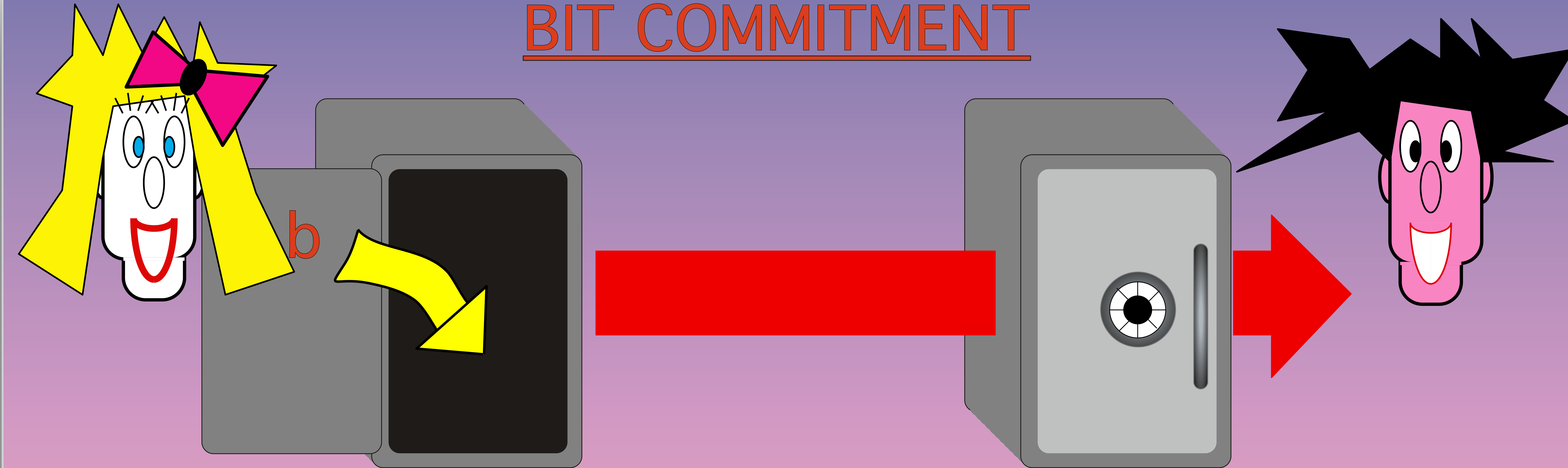
Introduction to theoretical quantum CRYPTOGRAPHY

Claude Crépeau

School of Computer Science
McGill University

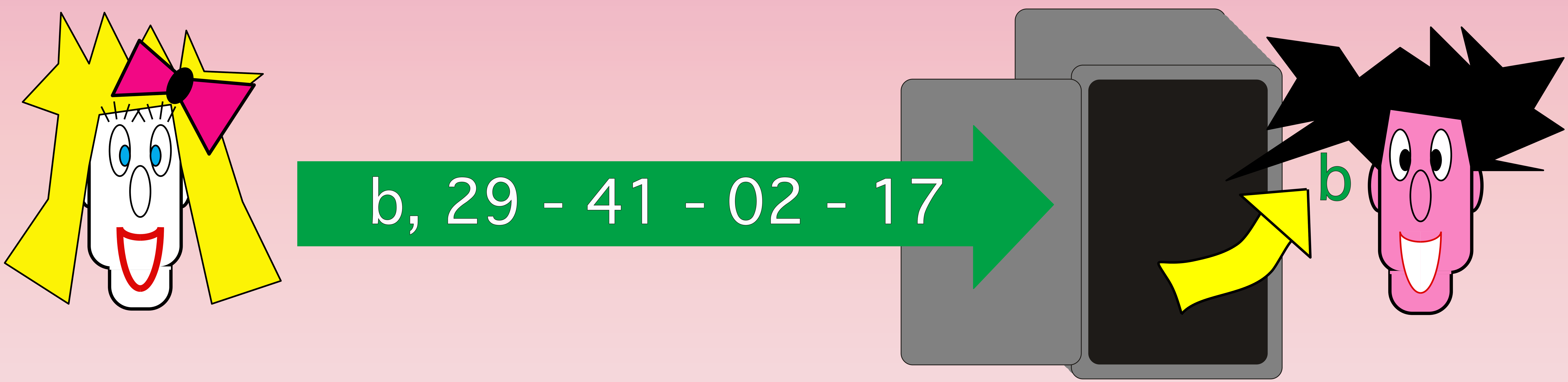
(4) two-party Cryptographic Protocols

BIT COMMITMENT

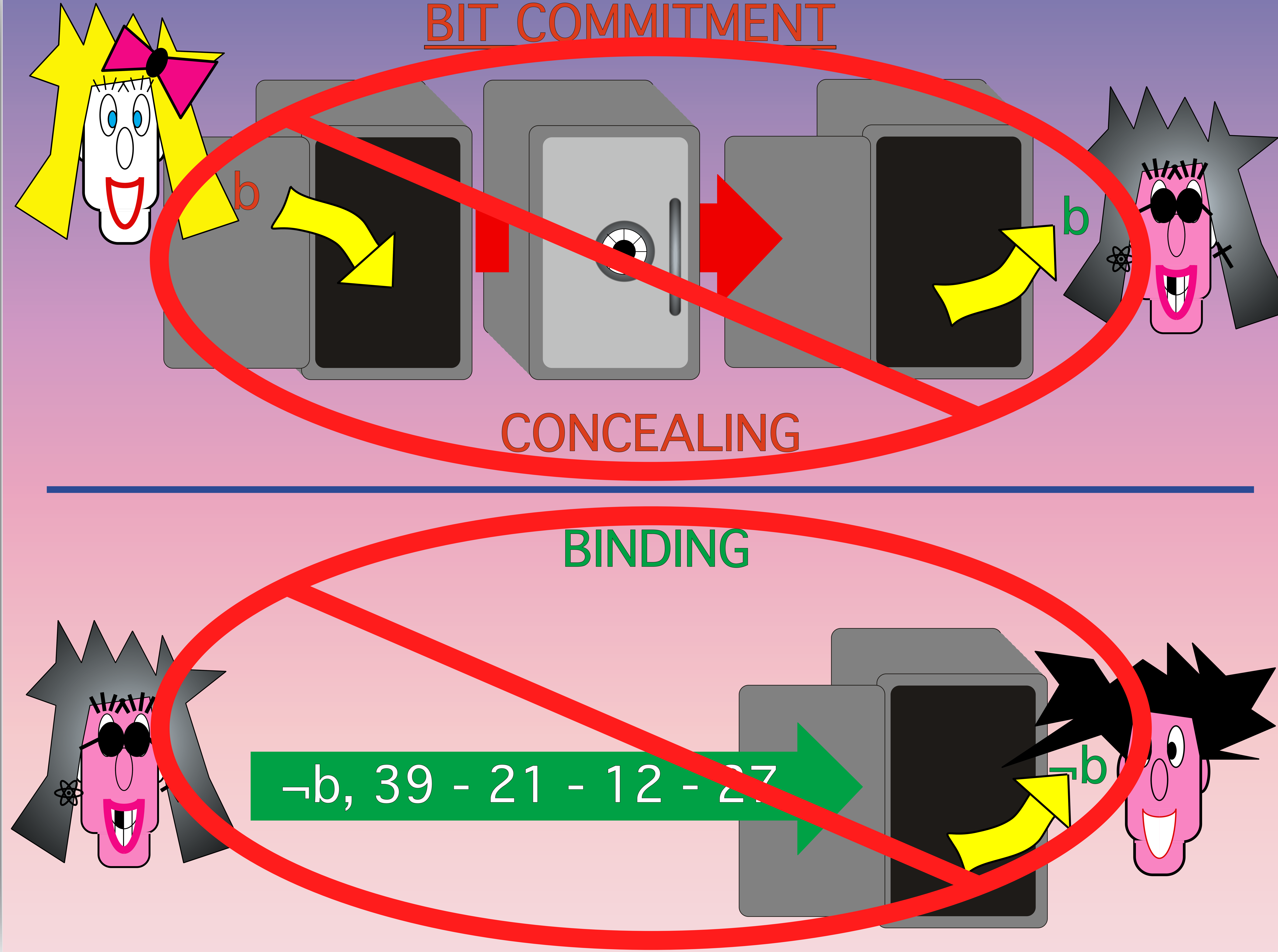


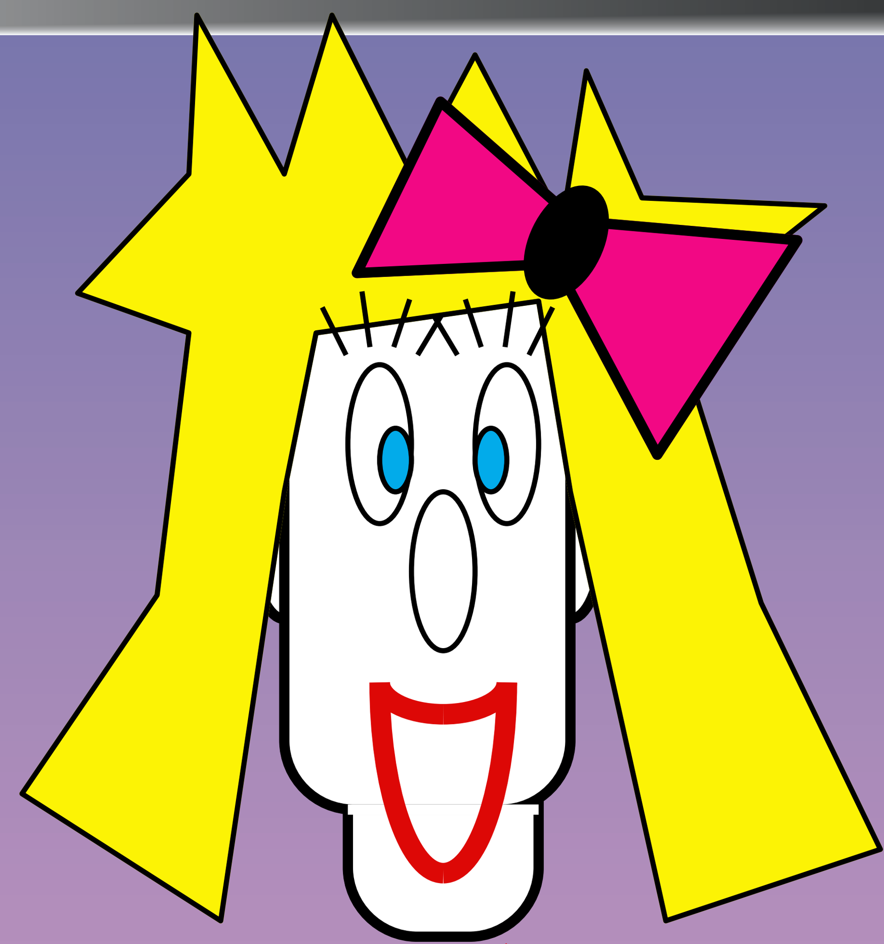
COMMIT

UNVEIL

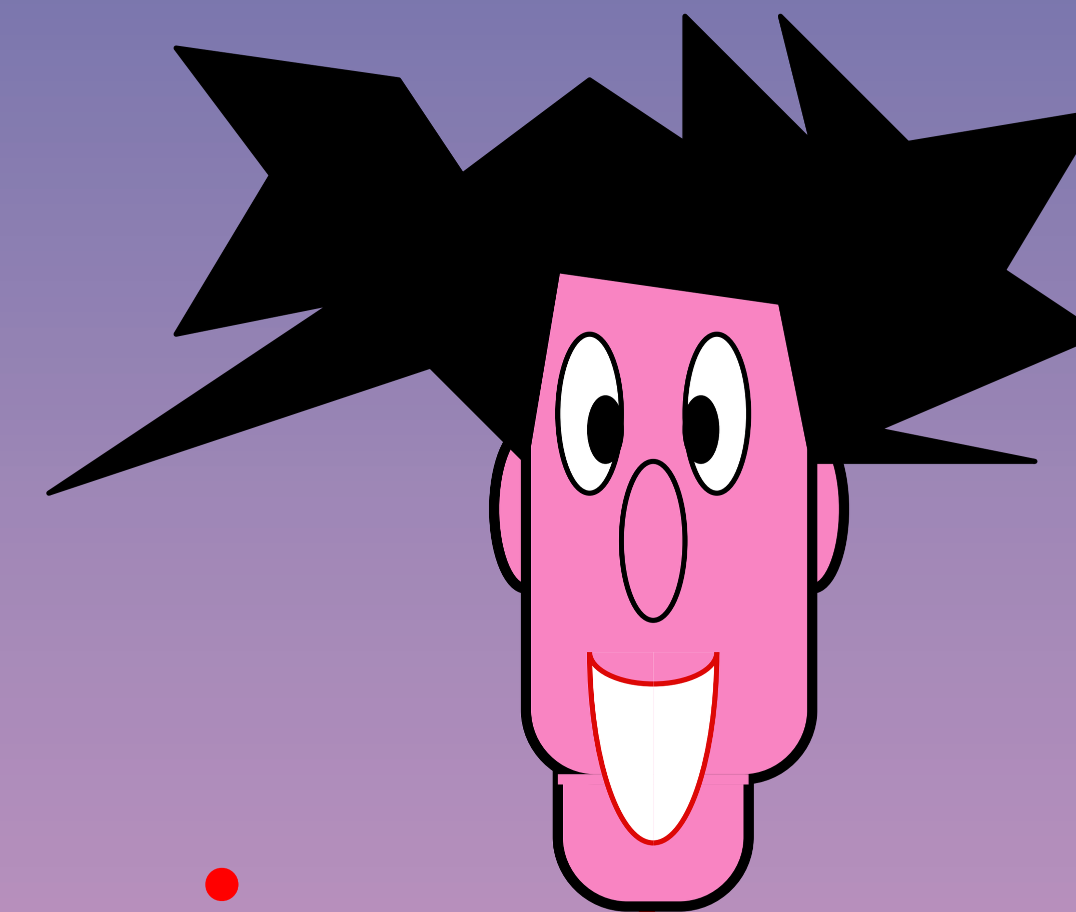


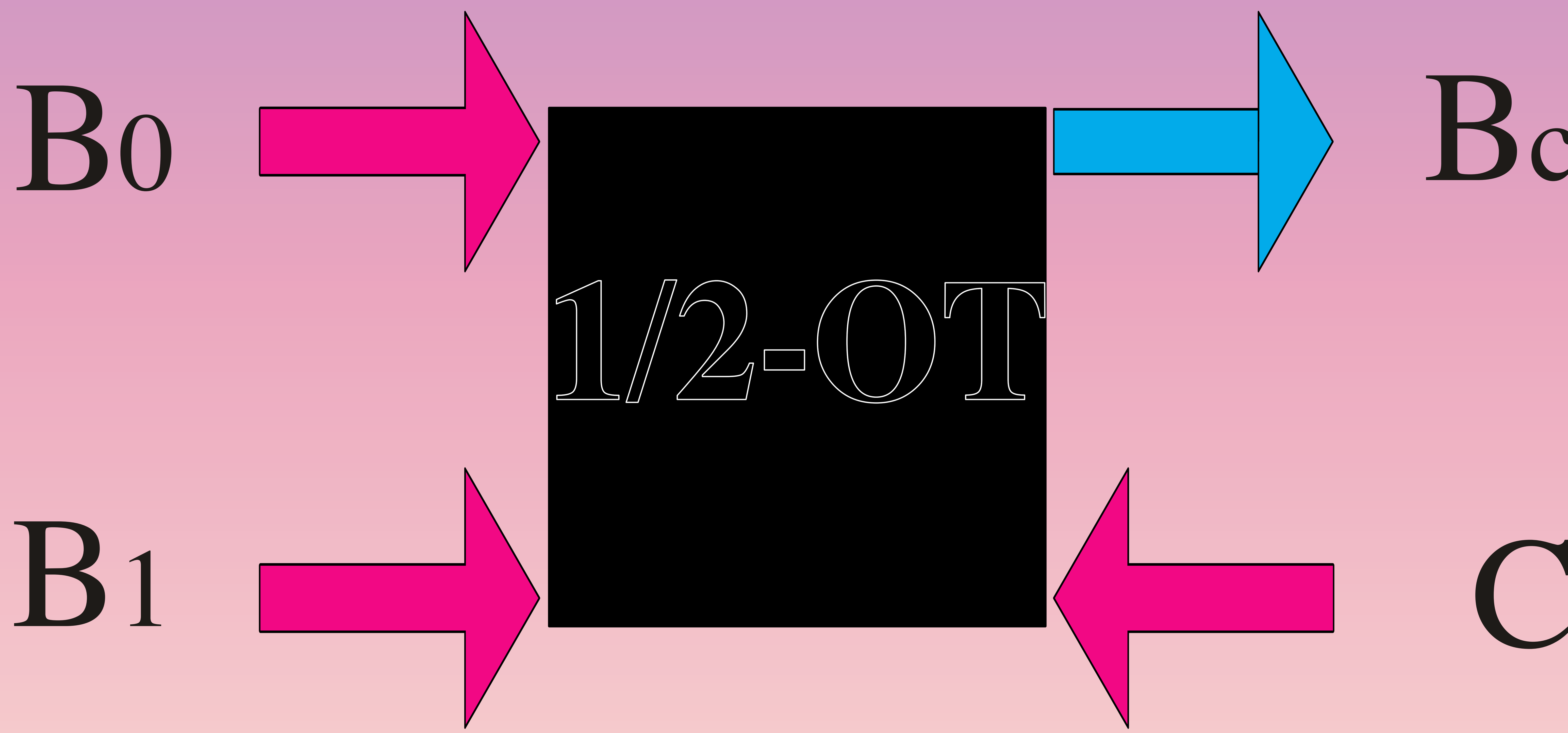
BIT COMMITMENT



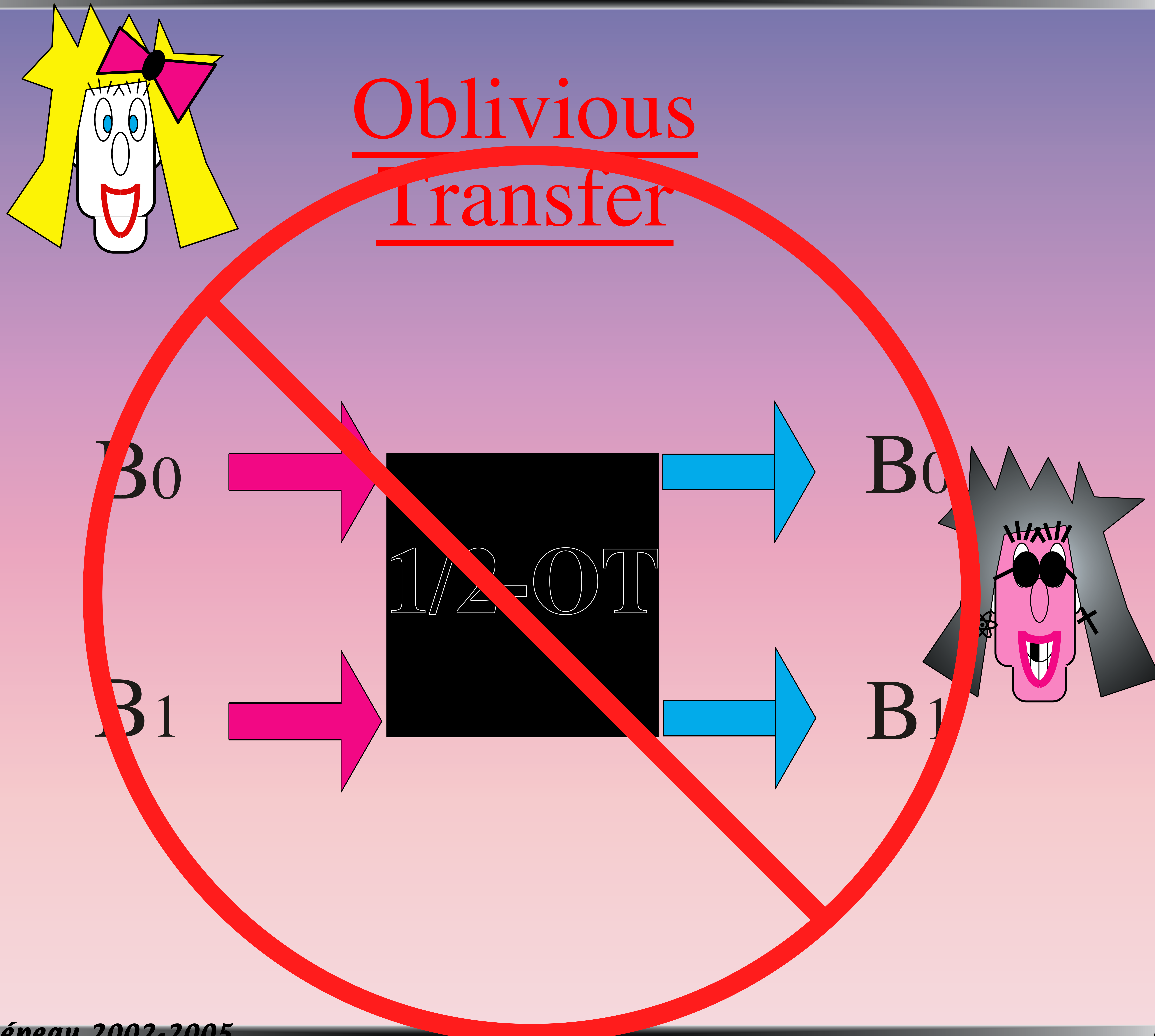


Oblivious Transfer (message multiplexing)

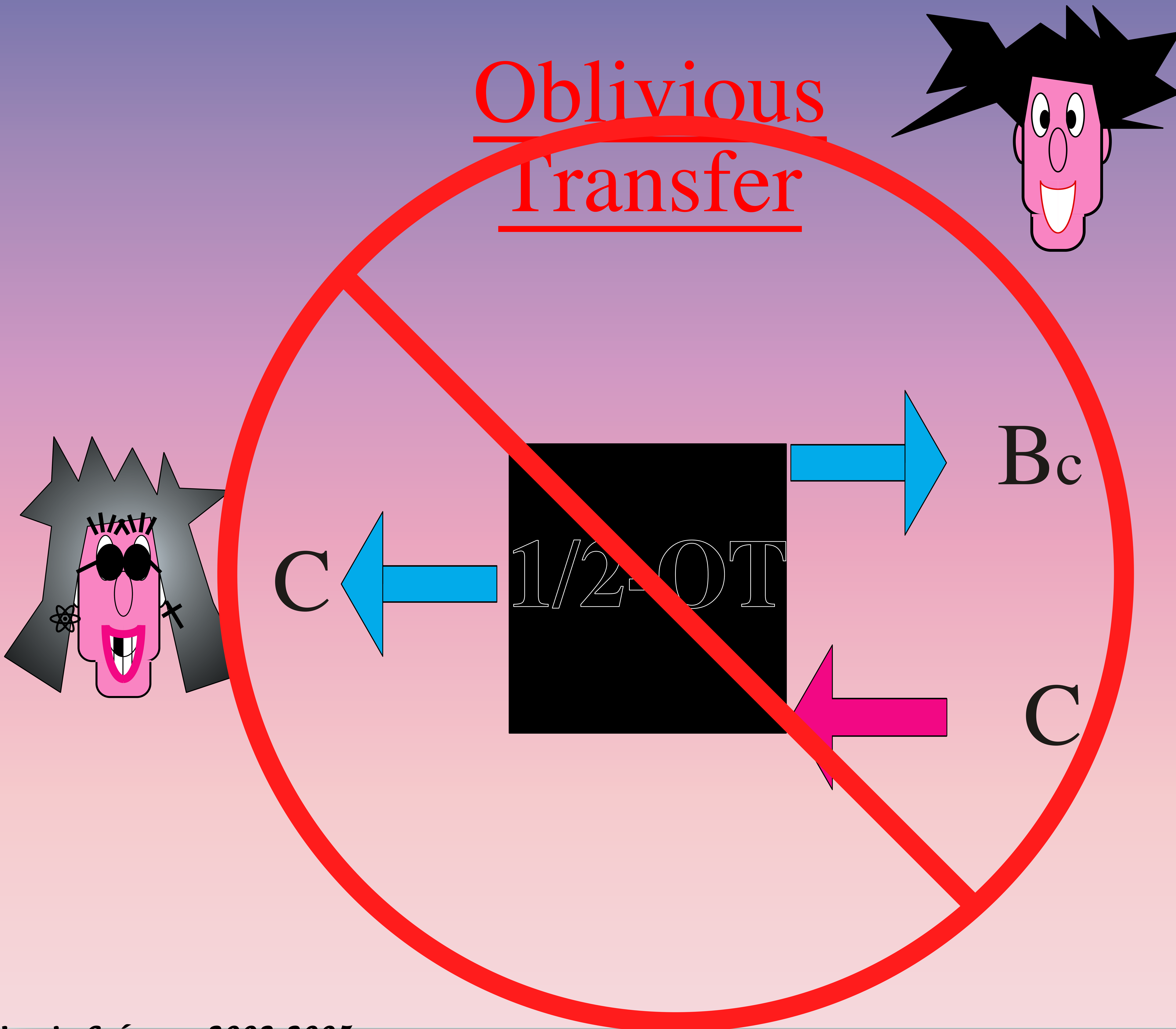


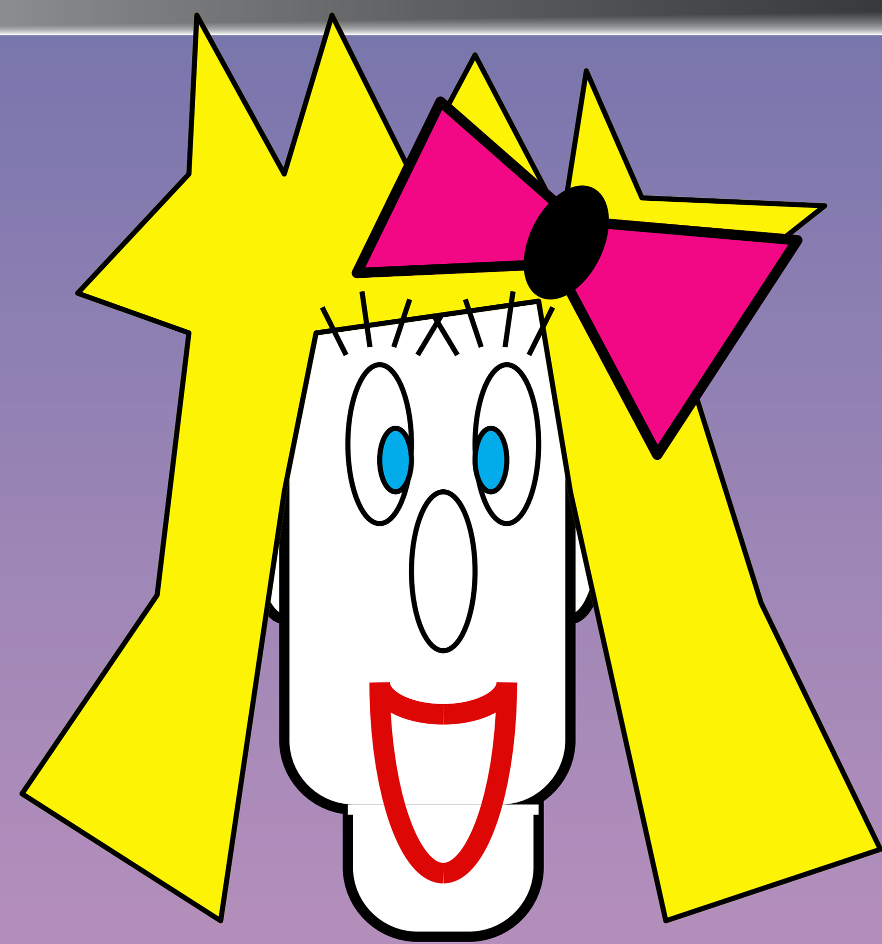


Oblivious Transfer

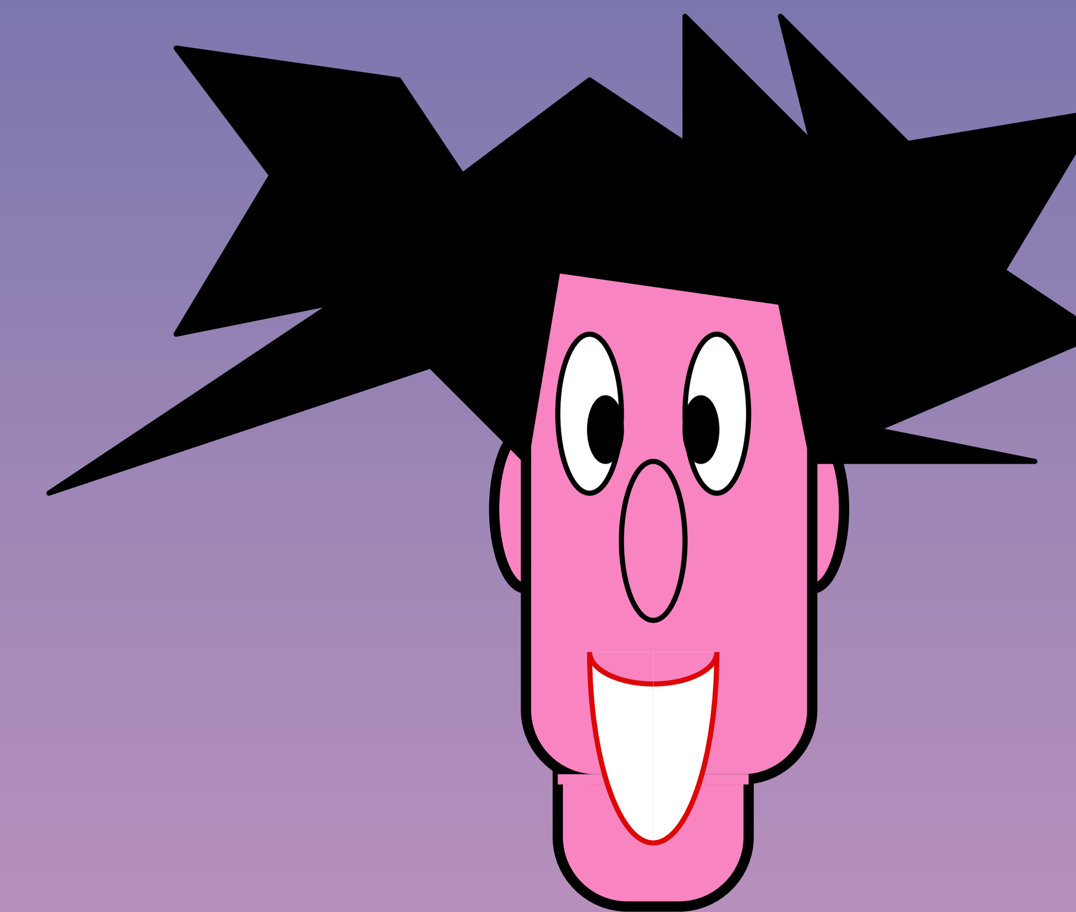


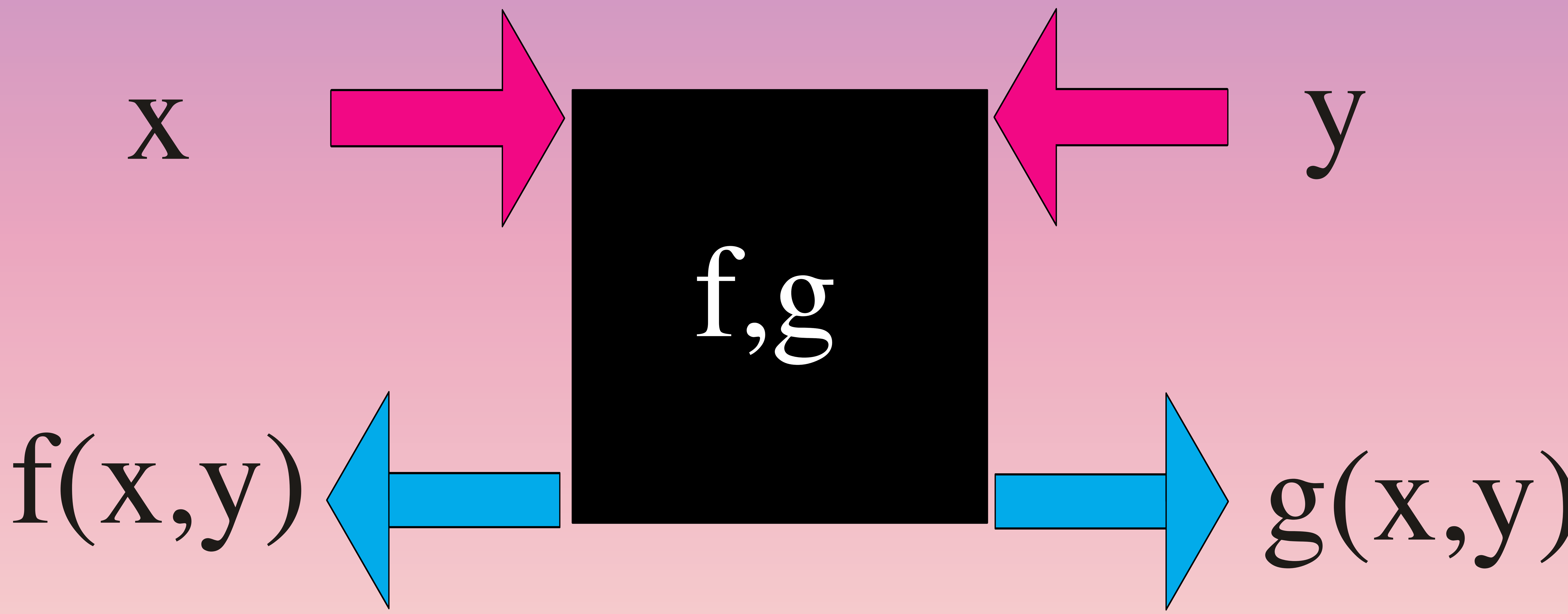
Oblivious Transfer

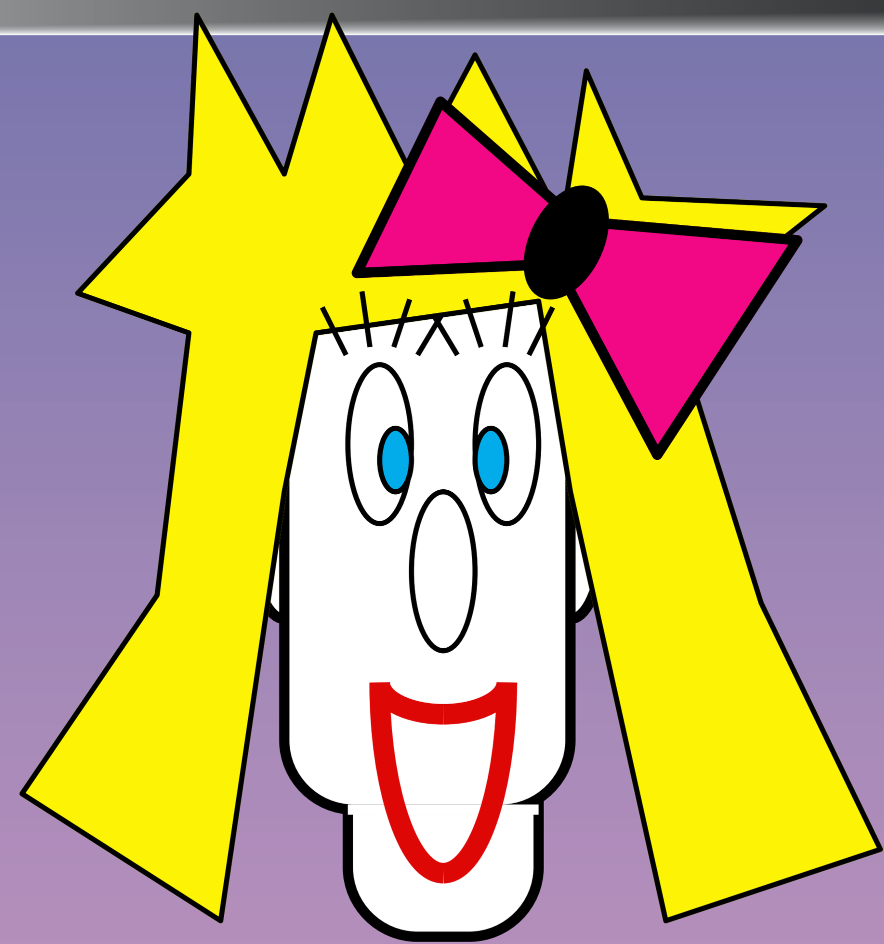




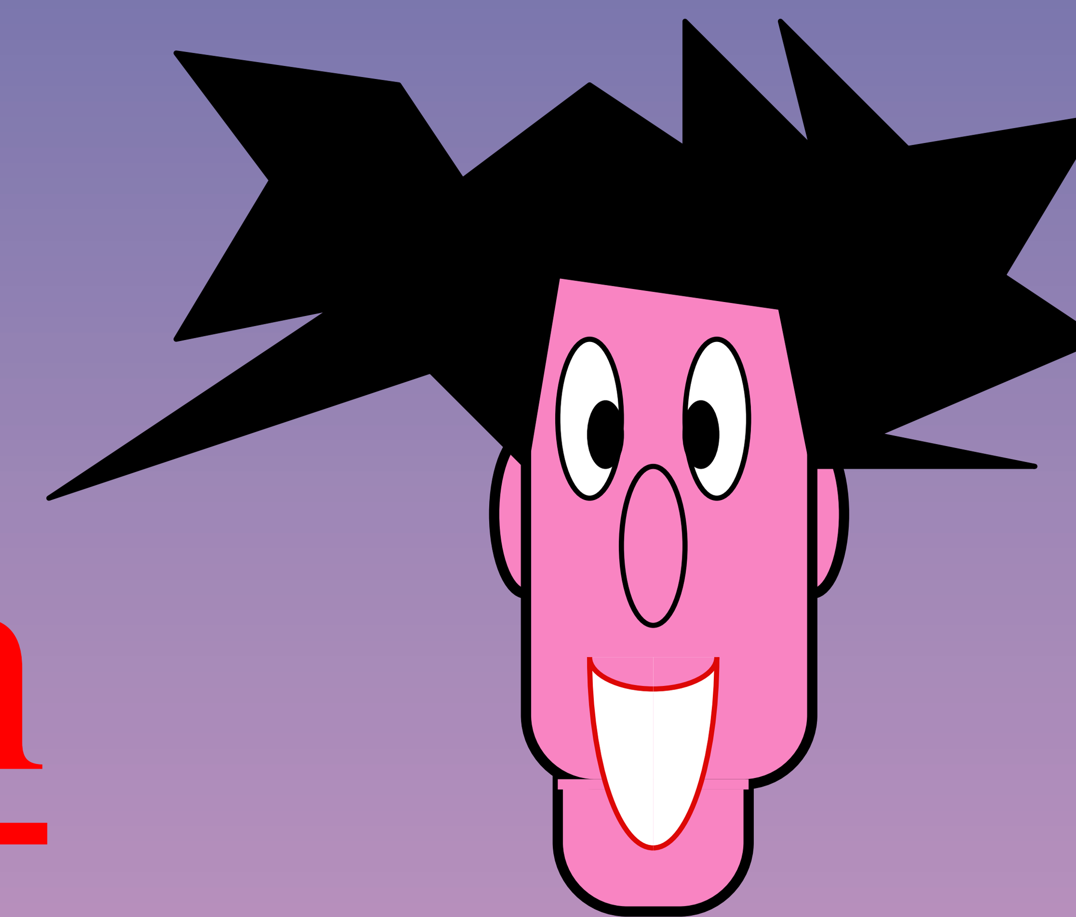
Oblivious Function Evaluation

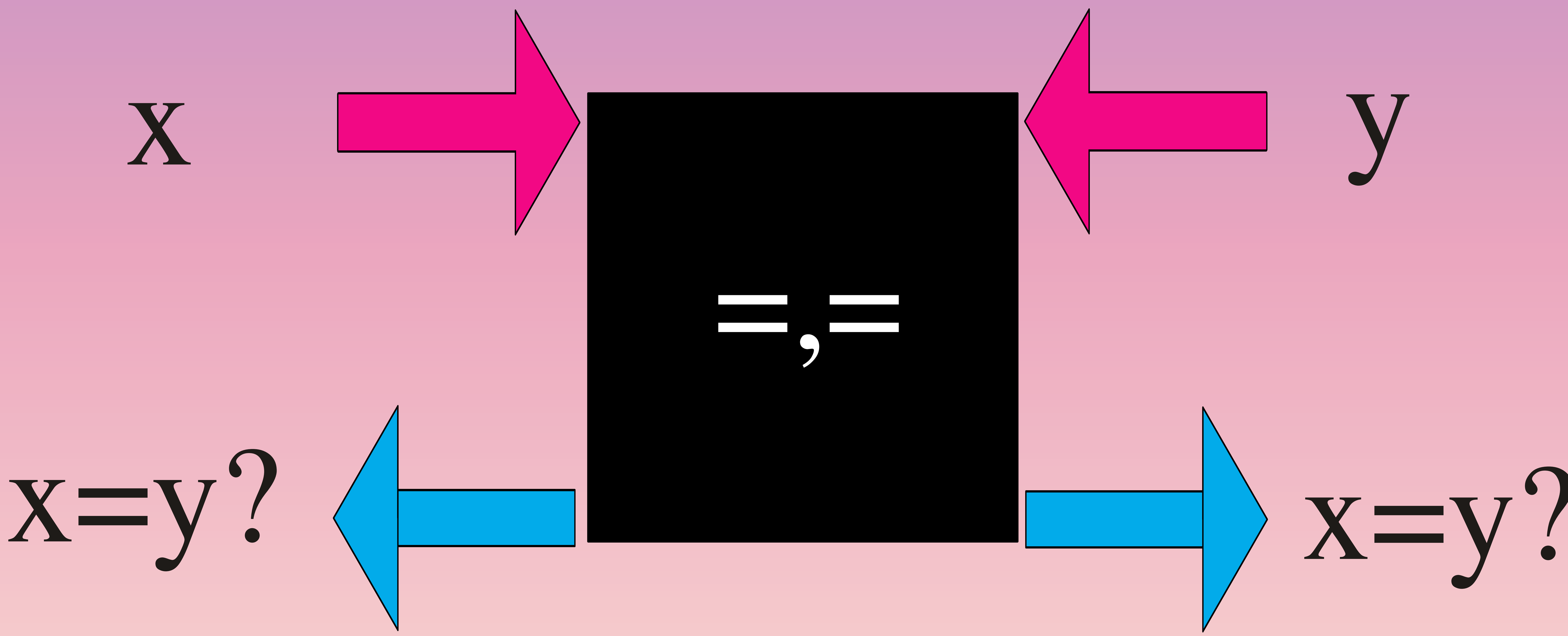




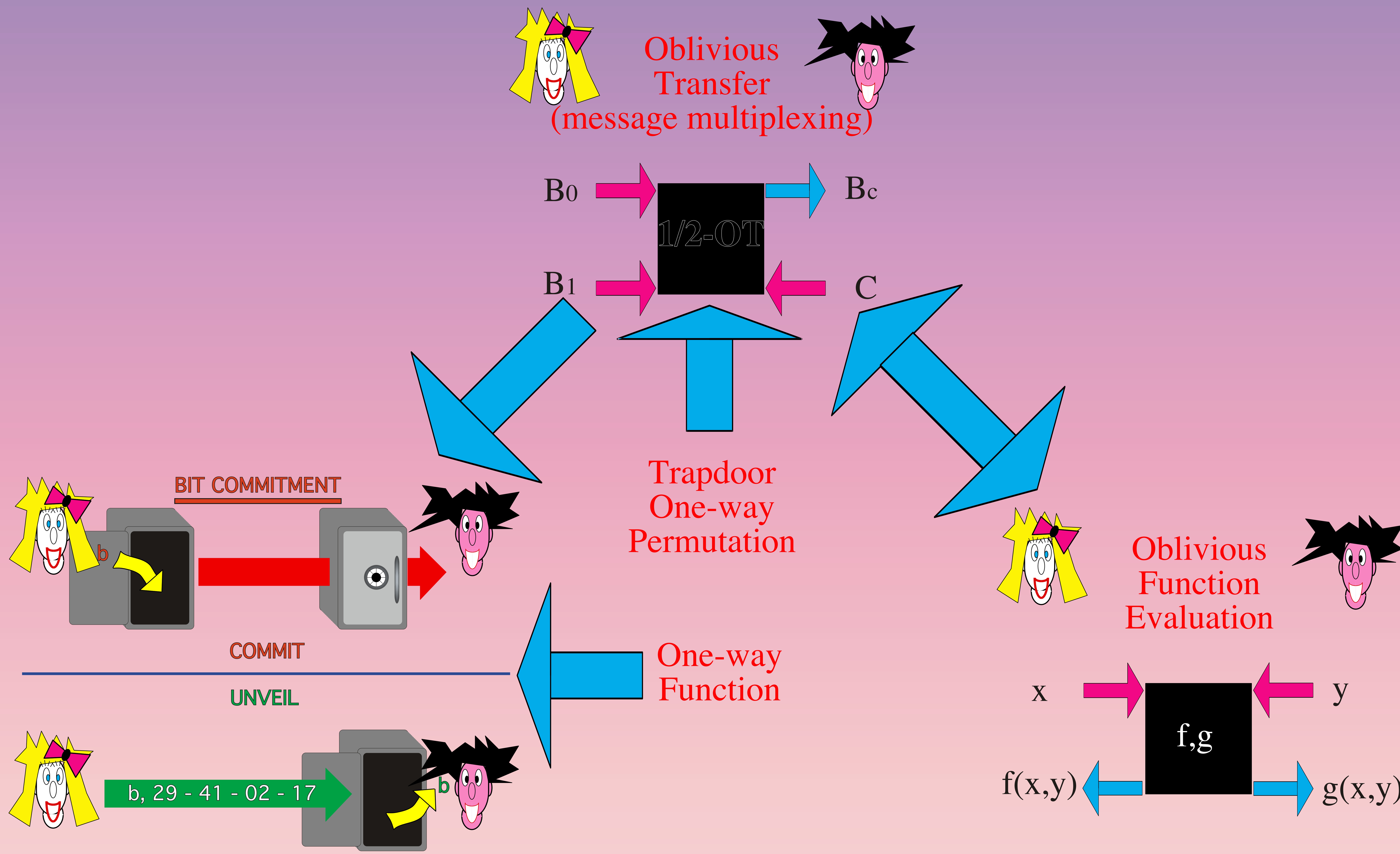


Mutual Identification

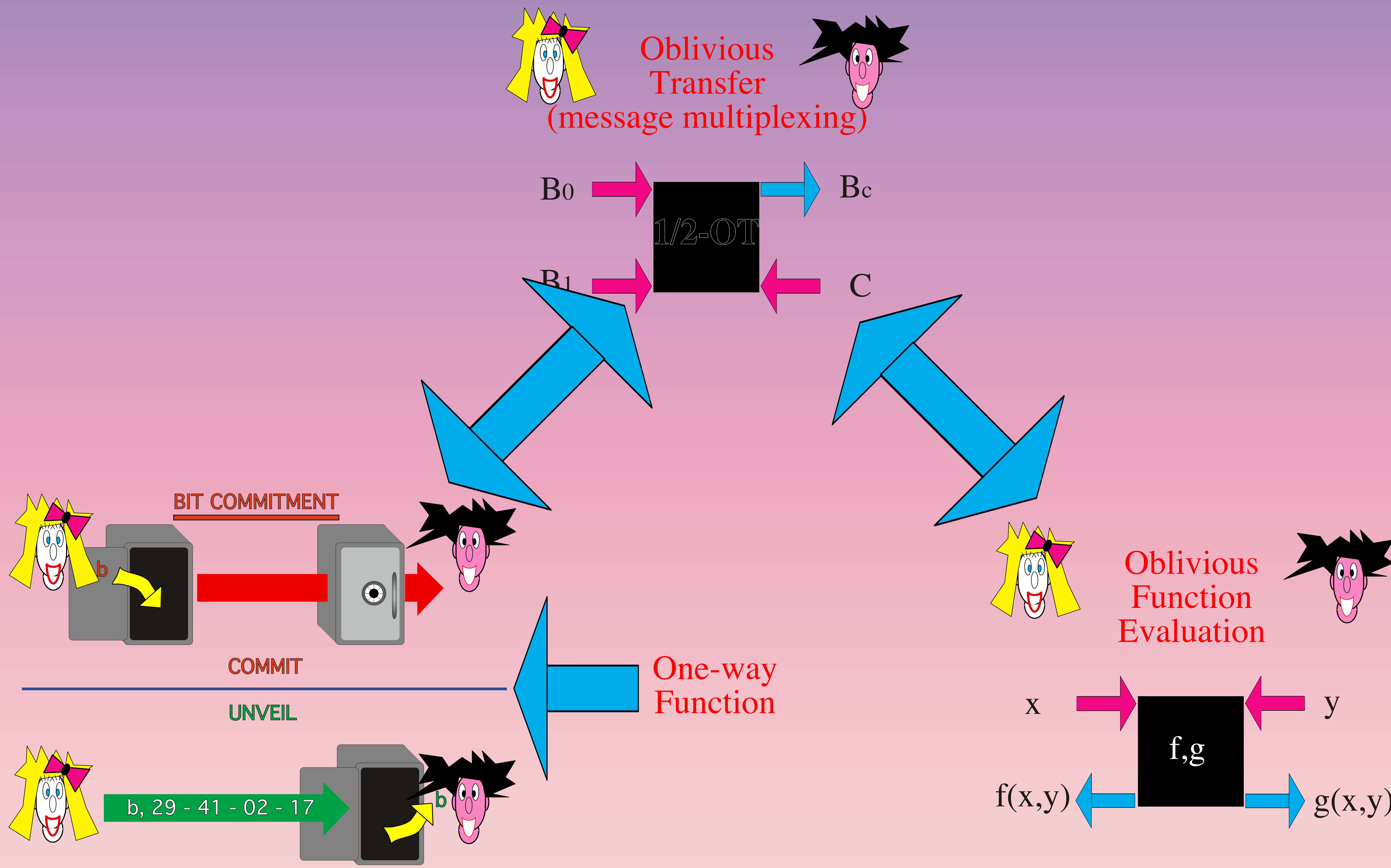




Classically

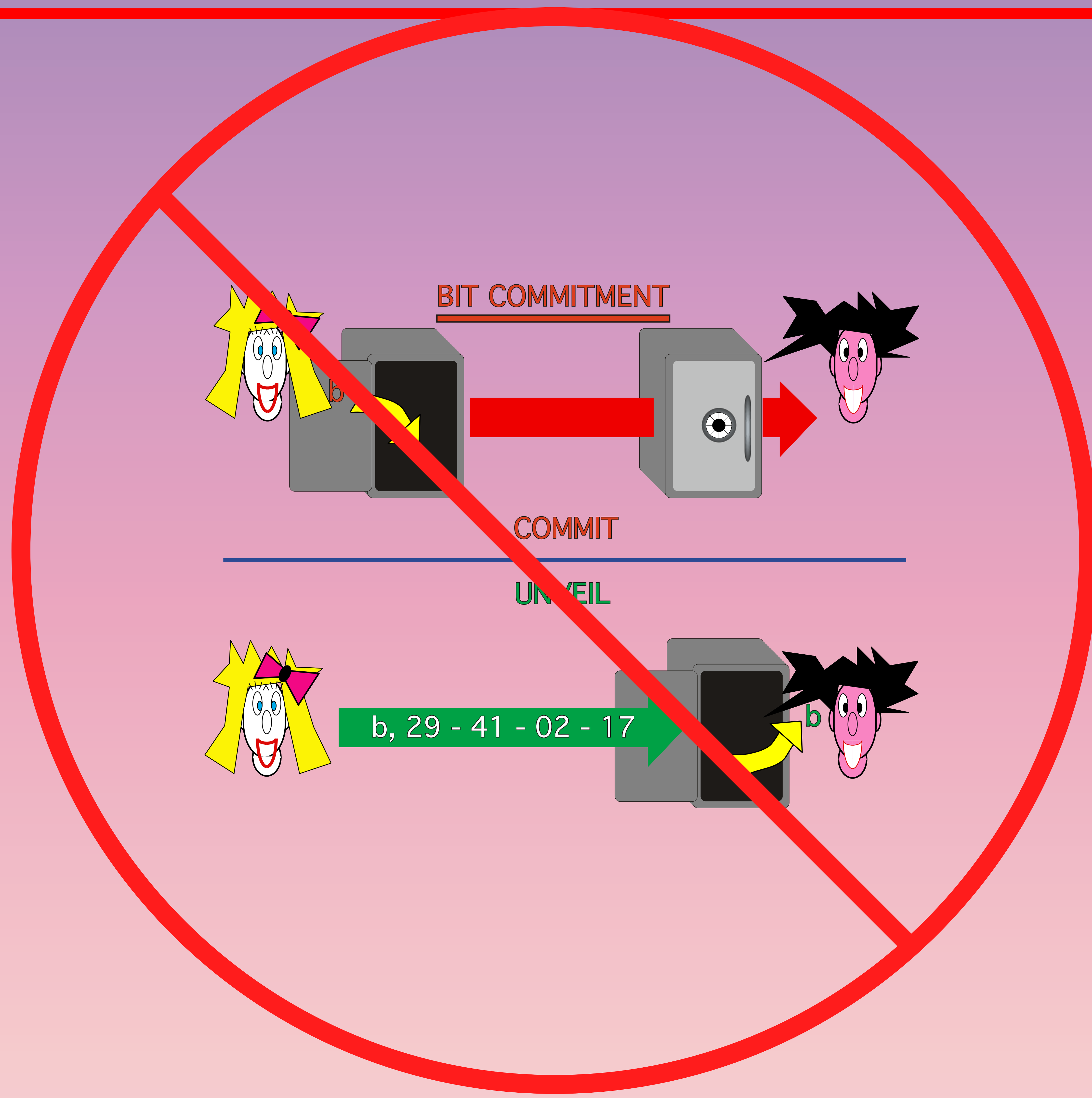


Quantumly



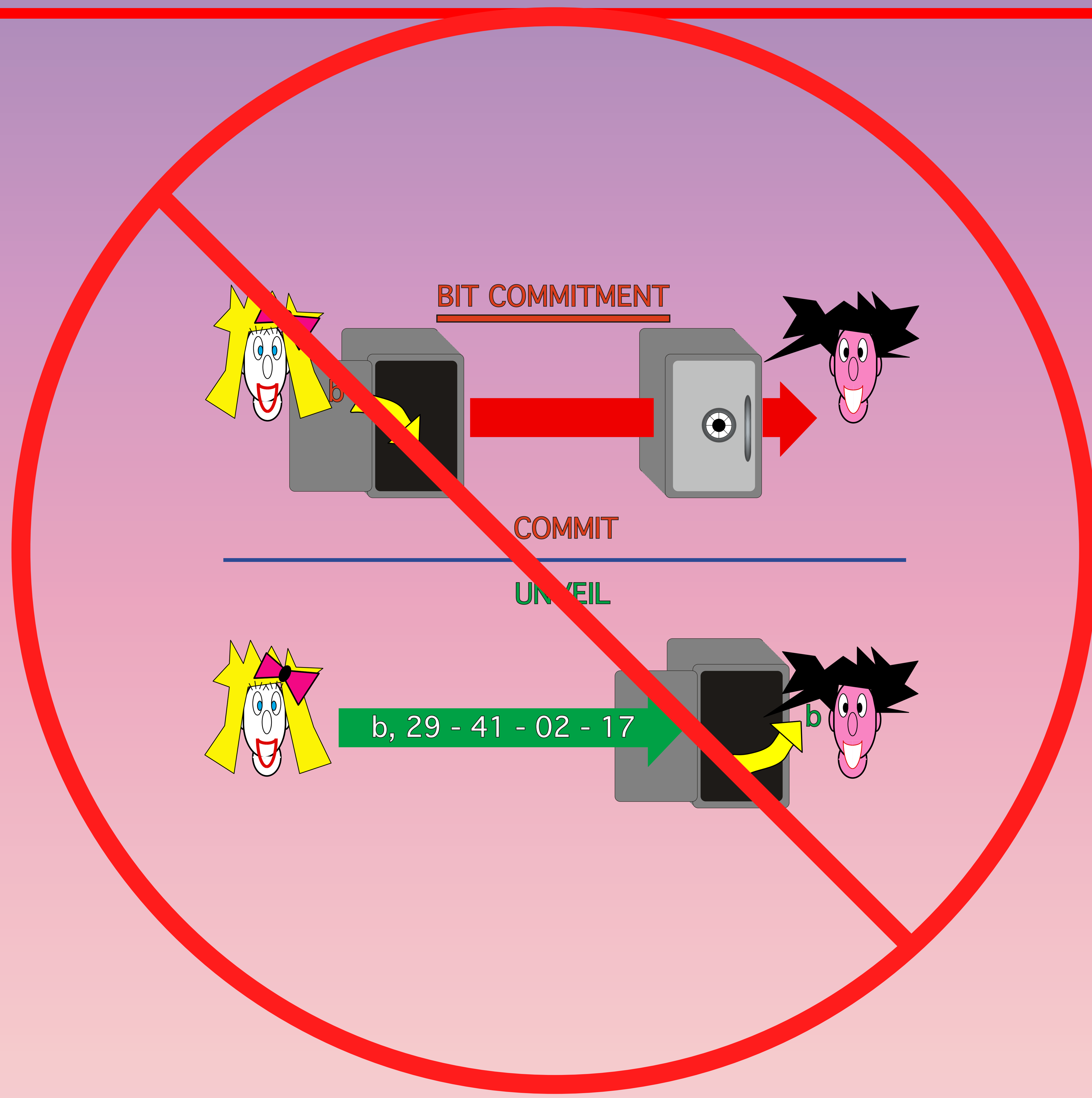
Oblivious
Transfer
(message multiplexing)
B0
B1
1/2-OT
Bc
C
BIT COMMITMENT
b
COMMIT
UNVEIL
b, 29 - 41 - 02 - 17
b
One-way
Function
Oblivious
Function
Evaluation
x
y
f,g
f(x,y)
g(x,y)

Classically (information theoretical)



Folklore

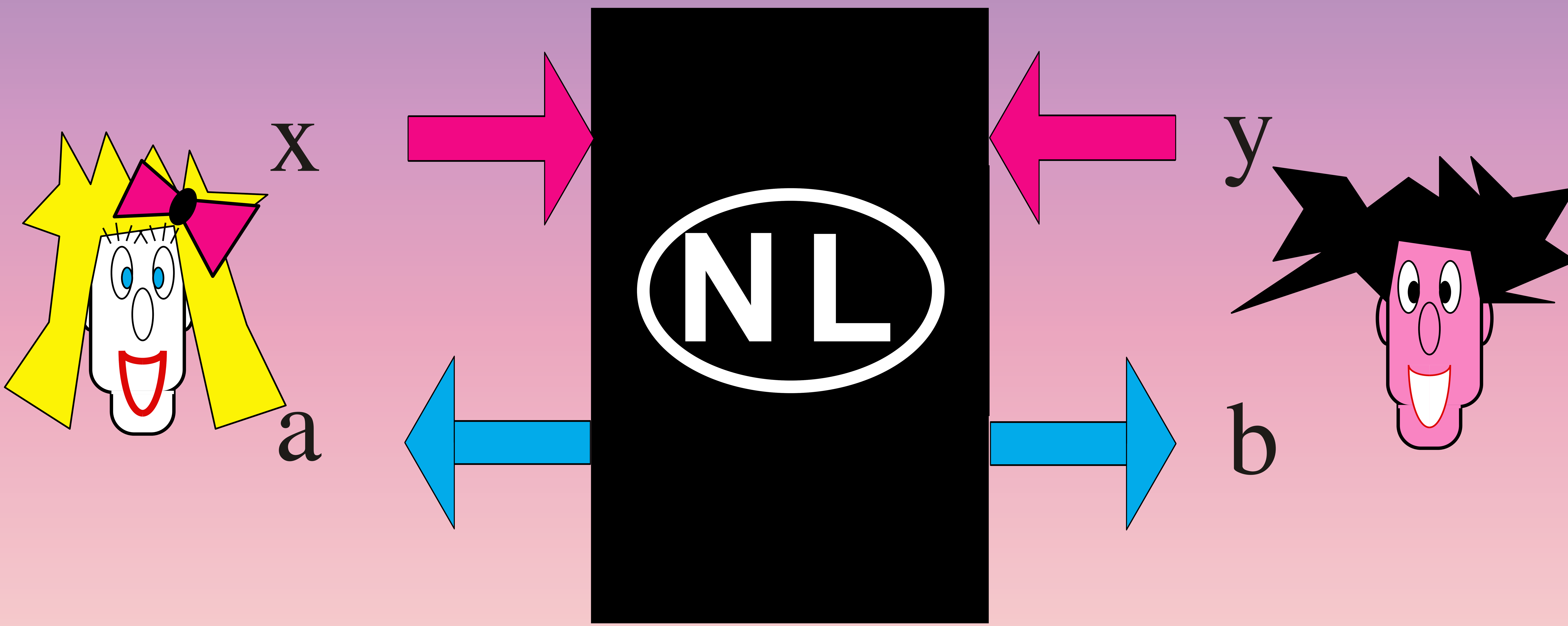
Quantumly (information theoretical)



Mayers, Lo-Chau

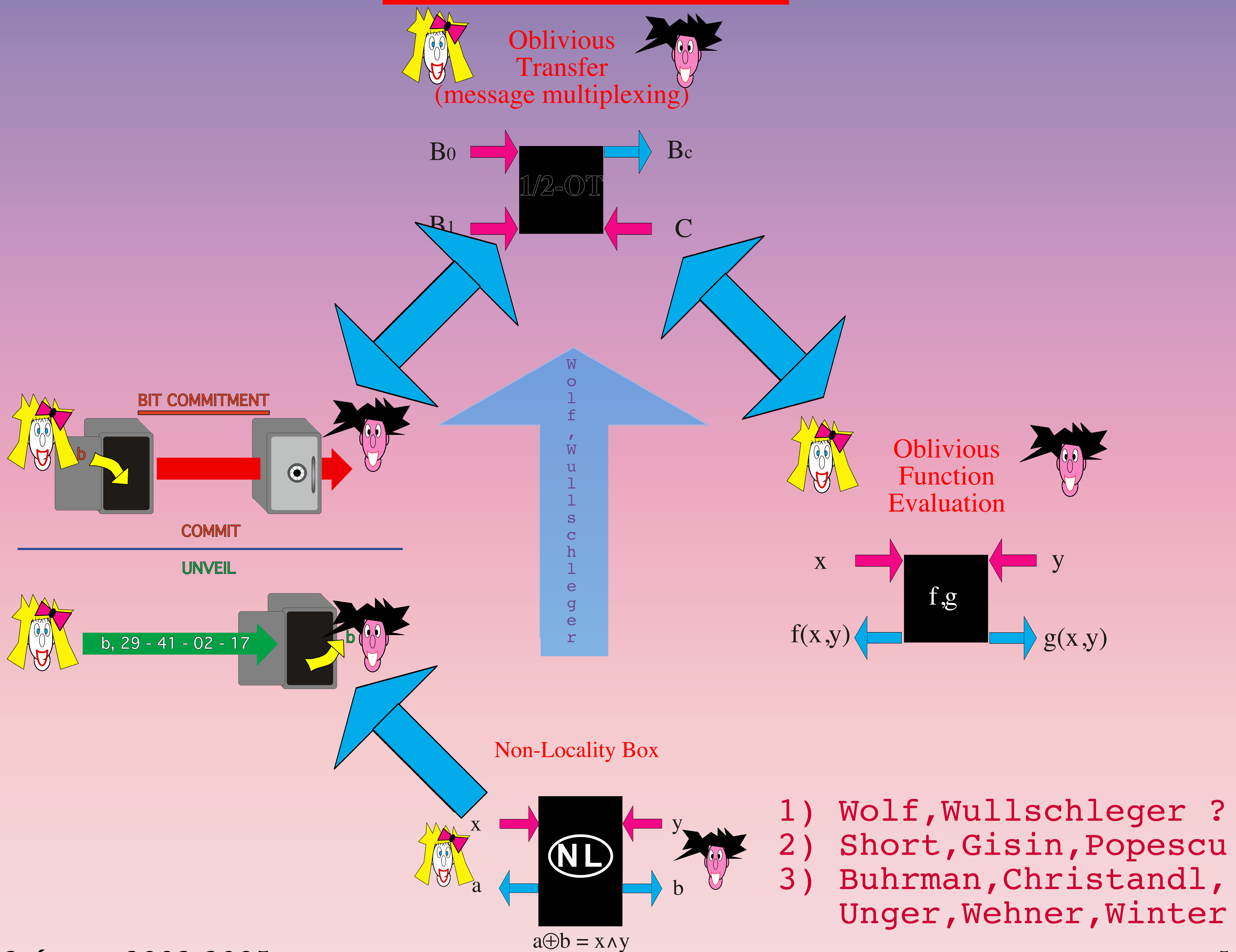
Non-Locality Box

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

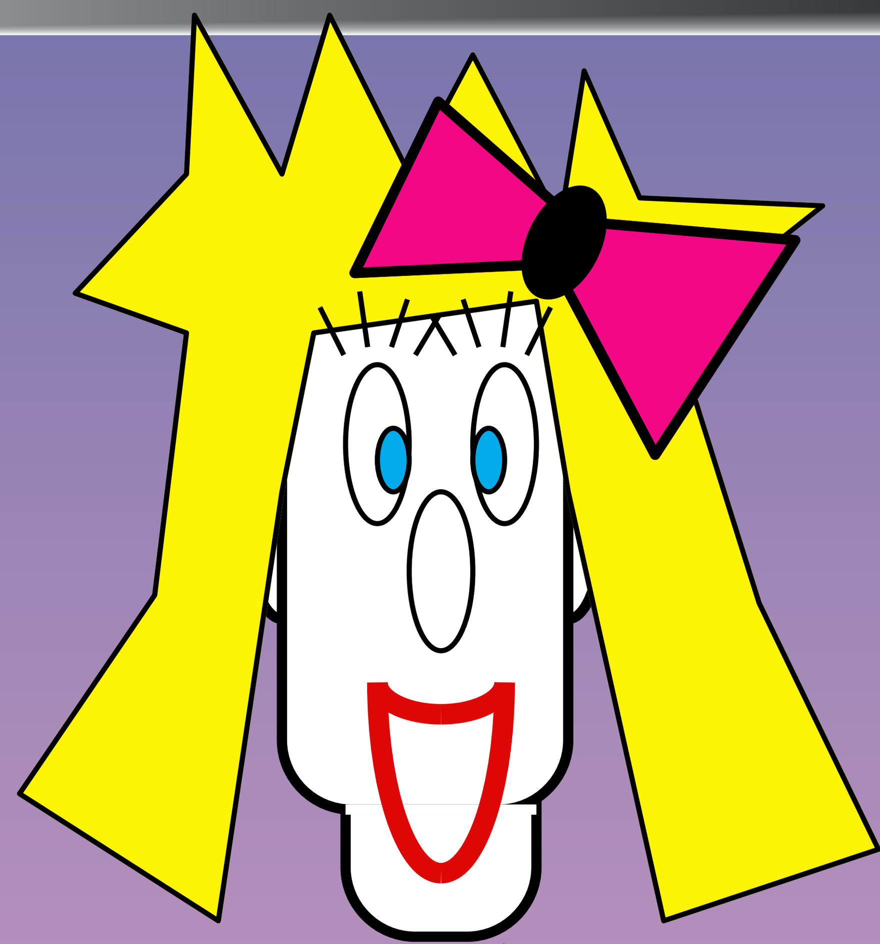


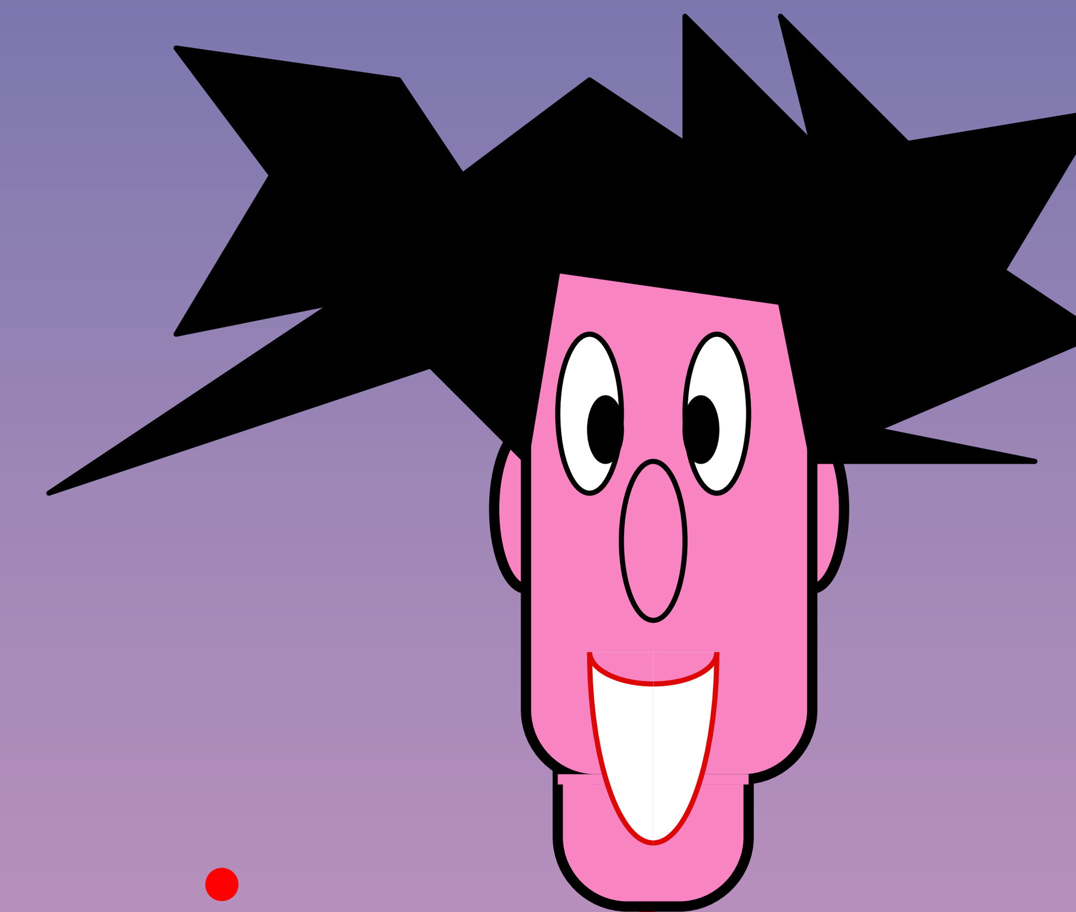
C: 3/4 Q: $\cos^2(\pi/8) \approx 85\%$

Quantumly

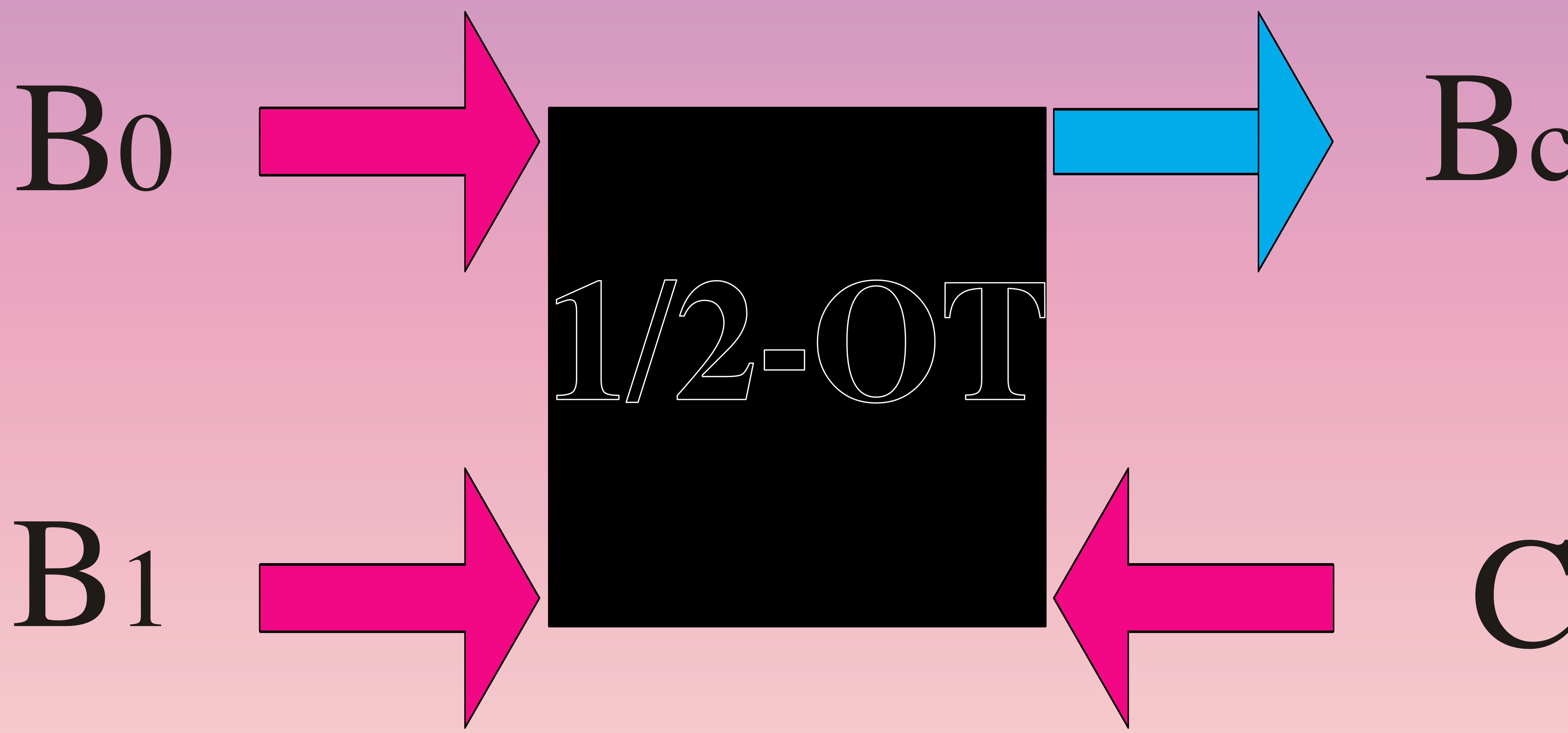

Oblivious
Transfer
(message multiplexing)
B0
Bc
1/2-OT
B1
C
BIT COMMITMENT
b
COMMIT
UNVEIL
b, 29 - 41 - 02 - 17
b
Wolf,Wullschleger
Oblivious
Function
Evaluation
x
y
f,g
f(x,y)
g(x,y)
Non-Locality Box
x
y
NL
a
b
a⊕b = x∧y
1) Wolf,Wullschleger ?
2) Short,Gisin,Popescu
3) Buhrman,Christandl,
Unger,Wehner,Winter

(5) Quantum Oblivious Transfer

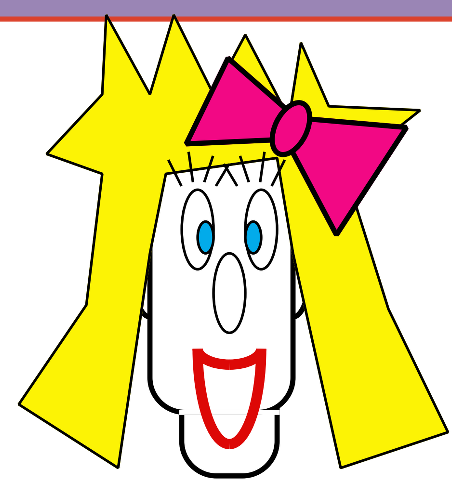




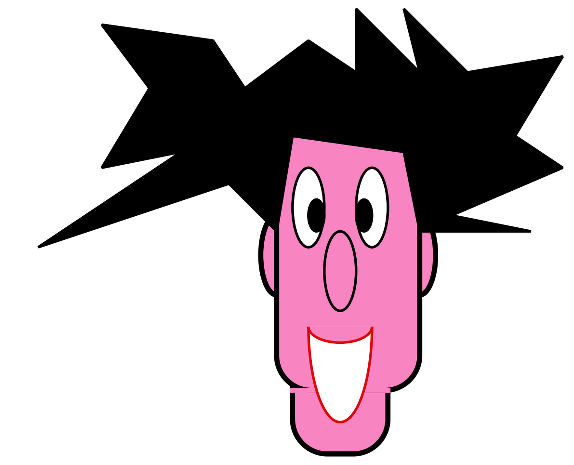
Oblivious Transfer (message multiplexing)



Q-OT



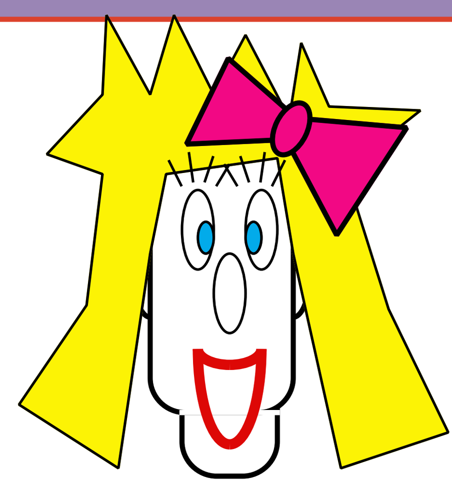
b_0 b_1



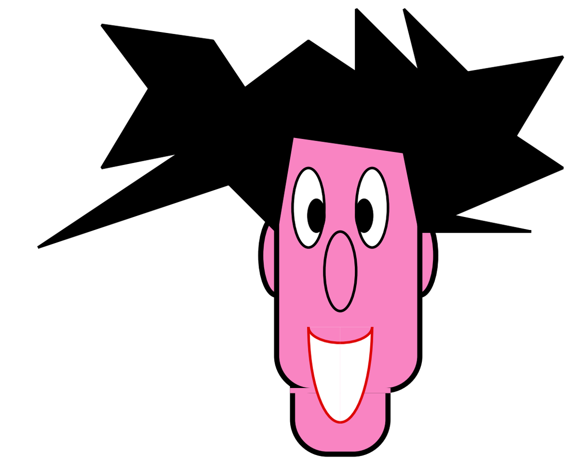
A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	×	×	+	+	×	+	+	+	×	+	+	×	×	×	+	×	×	×	+	+	×	+	×	+
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0
A:	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	0	👎	👎	0	👎	1	👎	👎	1	👎	0	👎	👎	👎	👎	1	0	👎	👎	1	👎	0	0	0
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	1	0	0	0	1	0	1
										⊕					⊕									
A:										b_0					b_1									
										⊕					⊕									
B:								b_0	=	0					👎	=	👎							

Crépeau-Kilian

Q-OT

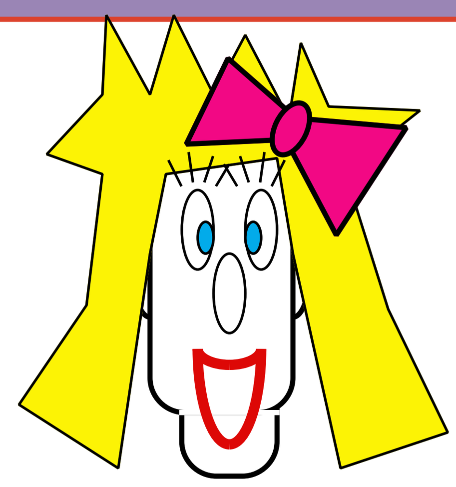
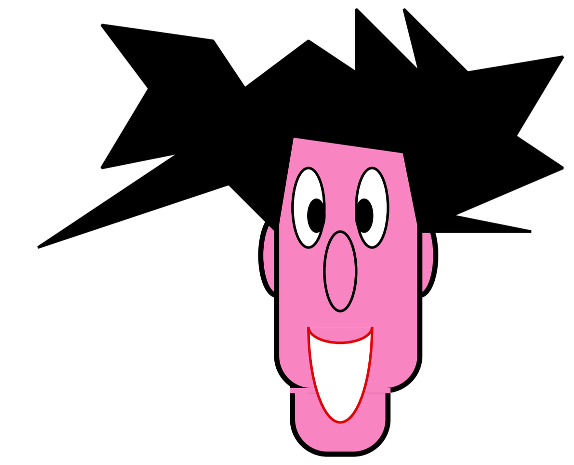


b_0 b_1



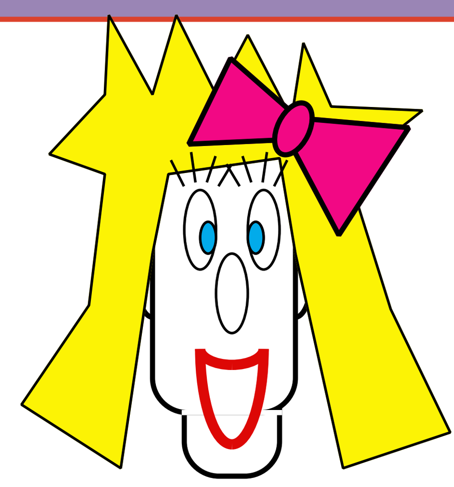
A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+

Q-OT

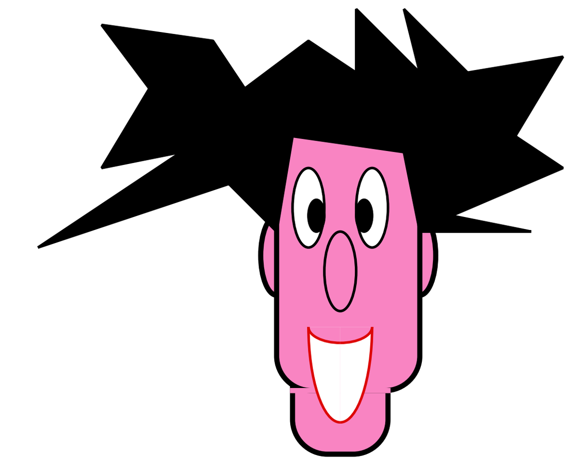
 b_0 b_1 

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

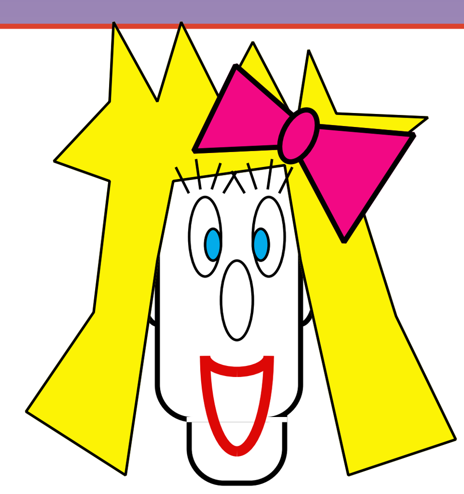


b_0 b_1

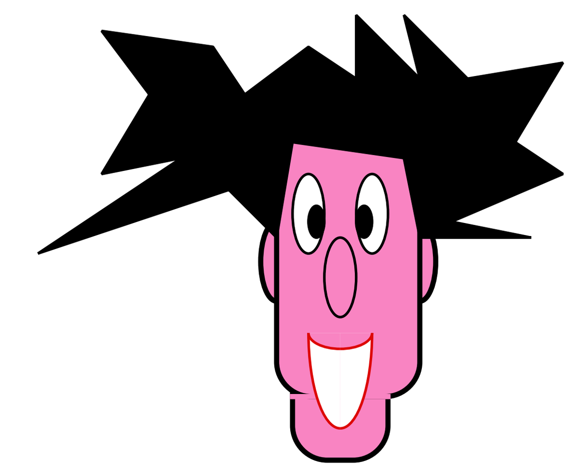


A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	×	×	+	+	×	+	+	+	×	+	+	×	×	×	+	×	×	×	+	+	×	+	×	+
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0
A:	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+

Q-OT

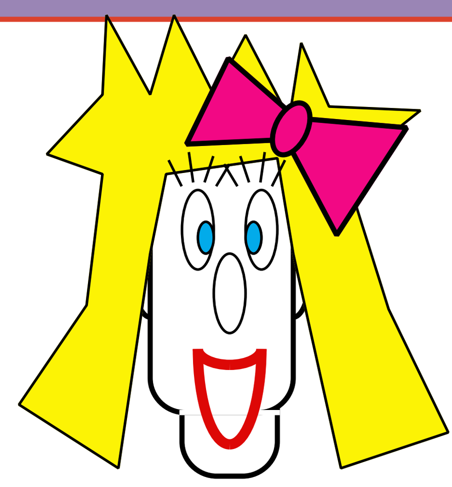


b_0 b_1

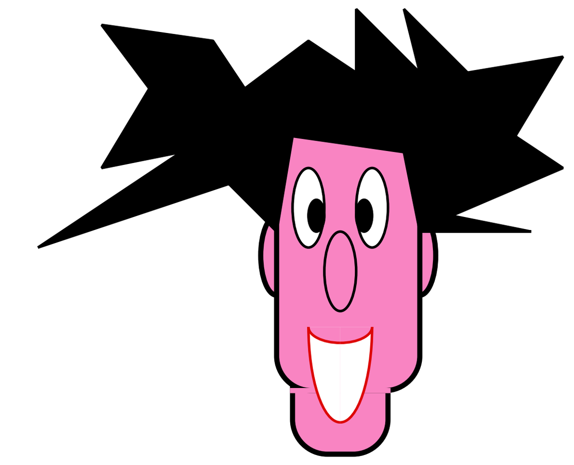


B:	×	×	+	+	×	+	+	+	×	+	+	×	×	×	+	×	×	×	+	+	×	+	×	+
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0
A:	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	0			0		1			1		0					1	0			1		0	0	0

Q-OT

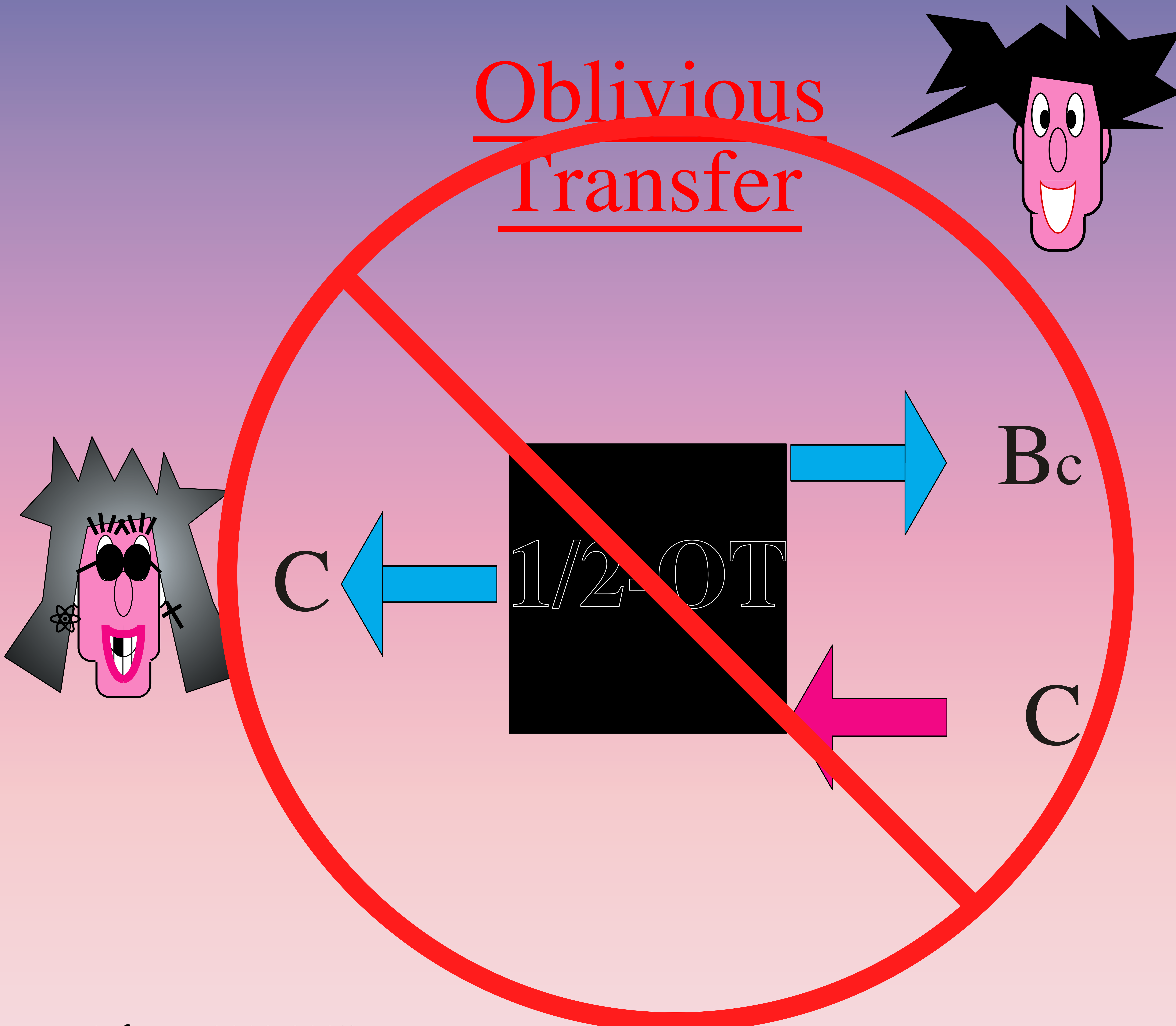


b_0 b_1

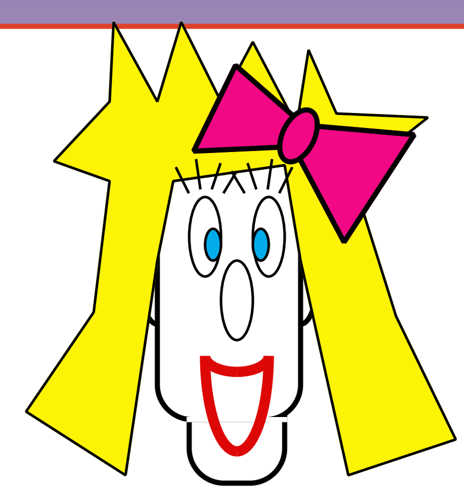


A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
B:	0			0		1			1		0					1	0			1		0	0	0
B:	0	0	1	1	0	1	0	1	0	0	0													
A:	0	0	1	1	0	1	0	1	0	0	0	1	1	0	0	0	1	1	0	0	0	1	0	1

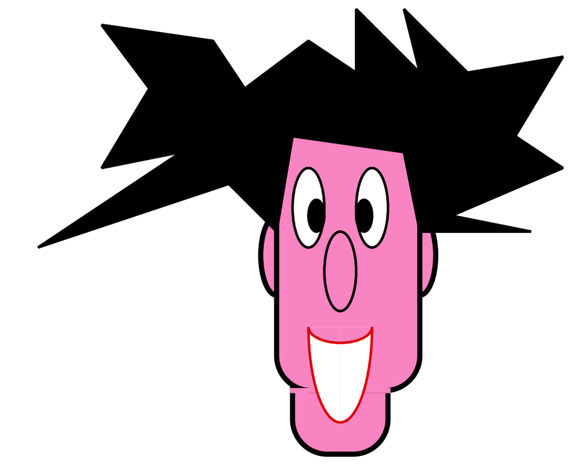
Oblivious Transfer



Q-OT



b_0 b_1



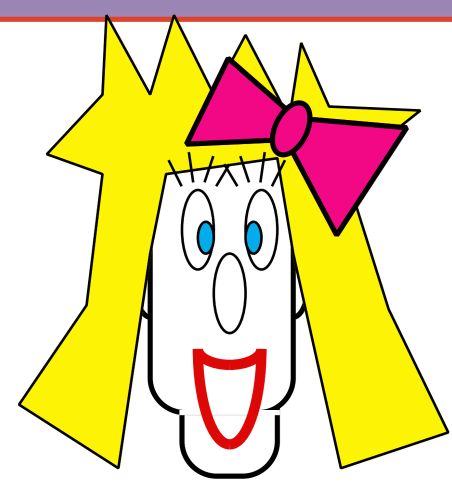
B: 0 0 1 1 0 1 0 1 0 0 0

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

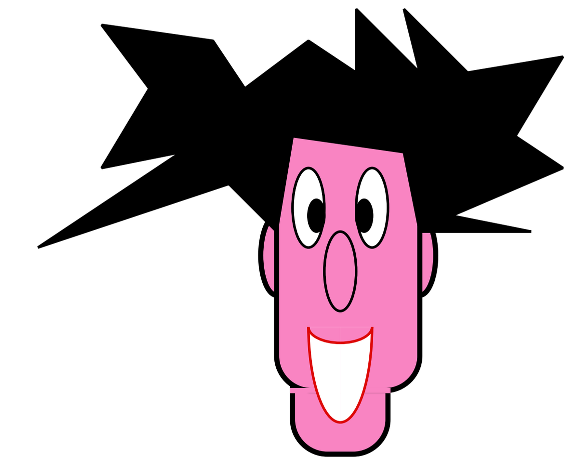
B: 0 0 1 1 0 1 0 1 = 0 =

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

Q-OT



b_0 b_1



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

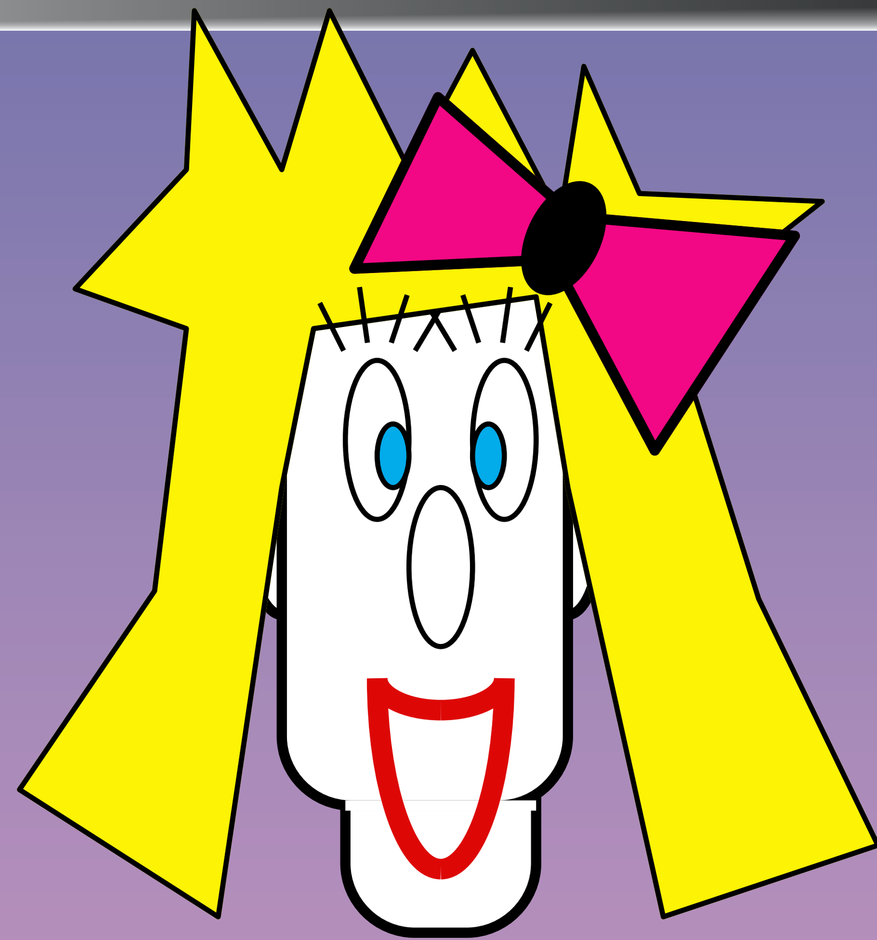
A: 0 0 1 1 0 1 0 1 = 0 0 = 1 1 0 0 0 1 0 1

$\oplus$ $\oplus$

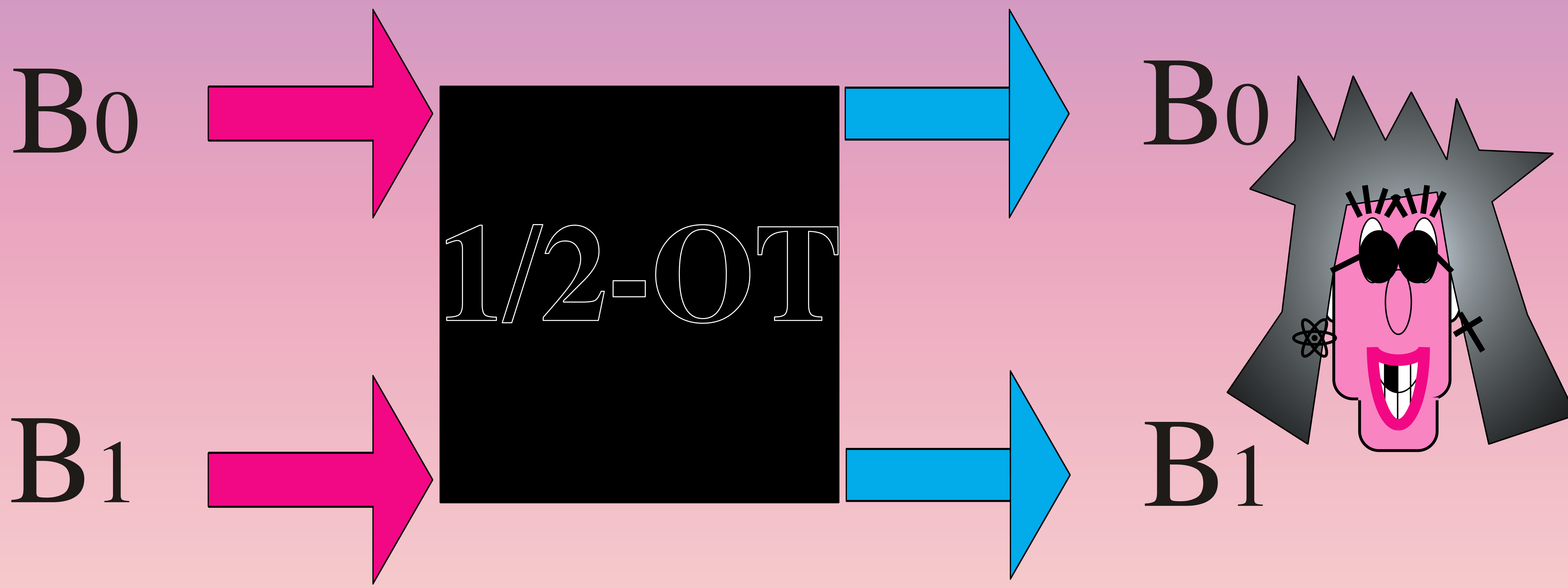
A: b_0 b_1

$\oplus$ $\oplus$

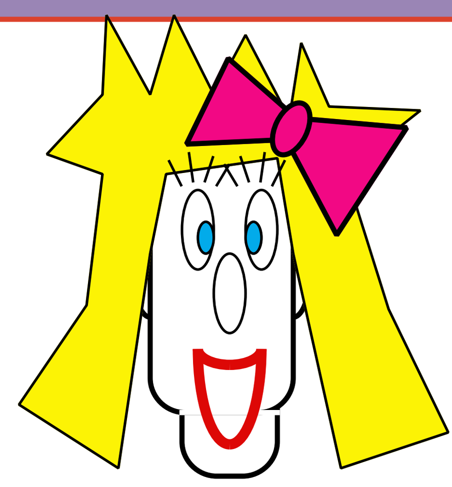
B: b_0 = 0 =



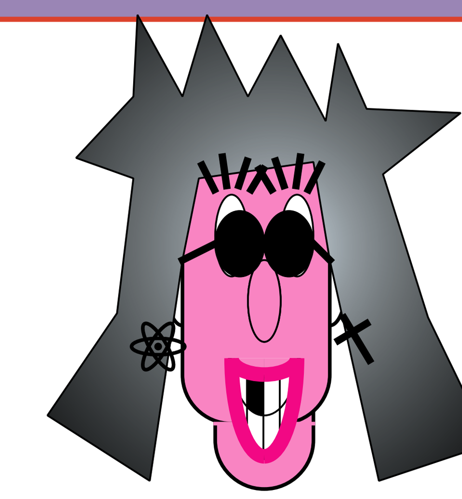
Oblivious Transfer



Q-OT



b_0 b_1



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: × + × + + + × × × × + + + + × × × + × + + + × +

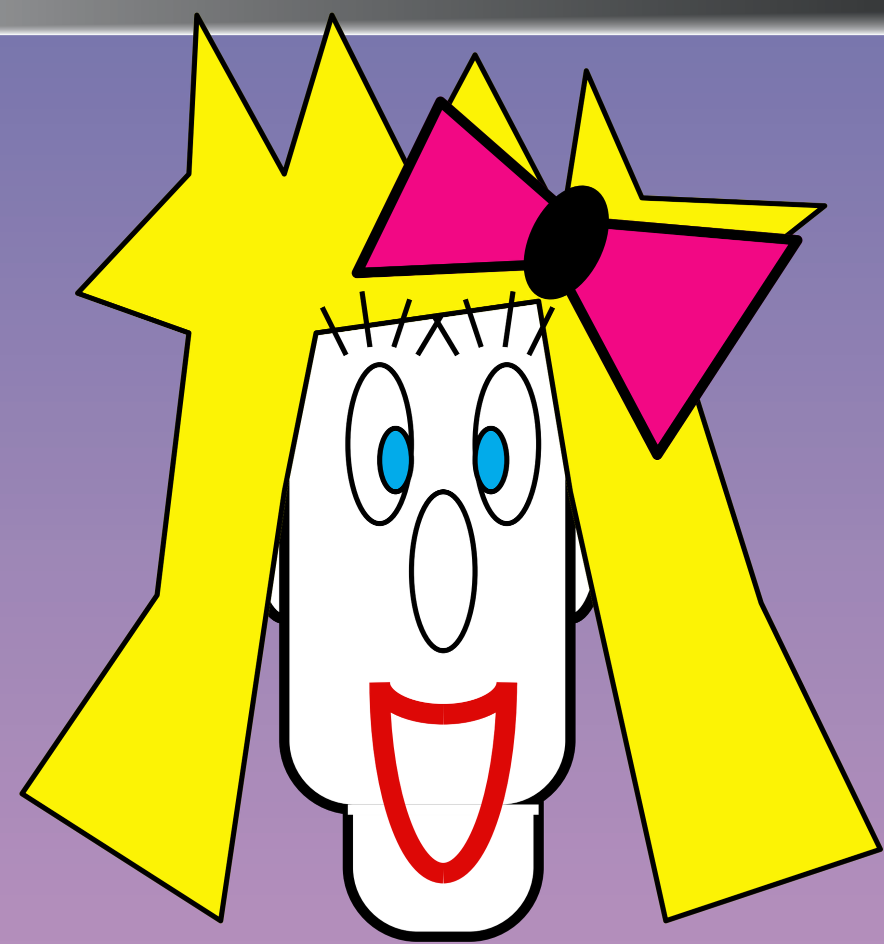
B: × + × + + + × × × × + + + + × × × + × + × + × +
0 1 1 0 0 1 0 0 1 1 0 1 0 0 0 1 1 1 0 1 1 0 0 0

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

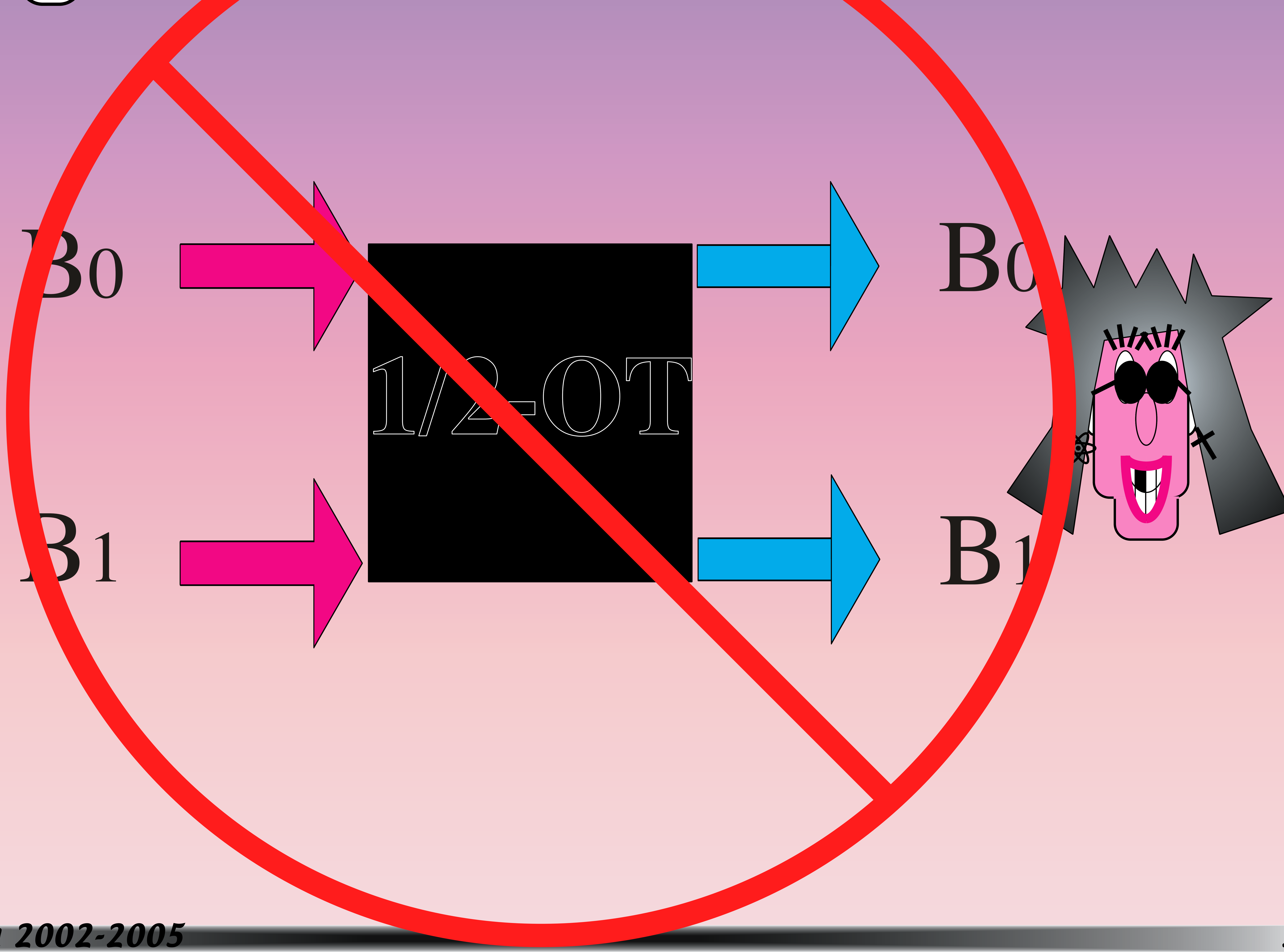
A: 0 0 1 1 0 1 0 1 = 0   0 = 1 1 0 0 0 1 0 1

A: $\oplus\, b_0\, \oplus$ $\oplus\, b_1\, \oplus$

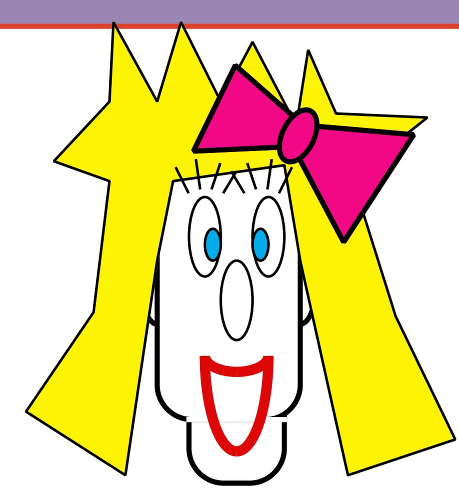
B: b_0 = 0   0 = b_1



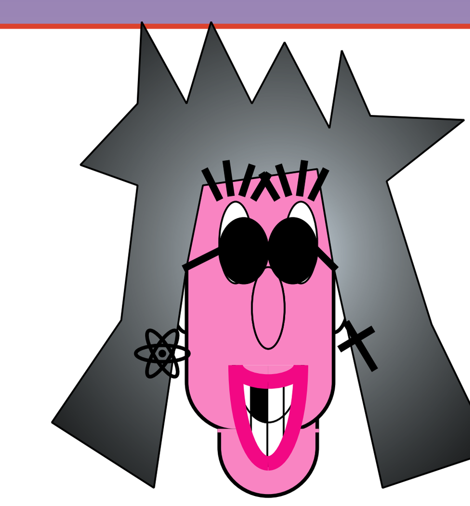
Oblivious Transfer

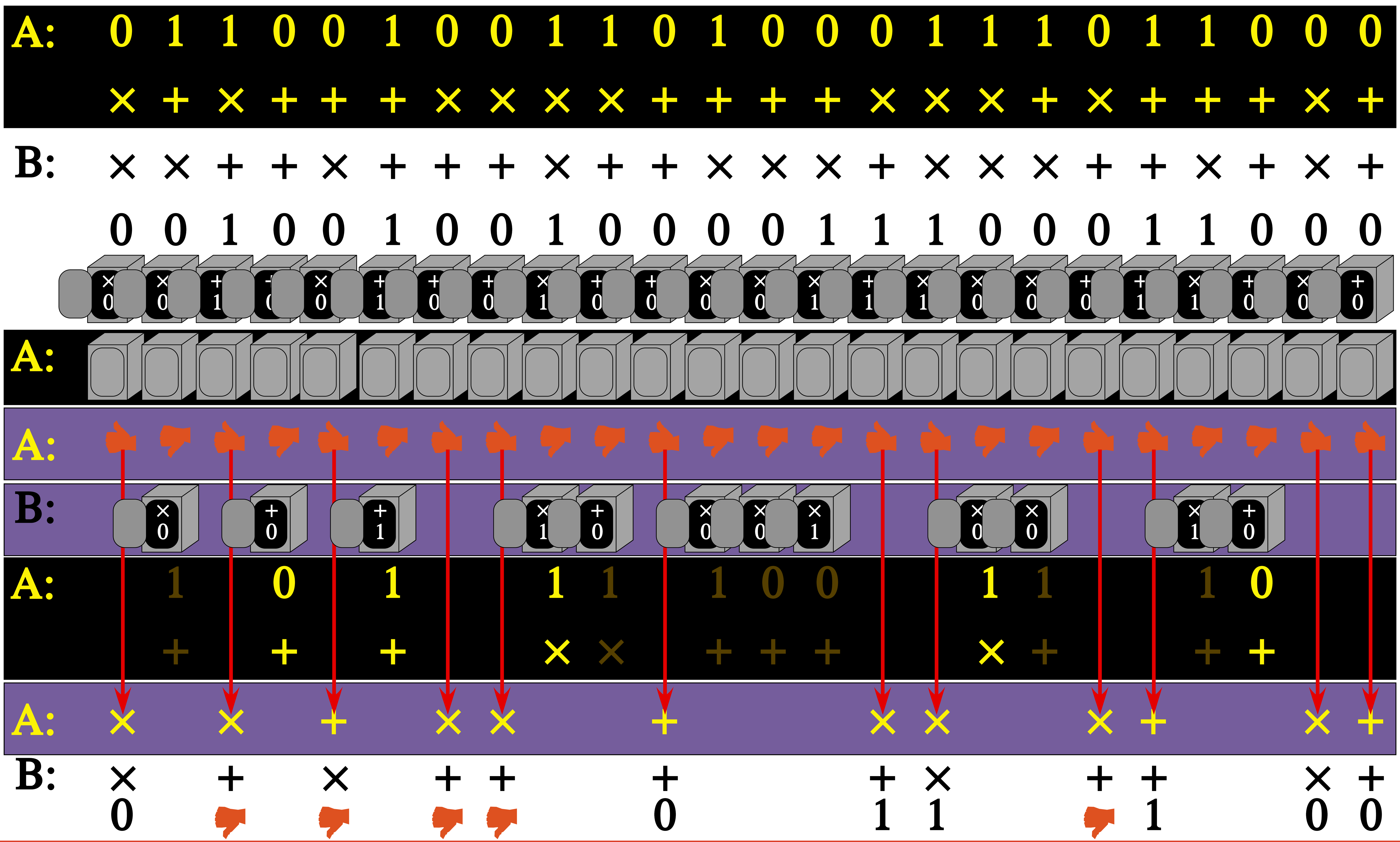


Q-OT from Q-BC

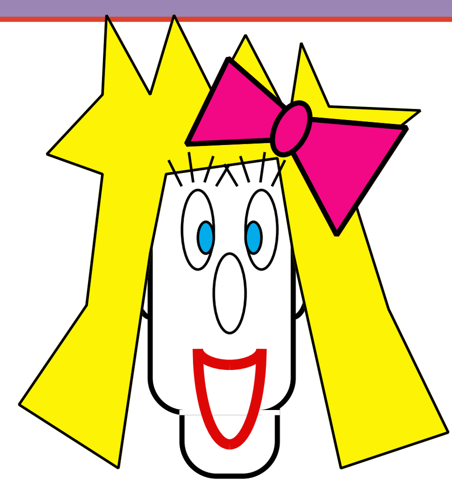


b_0 b_1



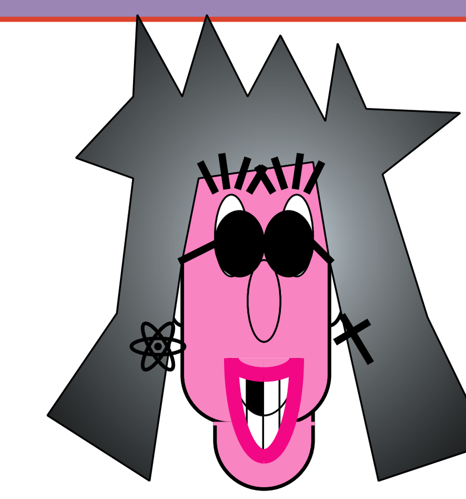


Q-OT



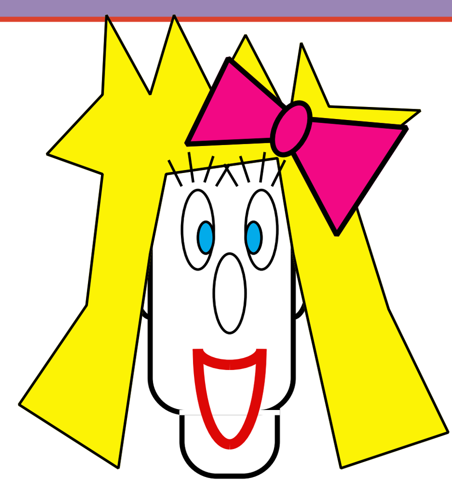
b_0 b_1

from Q-BC

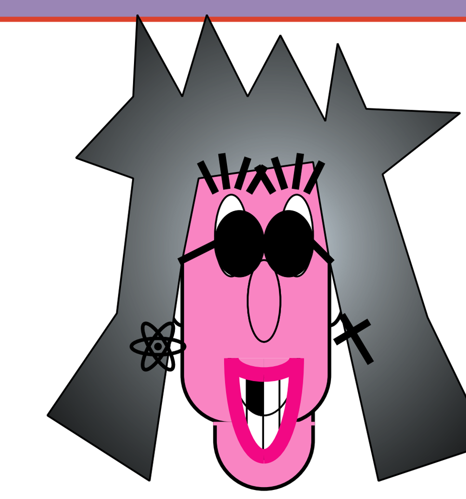


A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	×	×	+	+	×	+	+	+	×	+	+	×	×	×	+	×	×	×	+	+	×	+	×	+
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0

Q-OT
from Q-BC

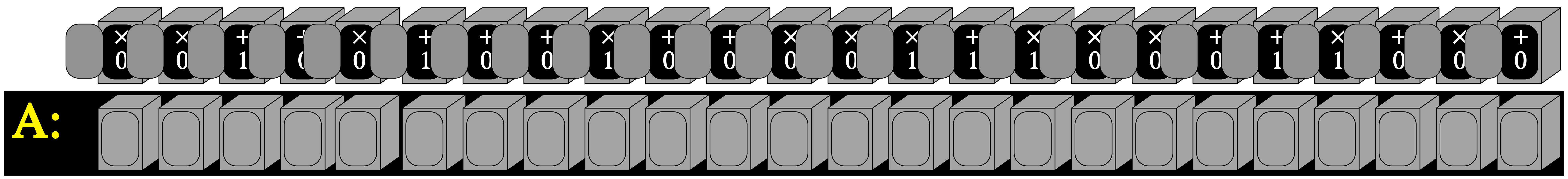


b_0 b_1

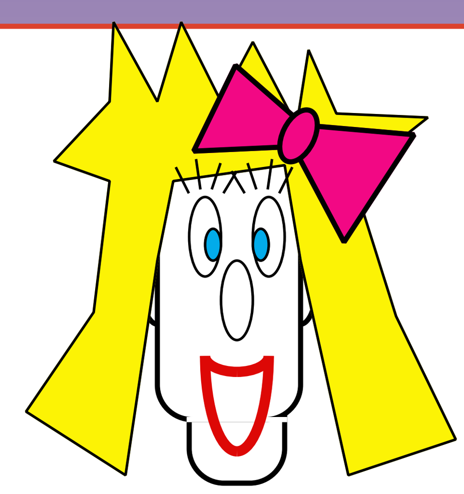


B: × × + + × + + + × + + × × × + × × × + + × + × +

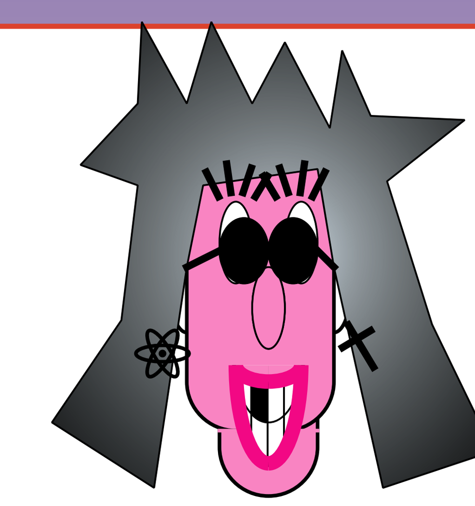
0 0 1 0 0 1 0 0 1 0 0 0 0 1 1 1 0 0 0 1 1 0 0 0

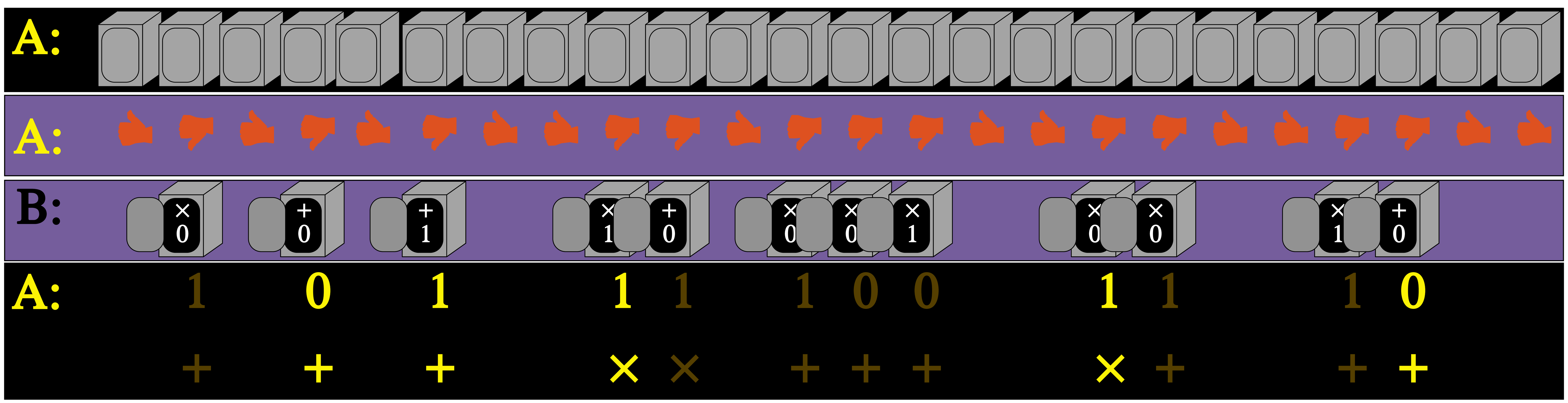


Q-OT from Q-BC

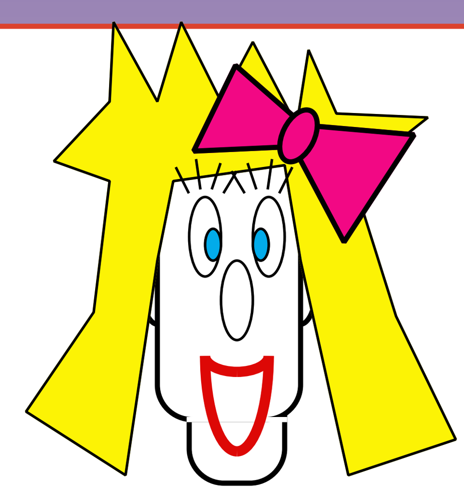


b_0 b_1

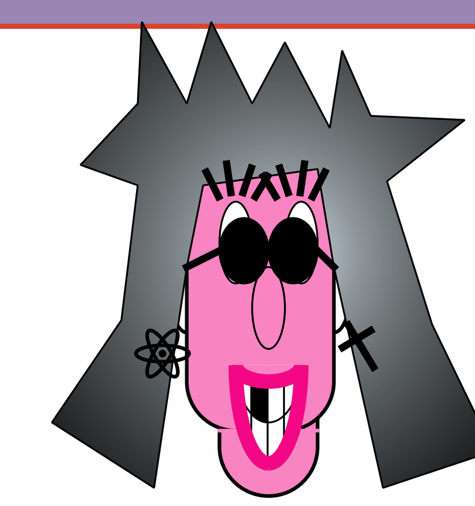


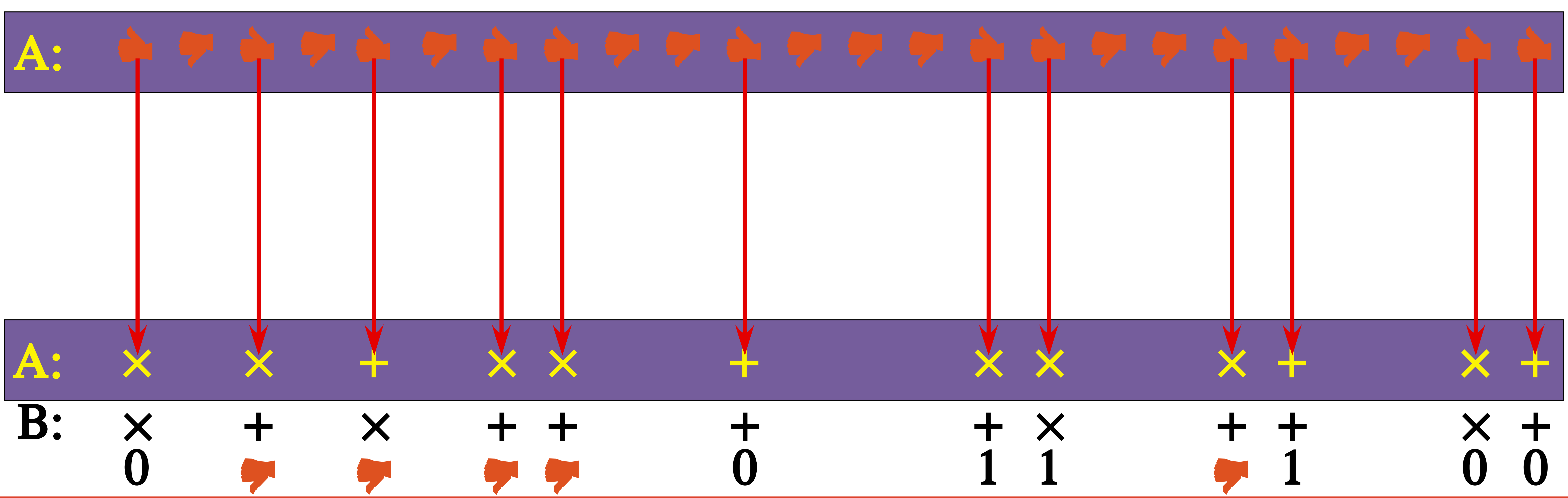


Q-OT from Q-BC

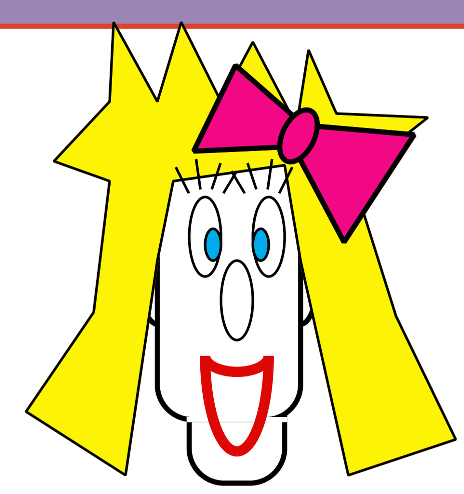


b_0 b_1

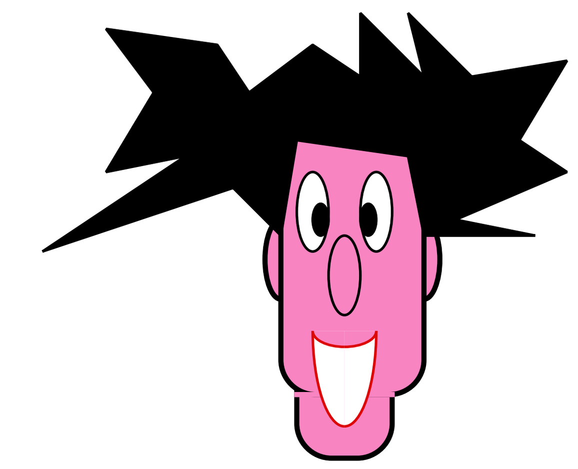




Q-OT



b_0 b_1



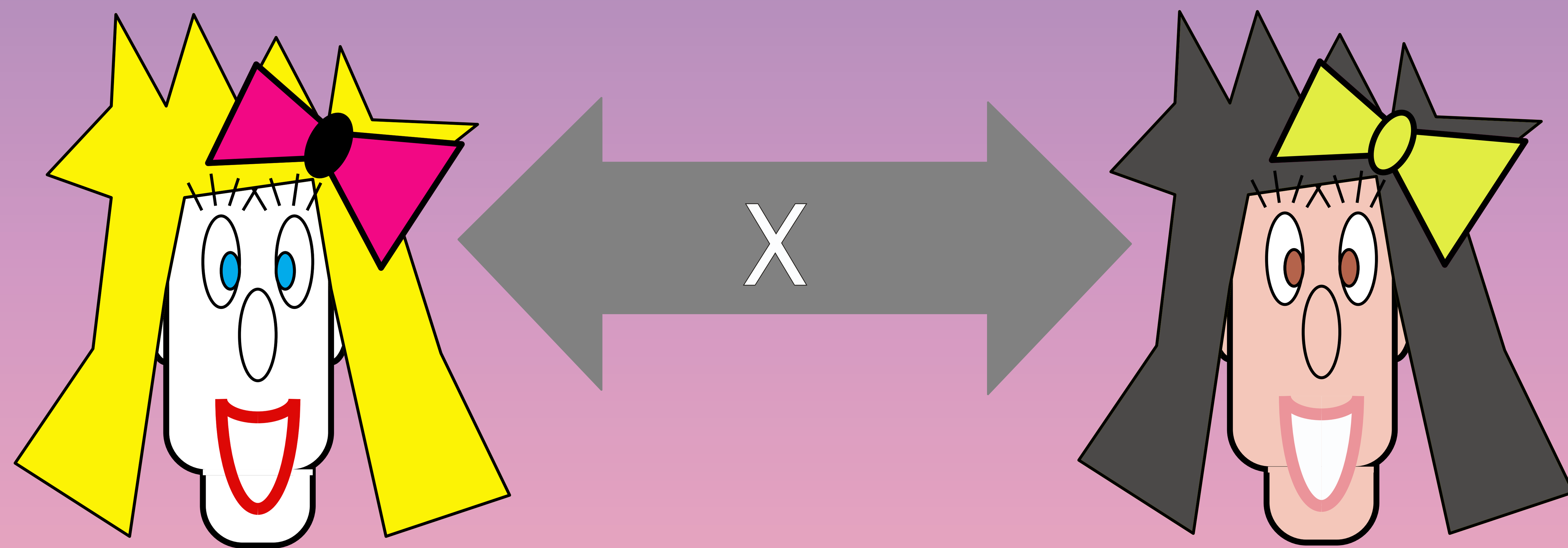
A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	×	×	+	+	×	+	+	+	×	+	+	×	×	×	+	×	×	×	+	+	×	+	×	+
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0
A:	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	0			0		1			1		0					1	0			1		0	0	0

(6)
two provers
Cryptographic Protocols

Classically

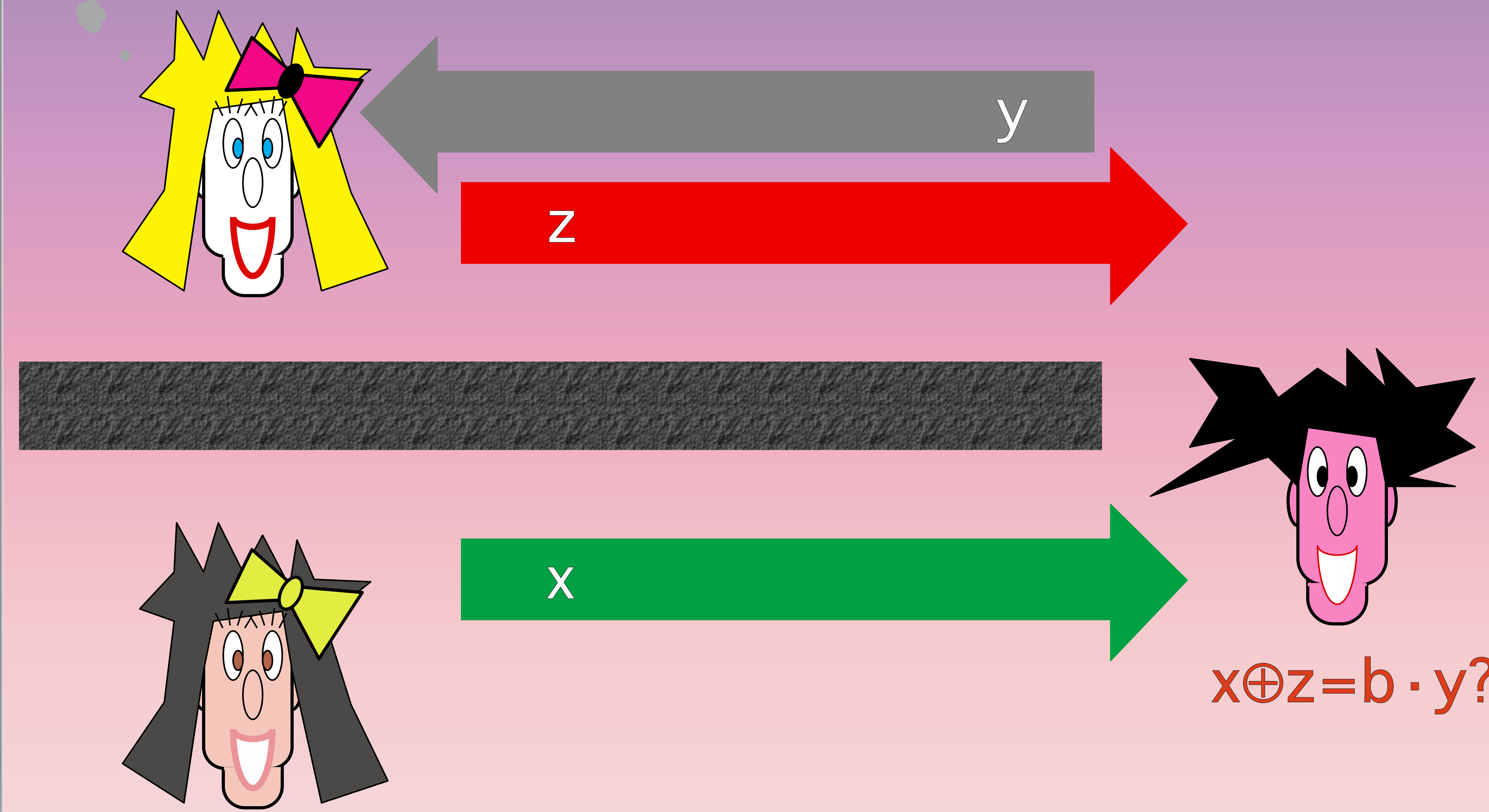
BGKW88

Classically



Ben-Or, Goldwasser, Kilian, Wigderson

$$z = x \quad \text{if } b = 0$$
$$z = x \oplus y \quad \text{if } b = 1$$



Ben-Or, Goldwasser, Kilian, Wigderson

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

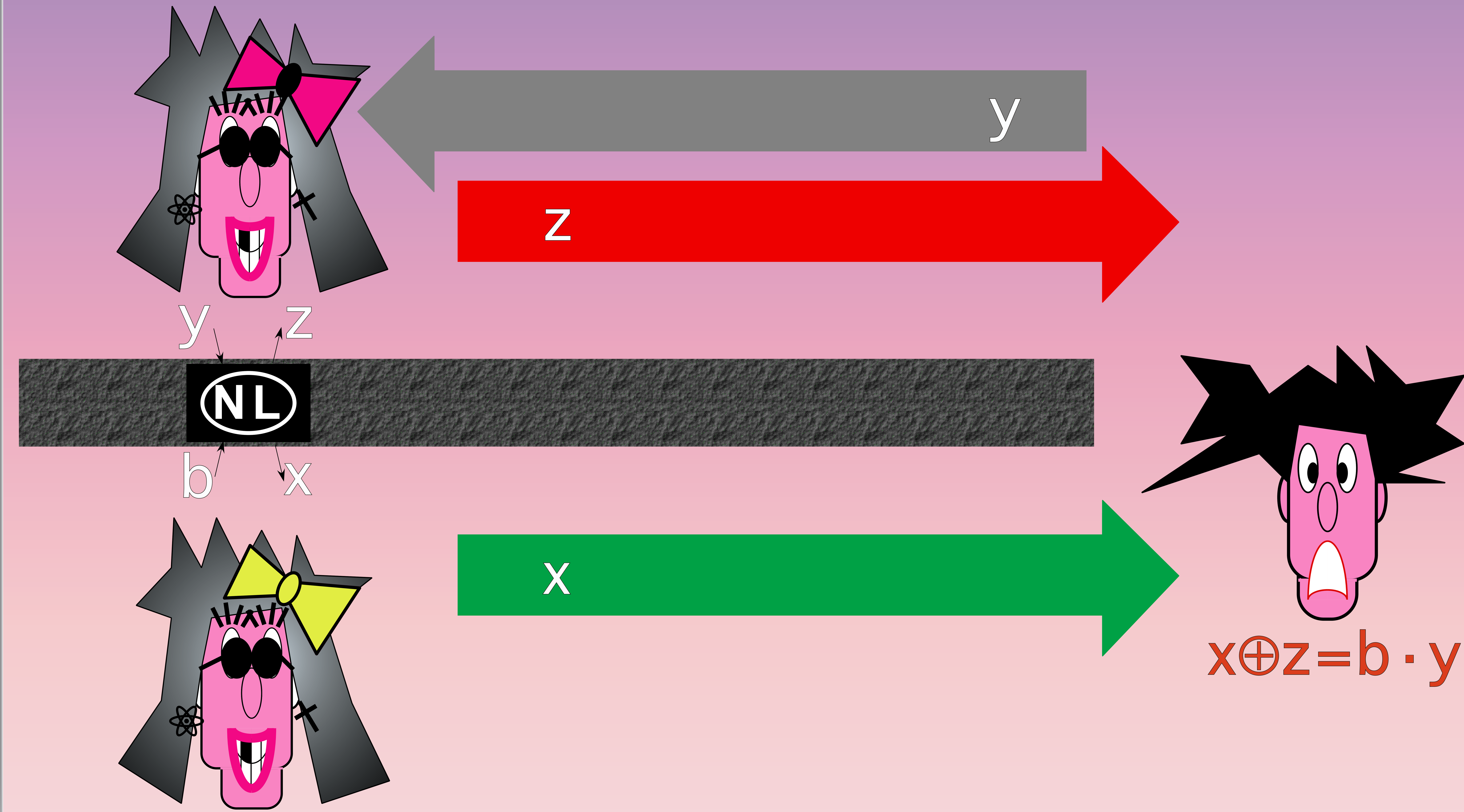
$x_1 \oplus z = 1 \cdot y = y$

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

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

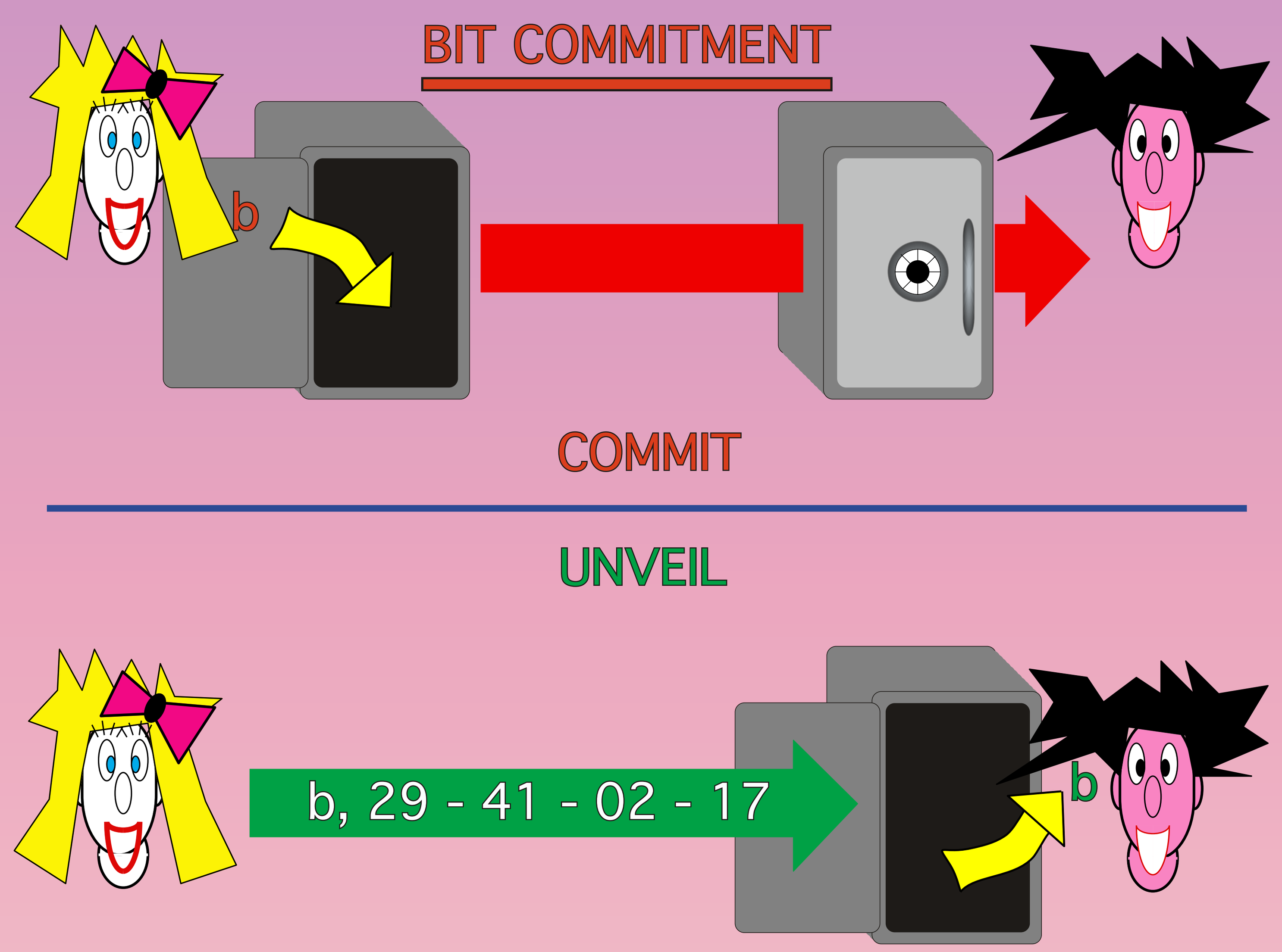
Ben-Or, Goldwasser, Kilian, Wigderson

Classically

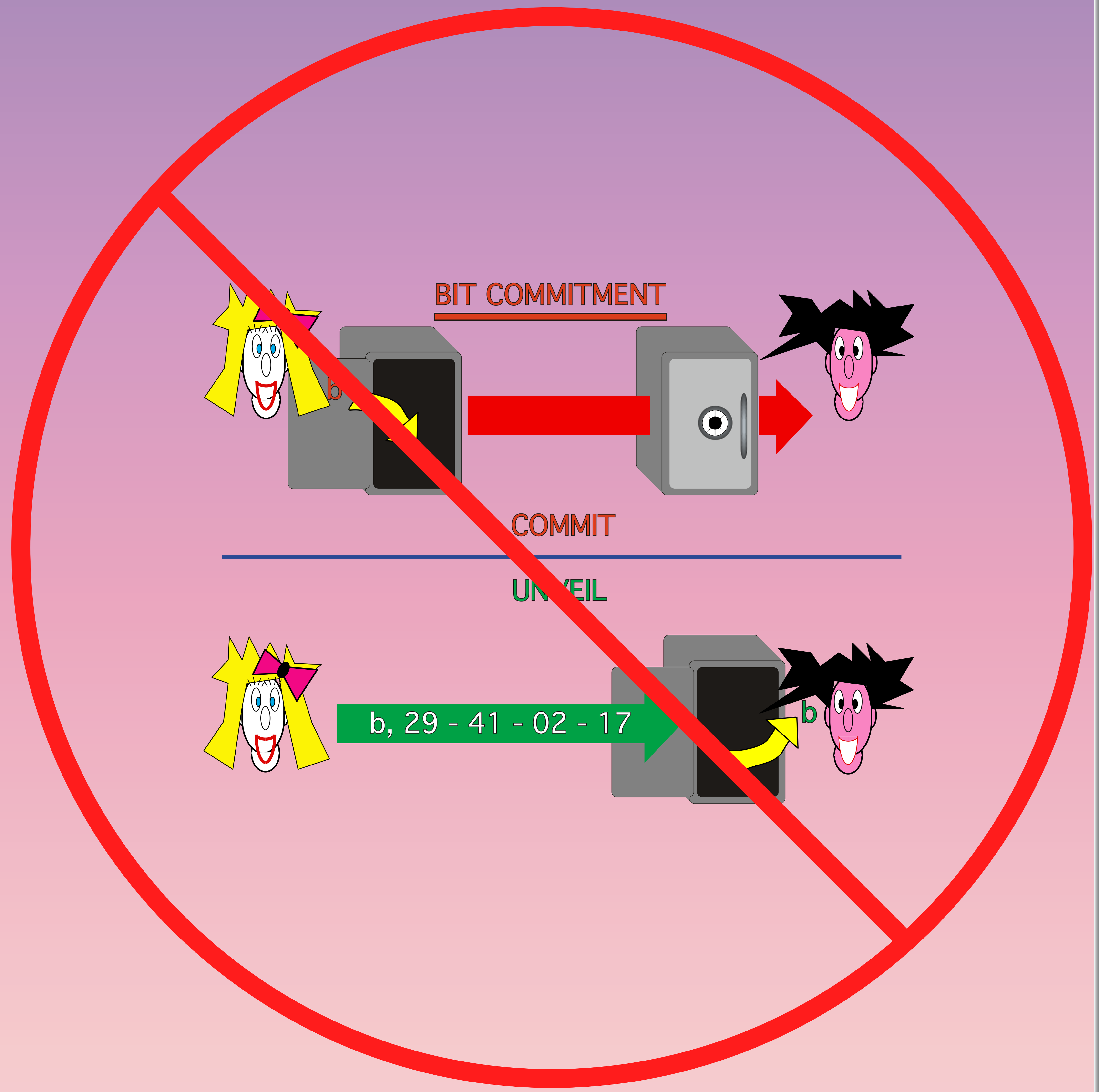


~~Ben-Or, Goldwasser, Kilian, Wigderson~~

Quantumly



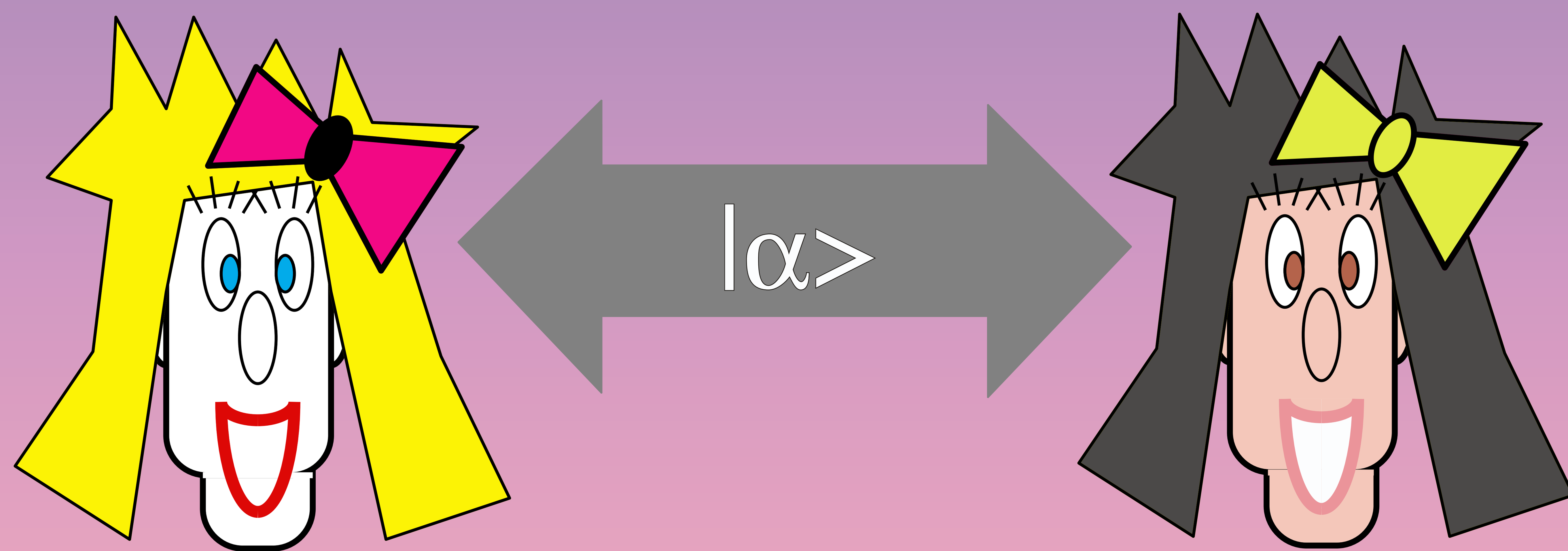
or



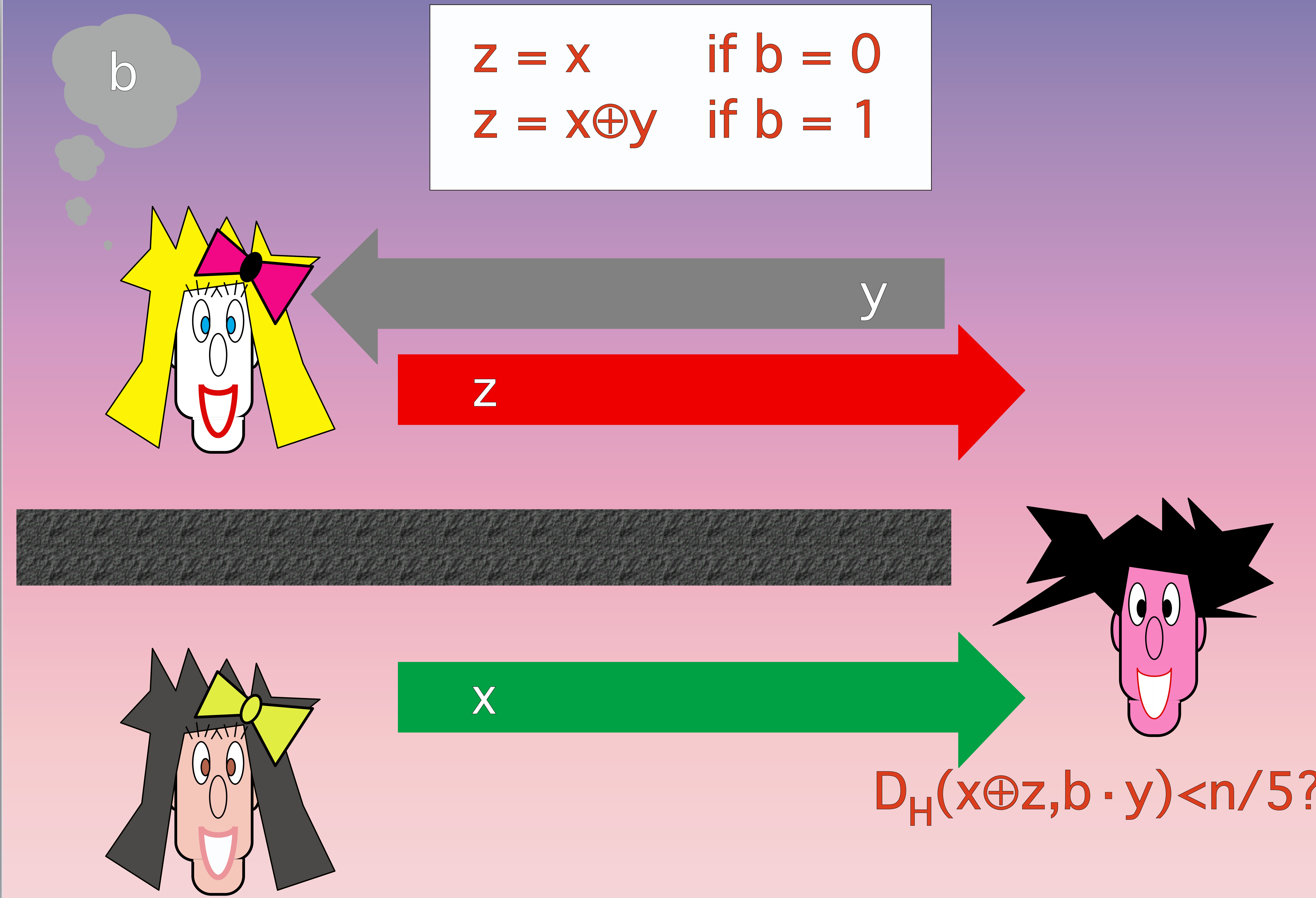
???

(7)
two provers BC
Classically Secure
Quantumly Insecure

Quantumly

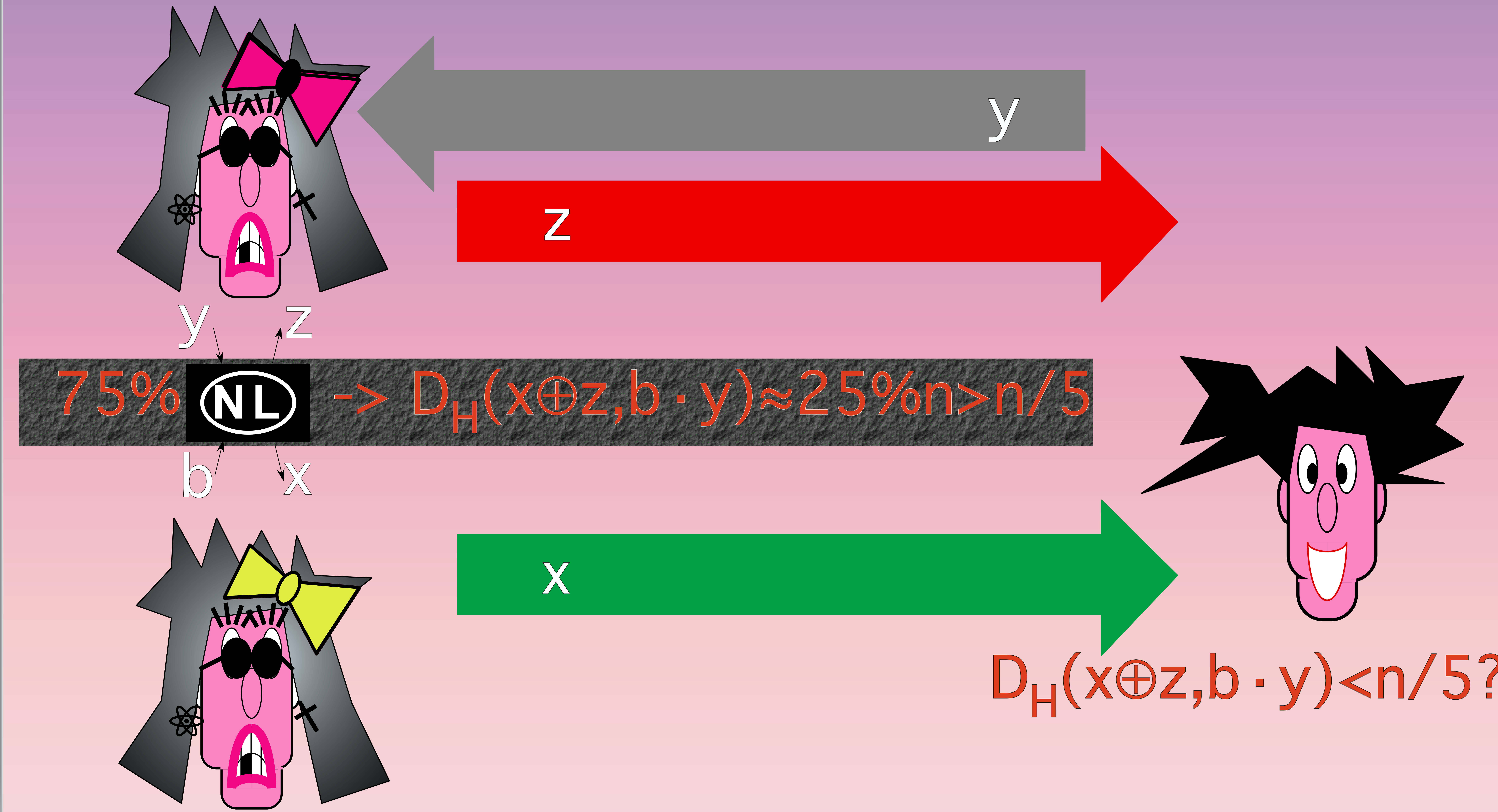


Ben-Or, Goldwasser, Kilian, Wigderson



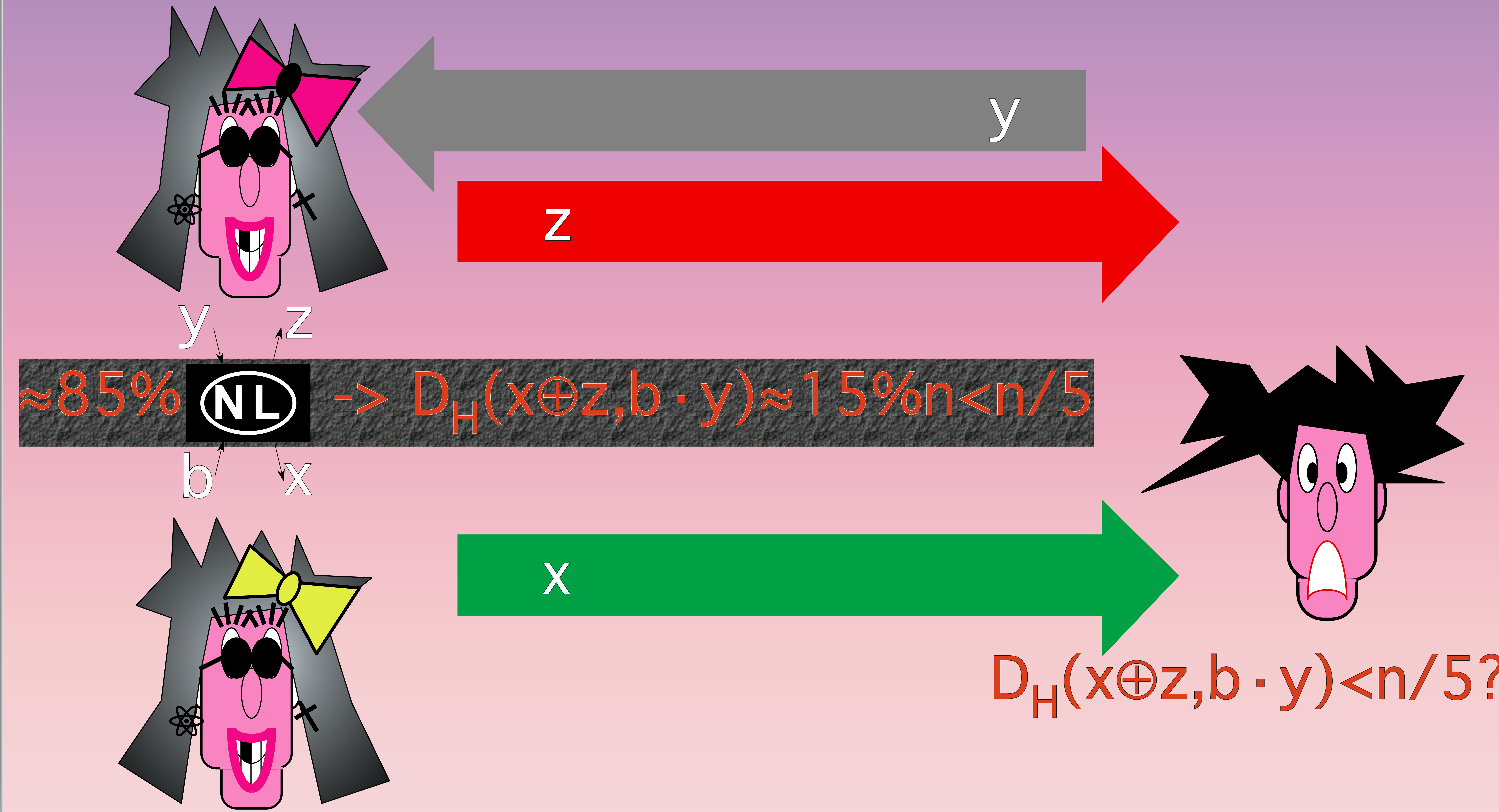
Ben-Or, Goldwasser, Kilian, Wigderson

Classically



Ben-Or, Goldwasser, Kilian, Wigderson

Quantumly



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

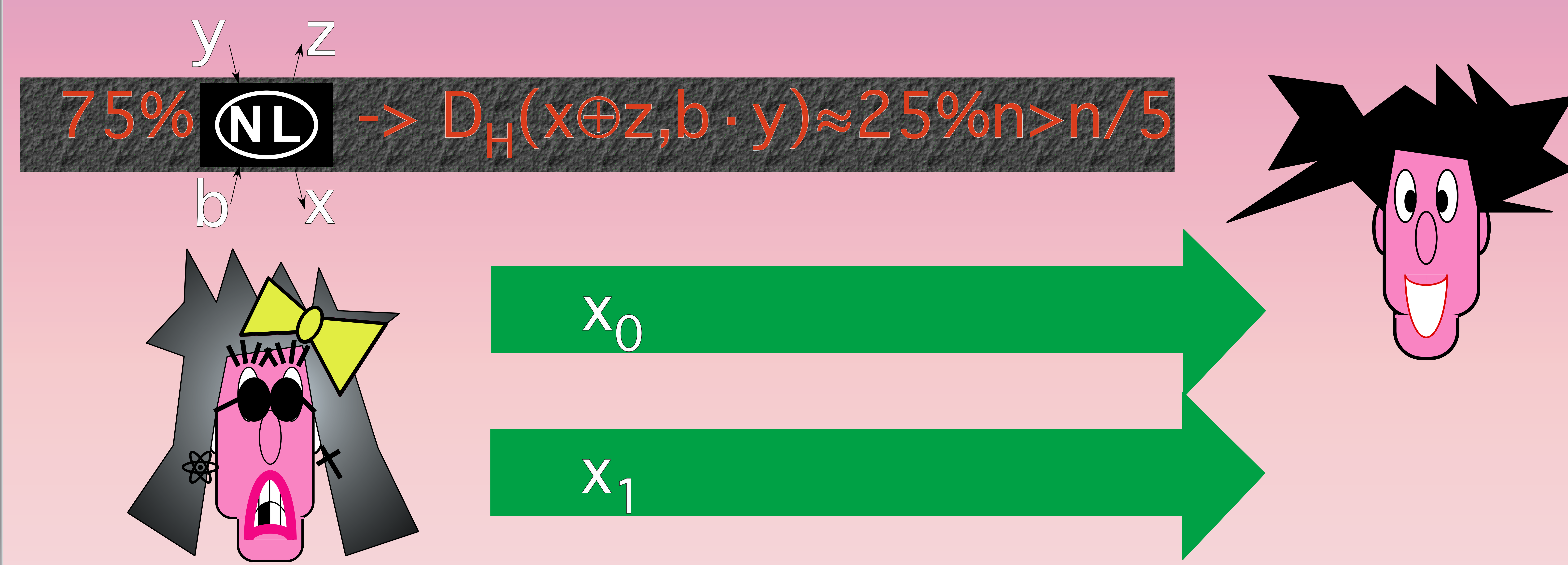
Classically

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

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

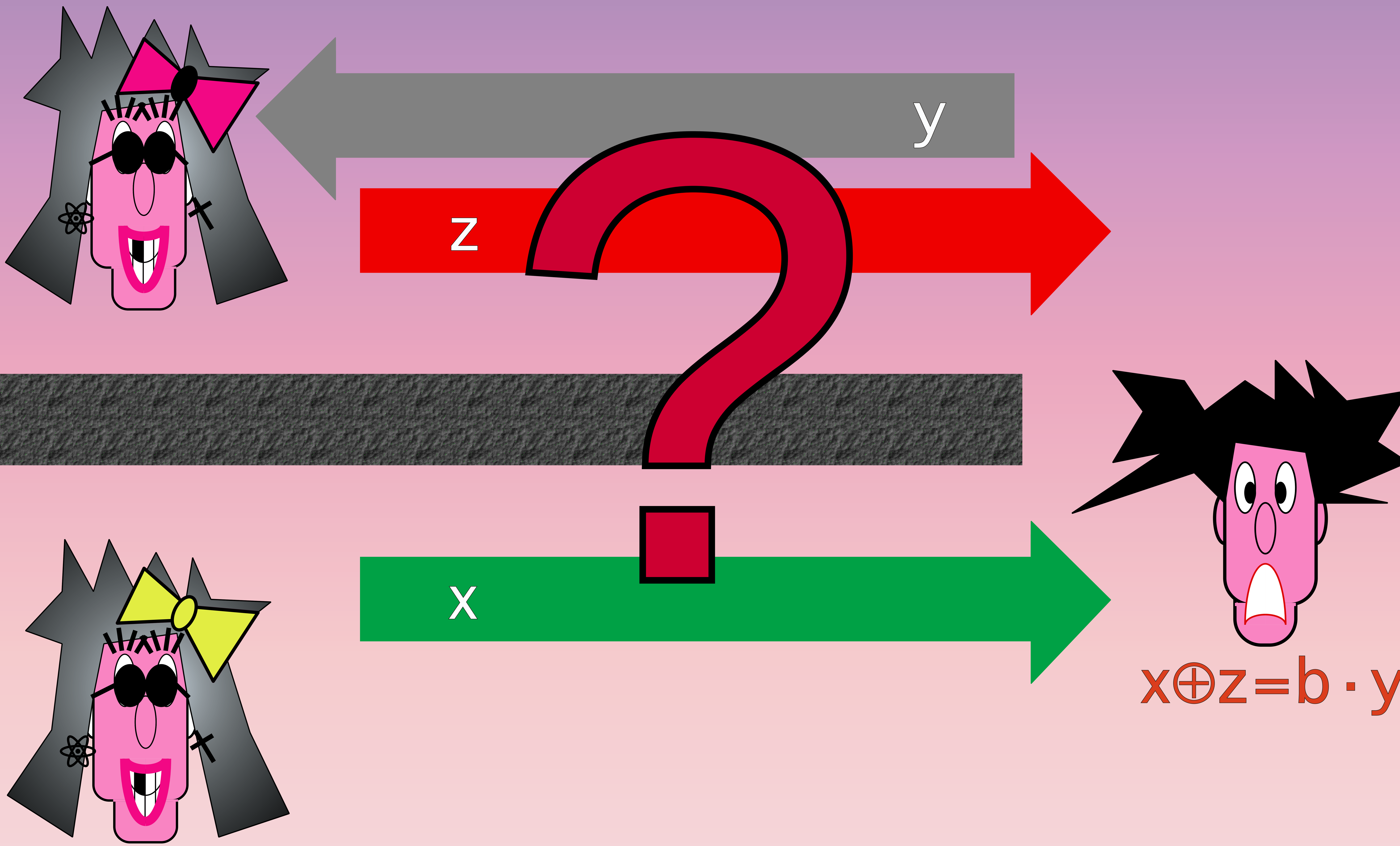
$D_H(x_0 \oplus x_1, y) = D_H((x_0 \oplus z) \oplus (x_1 \oplus z), y) < 2n/5 < n/2$

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



Ben-Or, Goldwasser, Kilian, Wigderson

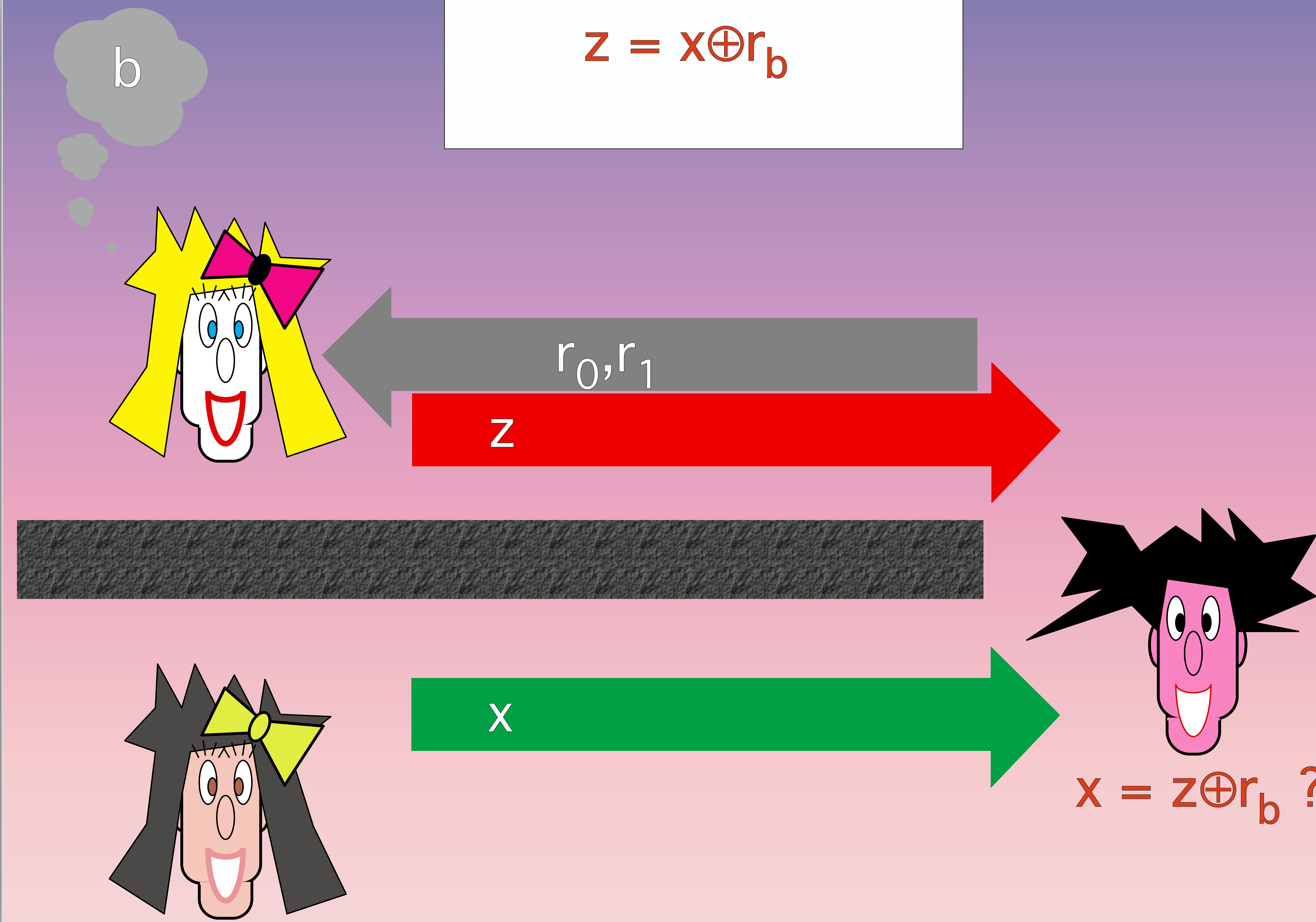
Quantumly



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

(8) two provers BC Classically and Quantumly Secure

$z = x \oplus r_b$



modified BGKW

Classically

$x_0 \oplus z = r_0$

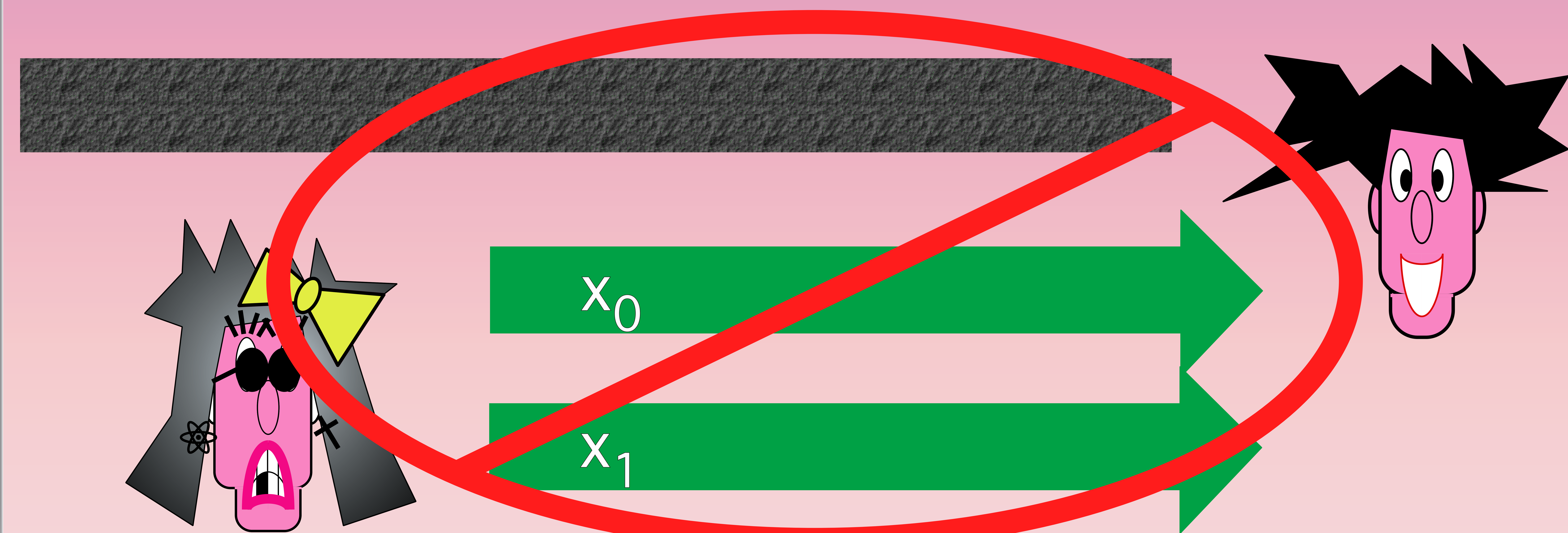
$x_1 \oplus z = r_1$

$x_0 \oplus x_1 = (x_0 \oplus z) \oplus (x_1 \oplus z) = r_0 \oplus r_1$

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

modified BGKW

Quantumly



modified BGKW

Quantumly

MAIN THEOREM

Let Z and O 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 $y_0 \oplus y_1$) > δ.

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

Imagine that Peggy and Paula would like to be able to unveil a certain instance of b both as 0 and as 1. Our only assumption is that Paula knows nothing about r_0, r_1. Let them share an unlimited quantity of entanglement in any form they wish. Without loss of generality to unveil a zero the message of Paula is defined by the outcome w_0 of a POVM $\mathbb{Z} = \{Z_1^\dagger Z_1, \cdots, Z_{2^n}^\dagger Z_{2^n}\}$ and to unveil a 1 by the outcome w_1 of a POVM $\mathbb{O} = \{O_1^\dagger O_1, \cdots, O_{2^n}^\dagger O_{2^n}\}$.

Each operator in a POVM is a positive matrix and can thus be decomposed into a linear combination of orthogonal projectors with coefficients between 0 and 1.

Let p_0 be the probability of successfully unveiling 0 and p_1 be the probability of successfully unveiling 1. Suppose there exists a pair of POVMs where $p_0 + p_1 > 1$. We show that any quantum player can then obtain *both* classical strings w_0, w_1 to unveil both values with probability strictly greater than zero. Notice that if we manage to make the probability of getting both strings w_0, w_1 greater than $1/2^n$, then Paula can compute $r_0 \oplus r_1 = w_0 \oplus w_1$ better than at random. This implies communication between Peggy and Paula, which is impossible by hypothesis.

The strategy of Paula is simply to perform both measurements, one after the other. Let's denote her state by ρ. Assume the right outcome for unveiling a zero is w_0 and the right outcome for unveiling a one is w_1.

The probability to obtain w_0 if $\mathbb{Z}$ is measured is

$$p_0 = Tr(Z_{w_0}^{\dagger} Z_{w_0} \rho)$$

and the state becomes

$$Z_{w_0} \rho Z_{w_0}^{\dagger} / p_0.$$

The probability to obtain w_1 if $\mathbb{O}$ is measured is

$$p_1 = Tr(O_{w_1}^{\dagger} O_{w_1} \rho)$$

and the state becomes

$$O_{w_1} \rho O_{w_1}^{\dagger} / p_1.$$

If $\mathbb{O}$ is measured after $\mathbb{Z}$ the probability to obtain w_0 and w_1 is given by

$$p_{01} \;=\; p_0 Tr[O_{w_1}^\dagger O_{w_1} Z_{w_0} \rho Z_{w_0}^\dagger / p_0] \;=\; Tr[O_{w_1}^\dagger O_{w_1} Z_{w_0} \rho Z_{w_0}^\dagger]$$

If $\mathbb{Z}$ is measured after $\mathbb{O}$ the probability to obtain w_1 and w_0 is given by

$$p_{10} \;=\; p_1 Tr[Z_{w_1}^\dagger Z_{w_1} O_{w_0} \rho O_{w_0}^\dagger / p_1] \;=\; Tr[Z_{w_1}^\dagger Z_{w_1} O_{w_0} \rho O_{w_0}^\dagger]$$

Both p_{01} and p_{10} must be smaller or equal to $1/2^n$ otherwise Paula learns something about $r_0 \oplus r_1 = w_0 \oplus w_1$ (which is impossible without communication).

Having all this in mind, consider the following sequence of implications:

$$p_{01} + p_{10} \leq 1/2^{n-1}$$
$$Tr[O^{\dagger}_{w_1} O_{w_1} Z_{w_0} \rho Z^{\dagger}_{w_0}] + Tr[Z^{\dagger}_{w_1} Z_{w_1} O_{w_0} \rho O^{\dagger}_{w_0}] \leq 1/2^{n-1}$$
$$Tr[(I - (I - O^{\dagger}_{w_1} O_{w_1})) Z_{w_0} \rho Z^{\dagger}_{w_0}] + Tr[(I - (I - Z^{\dagger}_{w_1} Z_{w_1})) O_{w_0} \rho O^{\dagger}_{w_0}] \leq 1/2^{n-1}$$
$$Tr[Z_{w_0} \rho Z^{\dagger}_{w_0}] - Tr[(I - O^{\dagger}_{w_1} O_{w_1}) Z_{w_0} \rho Z^{\dagger}_{w_0}] + Tr[O_{w_0} \rho O^{\dagger}_{w_0}] - Tr[(I - Z^{\dagger}_{w_1} Z_{w_1}) O_{w_0} \rho O^{\dagger}_{w_0}] \leq 1/2^{n-1}$$

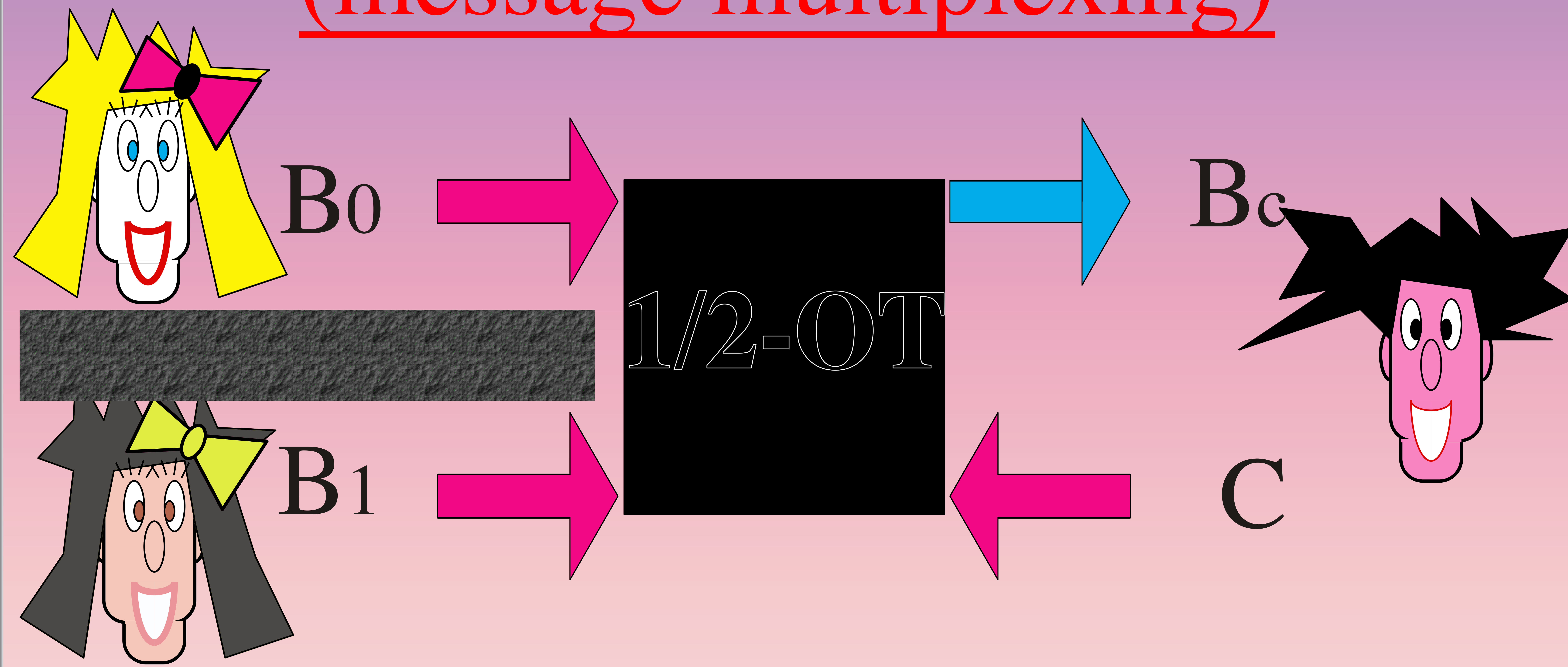
Using that $p_0 = Tr(Z^{\dagger}_{w_0} Z_{w_0} \rho)$ and $p_1 = Tr(O^{\dagger}_{w_1} O_{w_1} \rho)$ we get

$$p_0 + p_1 \leq Tr[(I - O^{\dagger}_{w_1} O_{w_1}) Z_{w_0} \rho Z^{\dagger}_{w_0}] + Tr[(I - Z^{\dagger}_{w_1} Z_{w_1}) O_{w_0} \rho O^{\dagger}_{w_0}] + 1/2^{n-1}$$
$$p_0 + p_1 \leq Tr[I - O^{\dagger}_{w_1} O_{w_1}] + Tr[I - Z^{\dagger}_{w_1} Z_{w_1}] + 1/2^{n-1}$$
$$p_0 + p_1 \leq (1 - p_0) + (1 - p_1) + 1/2^{n-1}$$
$$2(p_0 + p_1) \leq 2 + 1/2^{n-1}$$
$$p_0 + p_1 \leq 1 + 1/2^{n}$$

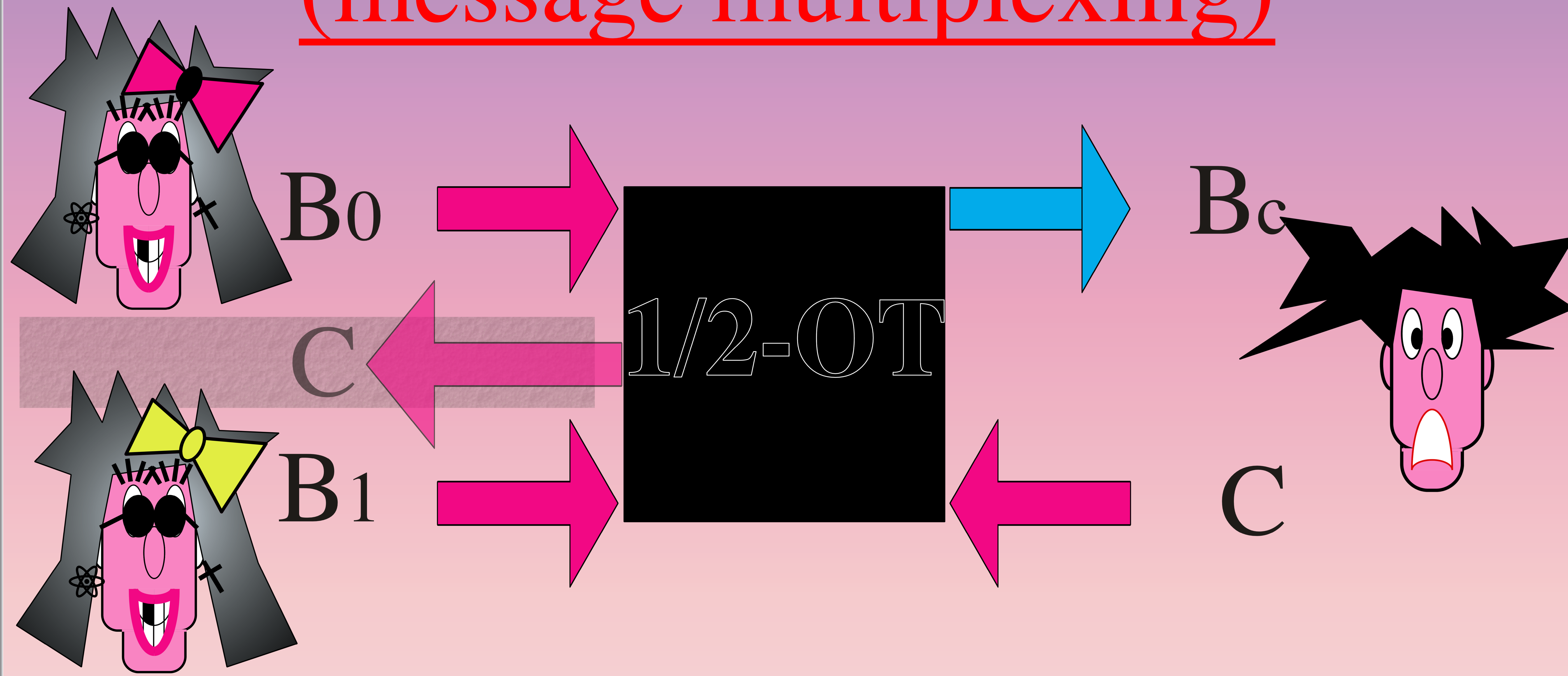
This last statement means that the probability of cheating the bit commitment scheme is only exponentially little better than in the honest case. This is the best we could hope for because this value is reached by Peggy-Paula acting nearly honestly: Peggy and Paula act honestly except that when Paula unveils if she wish to unveil the opposite bit to Peggy she sends a random string instead of w. With probability $1/2^n$ she succeeds in unveiling the opposite bit.

(9)
W A R N I N G !

Oblivious Transfer (message multiplexing)

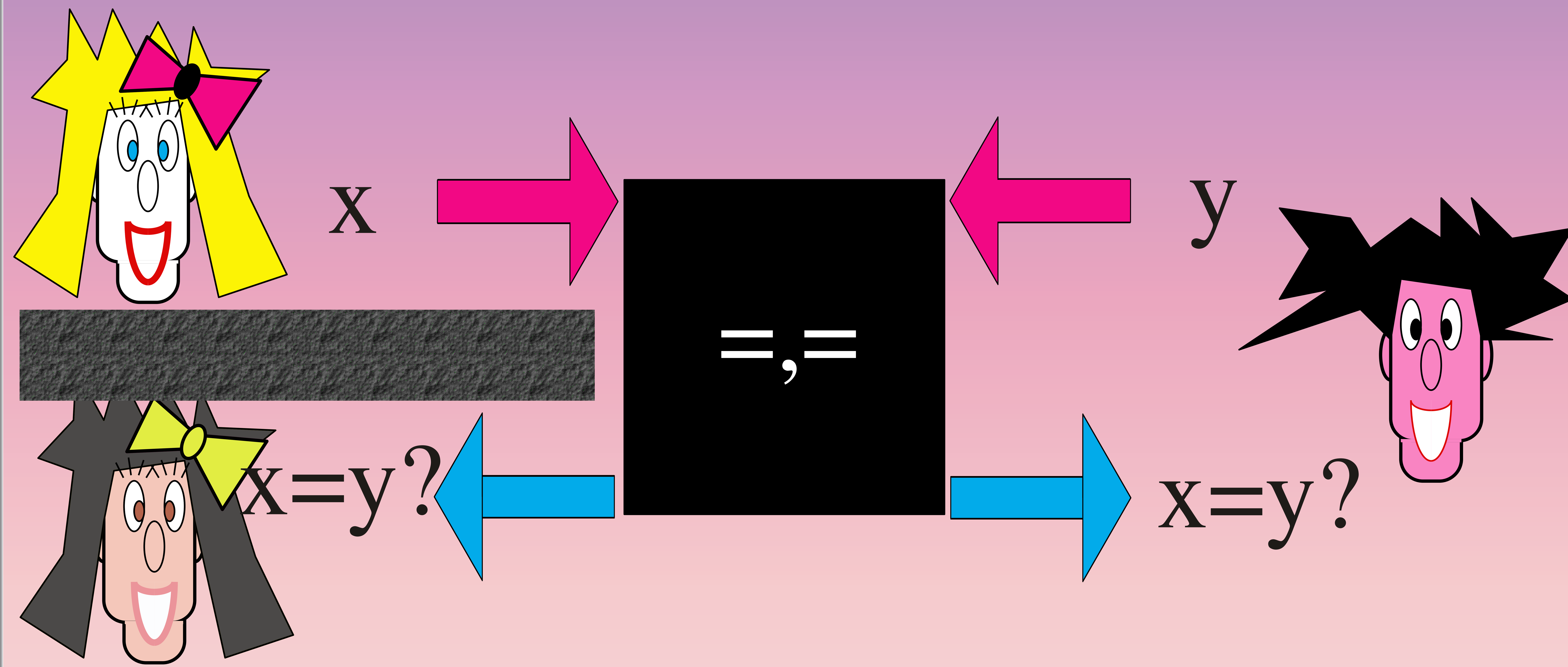


Oblivious Transfer (message multiplexing)

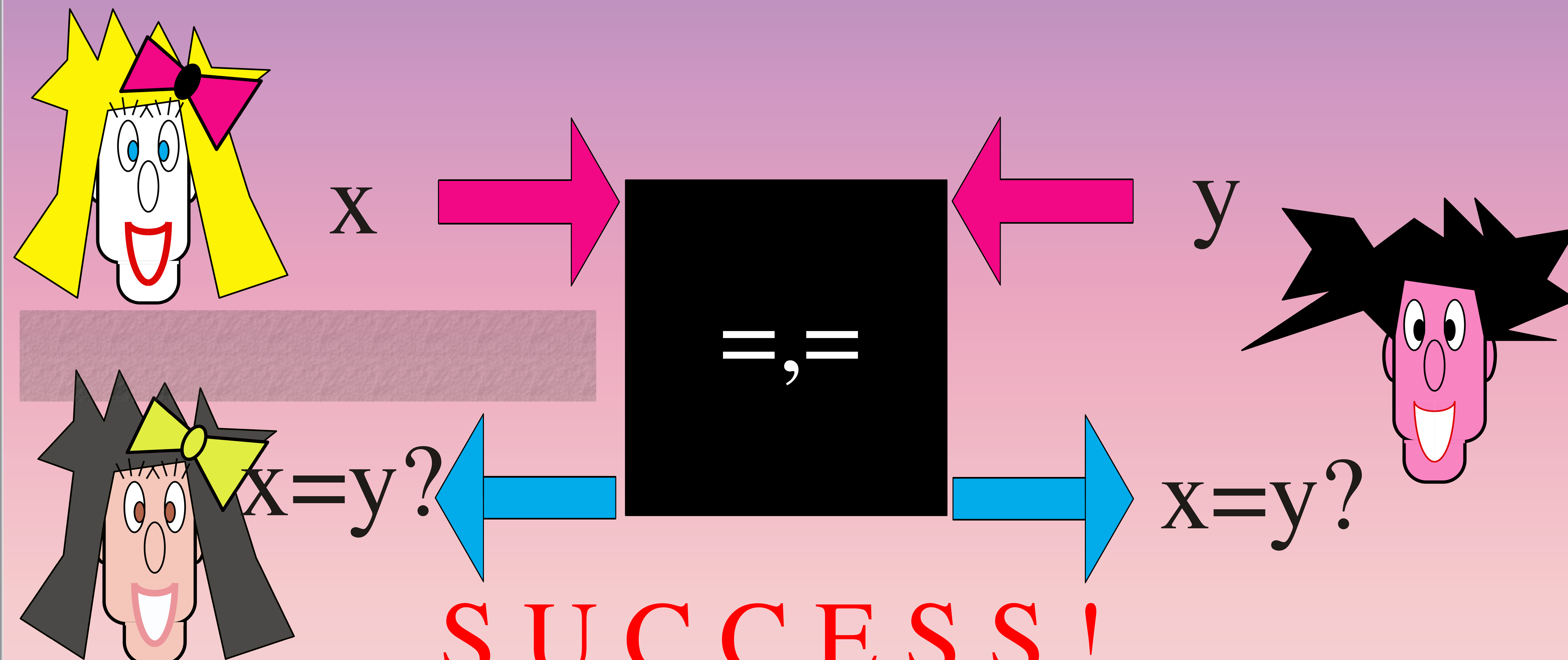


Brassard, Crépeau, Mayers, Salvail 97

Mutual Identification

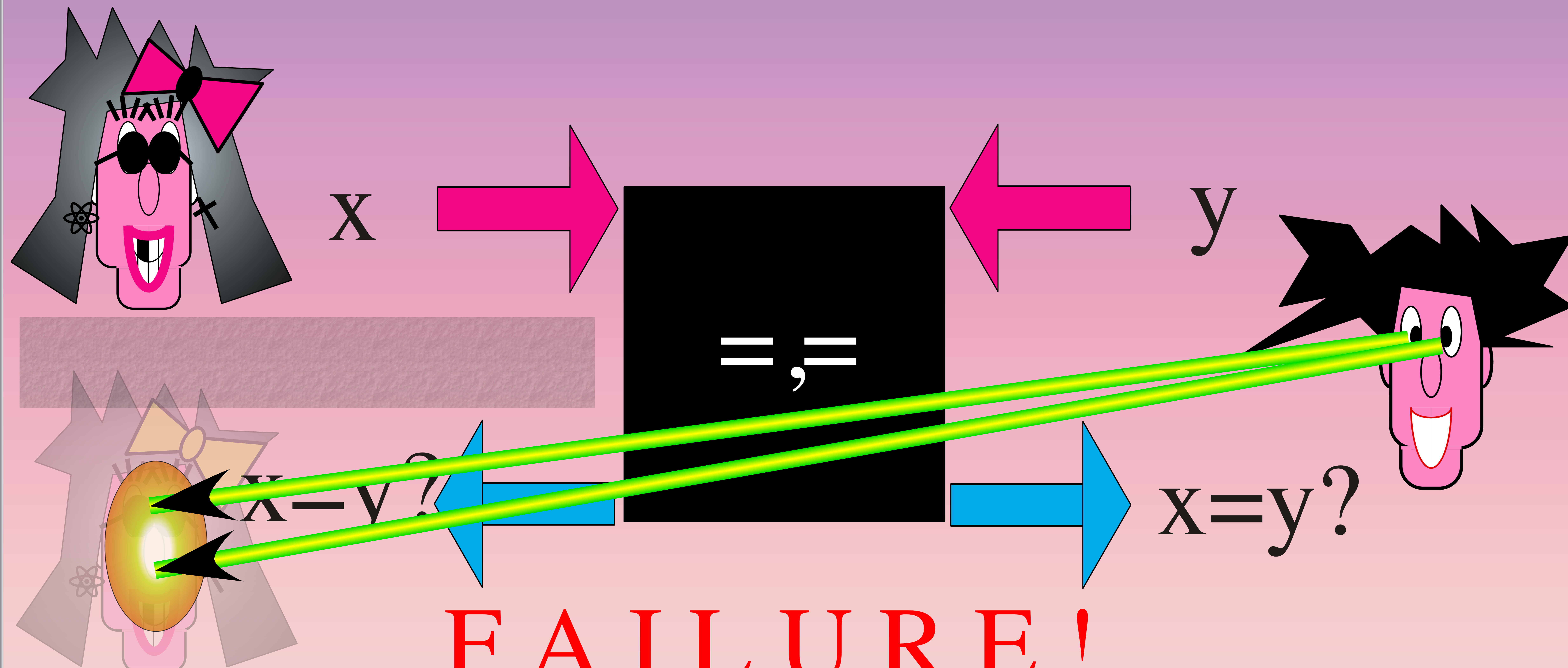


Mutual Identification



S U C C E S S !

Mutual Identification

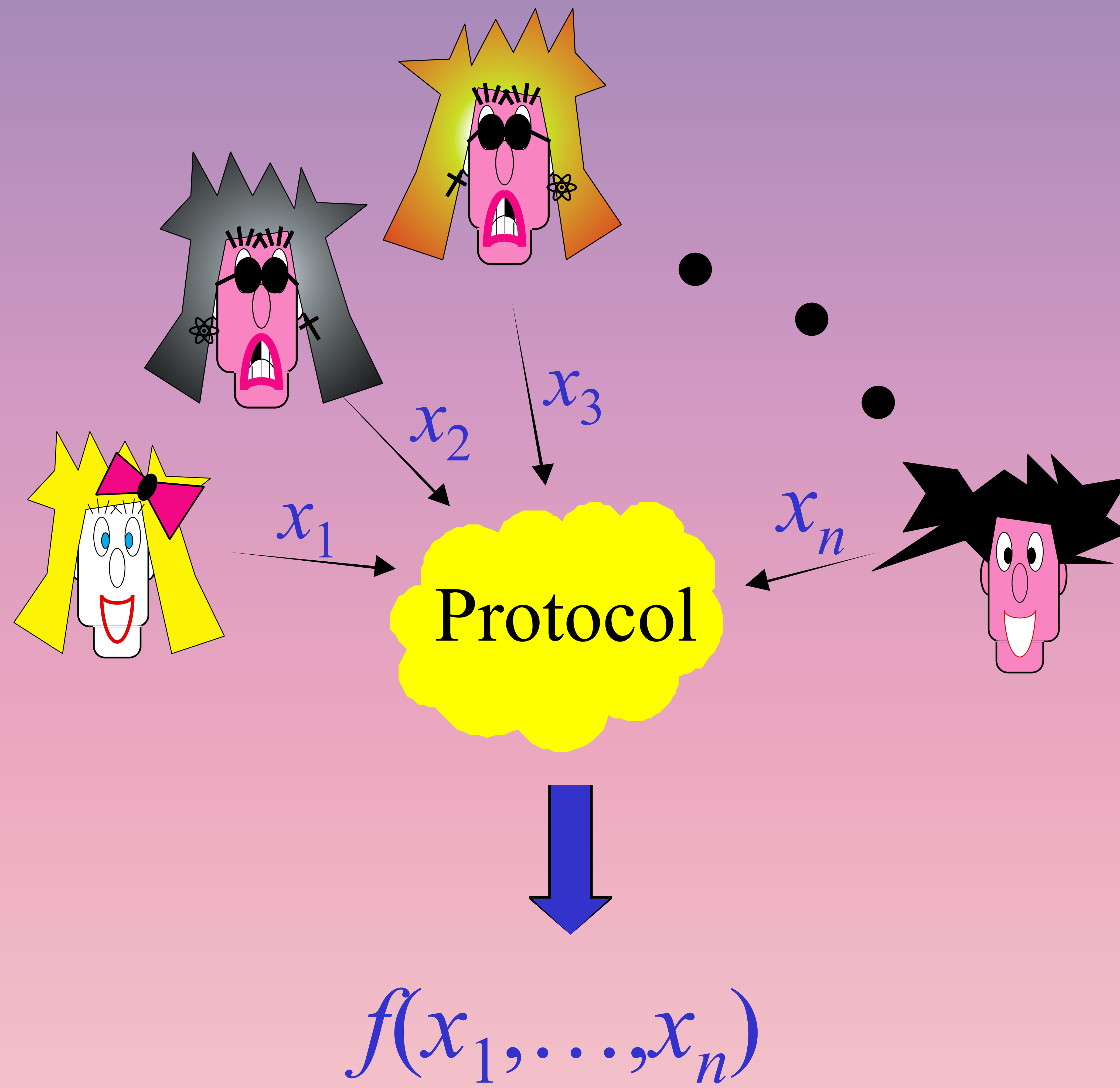


F A I L U R E !

(10) Classical Multi-party Computing

Classical Multi-party Computing

- Network of n players
- Each has input x_i
- Want to compute $f(x_1,\ldots,x_n)$ for some known function f
- *E.g.* electronic voting

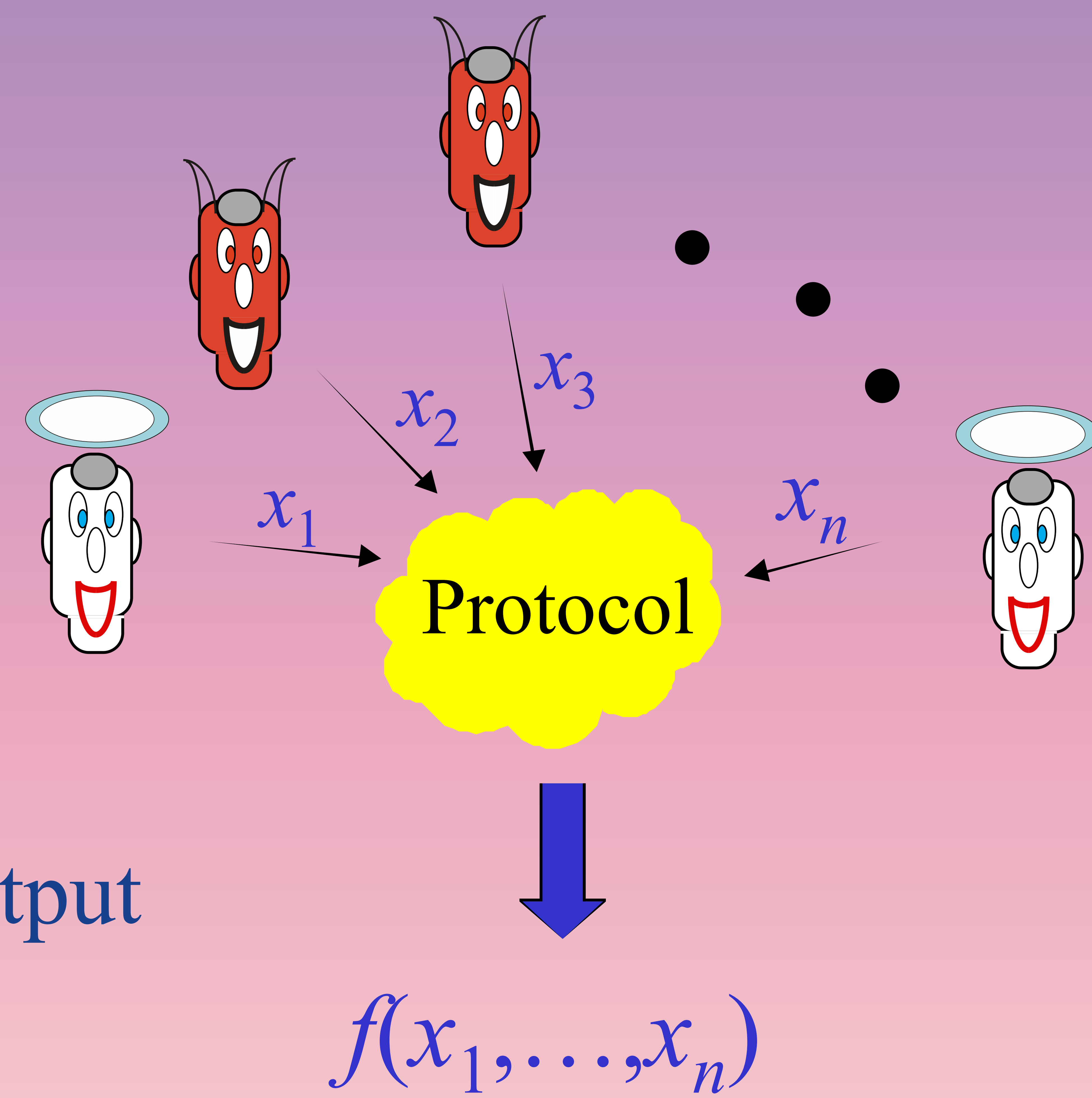


Classical Multi-party Computing

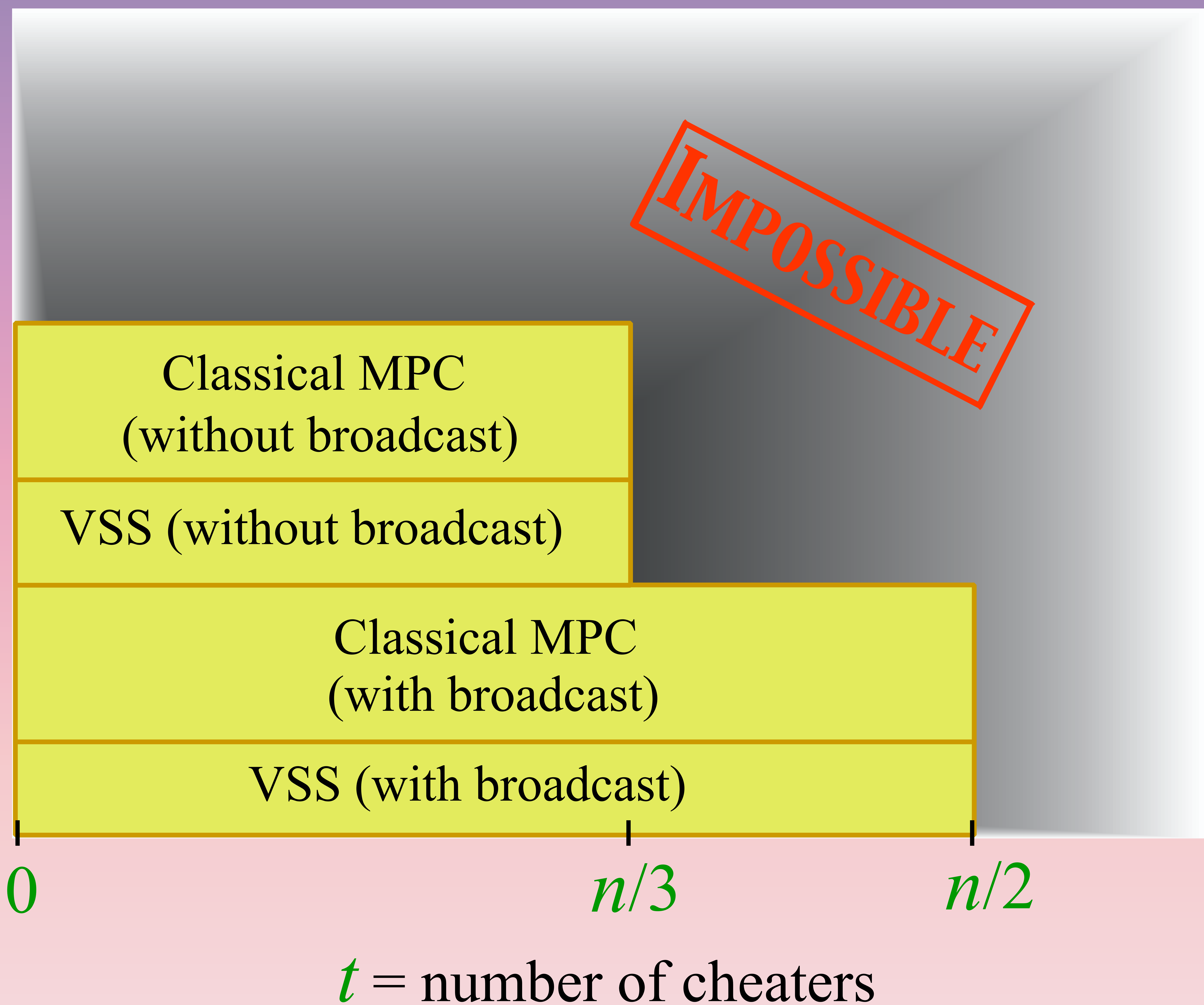
Even if t out of n players try to cheat:

1. Cheaters learn nothing (except output)

2. Cheaters cannot affect output (except by choice of input)



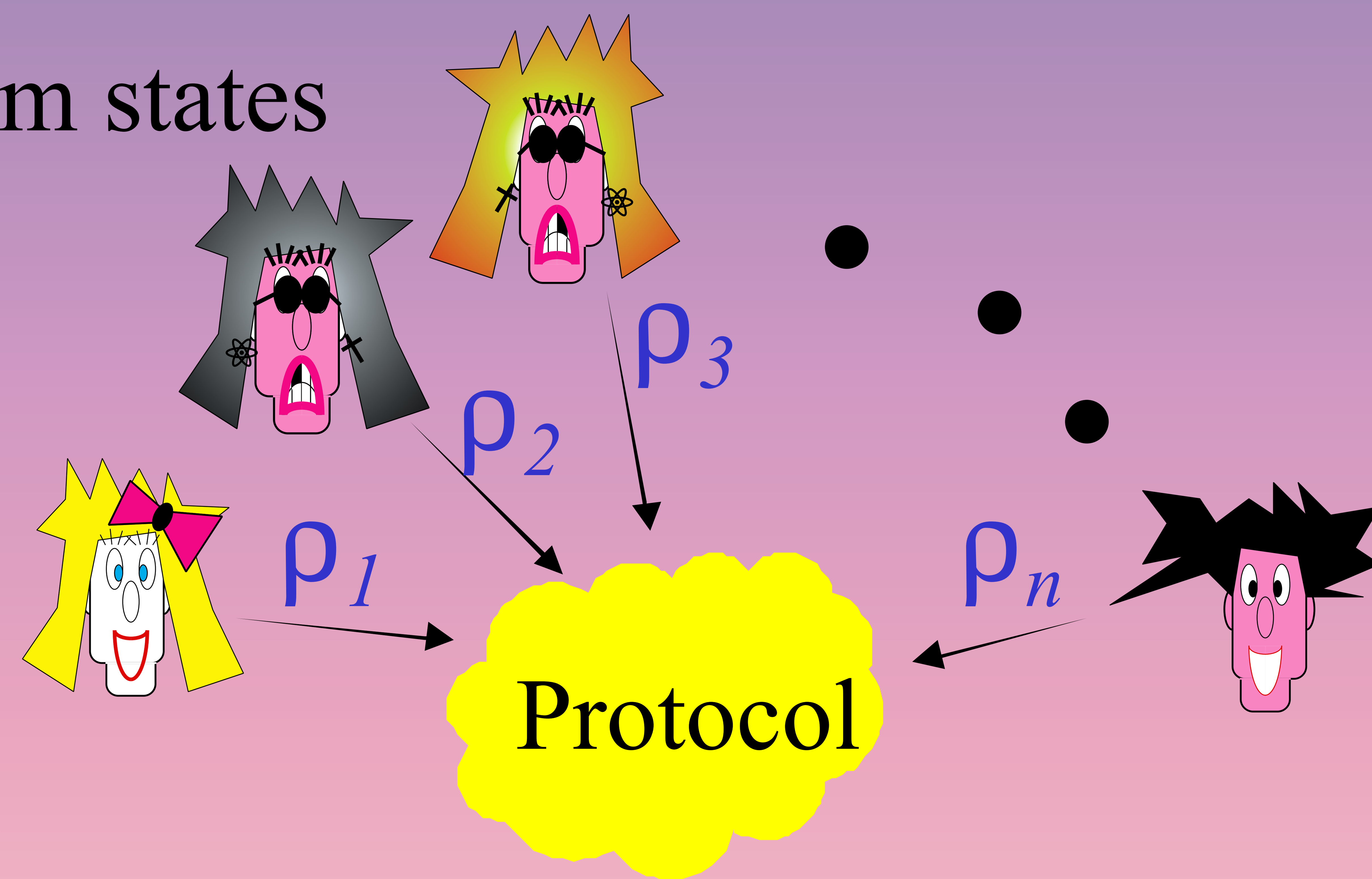
Results


Impossible
Classical MPC
(without broadcast)
VSS (without broadcast)
Classical MPC
(with broadcast)
VSS (with broadcast)
0
n/3
n/2
t = number of cheaters

(11) Multi-Party Quantum Computing

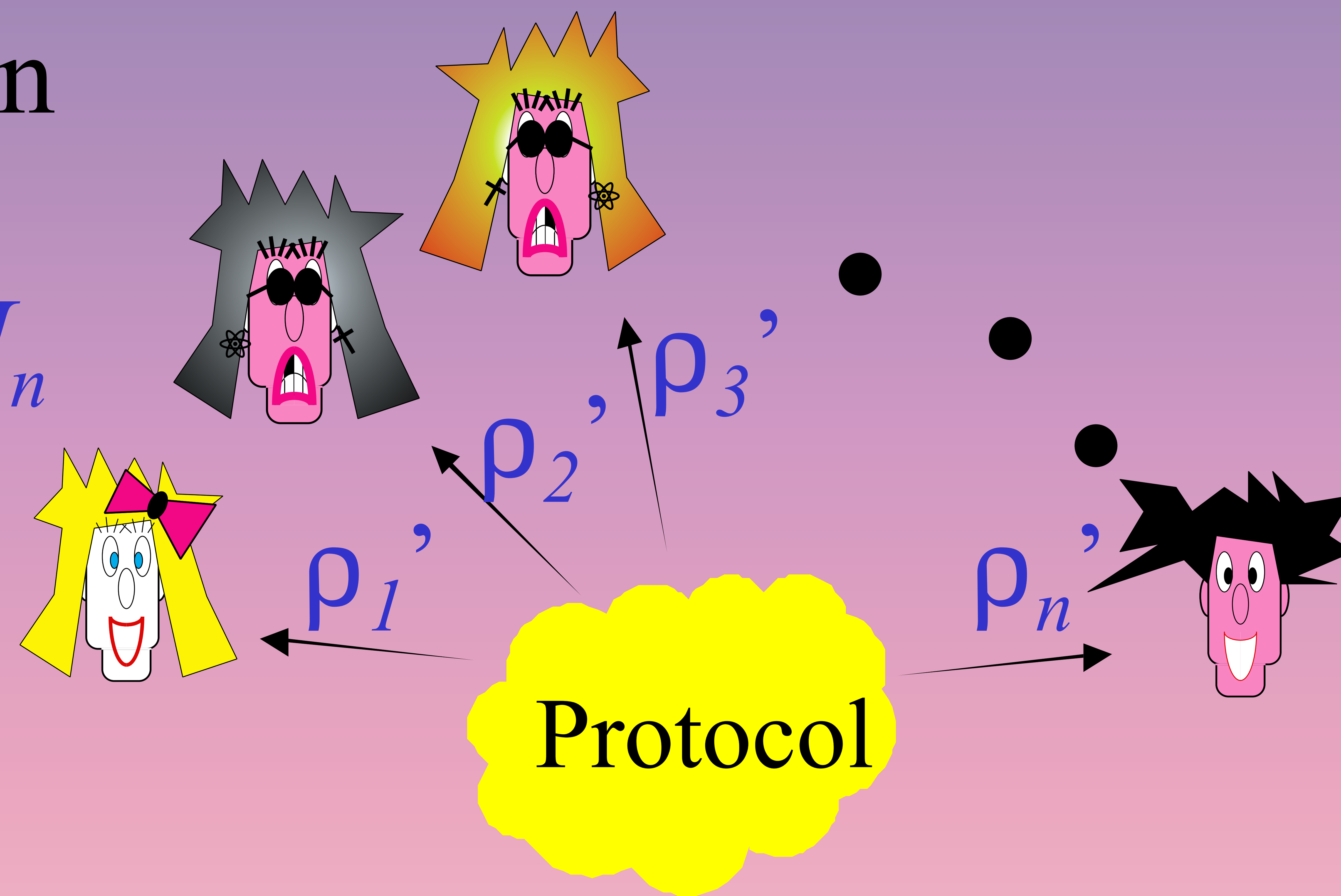
Multi-party Quantum Computing

- Players' inputs are quantum states
  - Possibly entangled
  - No description necessary (protocol is "oblivious")
- Output is quantum
- Want to evaluate a known quantum circuit U
- Player i gets i-th component of output



Multi-party Quantum Computing

- Players' inputs form an arbitrary state
  ρ in $H_1 \otimes H_2 \otimes \ldots \otimes H_n$
- Player *i* holds *i*-th component:
  ρ_i
- Each player gets one output:
  $\rho_i' = (U \rho U^\dagger)_i$

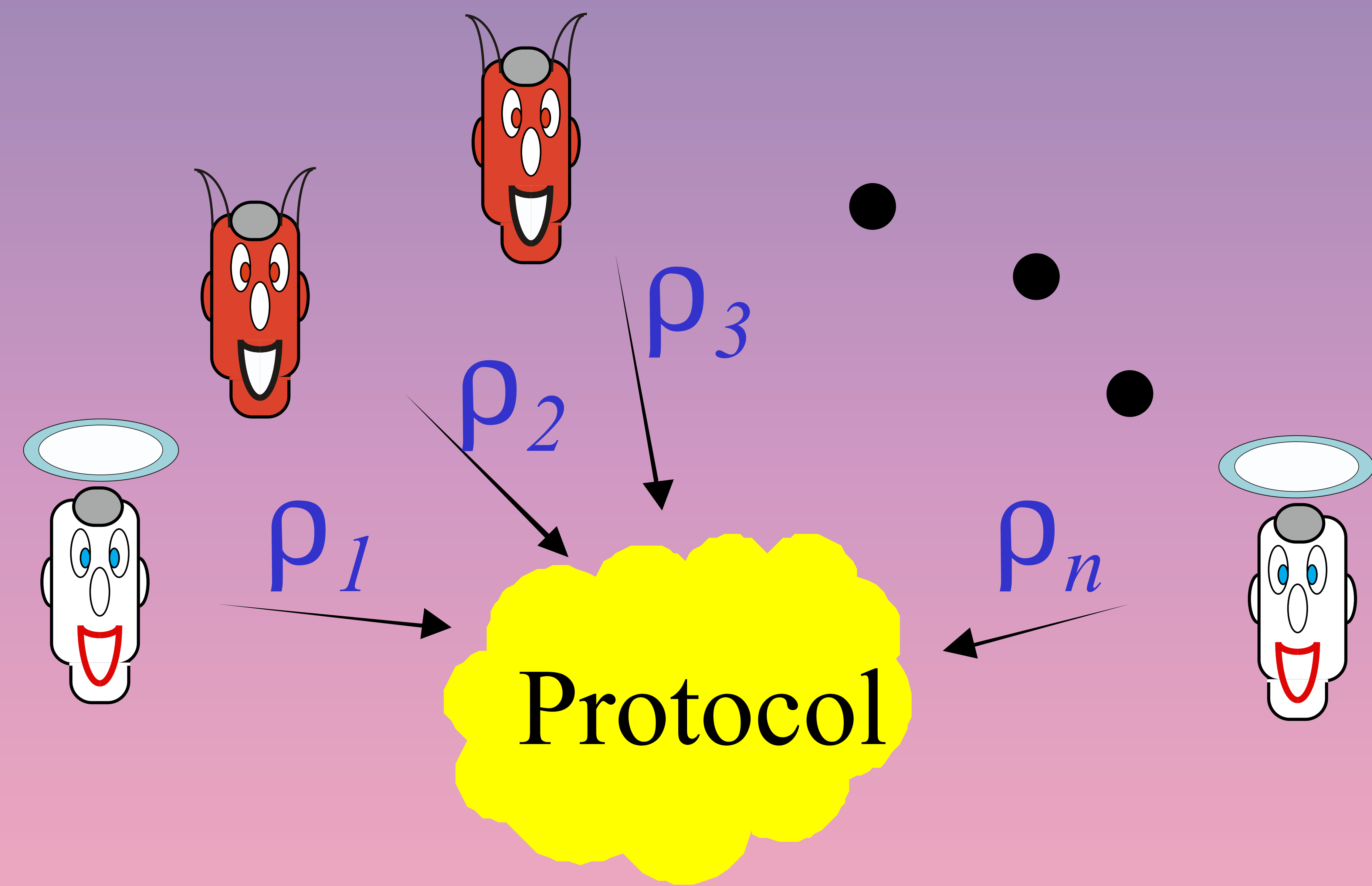


$\rho' = U \rho U^\dagger$

Multi-party Quantum Computing

Even if t out of n

players try to cheat:



1. Cheaters learn nothing
   (except output)

2. Cheaters cannot affect output
   (except by choice of inputs)

Results

- $t < n/6$:

  Any Multi-party Quantum Computation

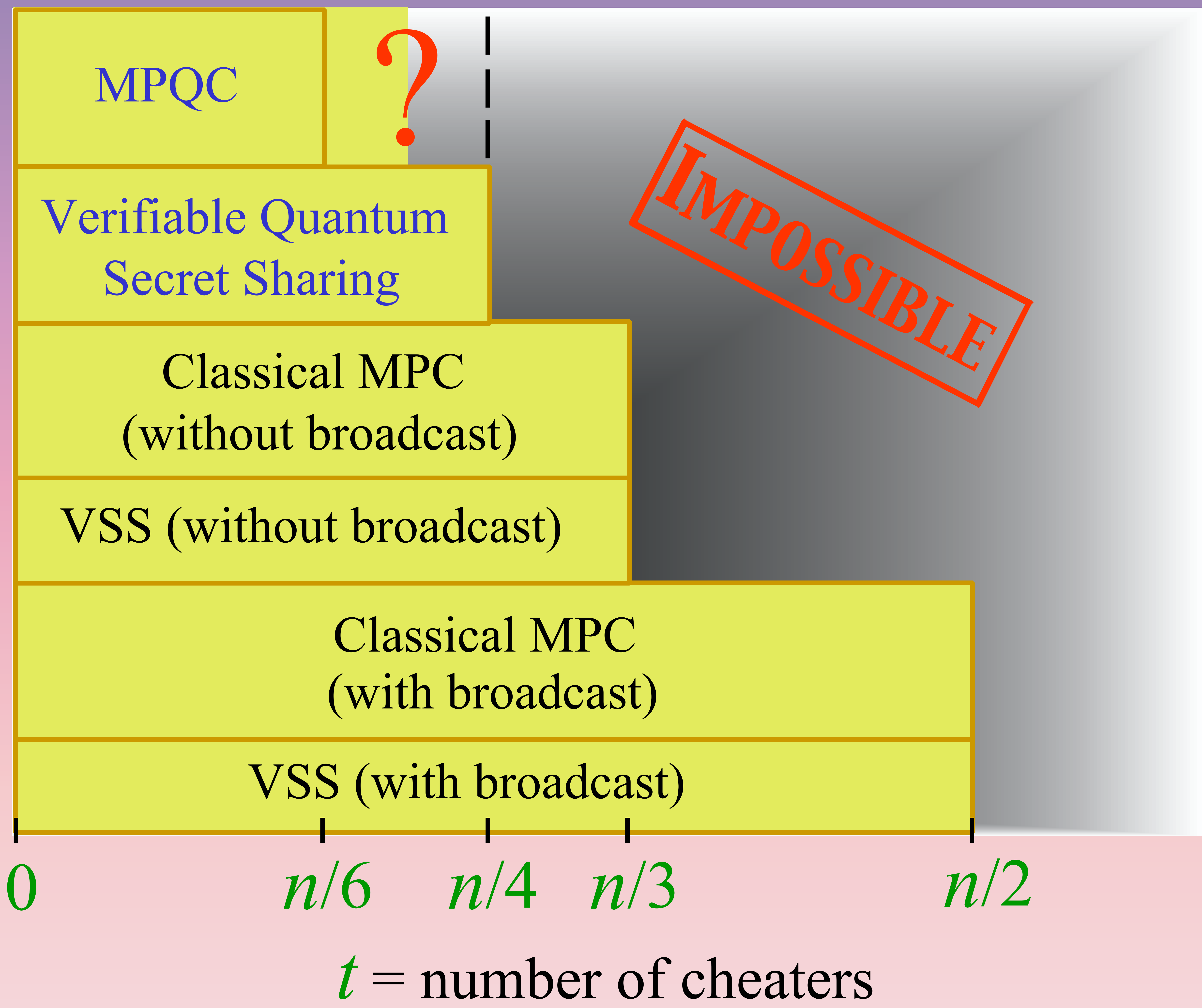
- $t < n/4$:

  Verifiable Quantum Secret-Sharing

- $t \geq n/4$:

  Even (perfect) VQSS is impossible

Results


MPQC
?
Verifiable Quantum Secret Sharing
IMPOSSIBLE
Classical MPC (without broadcast)
VSS (without broadcast)
Classical MPC (with broadcast)
VSS (with broadcast)
0
n/6
n/4
n/3
n/2
t = number of cheaters

MPQC and Fault-Tolerant Computing

- MPQC is like FTQC with a different error model...

	FTQC	MPQC
Type of errors	randomly spread, independent	maliciously placed, entangled with data
Error location	Can occur anywhere	At most t positions

  - Similar protocol techniques:
    Classical MPC [BGW,CCD] → FTQC [AB99] → MPQC [CGS]
  - Different proof techniques
    (Need different notion of “proximity” to coding subspaces)

an Introduction to theoretical quantum CRYPTOGRAPHY

Claude Crépeau

School of Computer Science
McGill University

