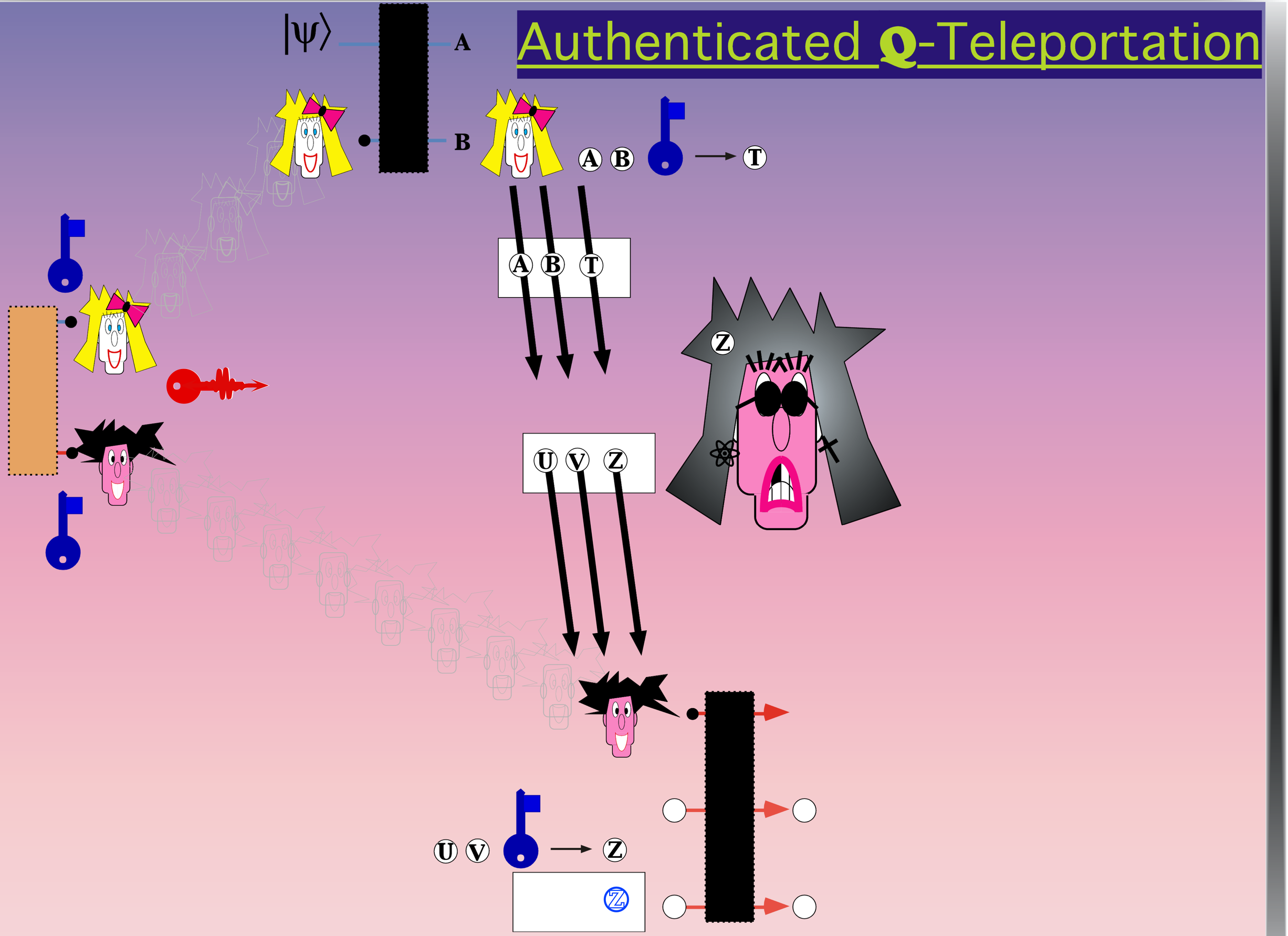




Authenticated Q-Teleportation

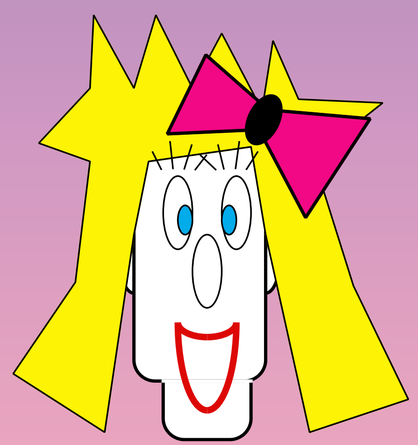


Authenticated Q-Teleportation



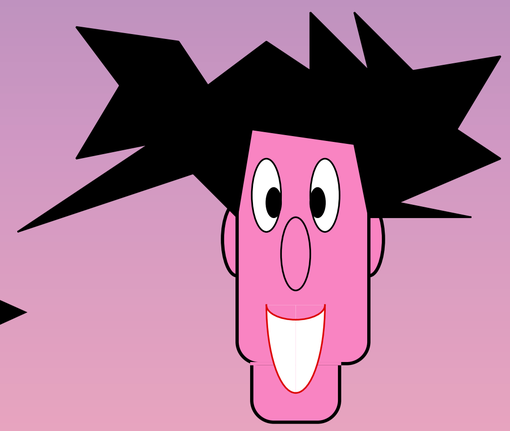
(3.1.3b) One-time Q-Authentication

Quantum key : 1x Authenticated Q-pad
Classical message+tag

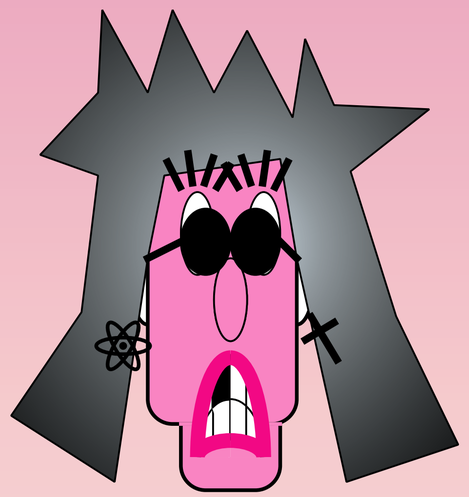


Ⓐ Ⓑ Ⓣ

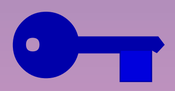
two authenticated random bits



$|\Psi\rangle$

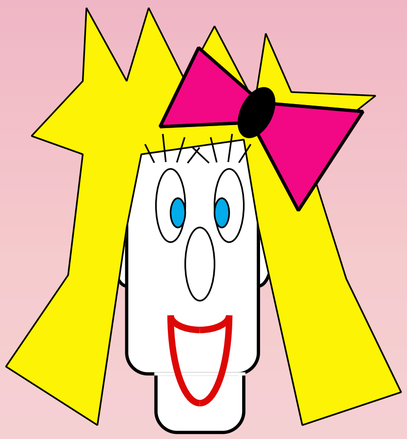


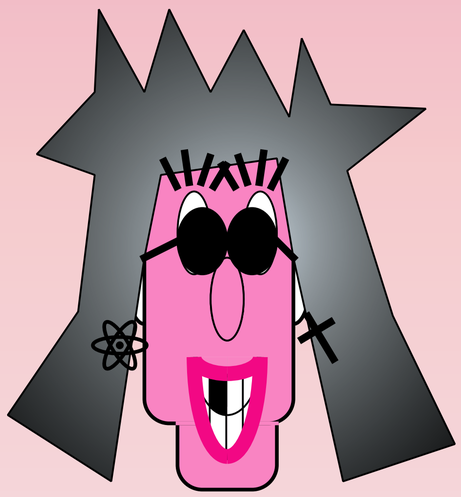
(3.1.3a) One-time Q-Authentication

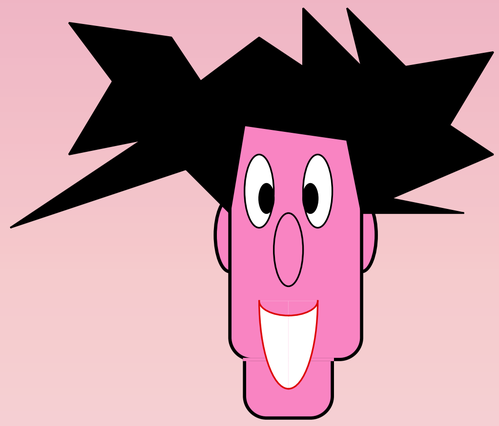


Classical key : Q-Authentication (BCGST)
Quantum message+tag

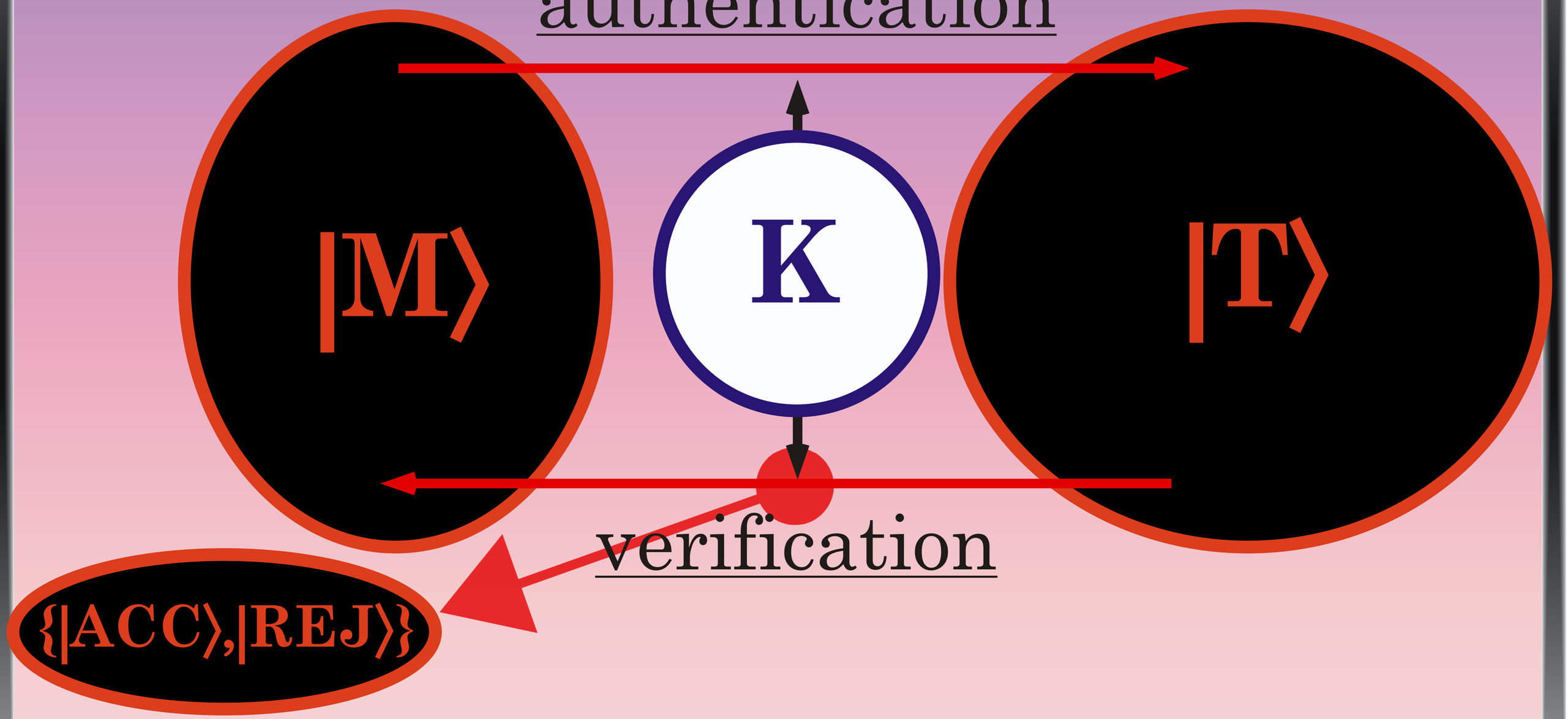
Quantum key : Authenticated Q-teleportation
Classical message+tag (BBCJPW)





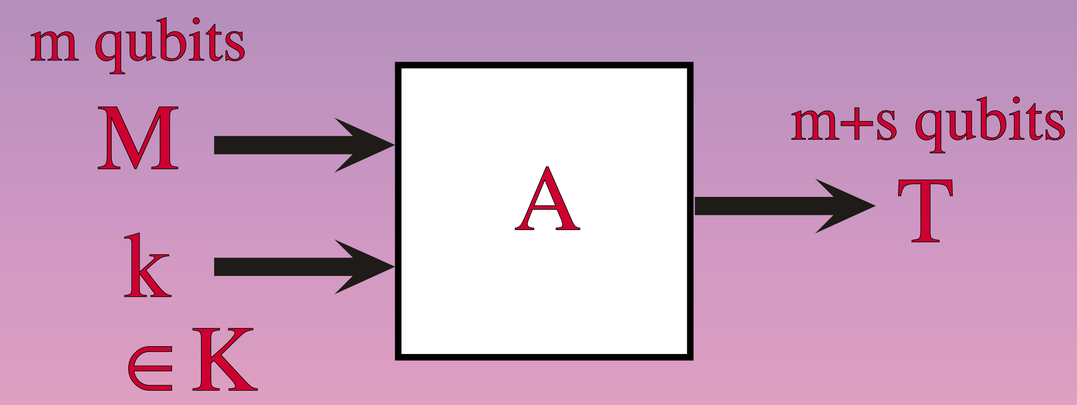


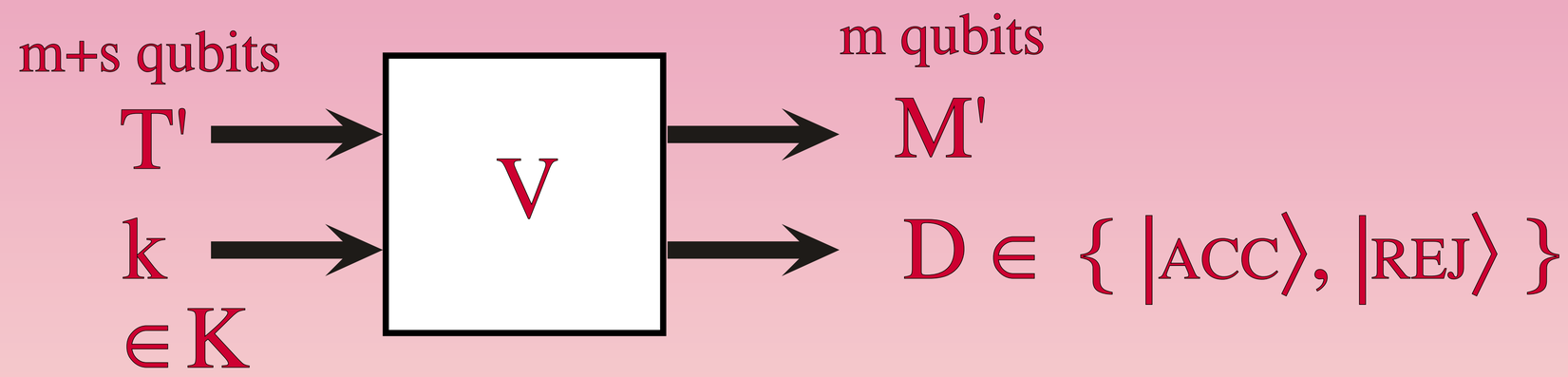
symmetric authentication of Quantum Messages



Information Theoretical Security

One-time Q-Authentication





One-time Q-Authentication

For any pure state $|\psi\rangle$ consider the measurement on (M',D) such that

- output Right if $M'=|\psi\rangle$ or if $D=|REJ\rangle$
- output Wrong otherwise

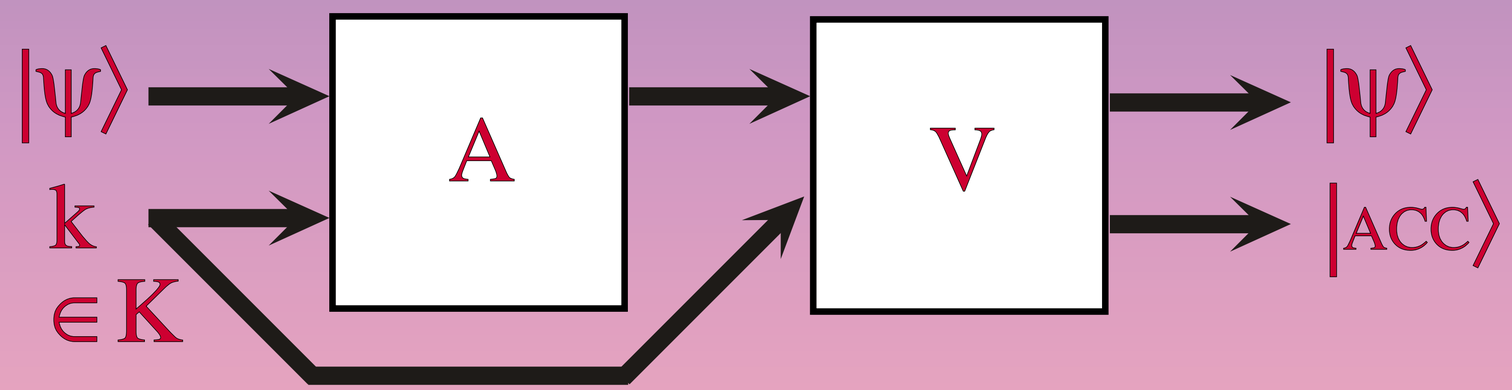
The corresponding projectors are

$$R_{|\psi\rangle} = |\psi\rangle\langle\psi| \otimes I_D + I_{M'} \otimes |REJ\rangle\langle REJ| - |\psi\rangle\langle\psi| \otimes |REJ\rangle\langle REJ|$$

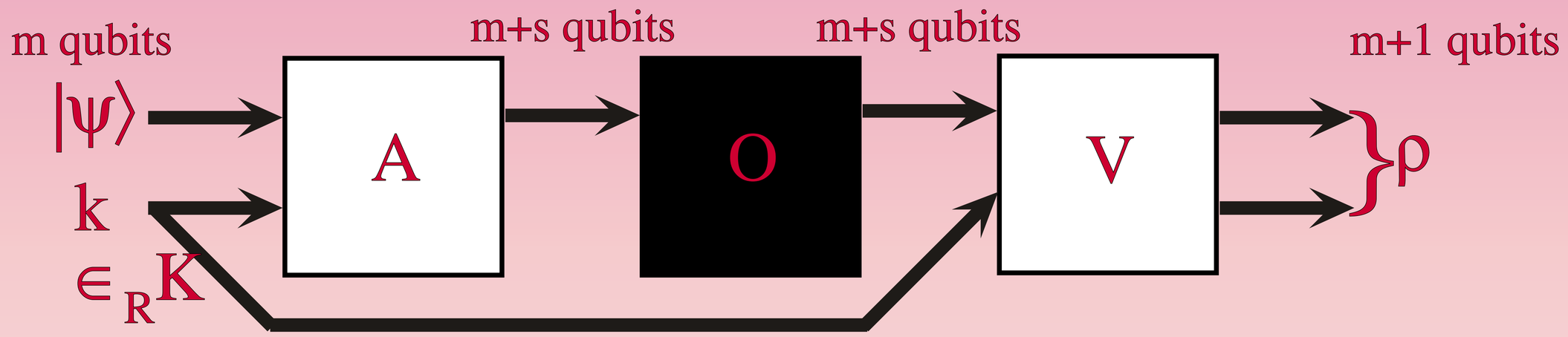
$$W_{|\psi\rangle} = (I_{M'} - |\psi\rangle\langle\psi|) \otimes |ACC\rangle\langle ACC|$$

One-time Q-Authentication

Completeness:

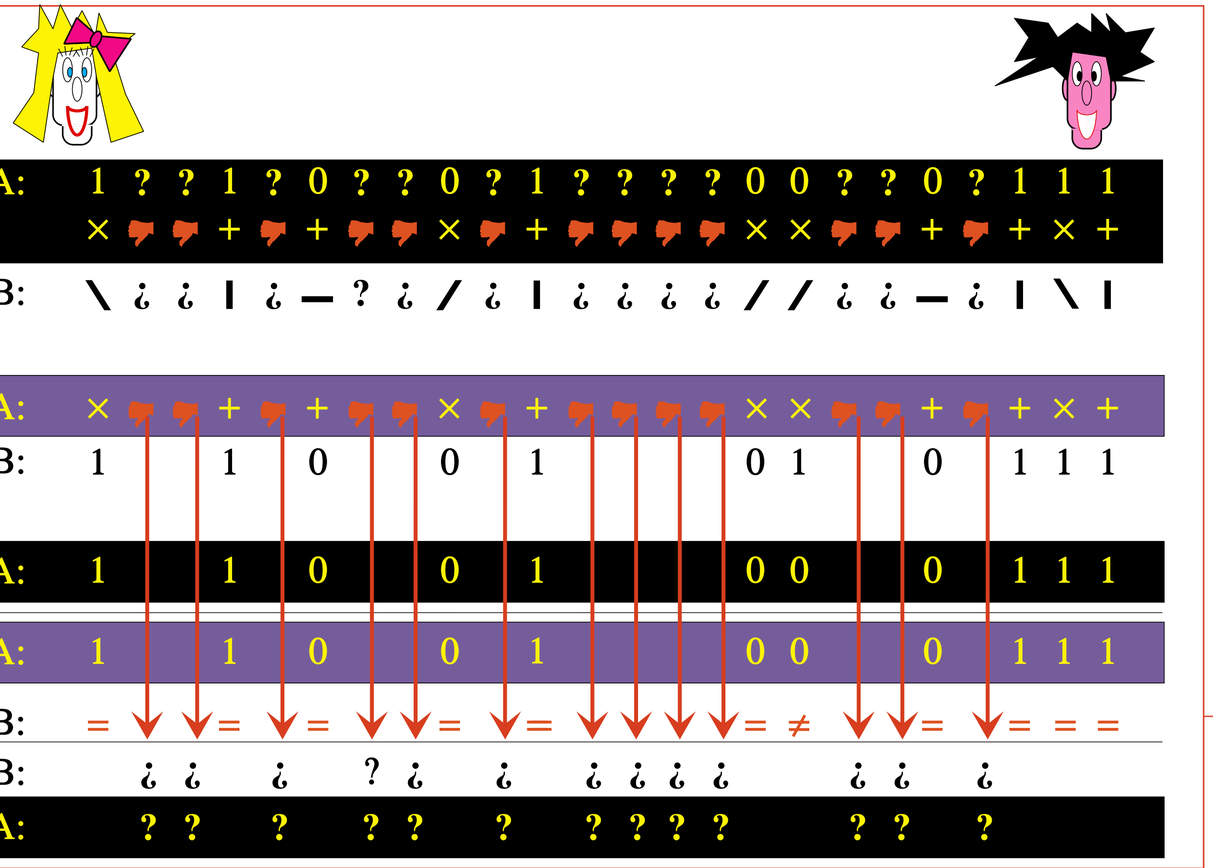


Soundness:

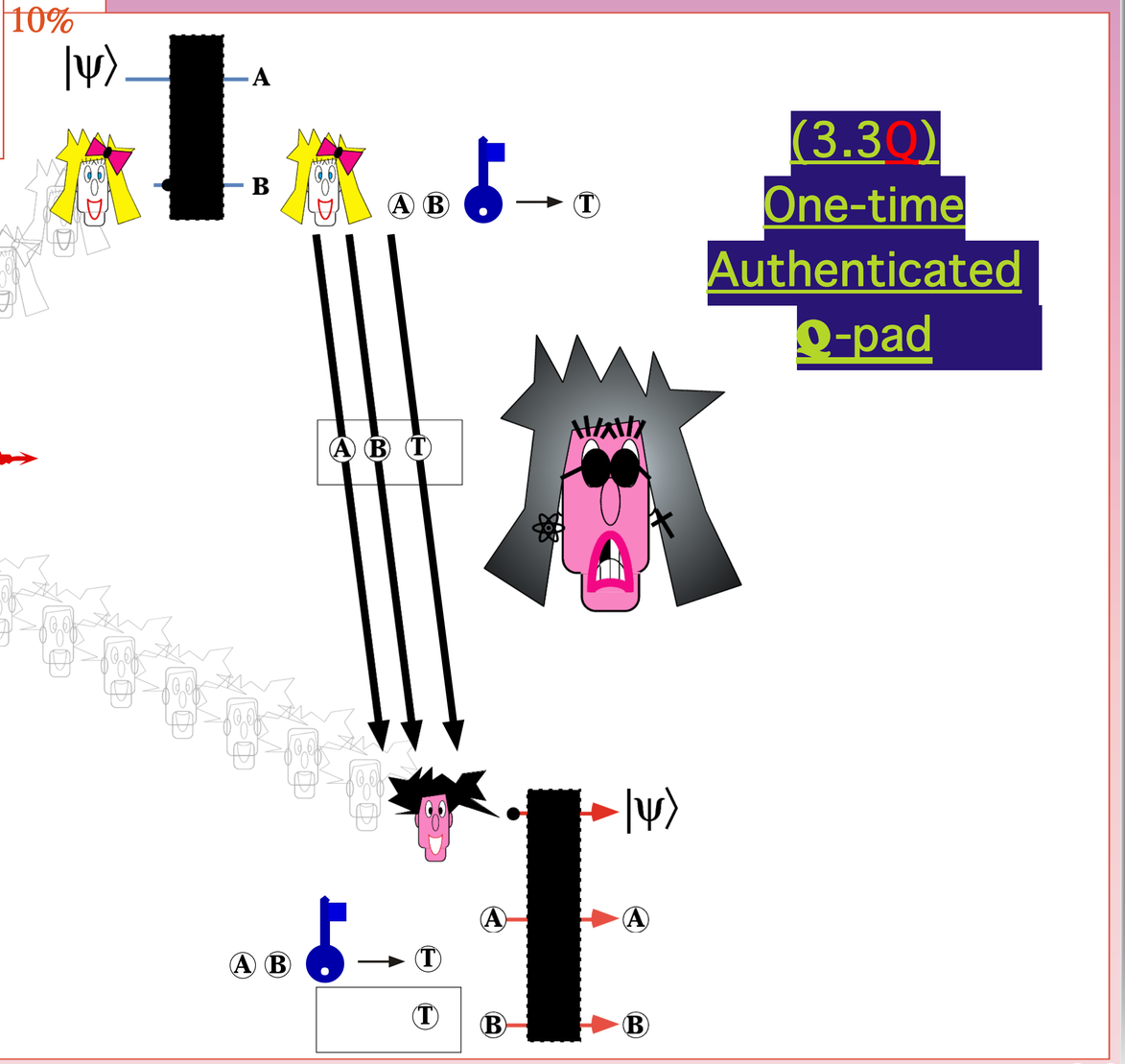


$$\forall|\psi\rangle\ \mathrm{Tr}(R_{|\psi\rangle}\rho)\geq 1-2^{-\Omega(s)}$$

(3.1Q) Quantum-Key distribution



Shor-Preskill



(3.3C) One-time interactive Q-Authentication

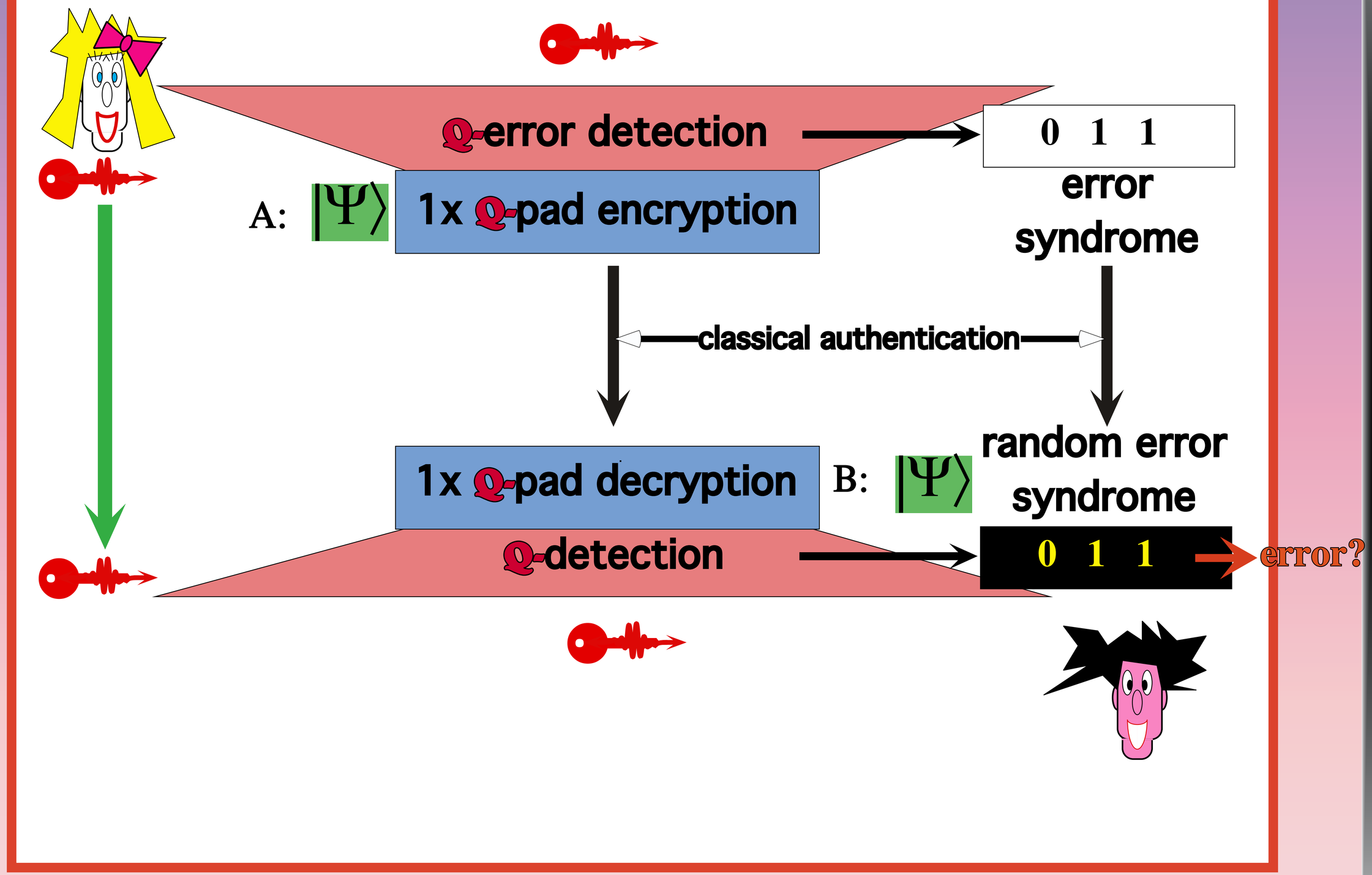
.....

- Transmit quantum key (EPR states)
- Quantum error-correction is used to purify (or test purity of) EPR states to form a smaller pure set

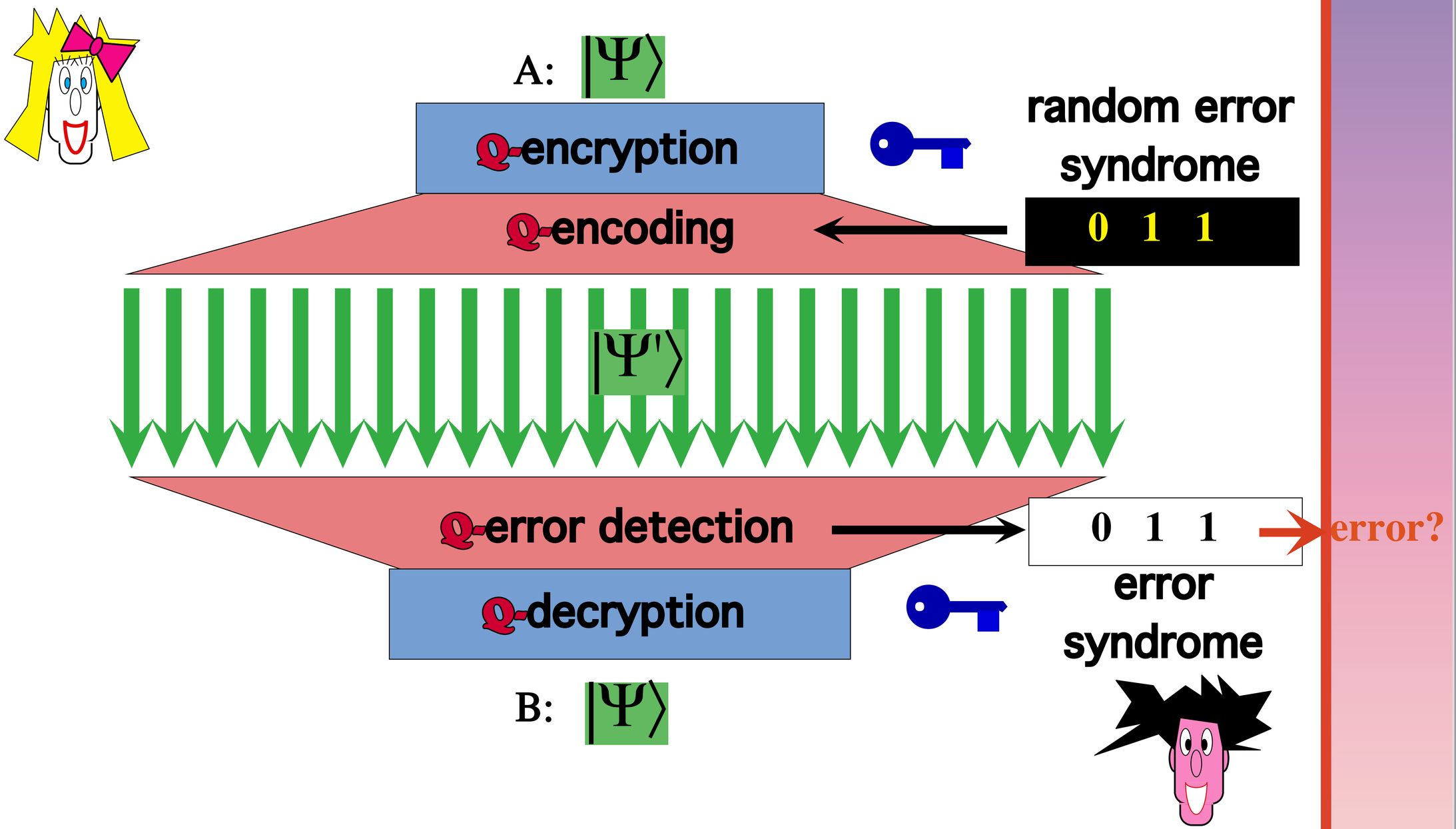
- one-time Authenticated Quantum pad is used to send message

.....

(3.3C) One-time interactive Q-Authentication



(3.1.3a) One-time Q-Authentication



Barnum-Crépeau-Gottesman-Smith-Tapp

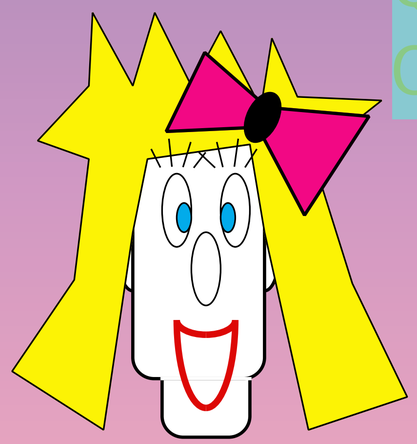
(3.1.3a) One-time Q-Authentication

Classical key : one-time Q-authentication

Quantum message+tag

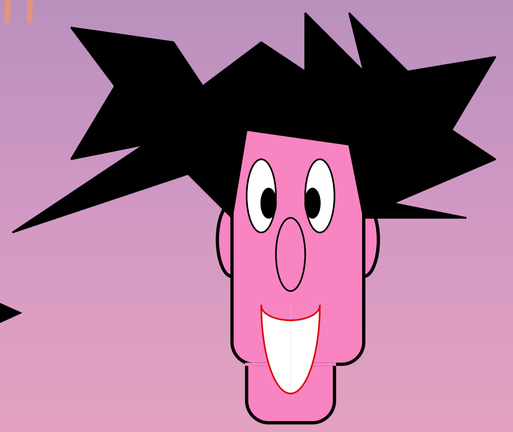
Quantum key : Authenticated Q-teleportation

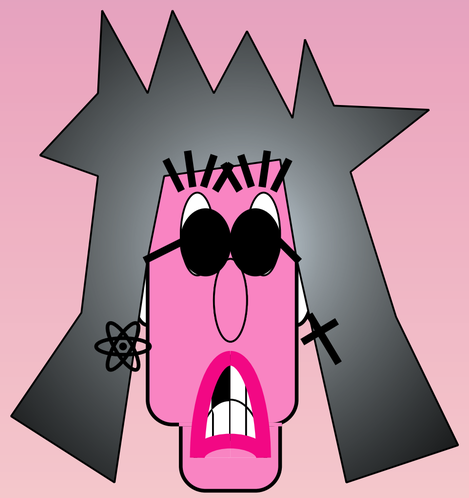
Classical message+tag



$|\Psi\rangle$

$|\Psi'\rangle$





- public Q-error-correcting code
- secret key for encryption & syndrome

Barnum-Crépeau-Gottesman-Smith-Tapp

one-time Q-authentication

⇒

Vernam Q-cipher

(authenticated quantum messages must be encrypted
which is false for classical messages!)

Main Lower Bound

A Quantum Authentication Scheme with error probability ε

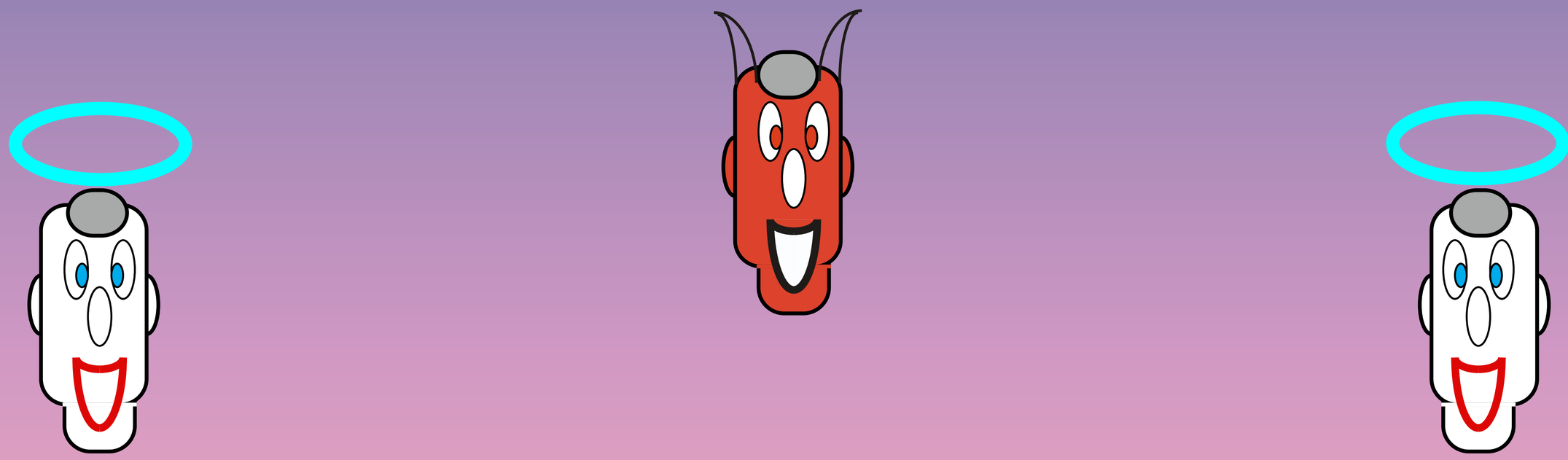
is

A Quantum Encryption Scheme with error probability $4\varepsilon^{1/6}$.

(3.2)

Complexity Theoretical Quantum Cryptography

(3.2) Complexity Theoretical Cryptography



. . . . .

(3.2.1) Public key cryptosystem : public-key **Q**-cryptosystem

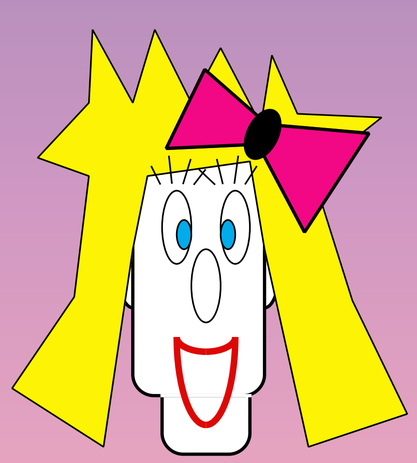
(3.2.2) Digital signature scheme : public-key **Q**-Authentication
Q-digital signature scheme

(3.2.3) (trapdoor) one-way functions : **Q**-cryptanalysis
(trapdoor) **Q**-one-way functions

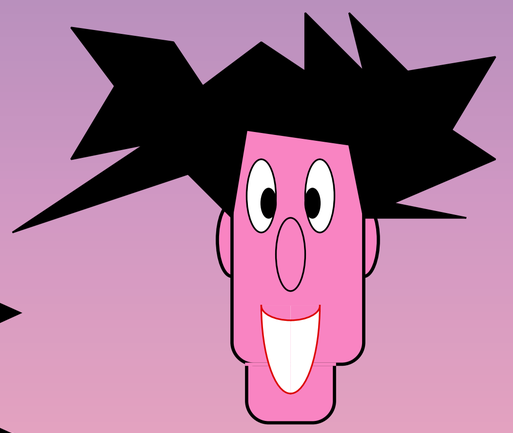
. . . . .

(3.2.1) Public-Key Q-Cryptosystem

Assuming Classical Public Key Cryptography

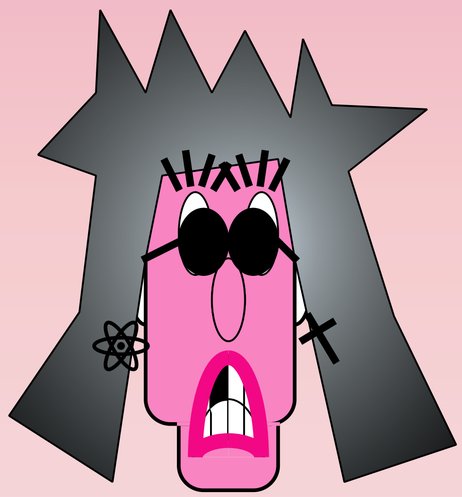


$|\Psi\rangle$



a,b random bits

$|\Psi'\rangle = \sigma_x^a \sigma_z^b |\Psi\rangle$

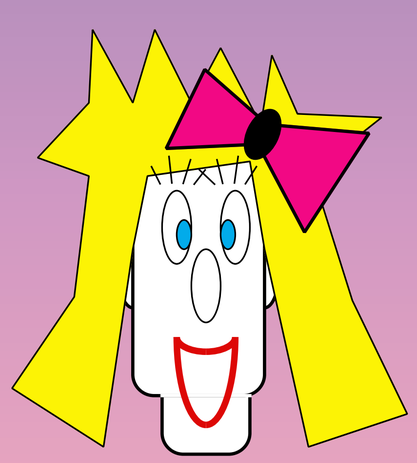


(a,b) := D(E(a,b))

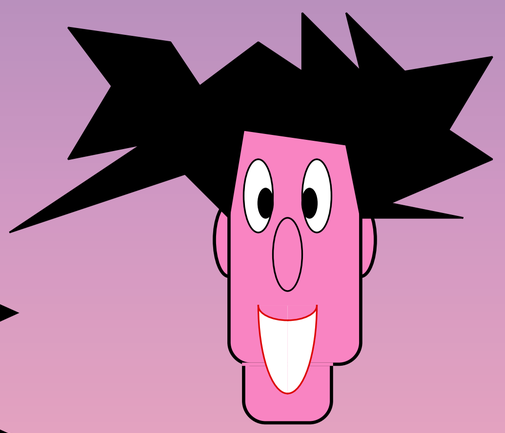
$|\Psi\rangle = \sigma_z^b \sigma_x^a |\Psi'\rangle$

(3.2.2a) Public-Key Q-Authentication

Assuming Classical Public Key Cryptography
Assuming Classical Digital Signature



$|\Psi\rangle$

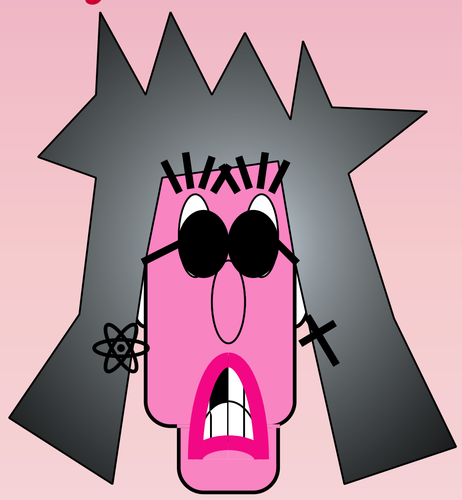


$|\Psi'\rangle$

Signed E(K)

K random authentication key

$|\Psi'\rangle := \text{Auth}_K(|\Psi\rangle)$

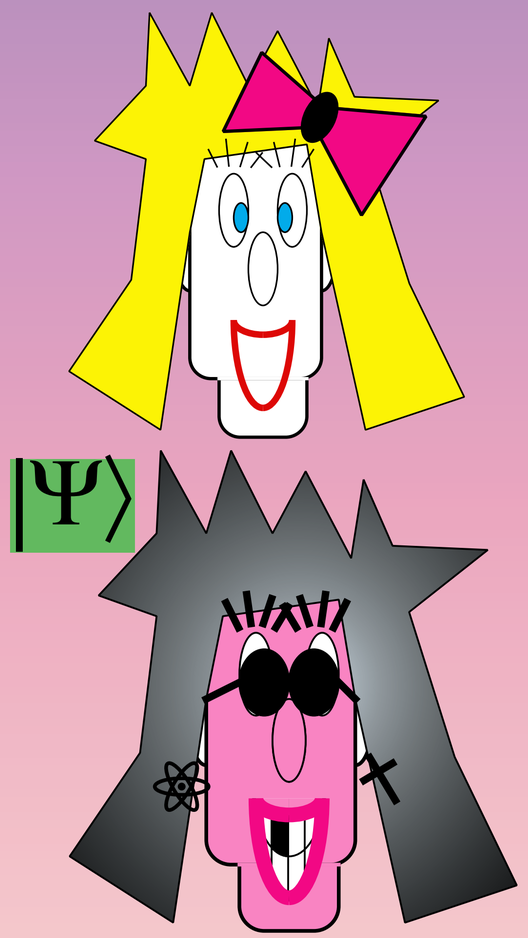


verify signed E(K)
K := D(E(K))

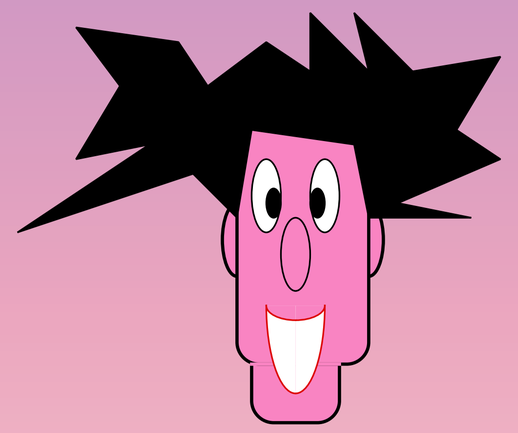
$|\Psi\rangle := \text{Auth}^{-1}_K(|\Psi'\rangle)$

(3.2.2b) Q-Digital Signature Scheme

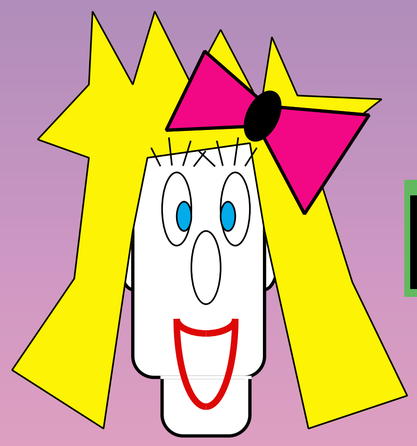
Assuming Classical Public Key Cryptography
Assuming Classical Digital Signature



IMPOSSIBLE



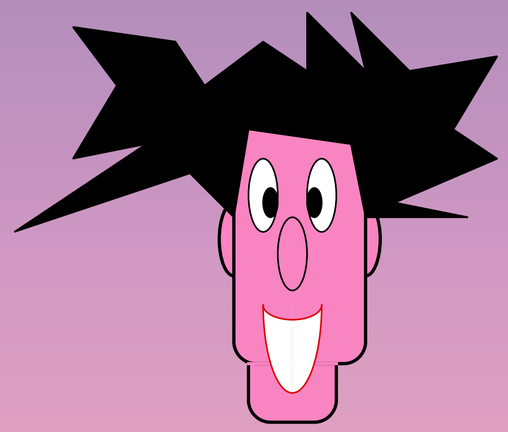
(3.2.2b) Q-Digital Signature Scheme

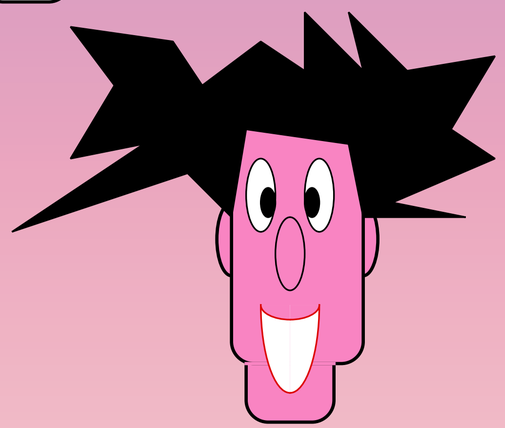


$|\Psi\rangle \otimes |0\rangle$

Signature

$|\Psi'\rangle$



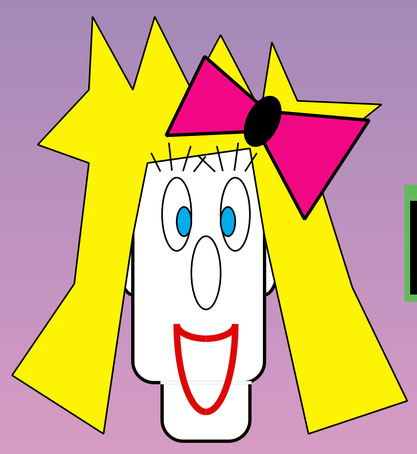


$|\Psi'\rangle$ → Validation → Valid, $|\Psi'\rangle$

$|\Psi'\rangle$ → Extract → $|\Psi\rangle \otimes |\varepsilon\rangle$

$|\Psi'\rangle$ → Validation → Valid, $|\Psi'\rangle$

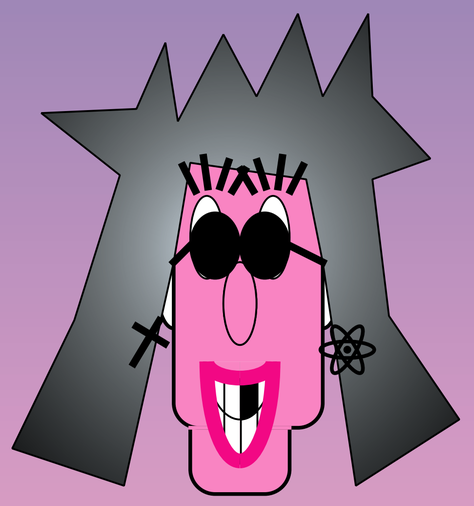
(3.2.2b) Q-Digital Signature Scheme

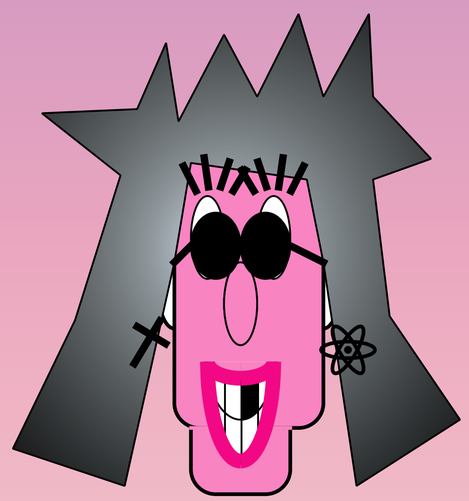


$|\Psi\rangle \otimes |0\rangle$

Signature

$|\Psi'\rangle$





$|\Psi''\rangle$ — Validation → Valid, $|\Psi''\rangle$

$|\Psi'\rangle$ — Extract → $|\Psi\rangle \otimes |\varepsilon\rangle$ → $|\phi\rangle \otimes |\varepsilon\rangle$ — Extract^{-1} → $|\Psi''\rangle$

$|\Psi''\rangle$ — Validation → Valid, $|\Psi''\rangle$

(3.2.3) (Trapdoor) Q-One-way functions

- generate a function f (and trapdoor) s.t.
- computing f(x) is easy
- finding x s.t. f(x)=y is hard
- finding x s.t. f(x)=y is easy with trapdoor

Q-cryptanalysis : Shor

Q-One-way function

Fischer-Stern

one-way function

(error correction code based)

generation : classical easy

computing f : classical easy

inverting f : classical /quantum hard ???

Trapdoor Q-One-way function

Okamoto-Tanaka-Uchiyama
trapdoor one-way permutation
(subset products problem based)

generation : quantum easy
computing f : classical easy
inverting f : classical /quantum hard ???
trapdooring f : classical easy

Trapdoor Q-One-way function

McEliece

trapdoor one-way permutation

(error correction code based)

generation : classical easy

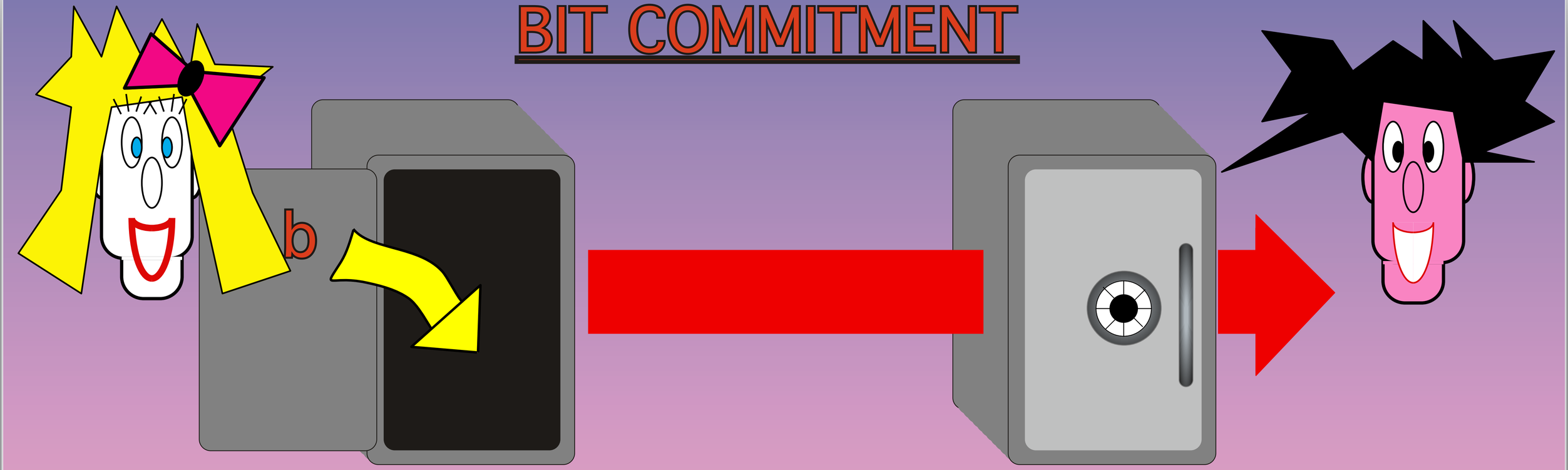
computing f : classical easy

inverting f : classical /quantum hard ???

trapdooring f : classical easy

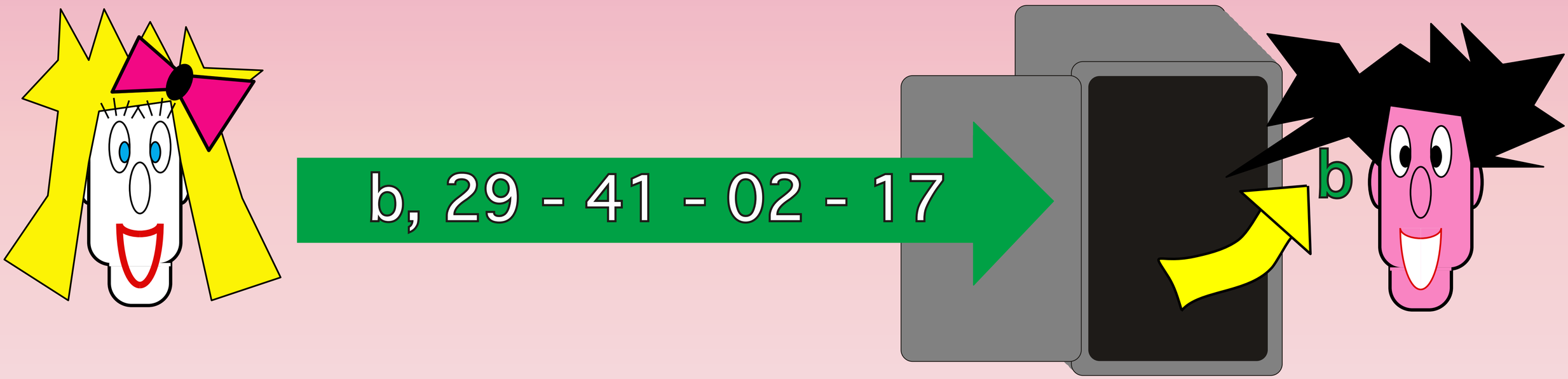
(4)
two-party
Cryptographic Protocols

BIT COMMITMENT

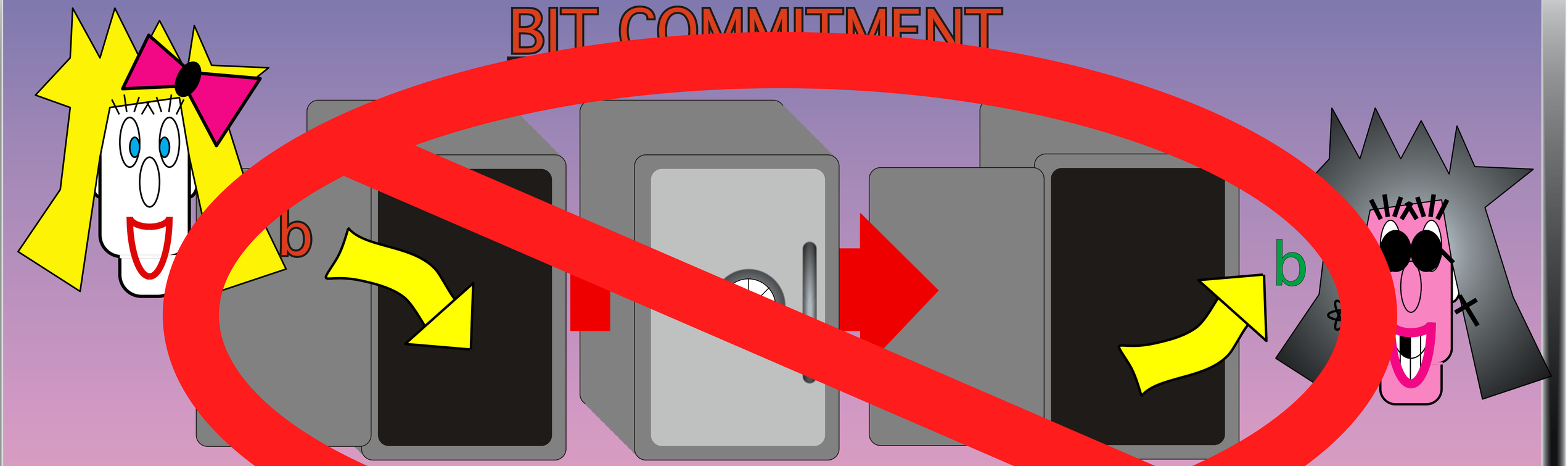


COMMIT

UNVEIL

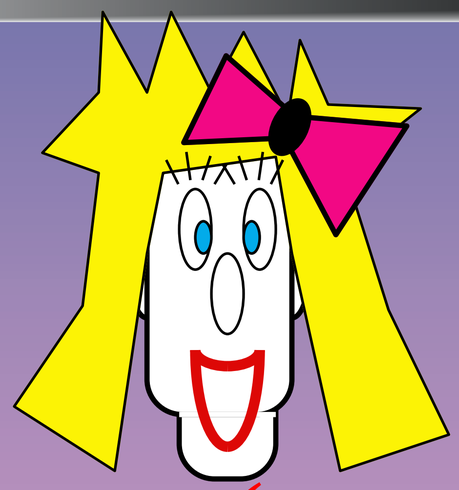


BIT COMMITMENT

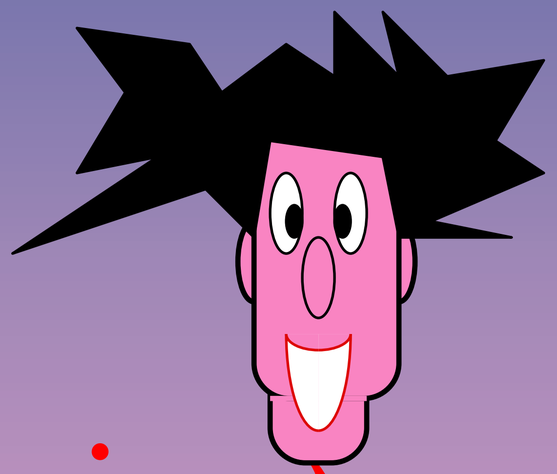


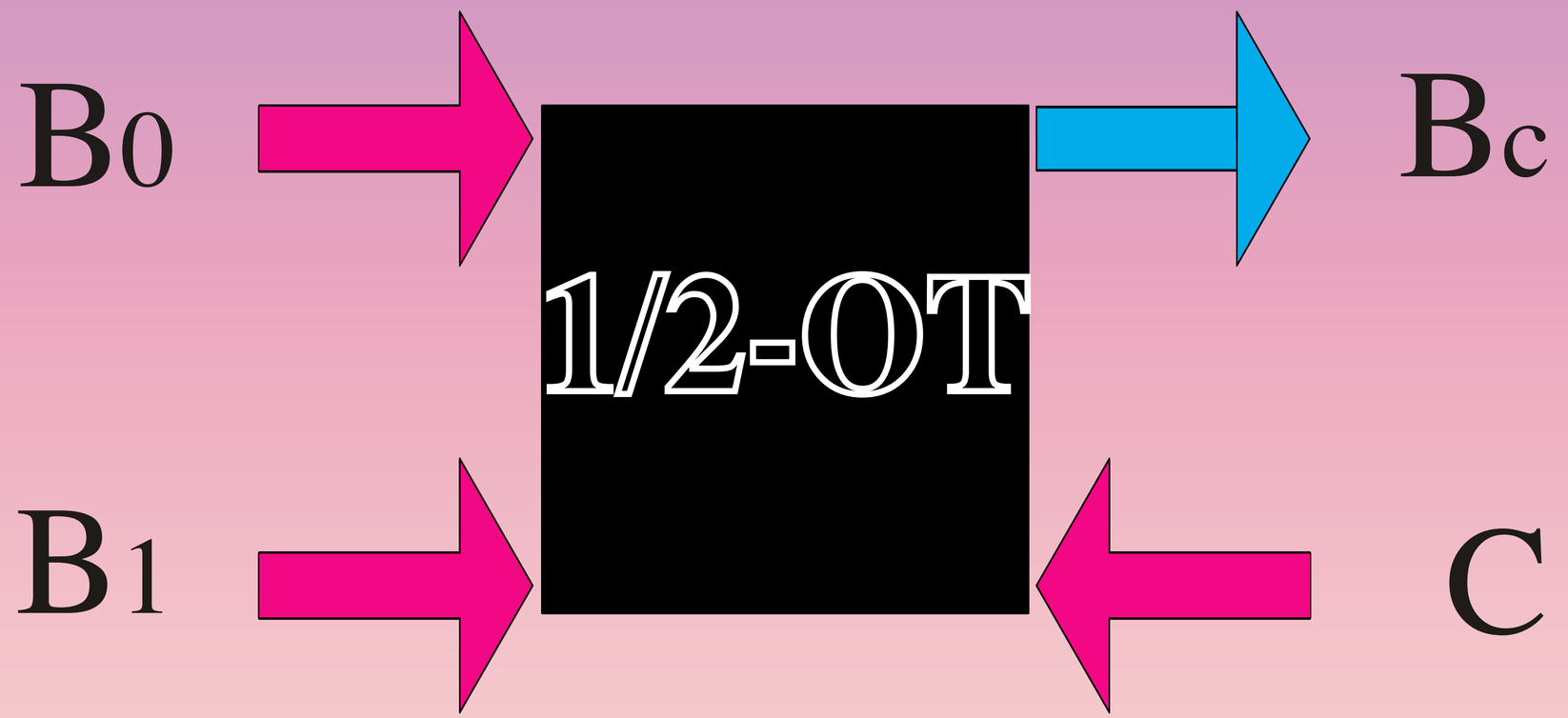
CONCEALING

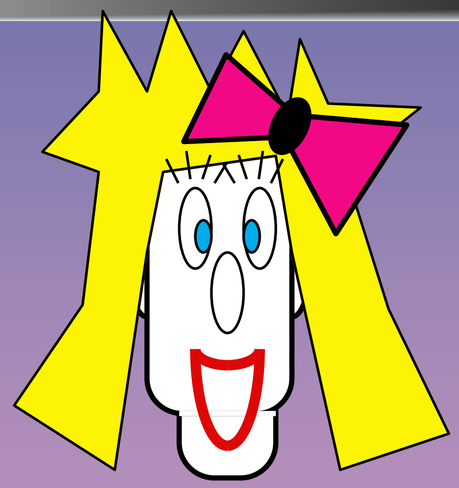
BINDING



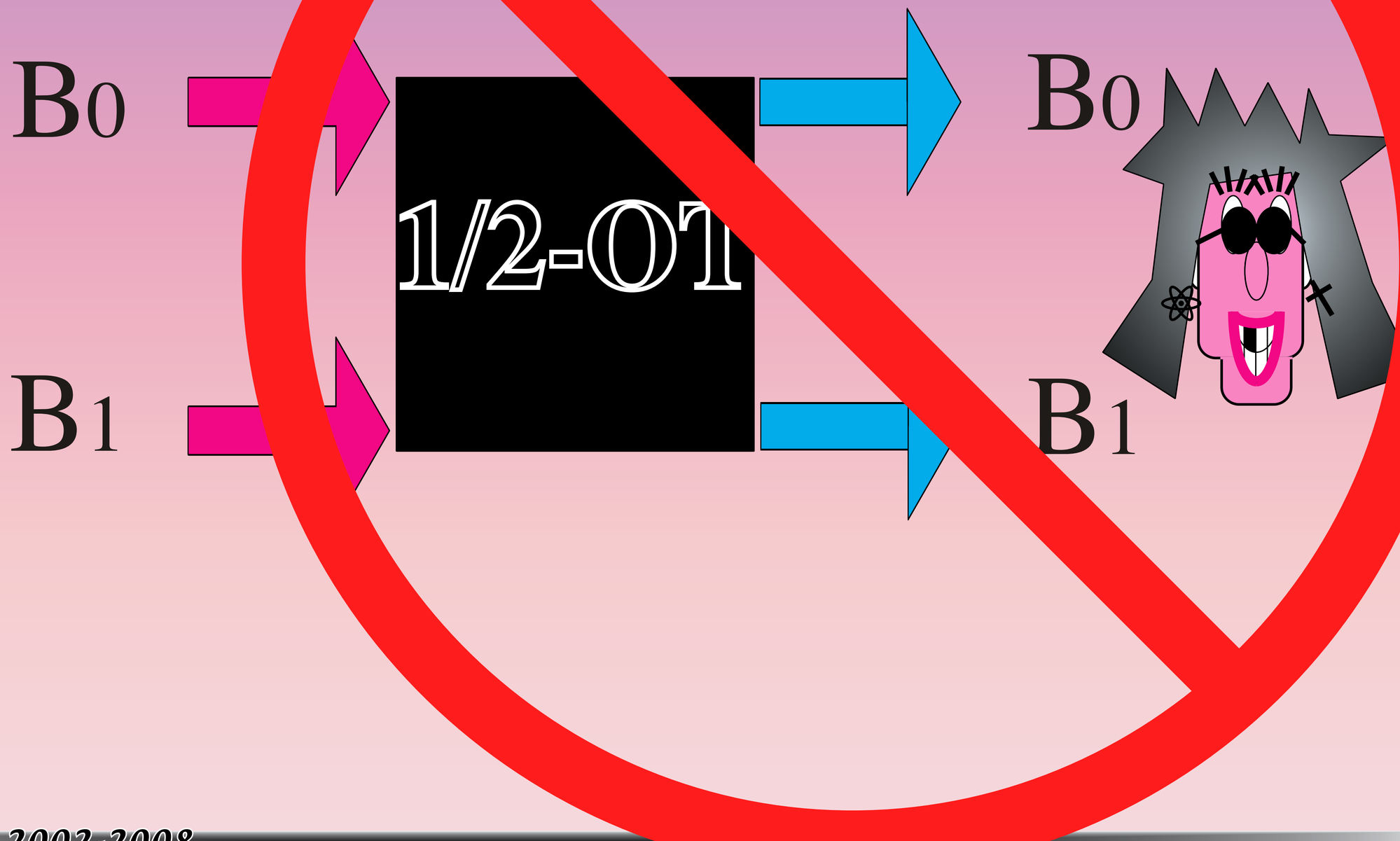
Oblivious Transfer (message multiplexing)



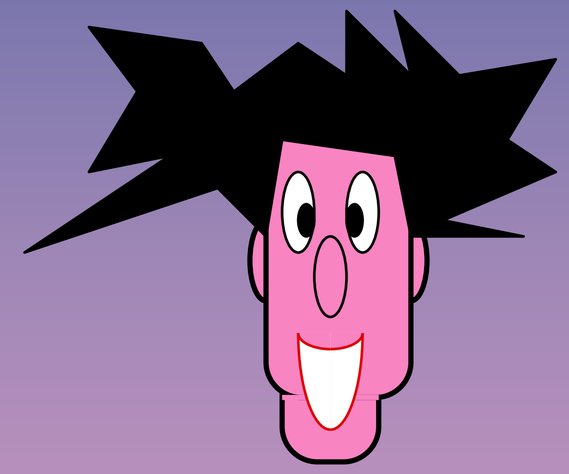


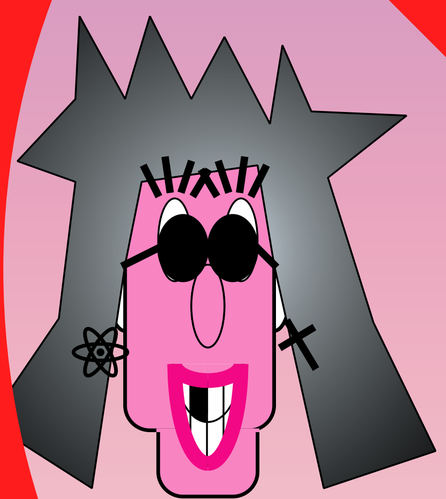


Oblivious Transfer



Oblivious Transfer

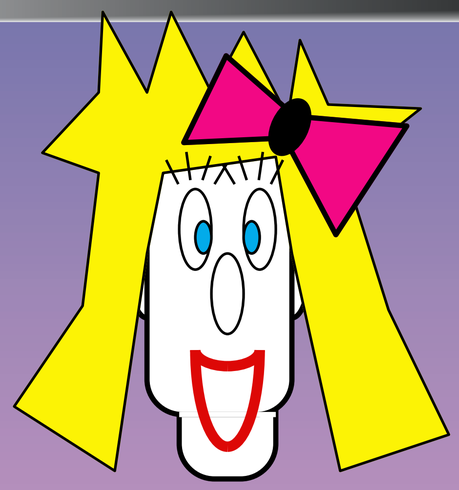




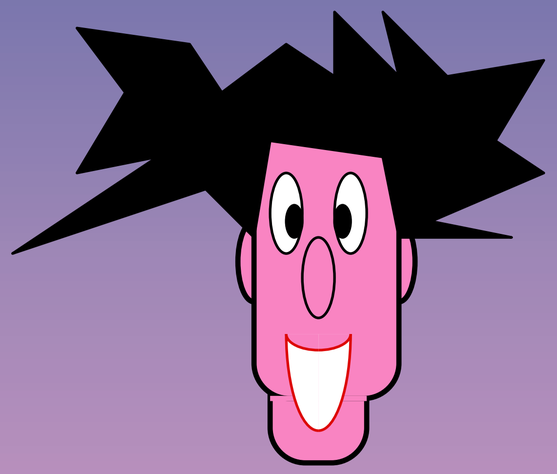
Bc

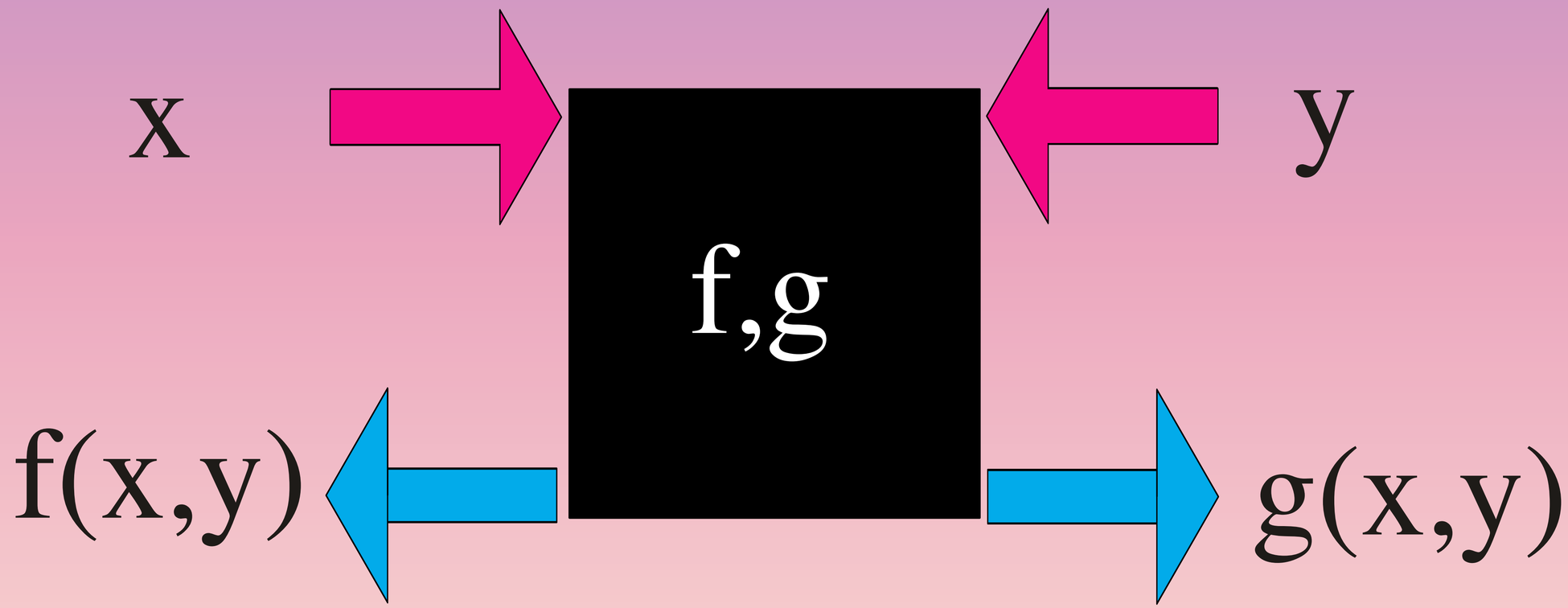
C

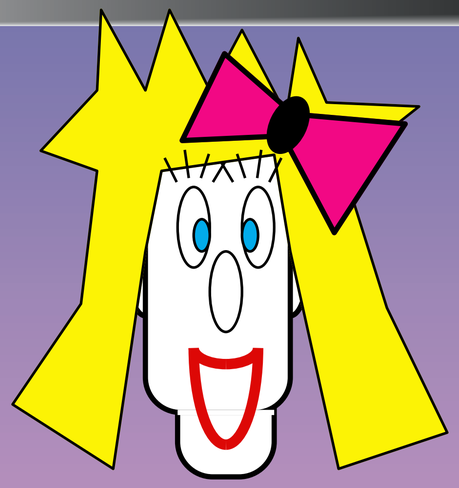
C



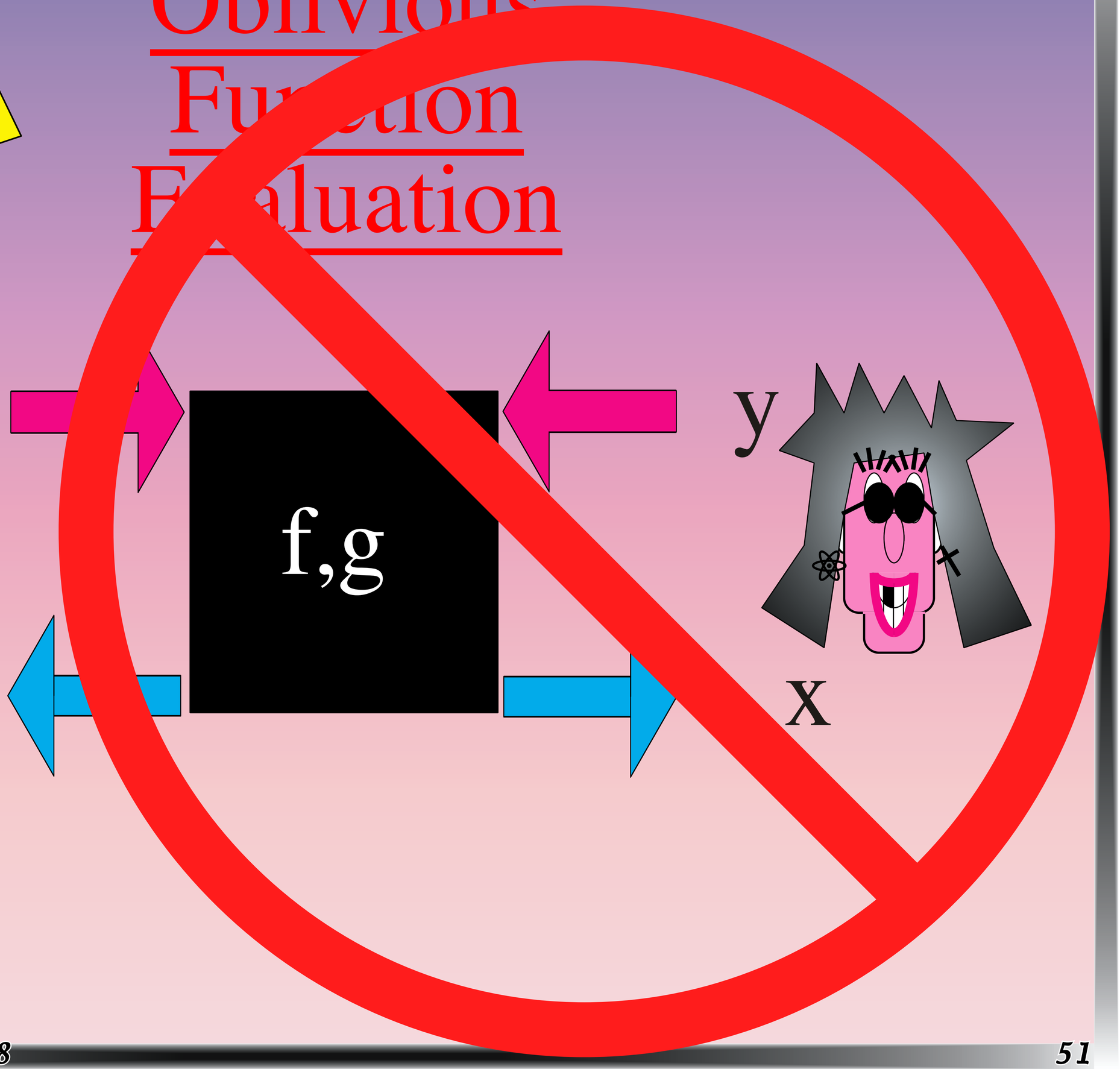
Oblivious Function Evaluation



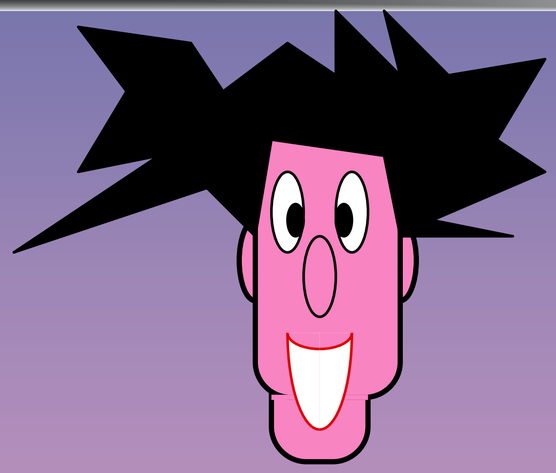


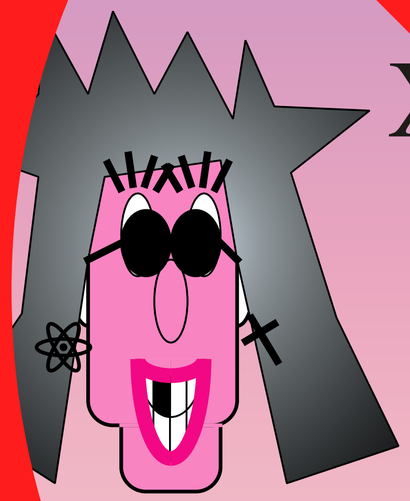


Oblivious Function Evaluation



Oblivious Function Evaluation





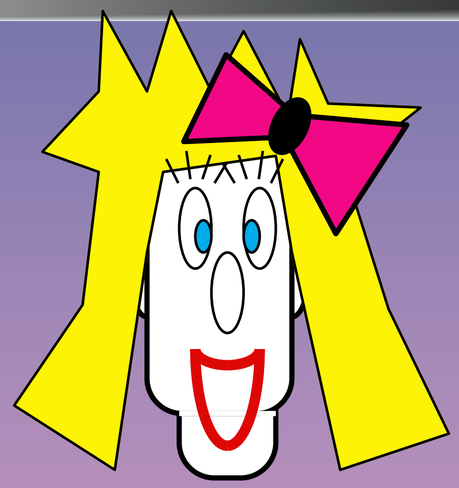
x

y

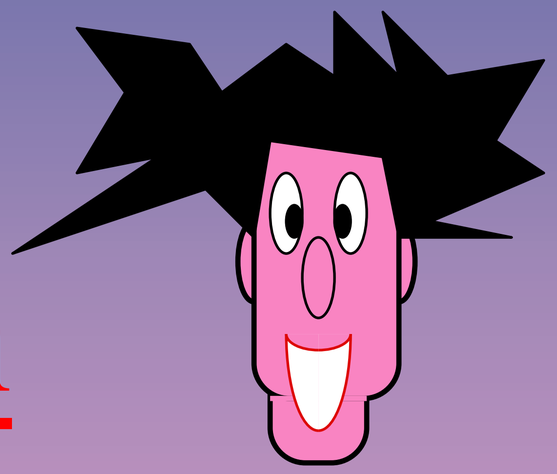
f,g

y

g’(x,y)



Mutual Identification



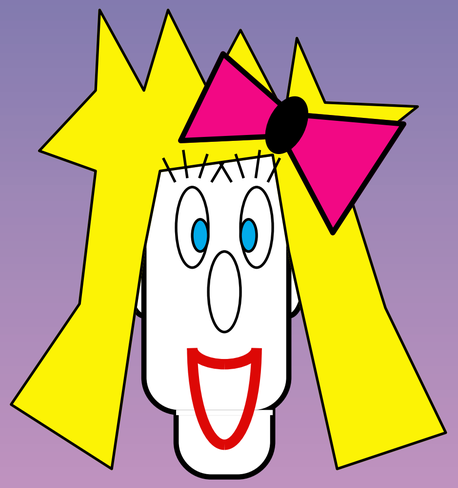
x

y

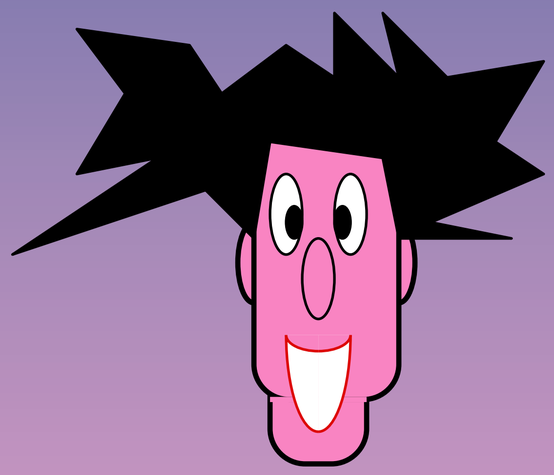
=,=

x=y?

x=y?



Oblivious DB query

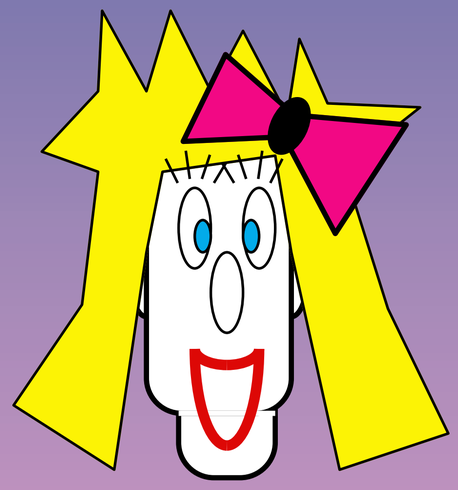


Q

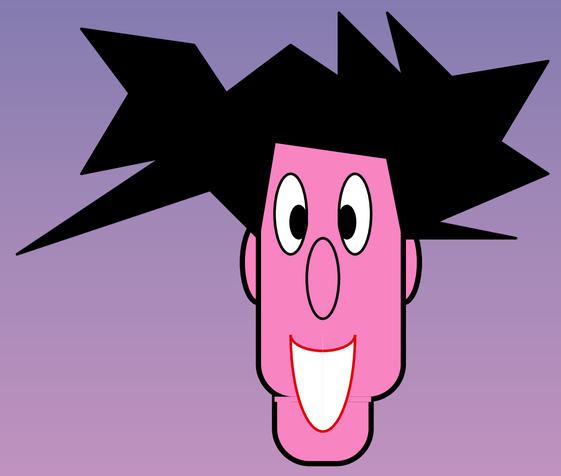
DB

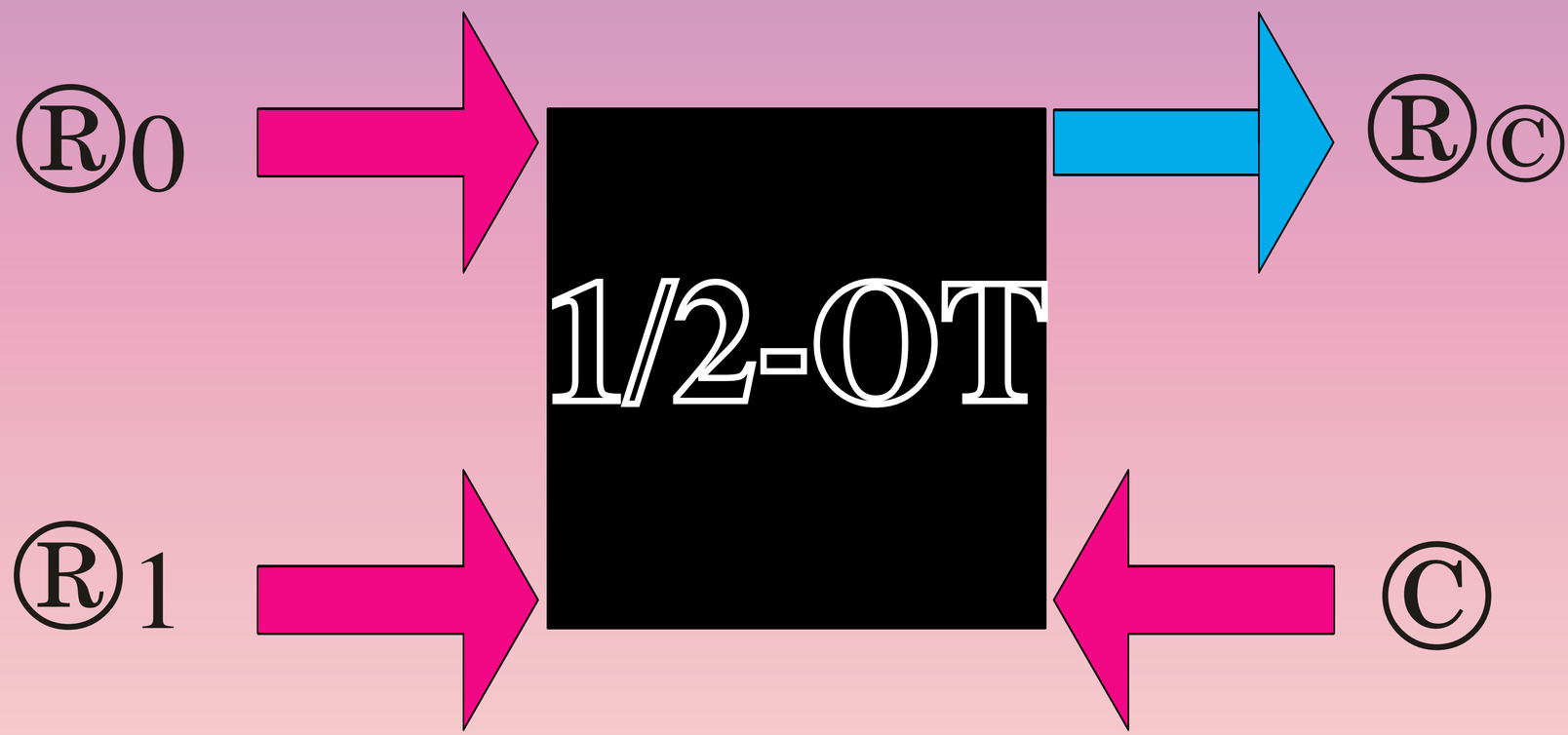
$Q \in ? DB$

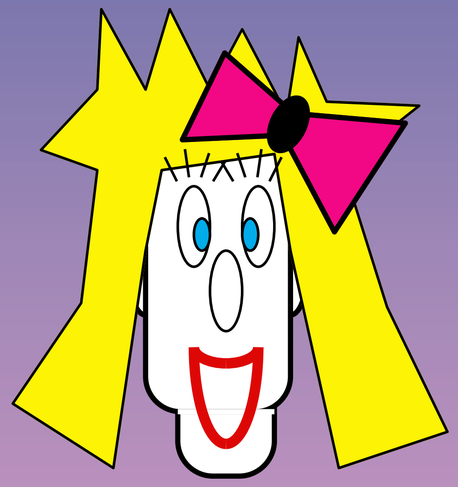
$data_Q$ /NO



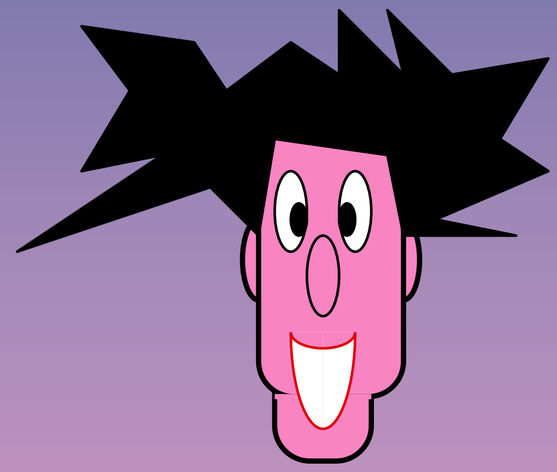
Randomized Oblivious Transfer

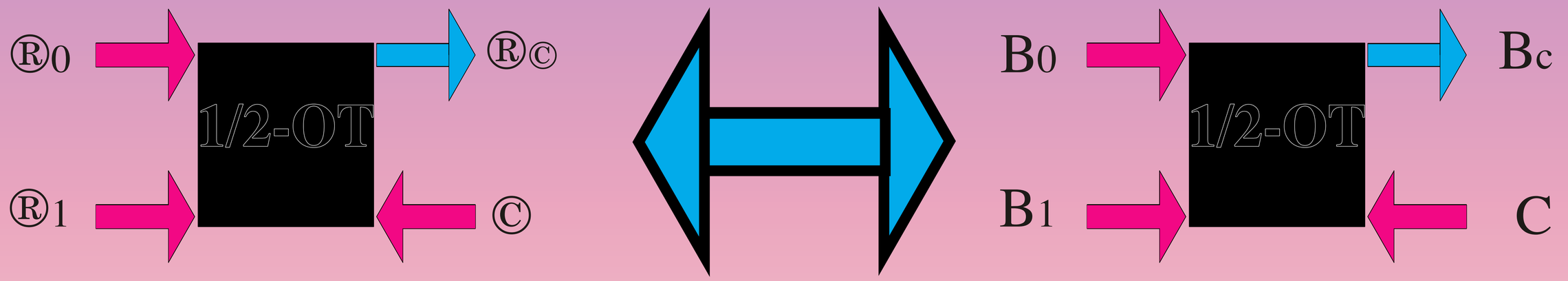


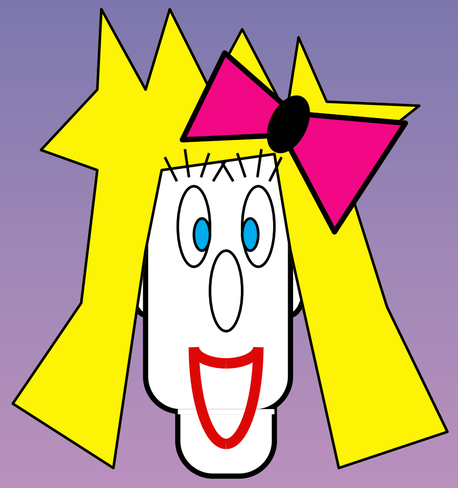




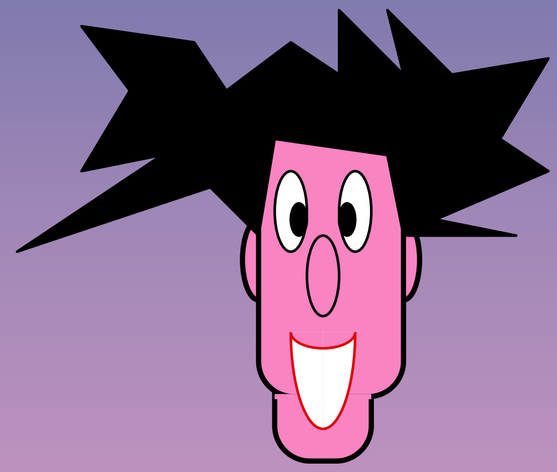
Randomized Oblivious Transfer

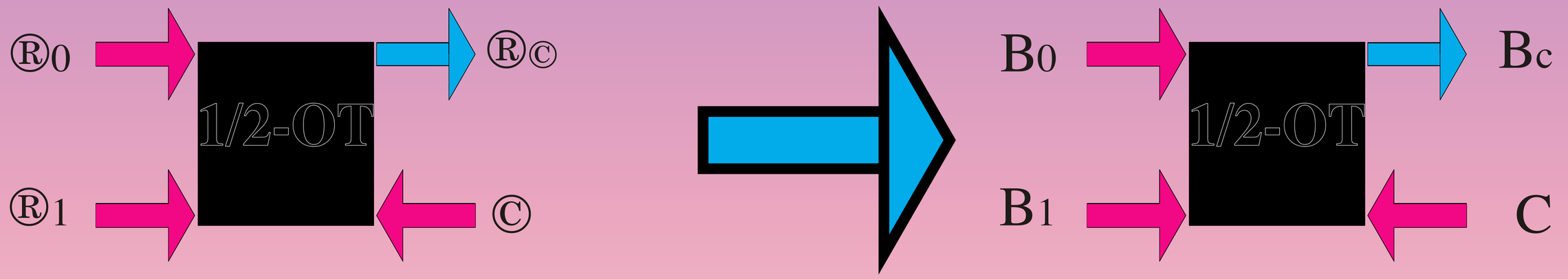


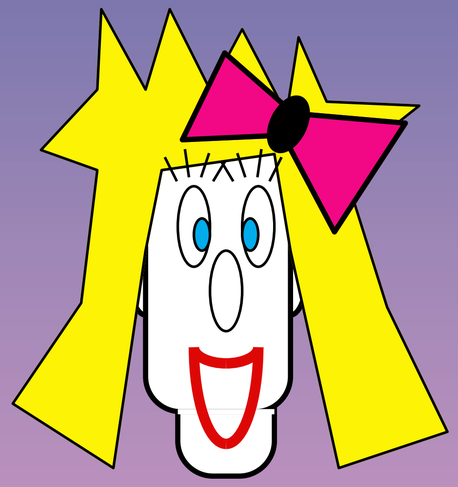




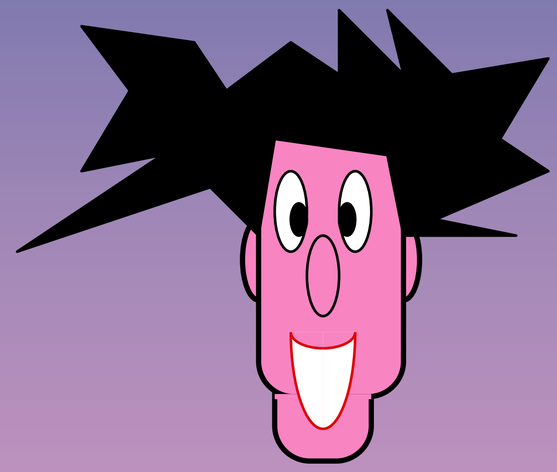
Randomized Oblivious Transfer

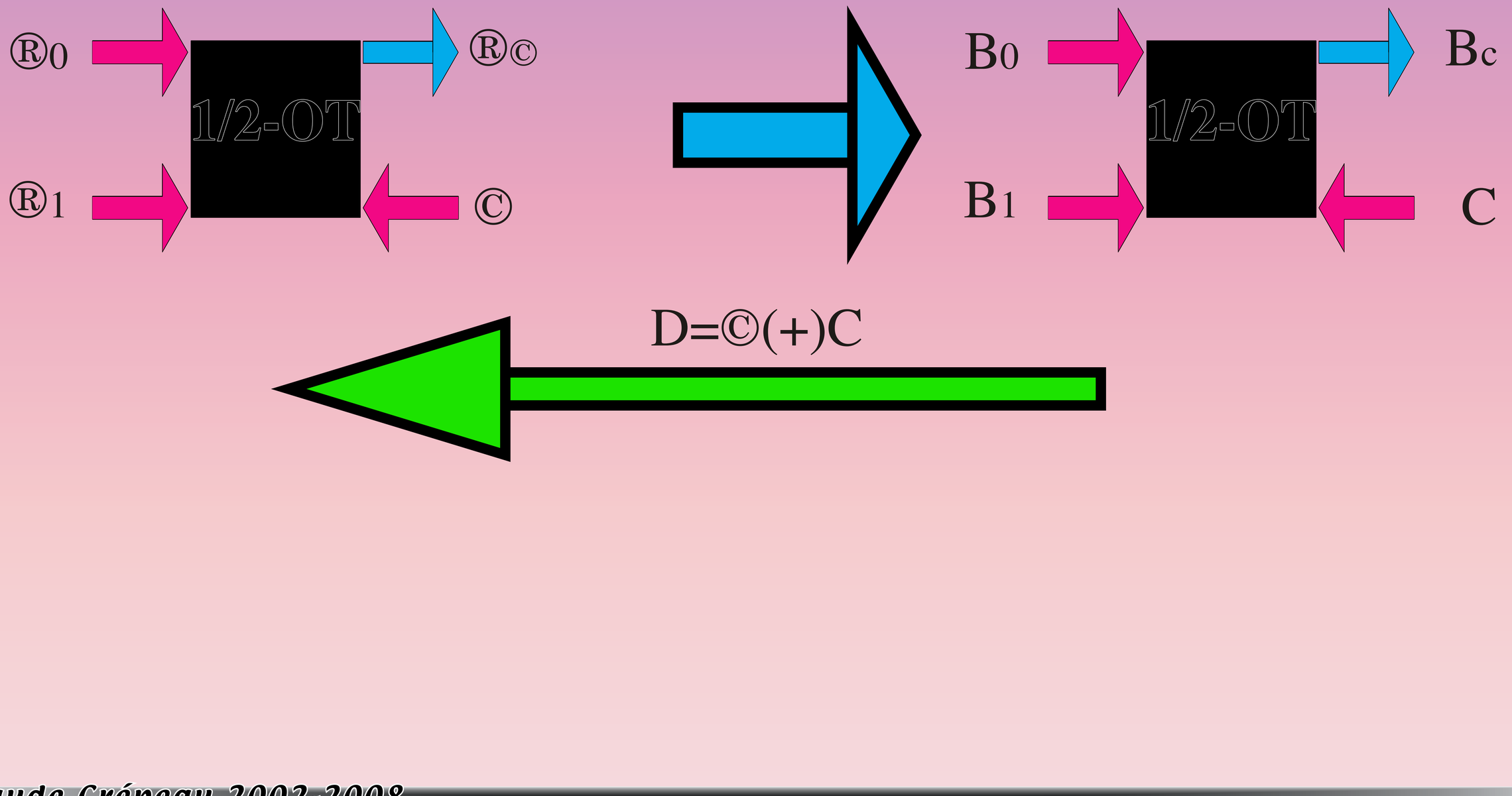


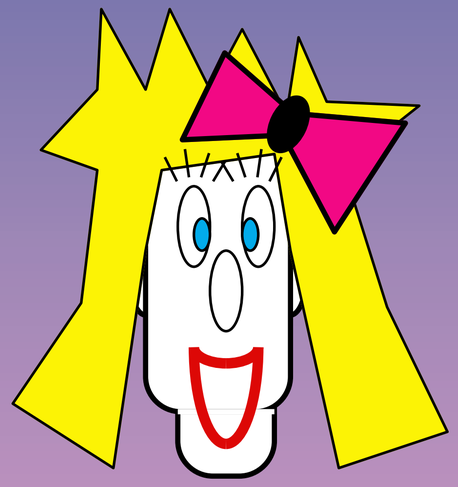




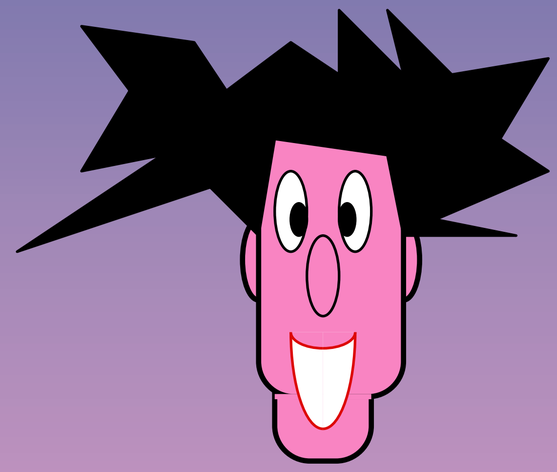
Randomized Oblivious Transfer

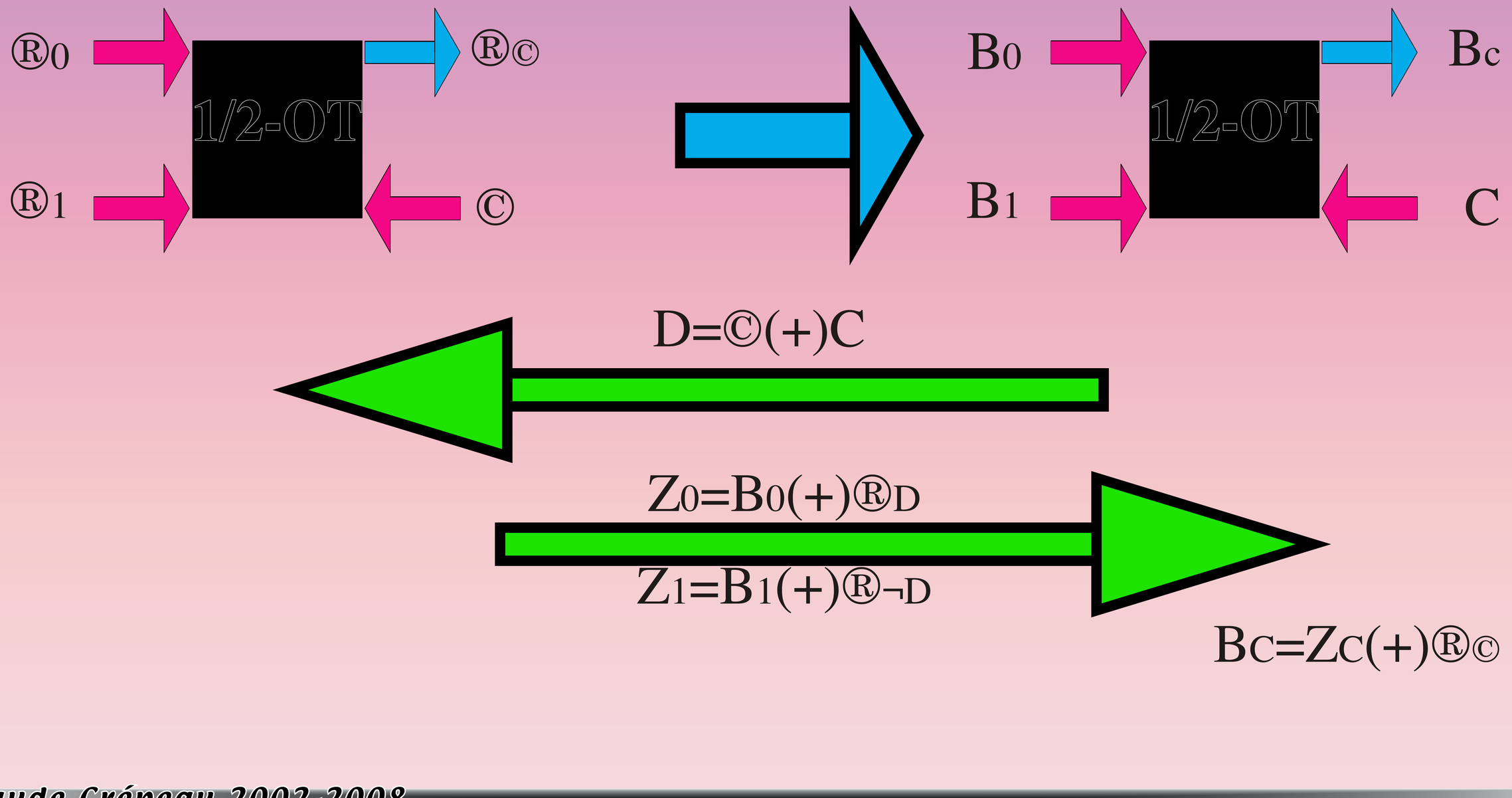


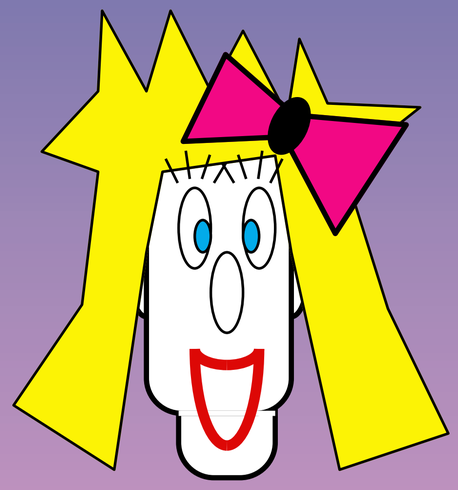




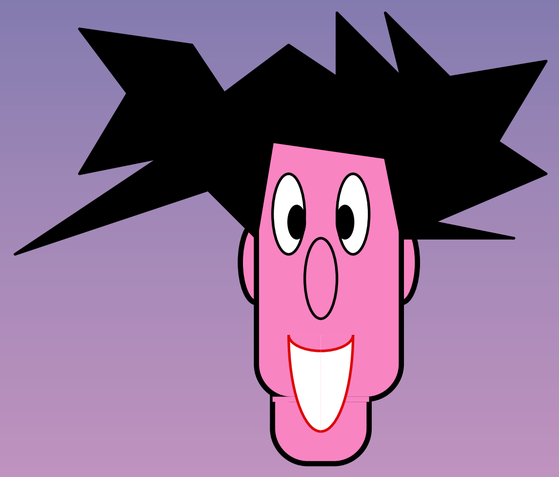
Randomized Oblivious Transfer

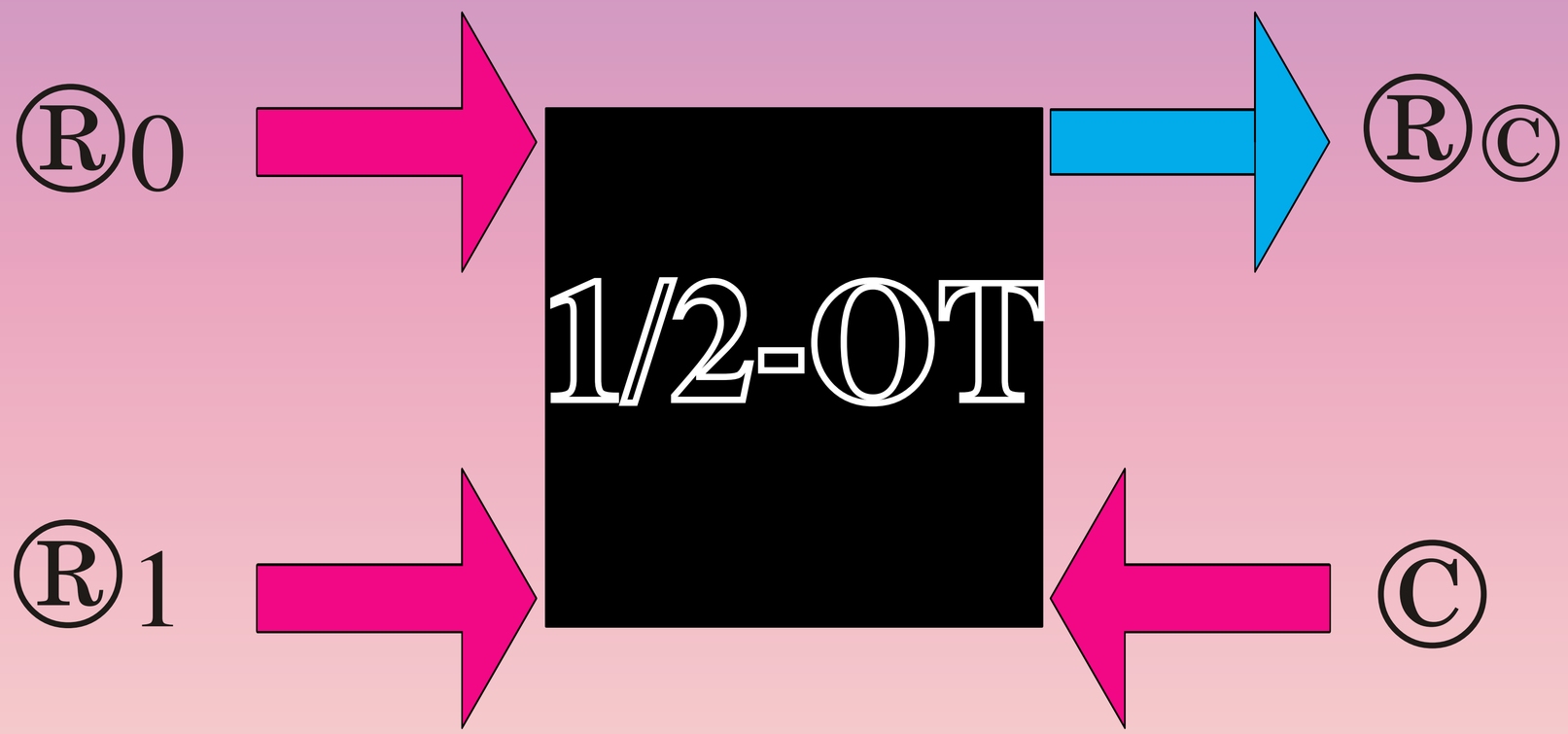






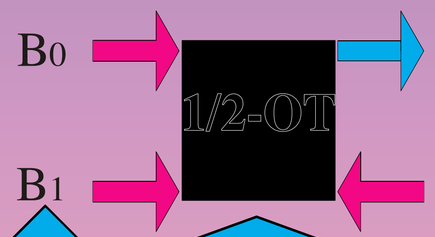
Randomized Oblivious Transfer

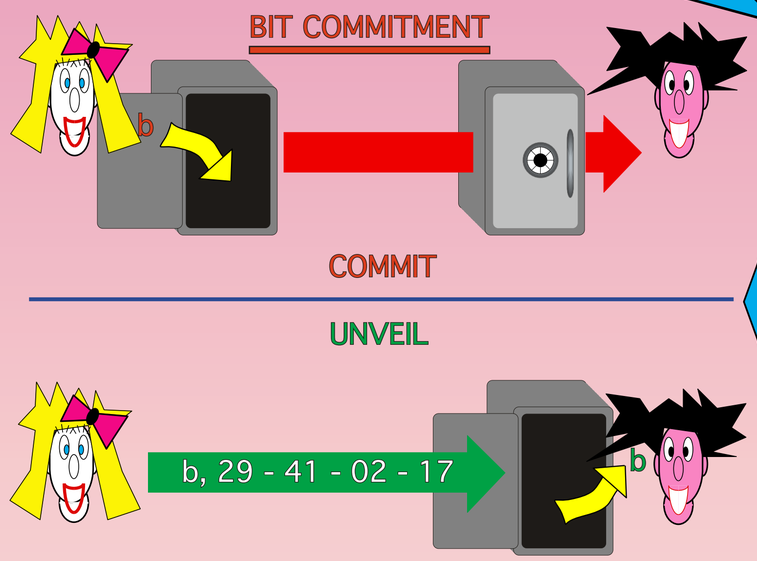


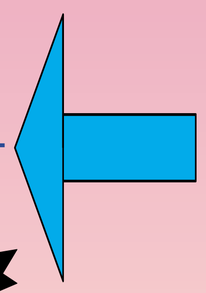


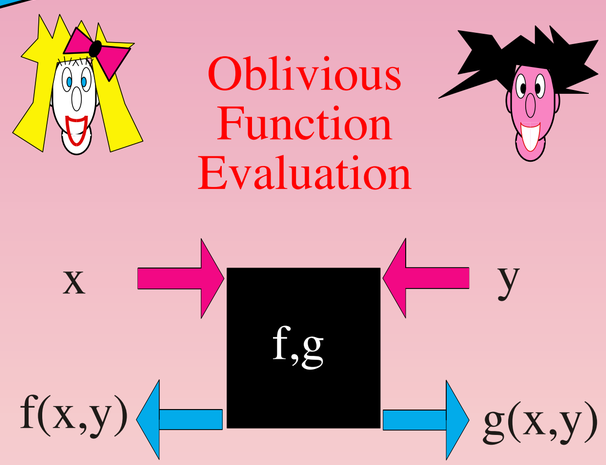
IS AN INVESTMENT IN THE FUTURE

Classically

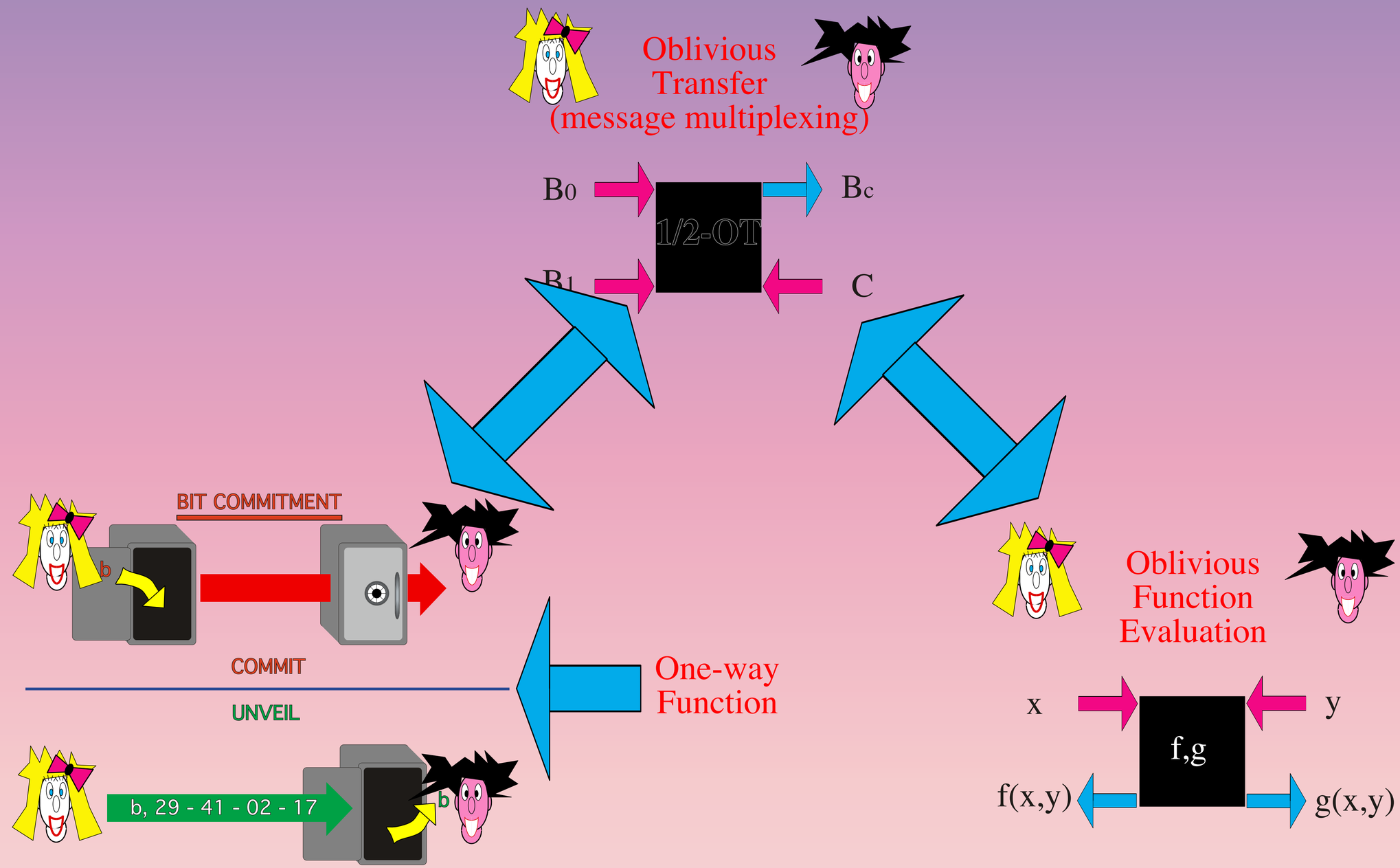




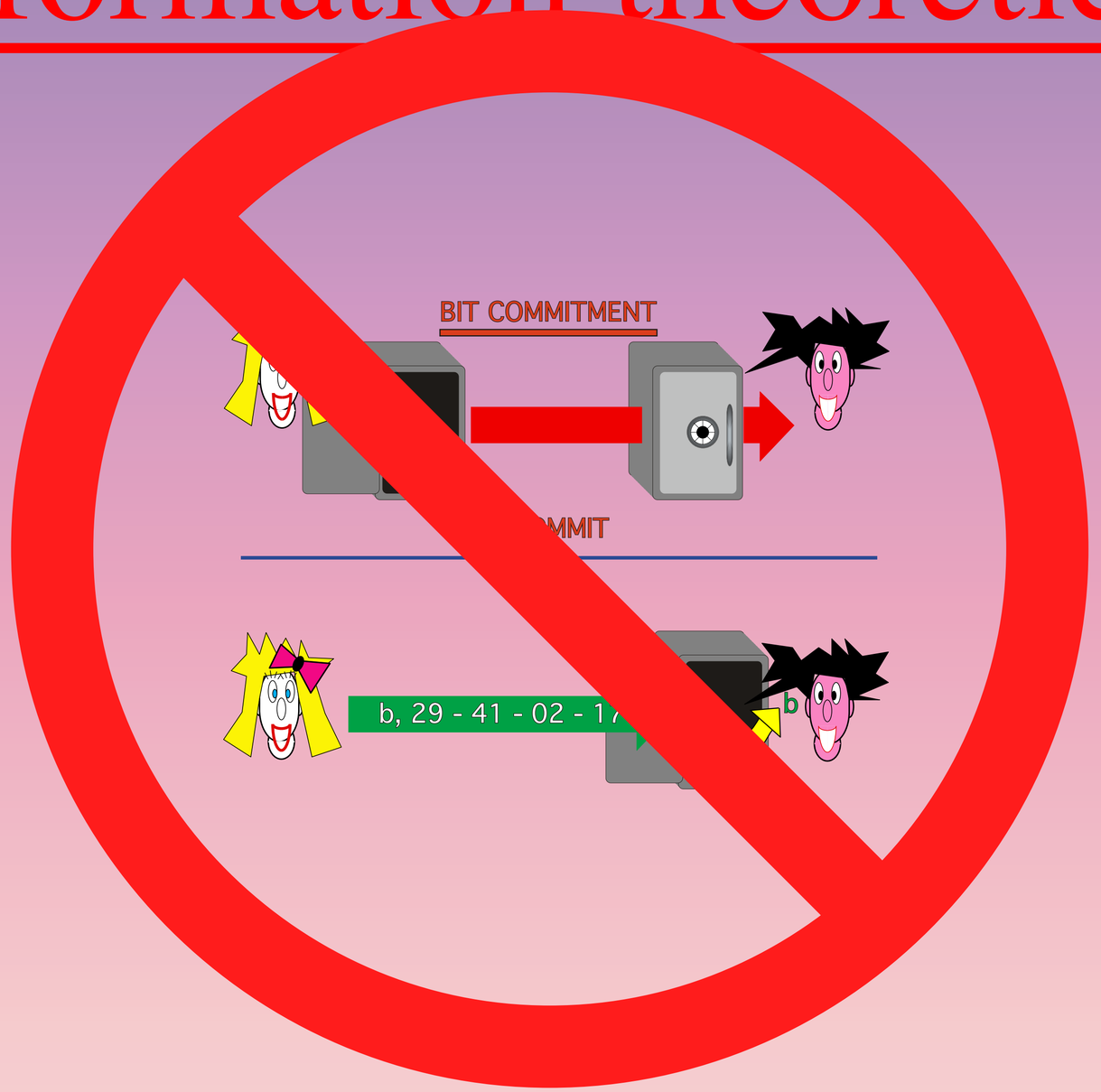




Quantumly

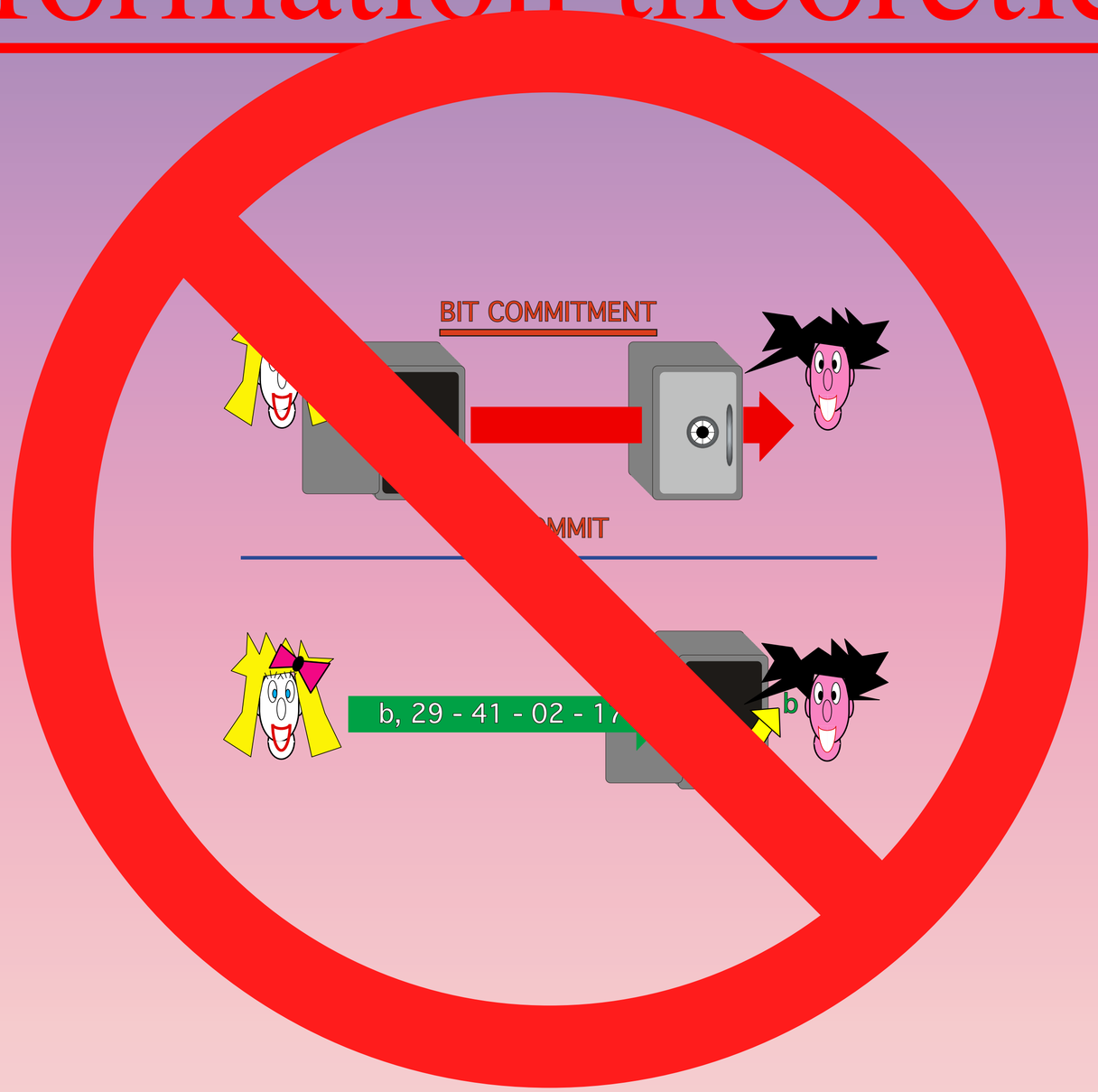


Classically (information theoretical)



Folklore

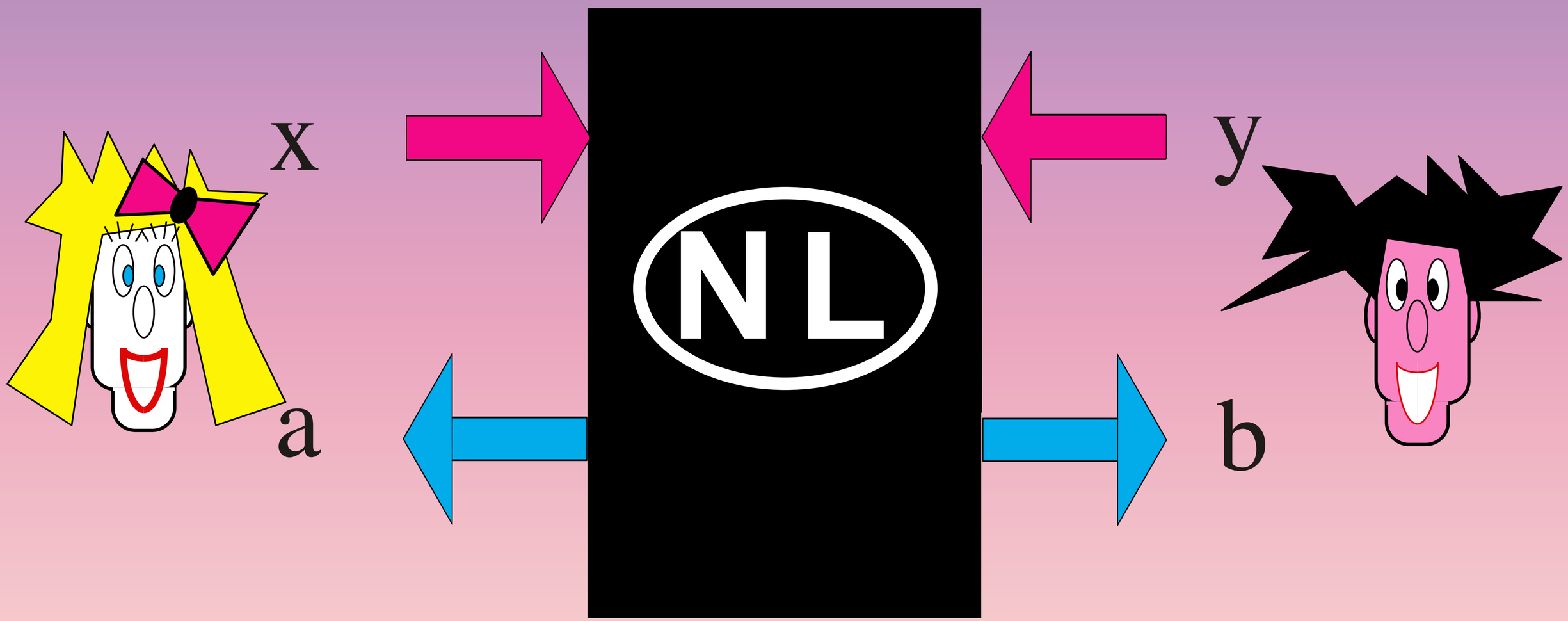
Quantumly (information theoretical)



Mayers, Lo-Chau

Non-Locality Box

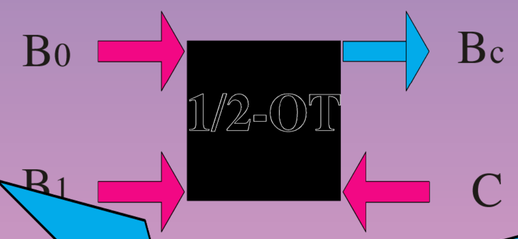
$$a \oplus b = x \barwedge y$$

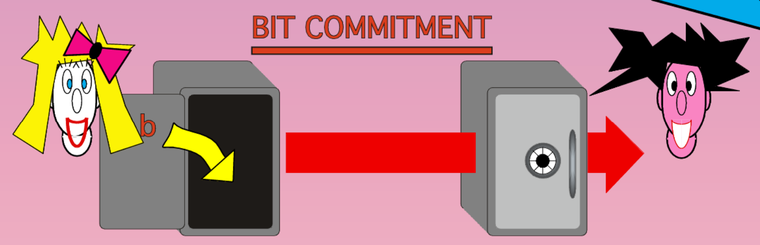


C: 3/4 Q: $\cos^2(\pi/8) \approx 85\%$

Quantumly

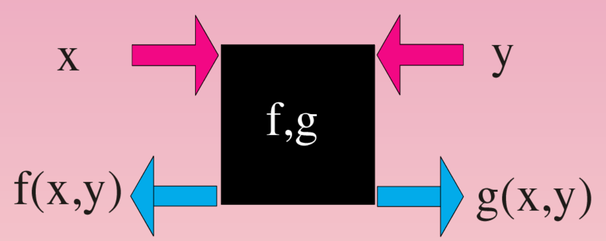
Oblivious
Transfer
(message multiplexing)



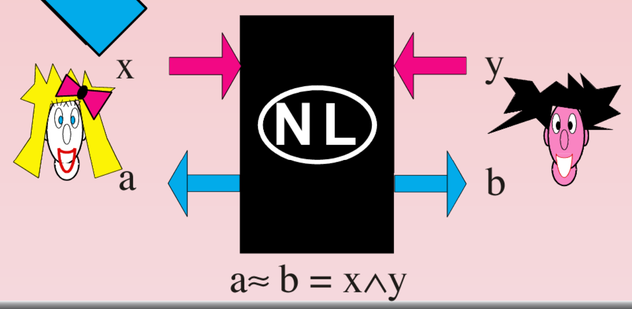


Wolf, Wullschleger

Oblivious
Function
Evaluation



Non-Locality Box

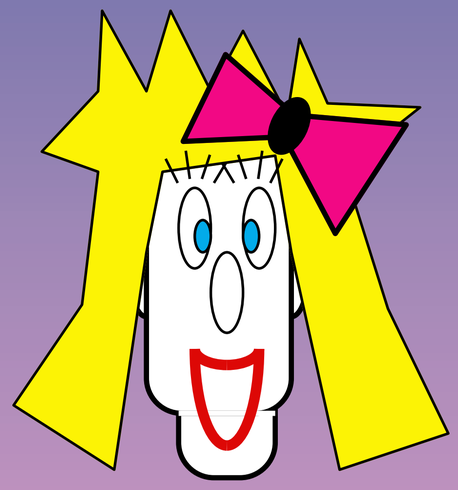


$a \approx b = x \wedge y$

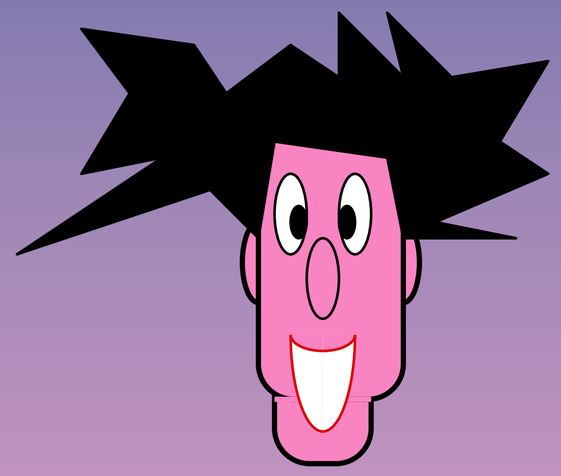
1) Wolf,Wullschleger ?
2) Short,Gisin,Popescu
3) Buhrman,Christandl,
Unger,Wehner,Winter

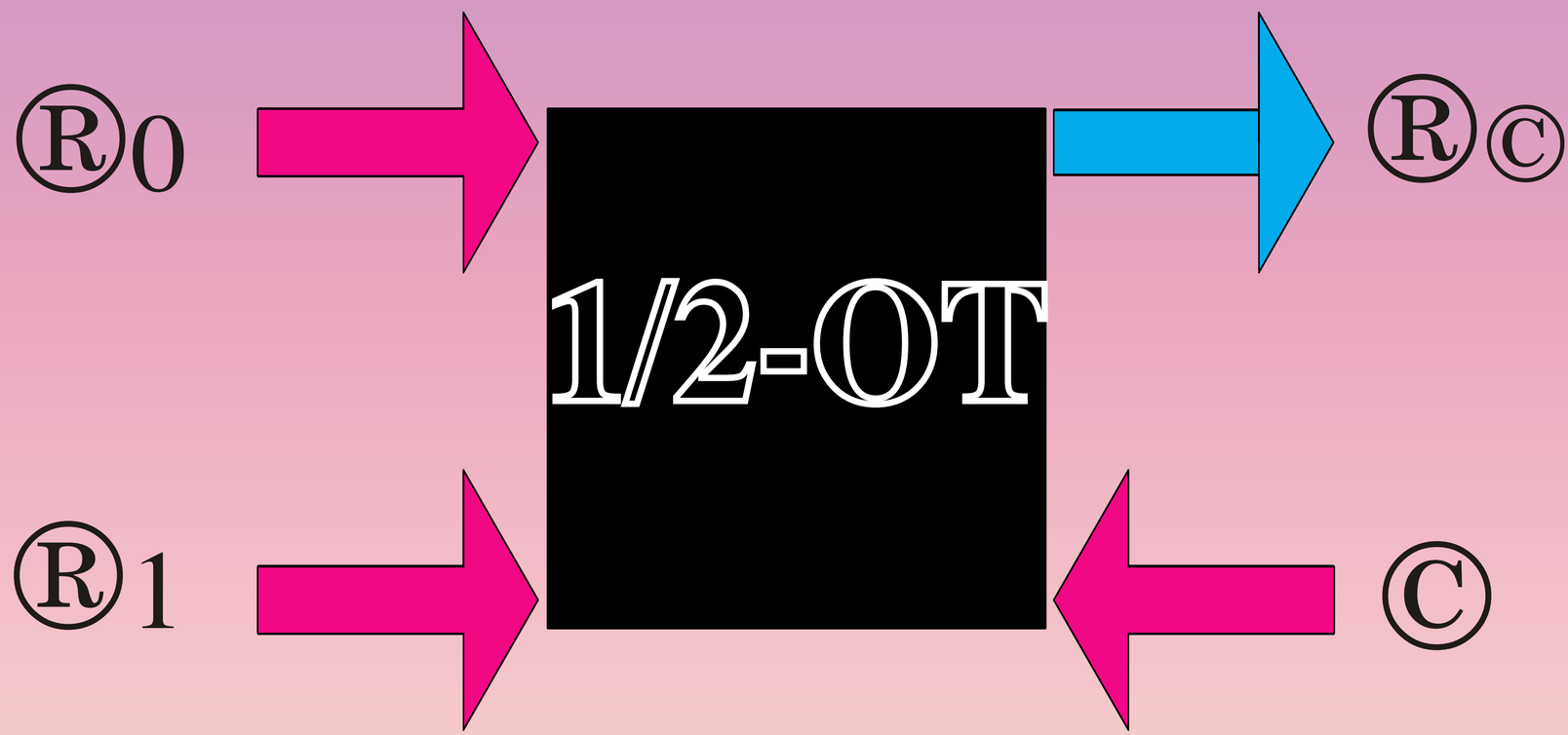
(5)

Quantum Oblivious Transfer

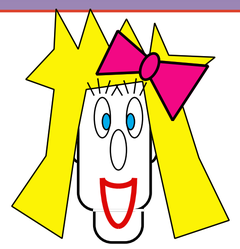


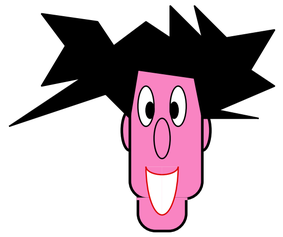
Randomized Oblivious Transfer





Q-ROT

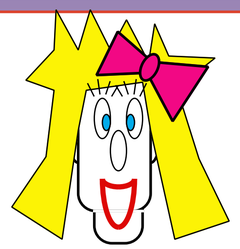


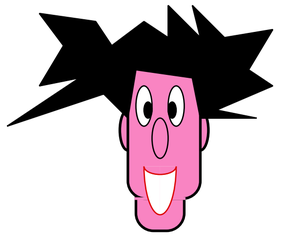


A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	×	×	+	+	×	+	+	+	×	+	+	×	×	×	+	×	×	×	+	+	×	+	×	+
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0
A:	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	0	☞	☞	0	☞	1	☞	☞	1	☞	0	☞	☞	☞	☞	1	0	☞	☞	1	☞	0	0	0
B:	0	0	1	1	0	1	0	1	0	0	0	☞	☞	☞	☞	☞	☞	☞	☞	☞	☞	☞	☞	☞
A:	0	0	1	1	0	1	0	1	0	0	0	1	1	0	0	0	1	1	0	0	0	1	0	1
B:	0	0	1	1	0	1	0	1	=	0							☞	=	☞	☞	☞	☞	☞	☞	☞
A:	0	0	1	1	0	1	0	1	=	$0=®_0$						$®_1=0$	=	1	1	0	0	0	1	0	1

Crépeau-Kilian

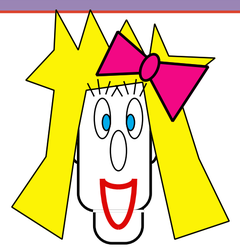
Q-OT

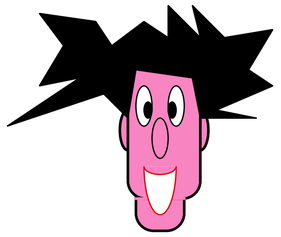




A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+

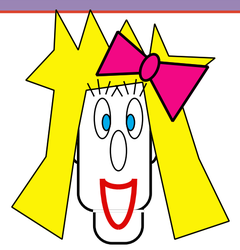
Q-OT

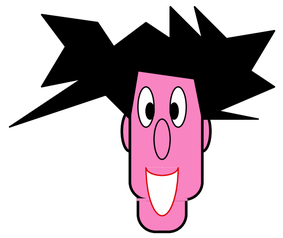




A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	×	×	+	+	×	+	+	+	×	+	+	×	×	×	+	×	×	×	+	+	×	+	×	+
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0

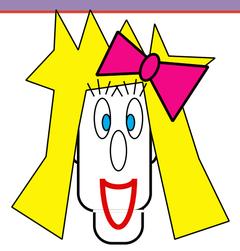
Q-OT

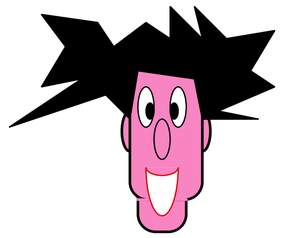




A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	×	×	+	+	×	+	+	+	×	+	+	×	×	×	+	×	×	×	+	+	×	+	×	+
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0
A:	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+

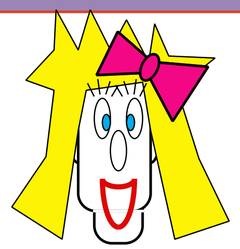
Q-OT

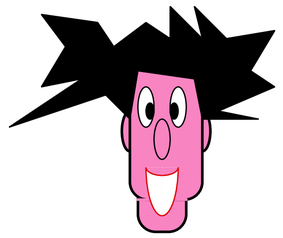




B:	×	×	+	+	×	+	+	+	×	+	+	×	×	×	+	×	×	×	+	+	×	+	×	+
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0
A:	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	0	↵	↵	0	↵	1	↵	↵	1	↵	0	↵	↵	↵	1	0	↵	↵	1	↵	0	0	0	

Q-OT





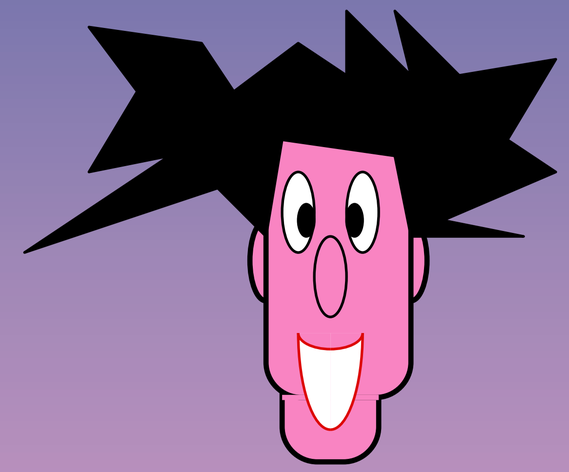
A: 0 1 1 0 0 1 0 0 1 1 0 1 0 0 0 1 1 1 0 1 1 0 0 0

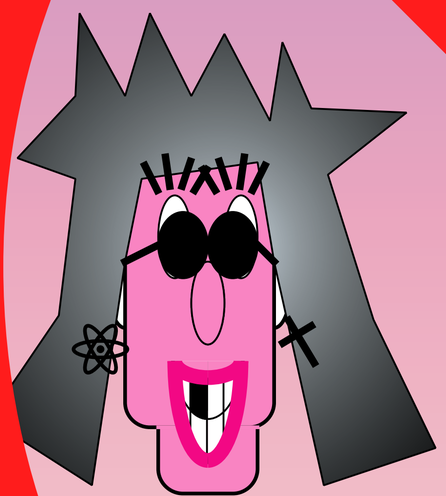
B: 0 0 1 0 1 1 0 1 0 0 0 1 0 1 1 0 0 0

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

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

Oblivious Transfer



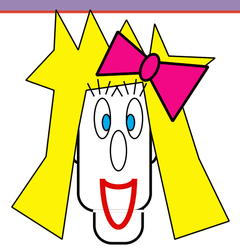


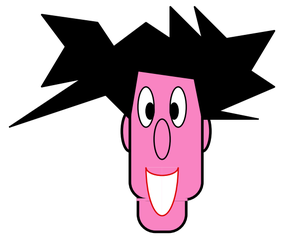
Bc

C

C

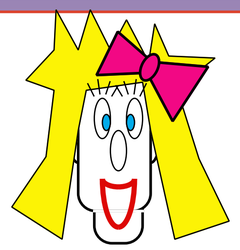
Q-OT

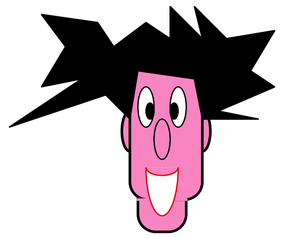




B:	0	0	1	1	0	1	0	1	0	0	0								
A:	0	0	1	1	0	1	0	1	0	0	0	1	1	0	0	1	1	0	0
B:	0	0	1	1	0	1	0	1	=	0			=						
A:	0	0	1	1	0	1	0	1	=	0=®$_0$			®$_1$=0	=	1	1	0	0	0	1	0	1

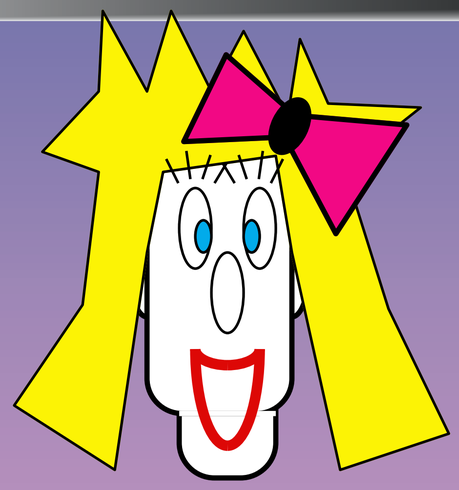
Q-OT



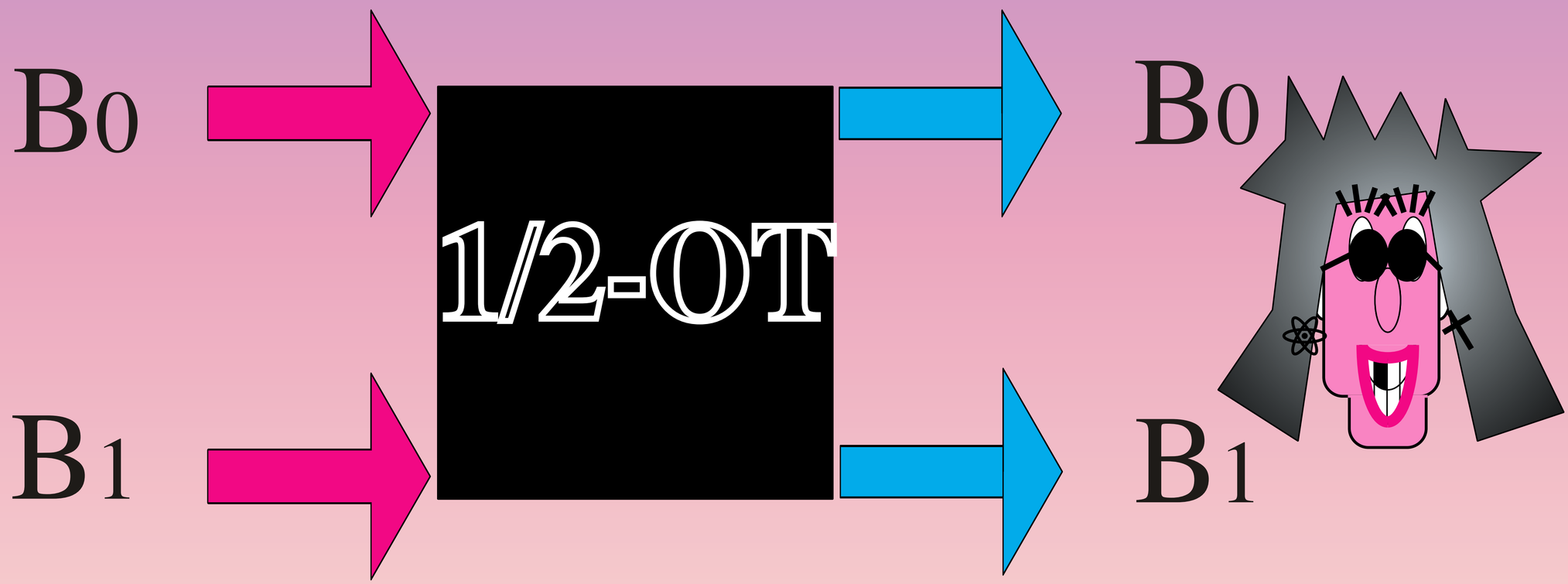


B: 0 0 1 1 0 1 0 1 = 0 = 0 0 0 0 0 0 0 0

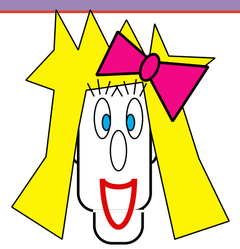
A: 0 0 1 1 0 1 0 1 = 0=®$_0$ ®$_1$=0 = 1 1 0 0 0 1 0 1



Oblivious Transfer



Q-OT

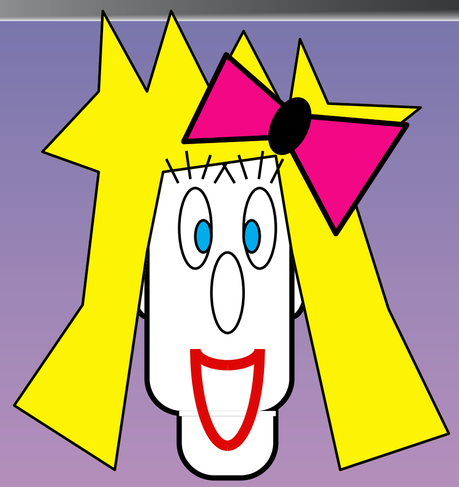


A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+

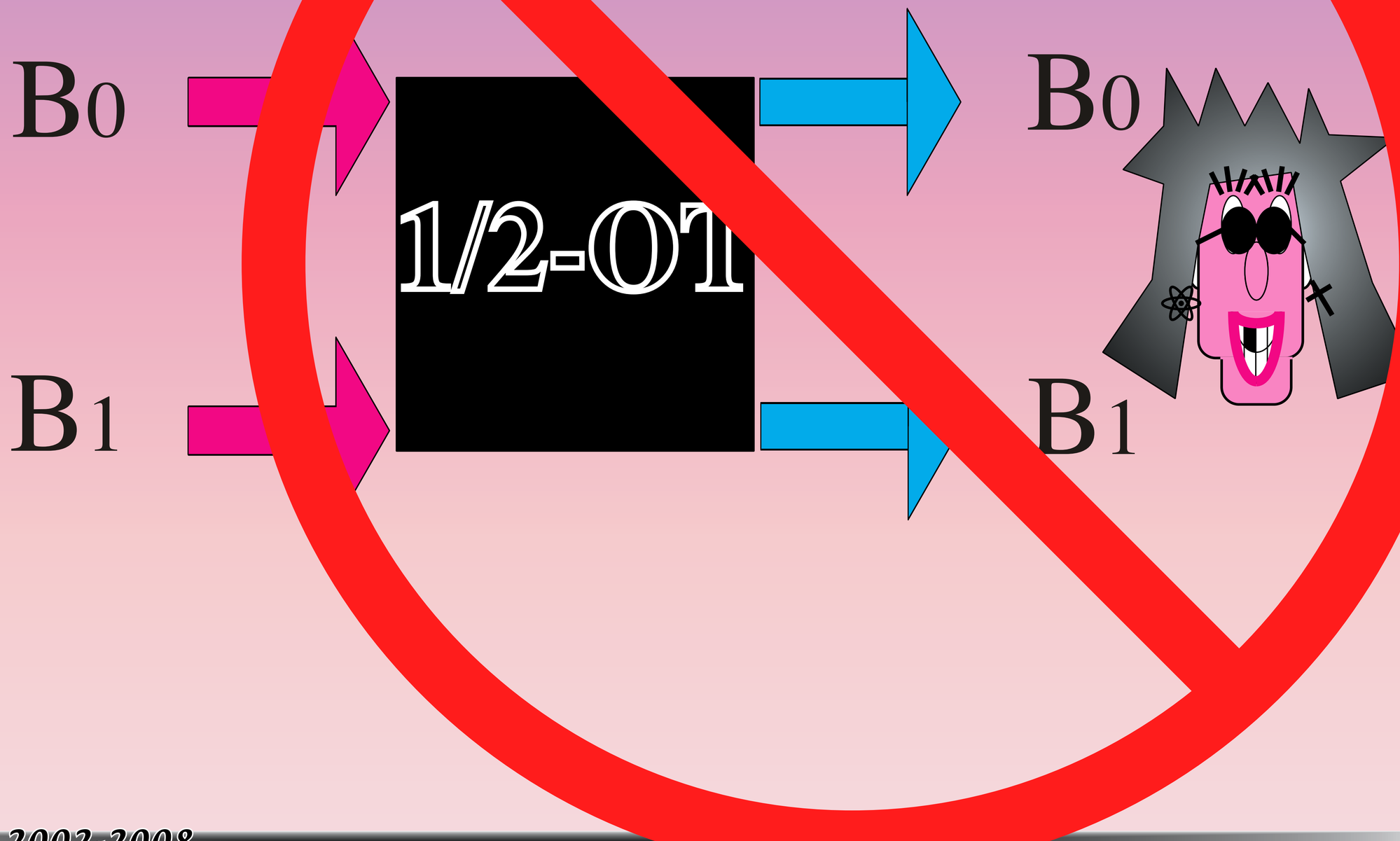
A:	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+

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

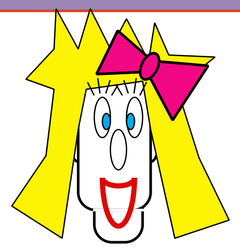
B:	0	0	1	1	0	1	0	1	=	0						0	=	1	1	0	0	0	1	0	1
A:	0	0	1	1	0	1	0	1	=	0	=	®	$_0$		®	$_1$	=	1	1	0	0	0	1	0	1

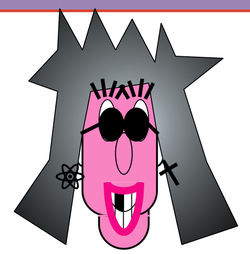


Oblivious Transfer



Q-OT from Q-BC



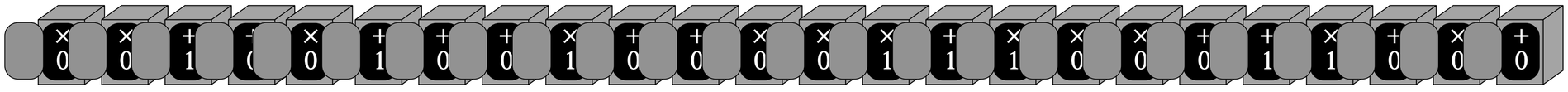


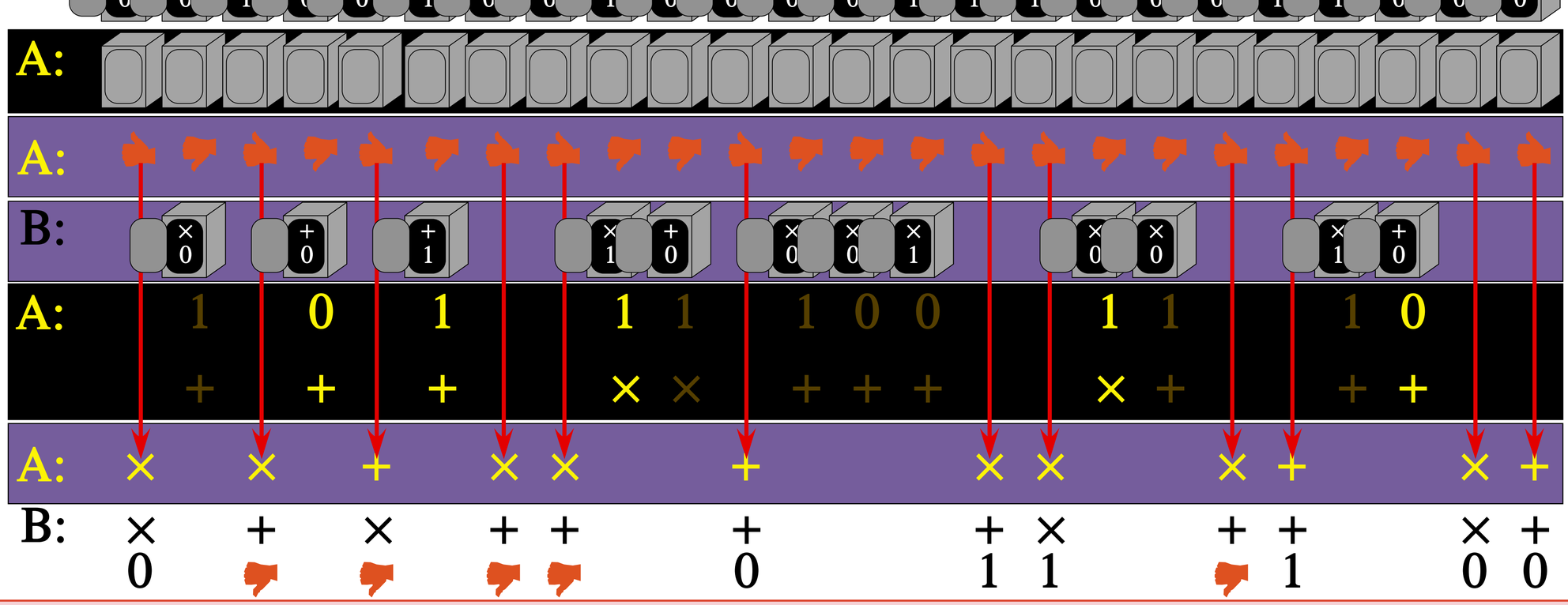
A: 0 1 1 0 0 1 0 0 1 1 0 1 0 0 0 1 1 1 0 1 1 0 0 0

× + × + + + × × × × + + + + × × × + × + + + × +

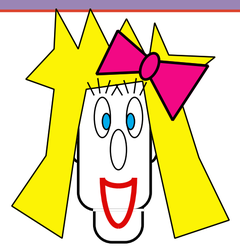
B: × × + + × + + + × + + × × × + × × × + + × + × +

0 0 1 0 0 1 0 0 1 0 0 0 0 1 1 1 0 0 0 1 1 0 0 0



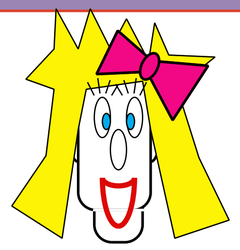


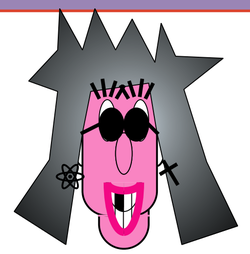
Q-OT from Q-BC

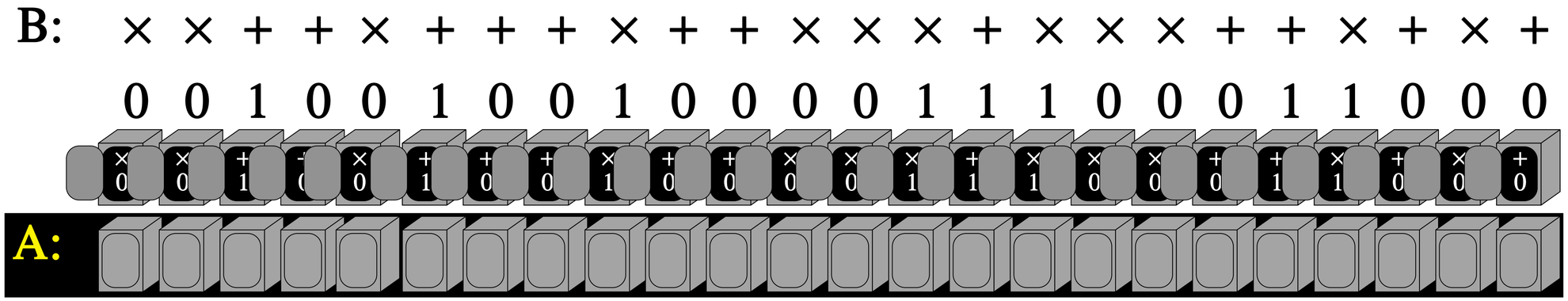


A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	×	×	+	+	×	+	+	+	×	+	+	×	×	×	+	×	×	×	+	+	×	+	×	+
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0

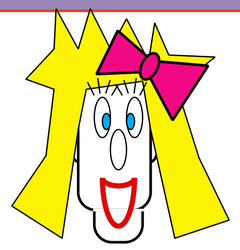
Q-OT from Q-BC

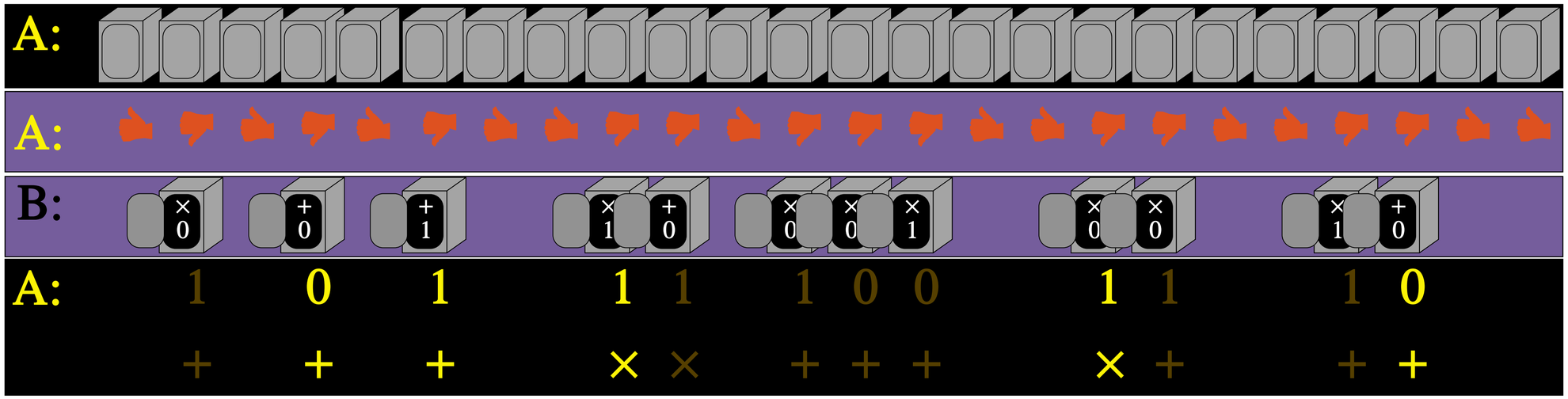




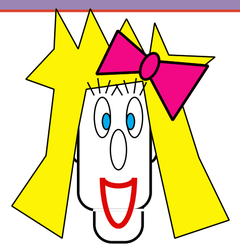


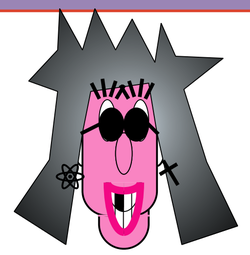
Q-OT from Q-BC

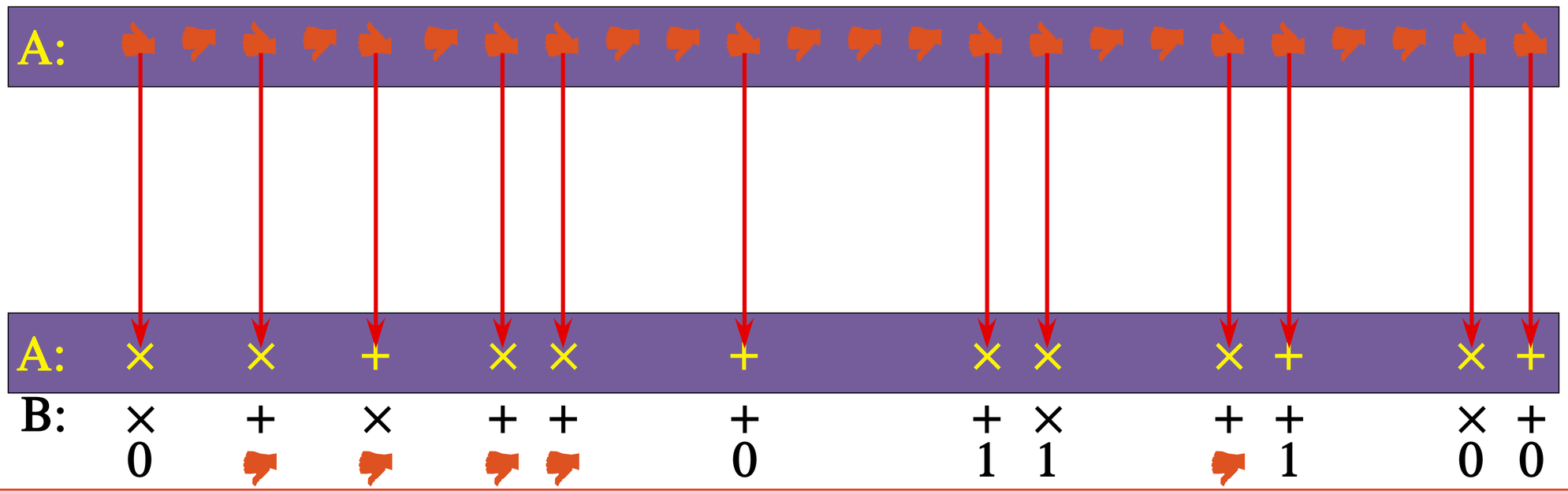




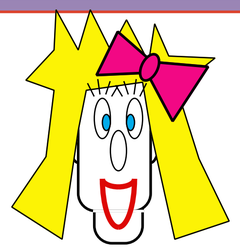
Q-OT from Q-BC

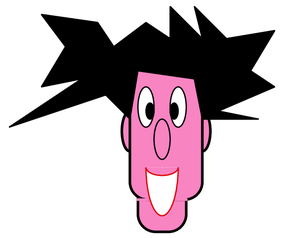






Q-OT





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

(6)

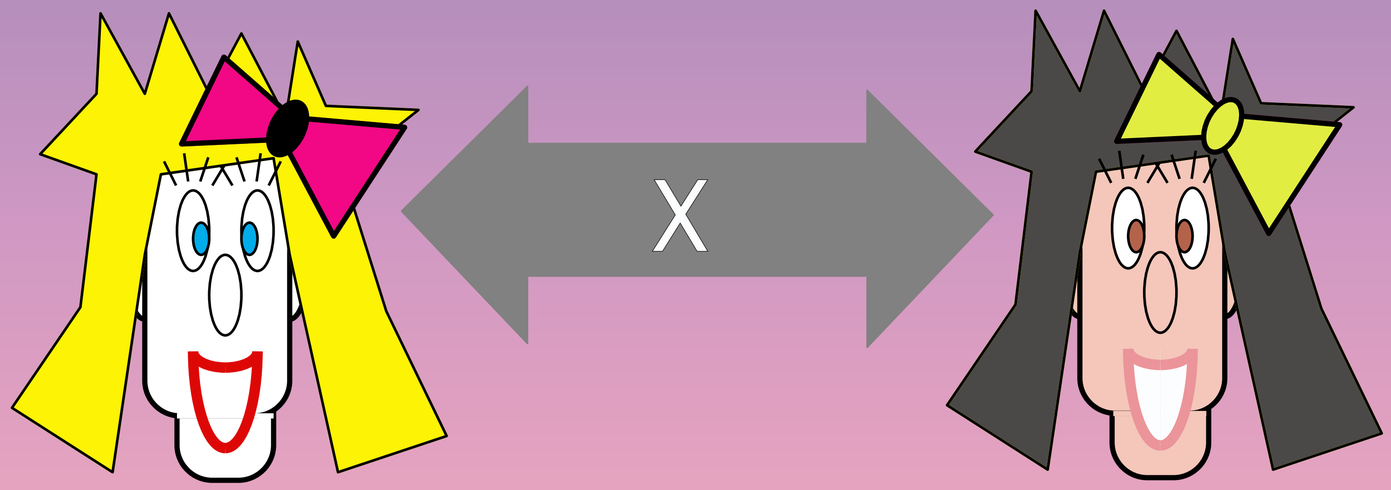
two provers

Cryptographic Protocols

Classically

BGKW88

Classically

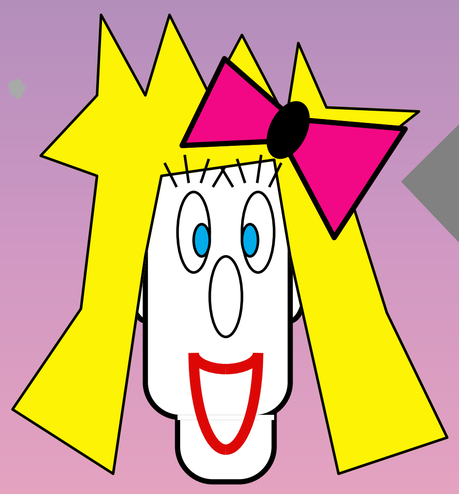


Ben-Or, Goldwasser, Kilian, Wigderson

b

$z = x$ if $b = 0$

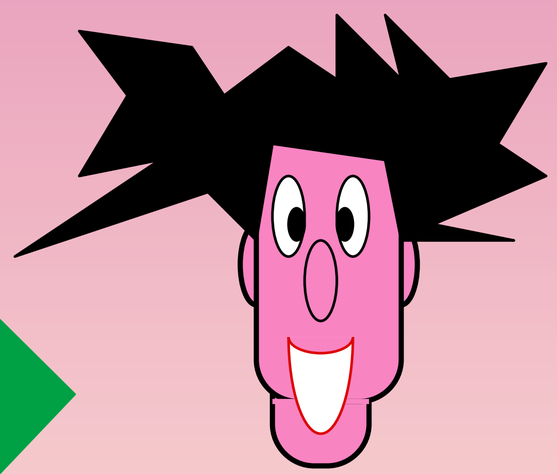
$z = x \oplus y$ if $b = 1$



y

z

x



$x \oplus z = b \cdot y$?

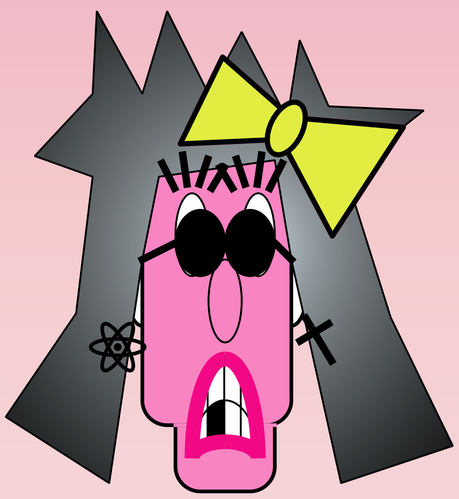
Ben-Or, Goldwasser, Kilian, Wigderson

$x_0 \oplus z = 0 \cdot y = 0$

$x_1 \oplus z = 1 \cdot y = y$

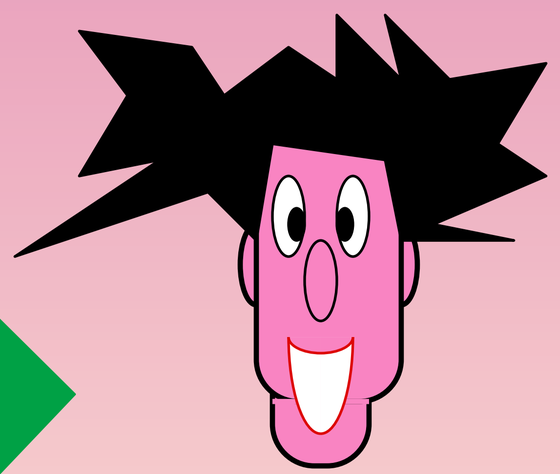
$x_0 \oplus x_1 = (x_0 \oplus z) \oplus (x_1 \oplus z) = y$

possible with prob. at most 2^{-n}



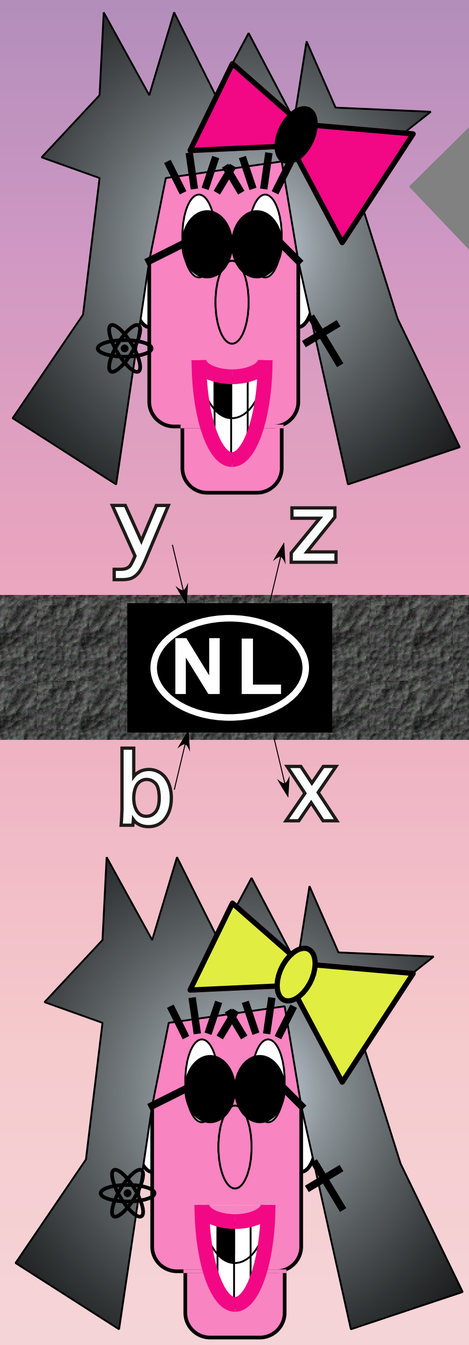
x_0

x_1



Ben-Or, Goldwasser, Kilian, Wigderson

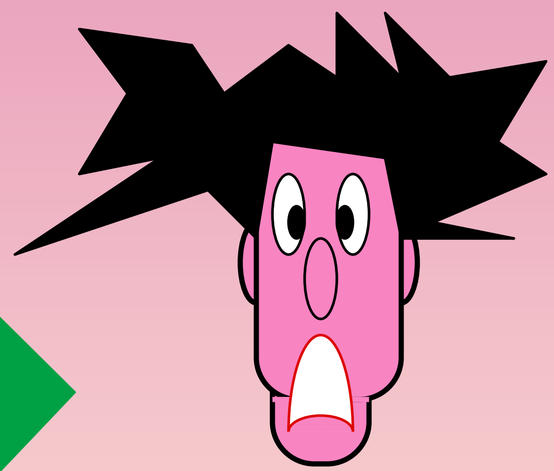
Classically



y

z

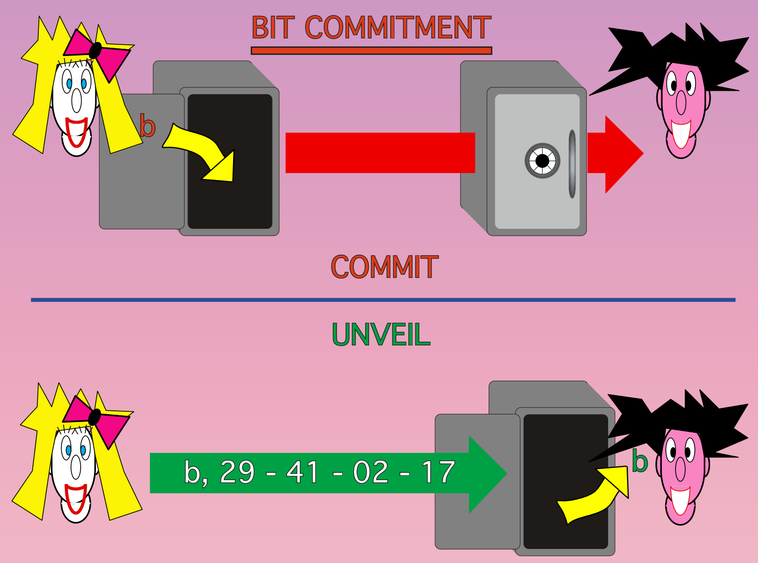
x



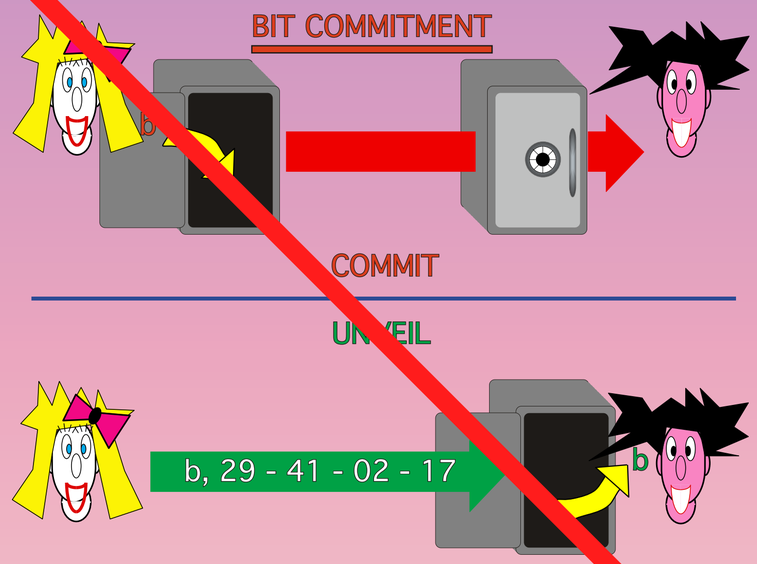
$x \oplus z = b \cdot y$

Ben-Or, Goldwasser, Kilian, Wigderson

Quantumly



or



???

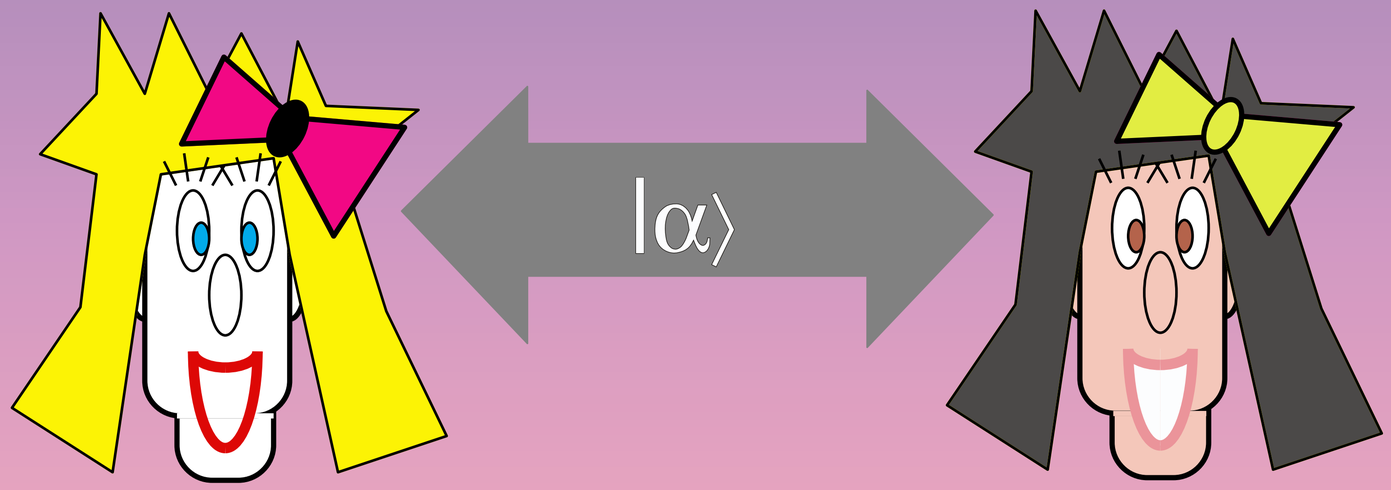
(7)

two provers BC

Classically Secure

Quantumly Insecure

Quantumly

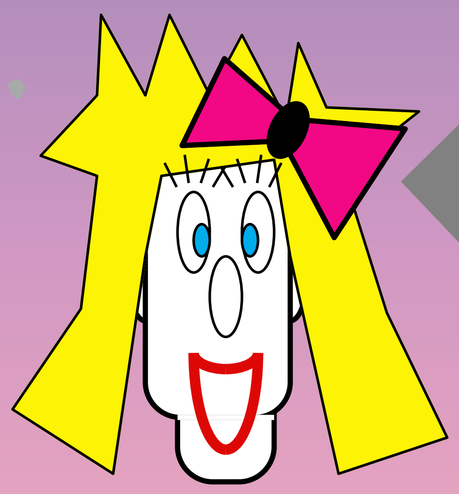


Ben-Or, Goldwasser, Kilian, Wigderson

b

$z = x$ if $b = 0$

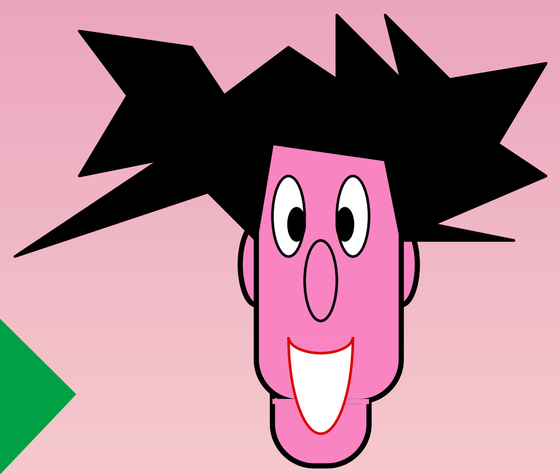
$z = x \oplus y$ if $b = 1$



y

z

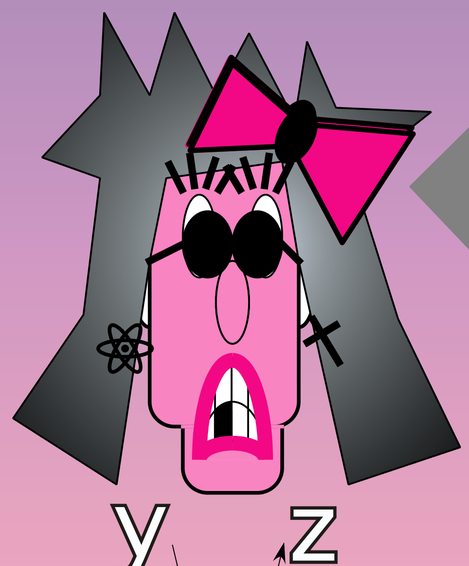
x



$D_H(x \oplus z, b \cdot y) < n/5?$

Ben-Or, Goldwasser, Kilian, Wigderson

Classically



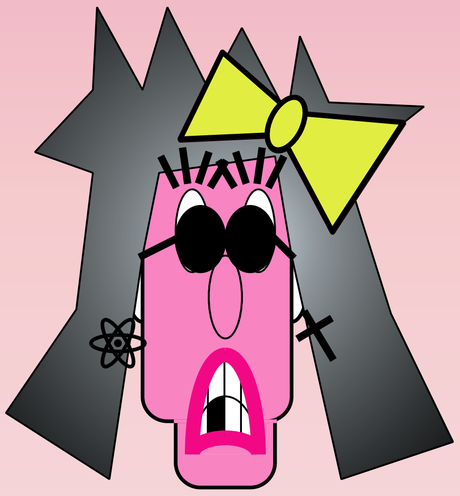
y

z

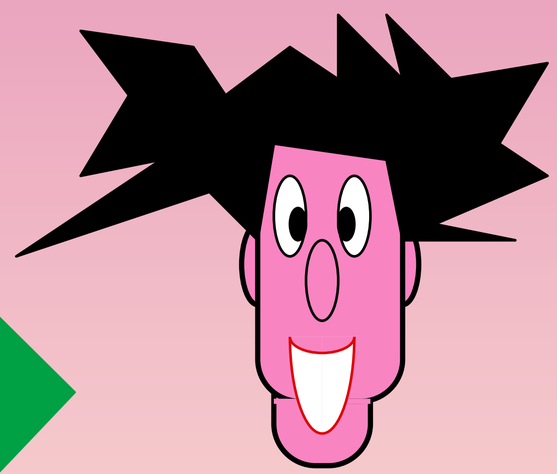
y z

75% NL -> $D_H(x \oplus z, b \cdot y) \approx 25\% n > n/5$

b x



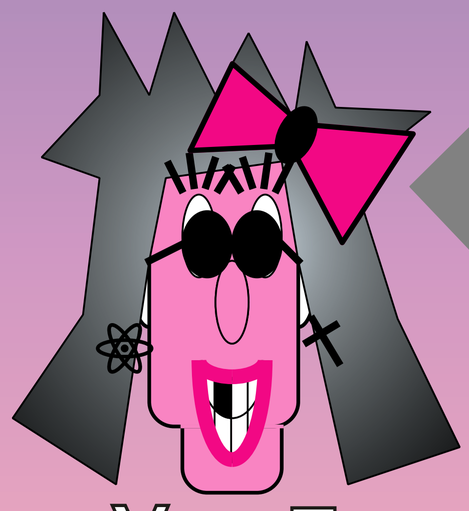
x



$D_H(x \oplus z, b \cdot y) < n/5$?

Ben-Or, Goldwasser, Kilian, Wigderson

Quantumly



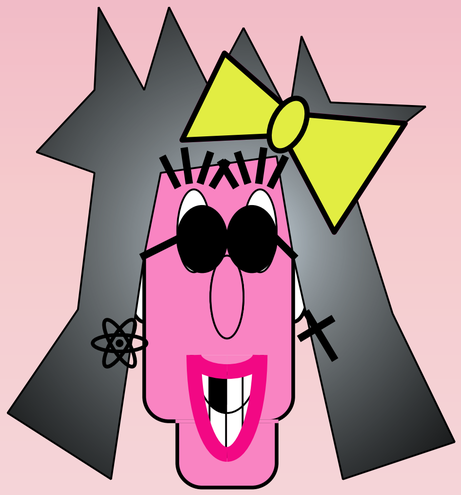
y

z

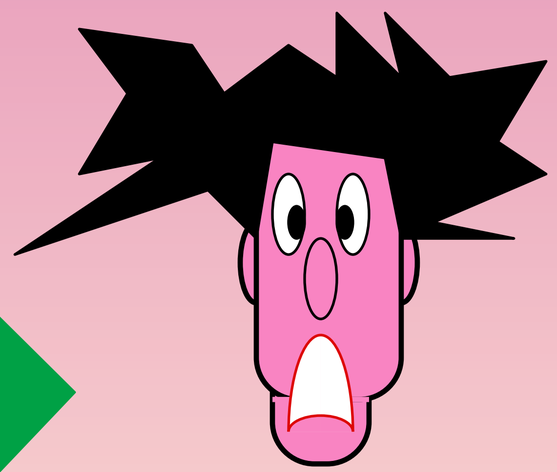
y z

≈85% NL -> $D_H(x \oplus z, b \cdot y) \approx 15\% n < n/5$

b x



x



$D_H(x \oplus z, b \cdot y) < n/5$?

~~Ben-Or, Goldwasser, Kilian, Wigderson~~

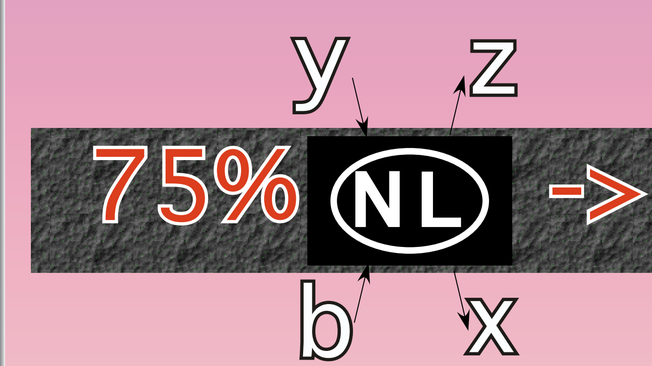
Classically

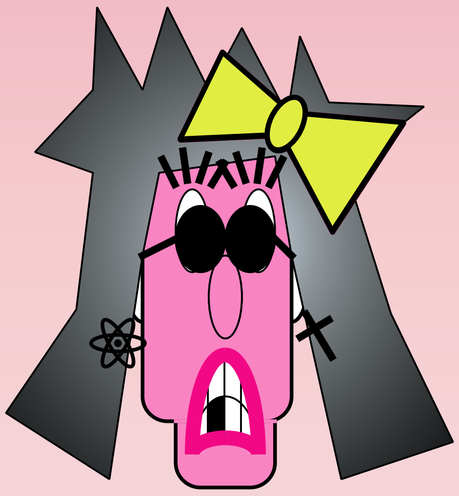
$D_H(x_0 \oplus z, 0 \cdot y) = D_H(x_0 \oplus z, 0) < n/5$

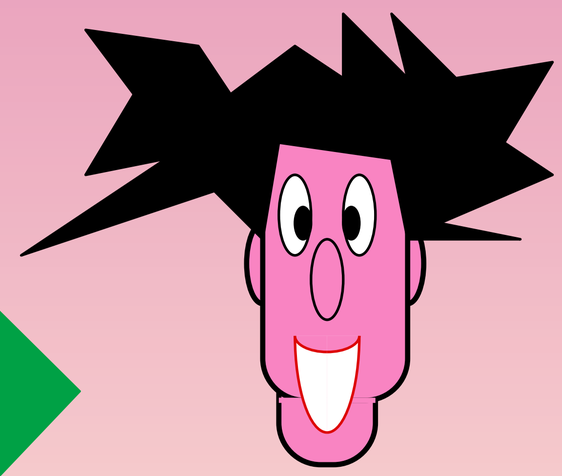
$D_H(x_1 \oplus z, 1 \cdot y) = D_H(x_1 \oplus z, y) < n/5$

$D_H(x_0 \oplus x_1, y) = D_H((x_0 \oplus z) \oplus (x_1 \oplus z), y) < 2n/5 < n/2$

possible with prob. at most c^{-n}





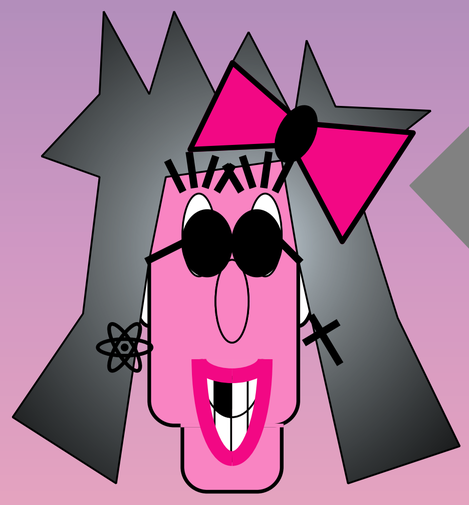


x_0

x_1

Ben-Or, Goldwasser, Kilian, Wigderson

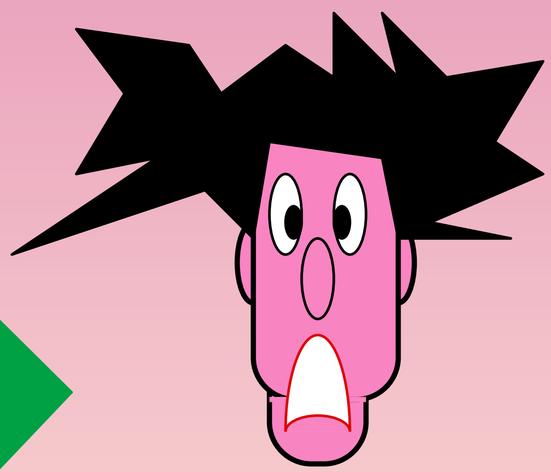
Quantumly



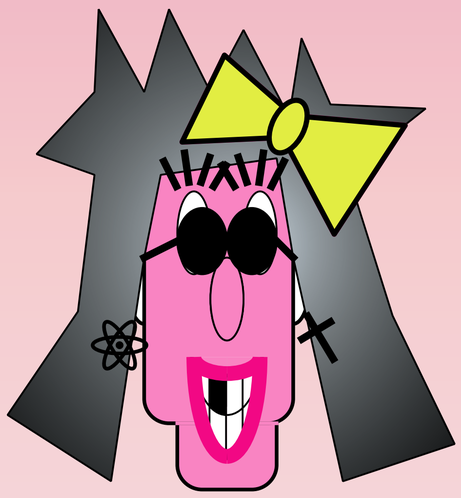
y

z

x



$x \oplus z = b \cdot y$



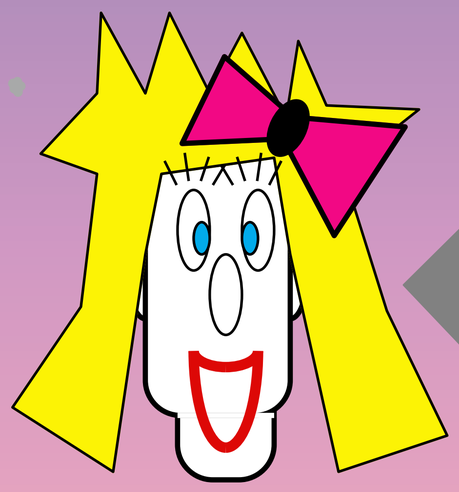
Ben-Or, Goldwasser, Kilian, Wigderson

(8)

two provers BC Classically and Quantumly Secure

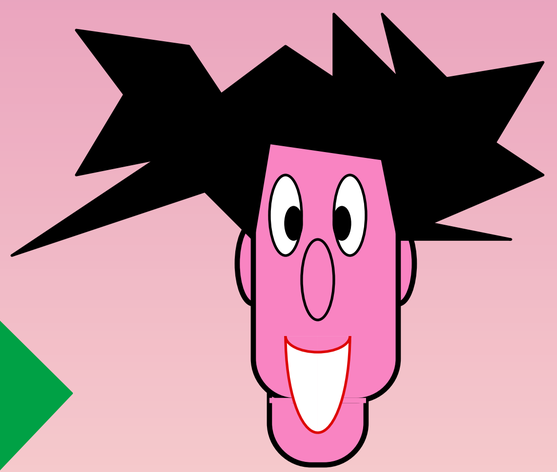
$z = x \oplus y_b$

b



y_0, y_1

z



$x = z \oplus y_b$?

x

modified BGKW

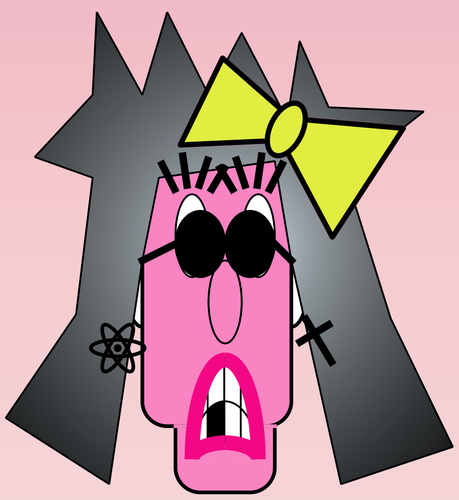
Classically

$x_0 \oplus z = y_0$

$x_1 \oplus z = y_1$

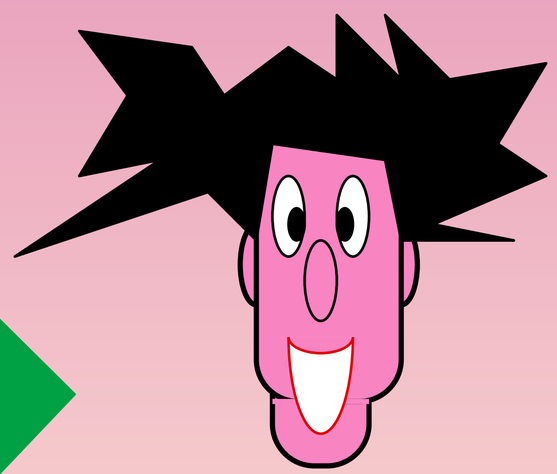
$x_0 \oplus x_1 = (x_0 \oplus z) \oplus (x_1 \oplus z) = y_0 \oplus y_1$

possible with prob. at most 2^{-n}



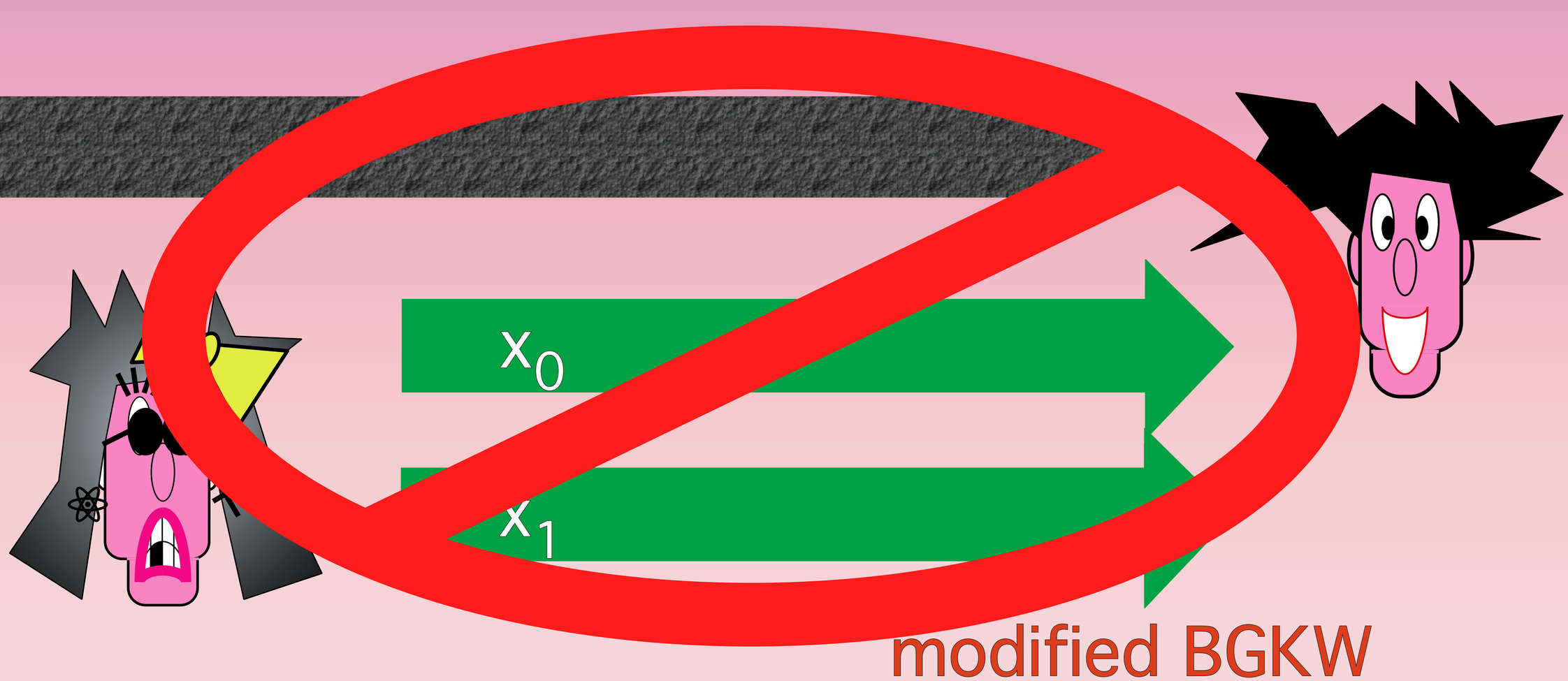
x_0

x_1



modified BGKW

Quantumly



modified BGKW

Quantumly

MAIN THEOREM

Let 0 and 1 be POVMs such that outputs x_0 and x_1 one could obtain by applying one of them to the state shared among the two provers.

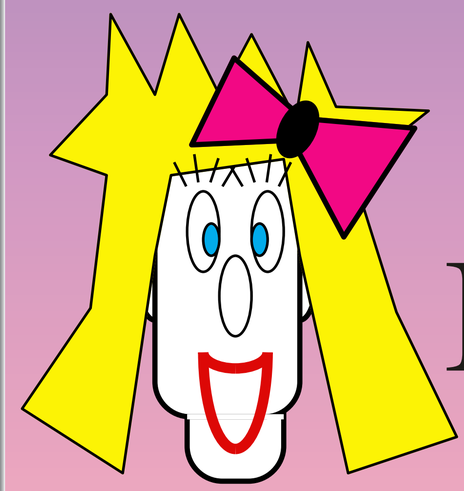
Suppose the success probability of unveiling is
$p_0+p_1 > 1+\delta$,
then the (prediction probability of $y_0 \oplus y_1$) $> \delta$.

This prediction probability is achieved by first applying 0 to the shared state followed by 1 on the leftover system or the other way around.

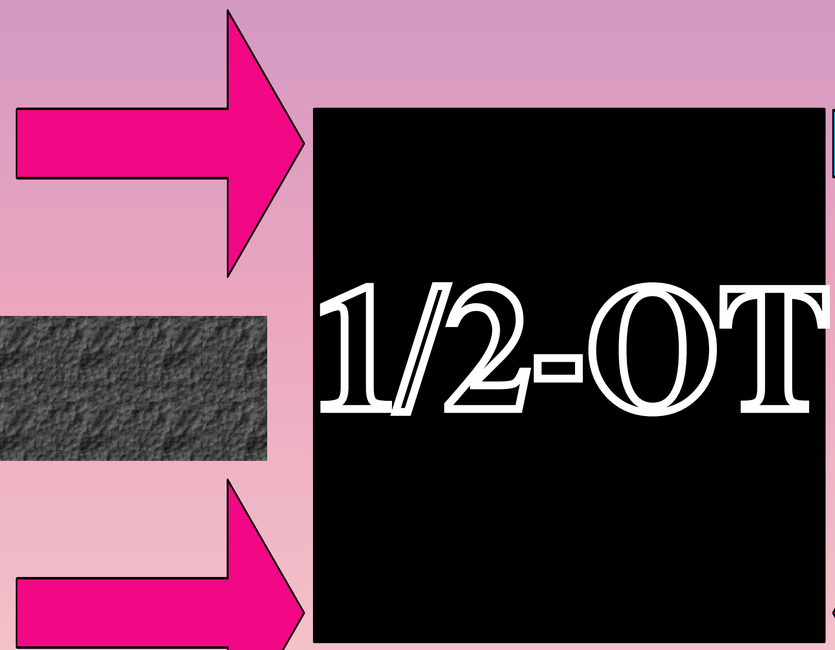
(9)

WARNING !

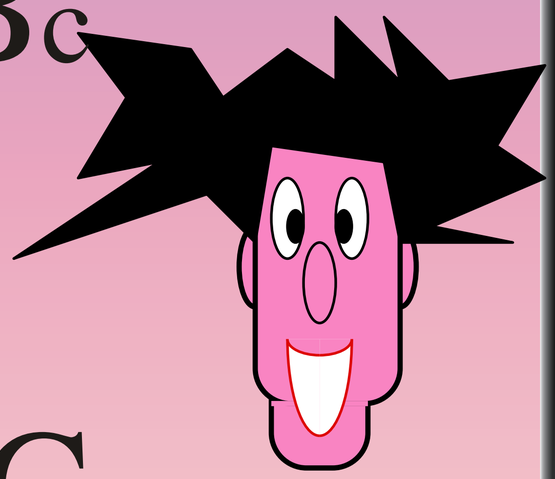
Oblivious Transfer (message multiplexing)



B_0



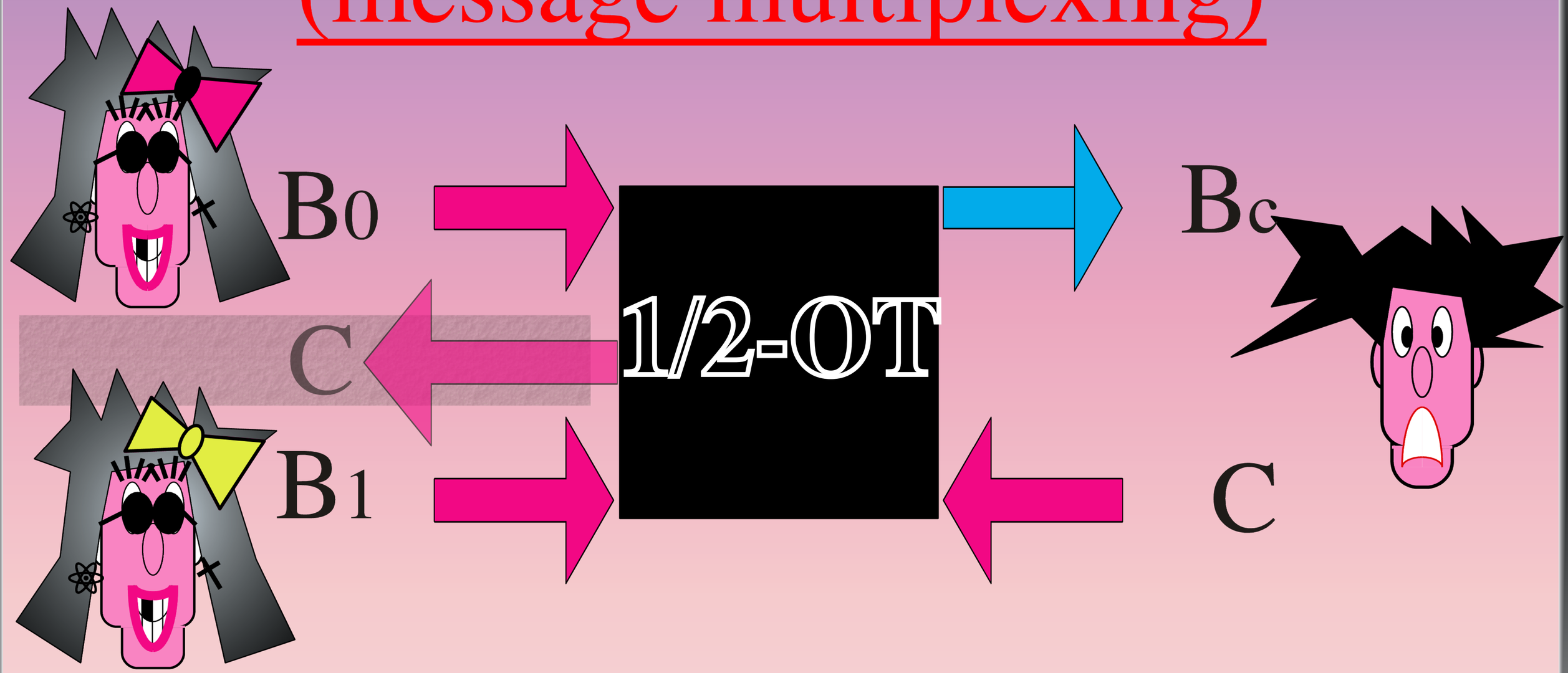
B_c



B_1

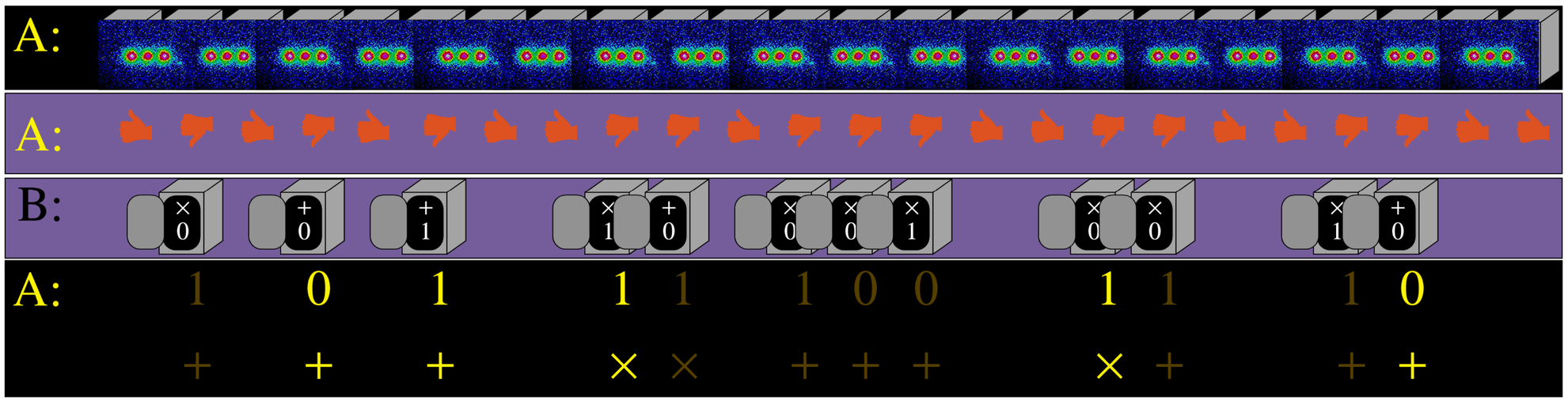
C

Oblivious Transfer (message multiplexing)

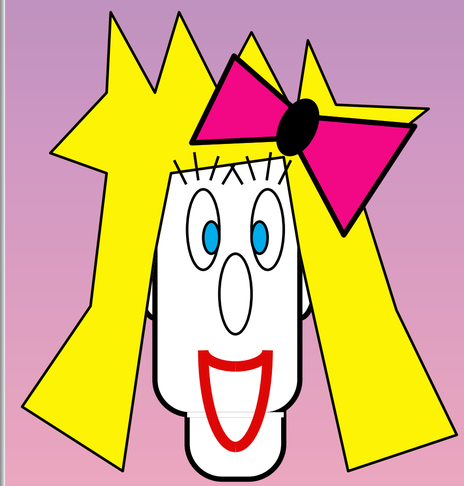


Brassard, Crépeau, Mayers, Salvail 97

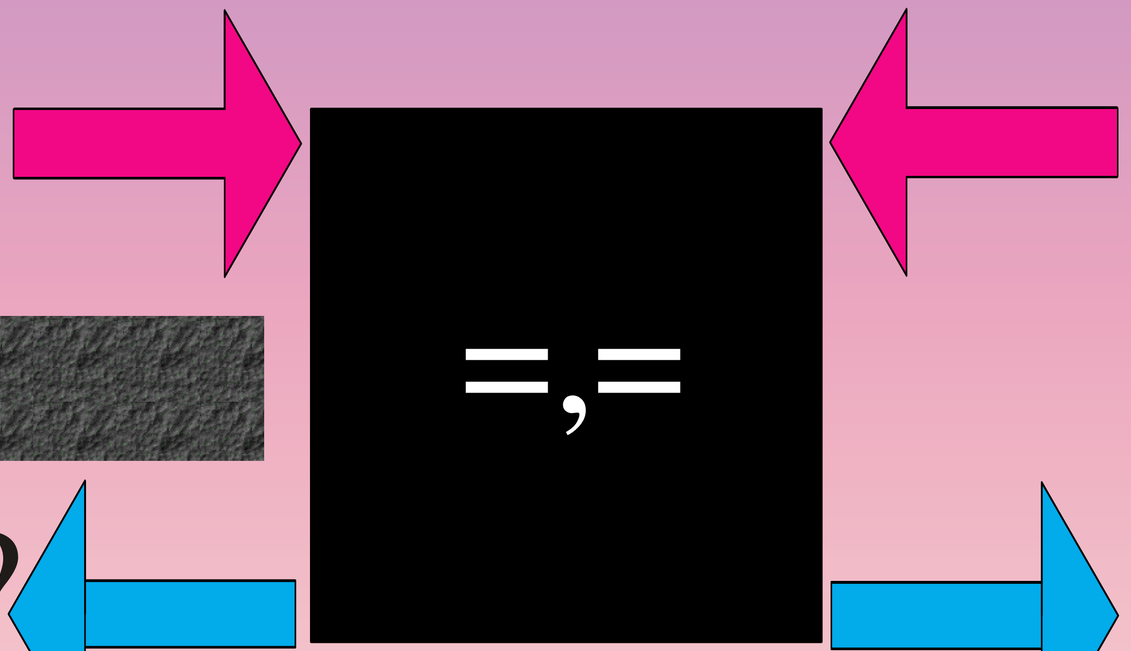
BCMS' attack



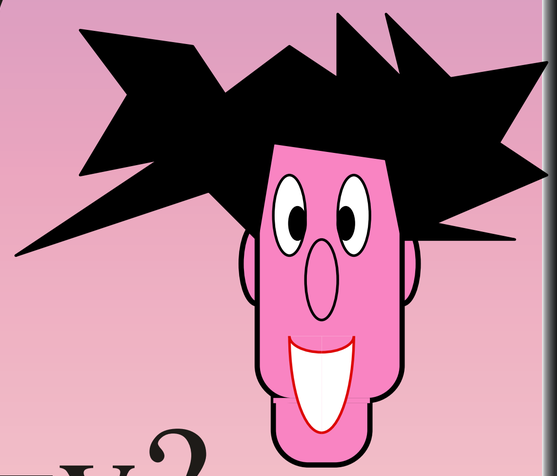
Mutual Identification



x



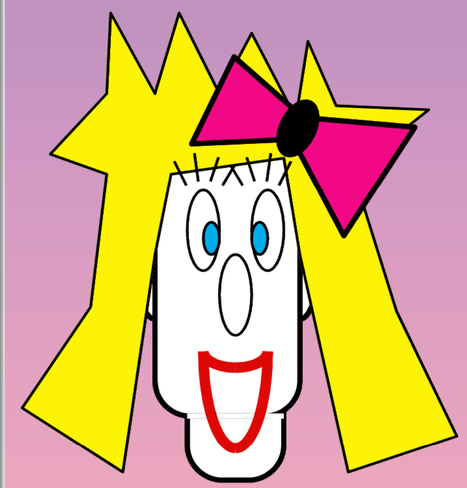
y



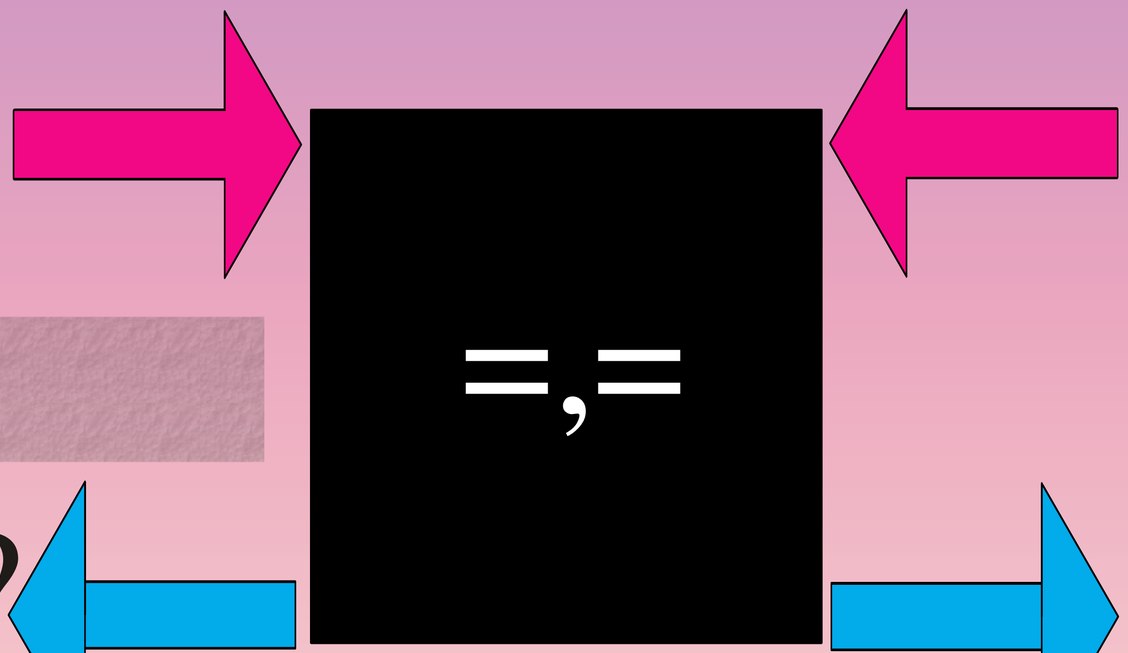
x=y?

x=y?

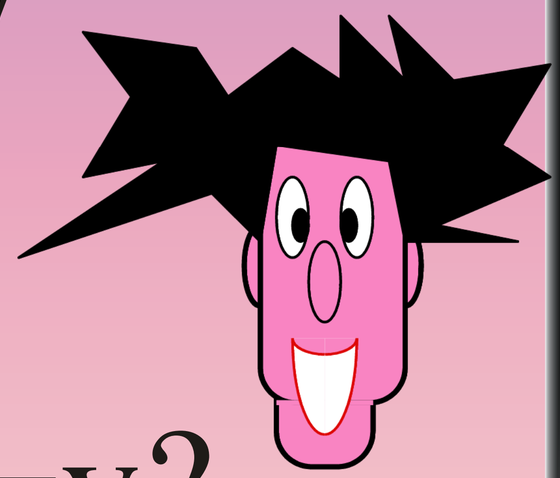
Mutual Identification



x



y

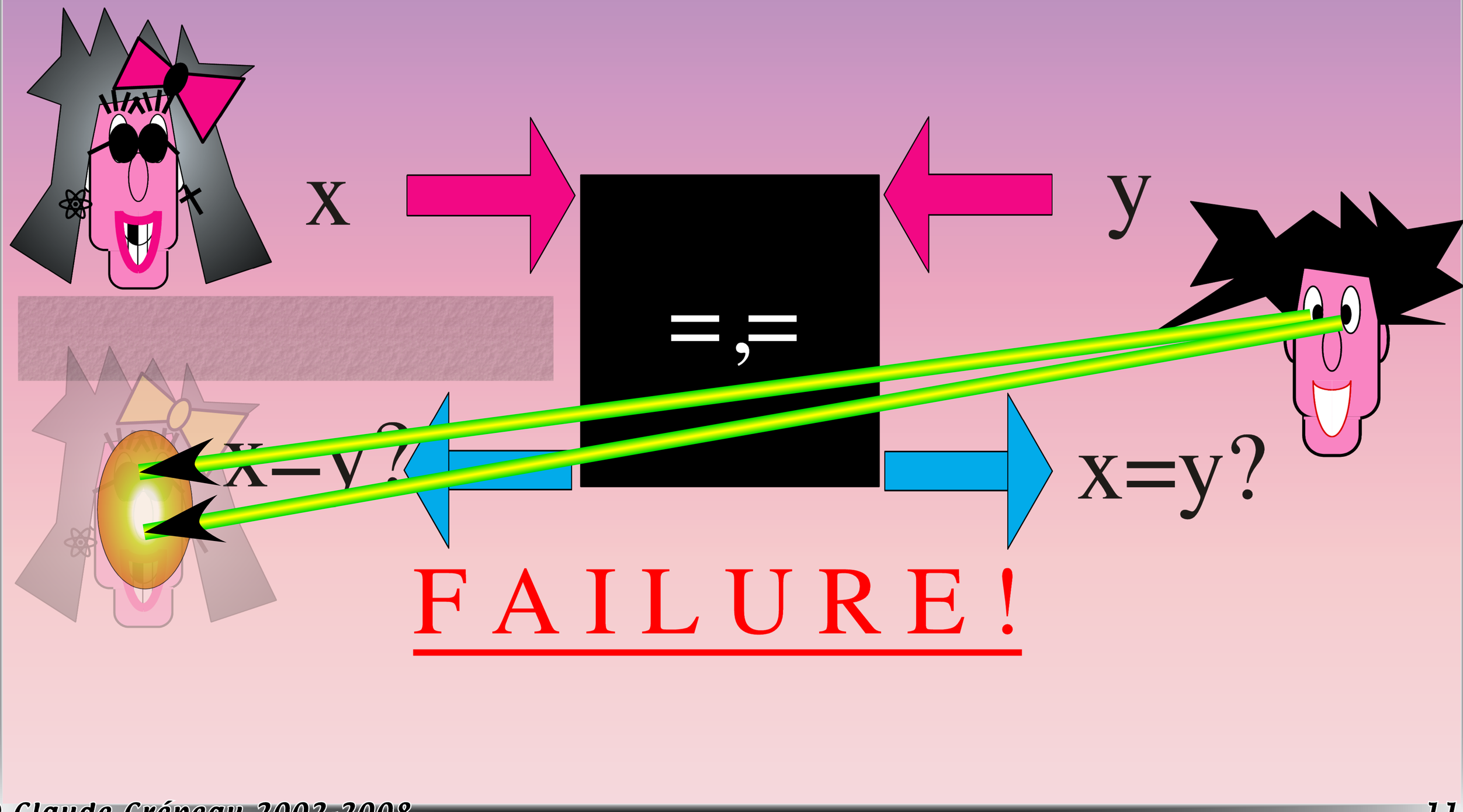


x=y?

x=y?

SUCCESS!

Mutual Identification



FAILURE!

an Introduction to theoretical quantum CRYPTOGRAPHY

Claude Crépeau

School of Computer Science
McGill University