Classical and |Quantum⟩ strategies for two-prover bit commitments

Claude Crépeau

School of Computer Science
McGill University

Joint work with J-R Simard and A Tapp

|Bit Commitment⟩ Strikes Back

Claude Crépeau

School of Computer Science
McGill University

Joint work with J-R Simard and A Tapp

EPISODE II

Classical and Quantum Strategies against Two-Prover Bit Commitments

Claude Crépeau[1] , Jean-Raymond Simard[1], and Alain Tapp[2]

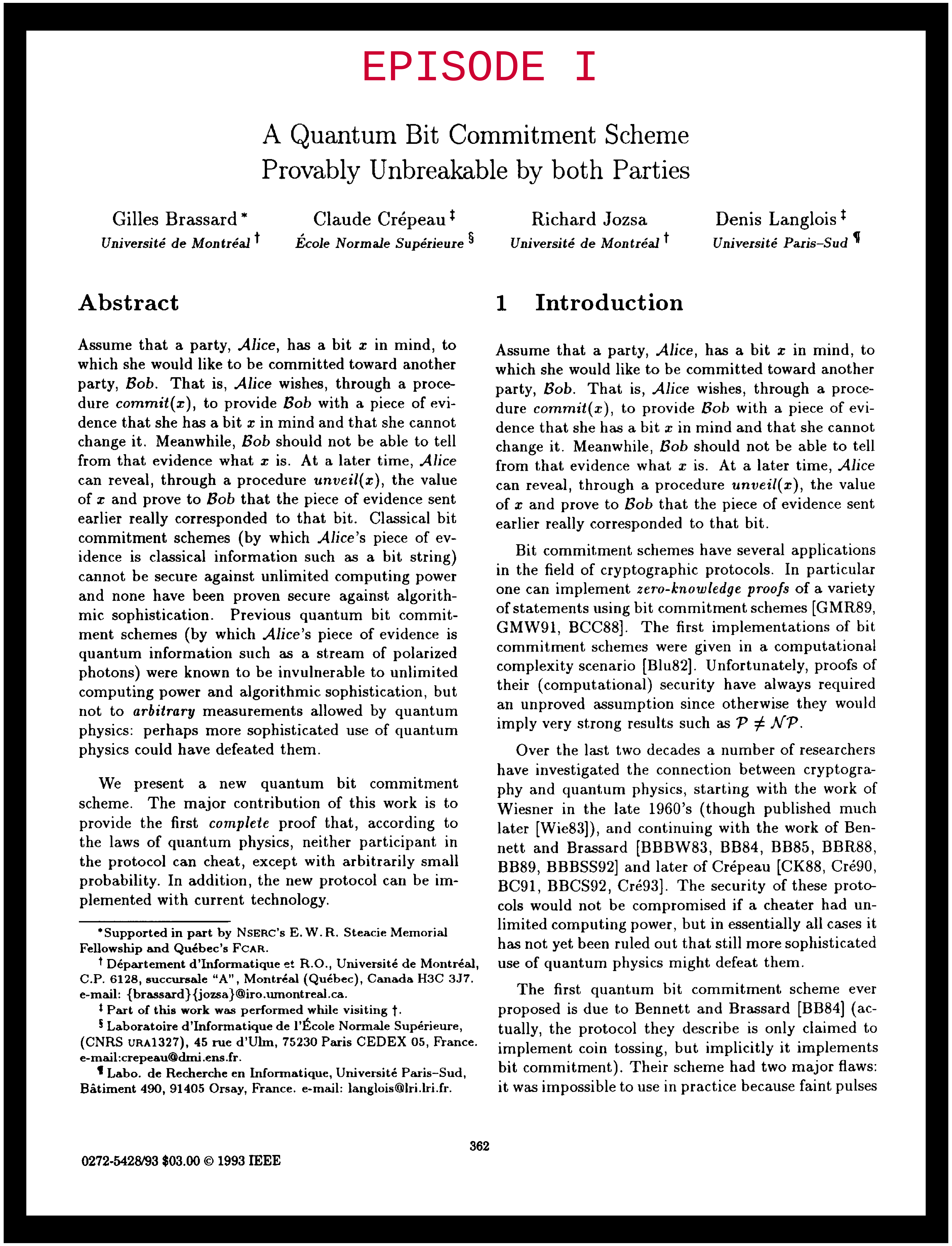
[1] School of Computer Science, McGill University,
Montréal, QC, Canada. {crepeau,jrsimard}@cs.mcgill.ca
[2] Département d'Informatique et R.O., Université de Montréal,
Montréal, QC, Canada. tappa@iro.umontreal.ca

Abstract. *First we show that the assumption behind the Two-Prover Zero-knowledge Interactive proof of BenOr, Goldwasser, Kilian and Wigderson is too weak and need be upgrated to preserve soundness of their construction. Secondly, we introduce a Two-Prover Zero-knowledge Interactive proof similar to theirs and demonstrate that classically it is equally secure as the original. However, we later show that if the provers are allowed to share quantum entanglement, they are able to sucesfully prove false statements to the verifier with probability one. Then we demonstrate that a small variation on the BGKW Two-Prover Zero-knowledge Interactive proof is classically secure with probability nearly one but obiviously quantum insecure with probability nearly one. We finally show that another variation of the original scheme of BGKW is quantumly secure.*

1 Introduction

The notion of Multi-Prover Interactive proofs was introduced by BenOr, Goldwasser, Kilian and Wigderson [?] together with the Zero-knowledge property of such proofs. In the Two-prover scenario, we have two provers, Peggy and Paula, that are allowed to share arbitrary information before the proof, but they become physically separated and isolated during the execution of the proof in order to prevent them from communicating.

The Two-prover Interactive proofs of BGKW rely on their construction of a



EPISODE I

A Quantum Bit Commitment Scheme Provably Unbreakable by both Parties

Gilles Brassard [*]
Université de Montréal [†]

Claude Crépeau [‡]
École Normale Supérieure [§]

Richard Jozsa
Université de Montréal [†]

Denis Langlois [‡]
Université Paris–Sud [¶]

Abstract

Assume that a party, *Alice*, has a bit x in mind, to which she would like to be committed toward another party, *Bob*. That is, *Alice* wishes, through a procedure *commit*(x), to provide *Bob* with a piece of evidence that she has a bit x in mind and that she cannot change it. Meanwhile, *Bob* should not be able to tell from that evidence what x is. At a later time, *Alice* can reveal, through a procedure *unveil*(x), the value of x and prove to *Bob* that the piece of evidence sent earlier really corresponded to that bit. Classical bit commitment schemes (by which *Alice*'s piece of evidence is classical information such as a bit string) cannot be secure against unlimited computing power and none have been proven secure against algorithmic sophistication. Previous quantum bit commitment schemes (by which *Alice*'s piece of evidence is quantum information such as a stream of polarized photons) were known to be invulnerable to unlimited computing power and algorithmic sophistication, but not to *arbitrary* measurements allowed by quantum physics: perhaps more sophisticated use of quantum physics could have defeated them.

We present a new quantum bit commitment scheme. The major contribution of this work is to provide the first *complete* proof that, according to the laws of quantum physics, neither participant in the protocol can cheat, except with arbitrarily small probability. In addition, the new protocol can be implemented with current technology.

1 Introduction

Assume that a party, *Alice*, has a bit x in mind, to which she would like to be committed toward another party, *Bob*. That is, *Alice* wishes, through a procedure *commit*(x), to provide *Bob* with a piece of evidence that she has a bit x in mind and that she cannot change it. Meanwhile, *Bob* should not be able to tell from that evidence what x is. At a later time, *Alice* can reveal, through a procedure *unveil*(x), the value of x and prove to *Bob* that the piece of evidence sent earlier really corresponded to that bit.

Bit commitment schemes have several applications in the field of cryptographic protocols. In particular one can implement *zero-knowledge proofs* of a variety of statements using bit commitment schemes [GMR89, GMW91, BCC88]. The first implementations of bit commitment schemes were given in a computational complexity scenario [Blu82]. Unfortunately, proofs of their (computational) security have always required an unproved assumption since otherwise they would imply very strong results such as $\mathcal{P} \neq \mathcal{NP}$.

Over the last two decades a number of researchers have investigated the connection between cryptography and quantum physics, starting with the work of Wiesner in the late 1960's (though published much later [Wie83]), and continuing with the work of Bennett and Brassard [BBBW83, BB84, BB85, BBR88, BB89, BBBSS92] and later of Crépeau [CK88, Cré90, BC91, BBCS92, Cré93]. The security of these protocols would not be compromised if a cheater had unlimited computing power, but in essentially all cases it has not yet been ruled out that still more sophisticated use of quantum physics might defeat them.

The first quantum bit commitment scheme ever proposed is due to Bennett and Brassard [BB84] (actually, the protocol they describe is only claimed to implement coin tossing, but implicitly it implements bit commitment). Their scheme had two major flaws: it was impossible to use in practice because faint pulses

[*] Supported in part by NSERC's E. W. R. Steacie Memorial Fellowship and Québec's FCAR.

[†] Département d'Informatique et R.O., Université de Montréal, C.P. 6128, succursale "A", Montréal (Québec), Canada H3C 3J7. e-mail: {brassard}{jozsa}@iro.umontreal.ca.

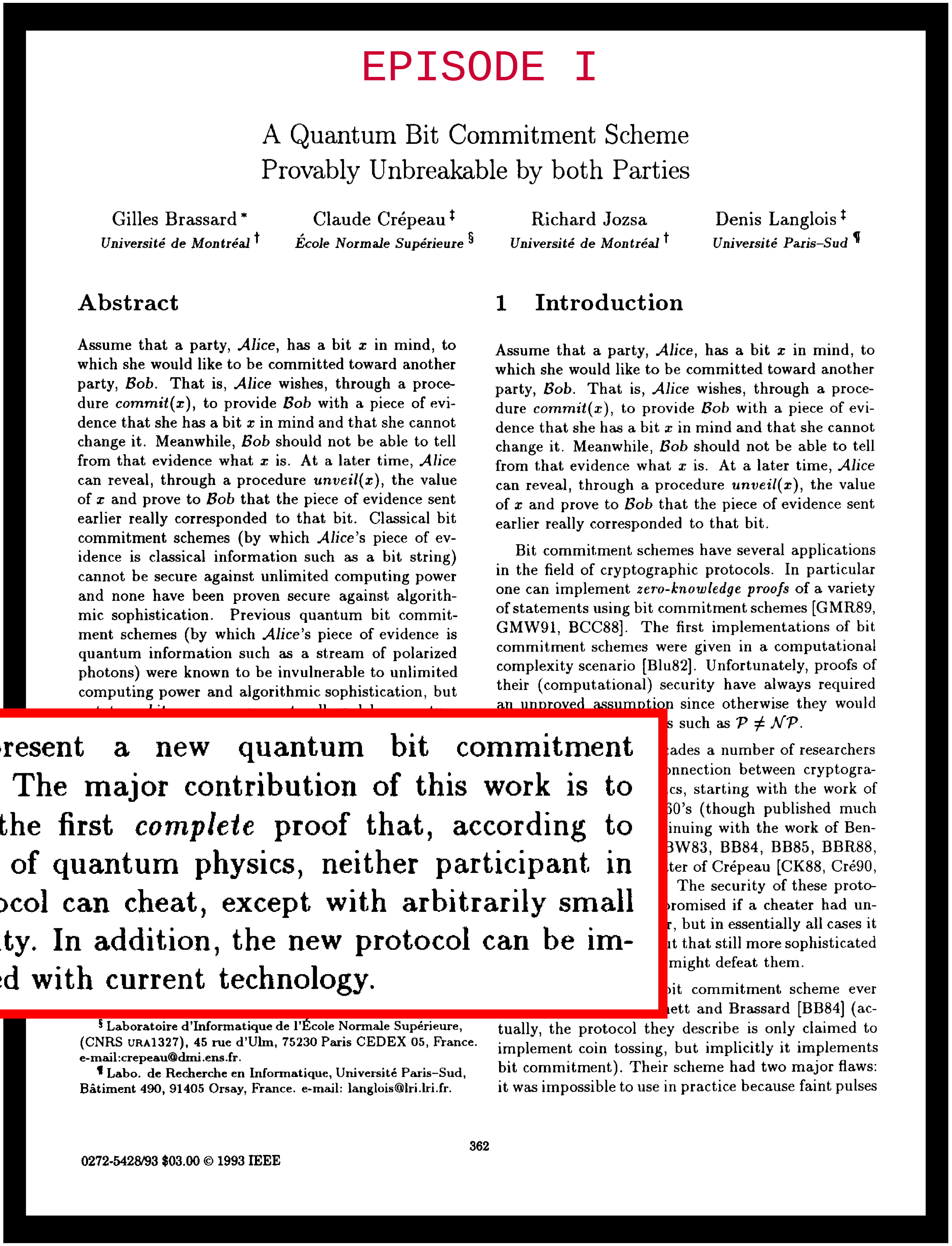
[‡] Part of this work was performed while visiting †.

[§] Laboratoire d'Informatique de l'École Normale Supérieure, (CNRS URA1327), 45 rue d'Ulm, 75230 Paris CEDEX 05, France. e-mail:crepeau@dmi.ens.fr.

[¶] Labo. de Recherche en Informatique, Université Paris–Sud, Bâtiment 490, 91405 Orsay, France. e-mail: langlois@lri.lri.fr.

0272-5428/93 $03.00 © 1993 IEEE

F O C S 1 9 9 3



EPISODE I

A Quantum Bit Commitment Scheme Provably Unbreakable by both Parties

Gilles Brassard [*] Université de Montréal [†]
Claude Crépeau [‡] École Normale Supérieure [§]
Richard Jozsa Université de Montréal [†]
Denis Langlois [‡] Université Paris–Sud [¶]

Abstract

Assume that a party, *Alice*, has a bit x in mind, to which she would like to be committed toward another party, *Bob*. That is, *Alice* wishes, through a procedure *commit*(x), to provide *Bob* with a piece of evidence that she has a bit x in mind and that she cannot change it. Meanwhile, *Bob* should not be able to tell from that evidence what x is. At a later time, *Alice* can reveal, through a procedure *unveil*(x), the value of x and prove to *Bob* that the piece of evidence sent earlier really corresponded to that bit. Classical bit commitment schemes (by which *Alice*'s piece of evidence is classical information such as a bit string) cannot be secure against unlimited computing power and none have been proven secure against algorithmic sophistication. Previous quantum bit commitment schemes (by which *Alice*'s piece of evidence is quantum information such as a stream of polarized photons) were known to be invulnerable to unlimited computing power and algorithmic sophistication, but

We present a new quantum bit commitment scheme. The major contribution of this work is to provide the first *complete* proof that, according to the laws of quantum physics, neither participant in the protocol can cheat, except with arbitrarily small probability. In addition, the new protocol can be implemented with current technology.

1 Introduction

Assume that a party, *Alice*, has a bit x in mind, to which she would like to be committed toward another party, *Bob*. That is, *Alice* wishes, through a procedure *commit*(x), to provide *Bob* with a piece of evidence that she has a bit x in mind and that she cannot change it. Meanwhile, *Bob* should not be able to tell from that evidence what x is. At a later time, *Alice* can reveal, through a procedure *unveil*(x), the value of x and prove to *Bob* that the piece of evidence sent earlier really corresponded to that bit.

Bit commitment schemes have several applications in the field of cryptographic protocols. In particular one can implement *zero-knowledge proofs* of a variety of statements using bit commitment schemes [GMR89, GMW91, BCC88]. The first implementations of bit commitment schemes were given in a computational complexity scenario [Blu82]. Unfortunately, proofs of their (computational) security have always required an unproved assumption since otherwise they would
s such as $\mathcal{P} \neq \mathcal{NP}$.

ades a number of researchers
nnection between cryptogra-
cs, starting with the work of
60's (though published much
inuing with the work of Ben-
BW83, BB84, BB85, BBR88,
ter of Crépeau [CK88, Cré90,
The security of these proto-
promised if a cheater had un-
r, but in essentially all cases it
it that still more sophisticated
might defeat them.

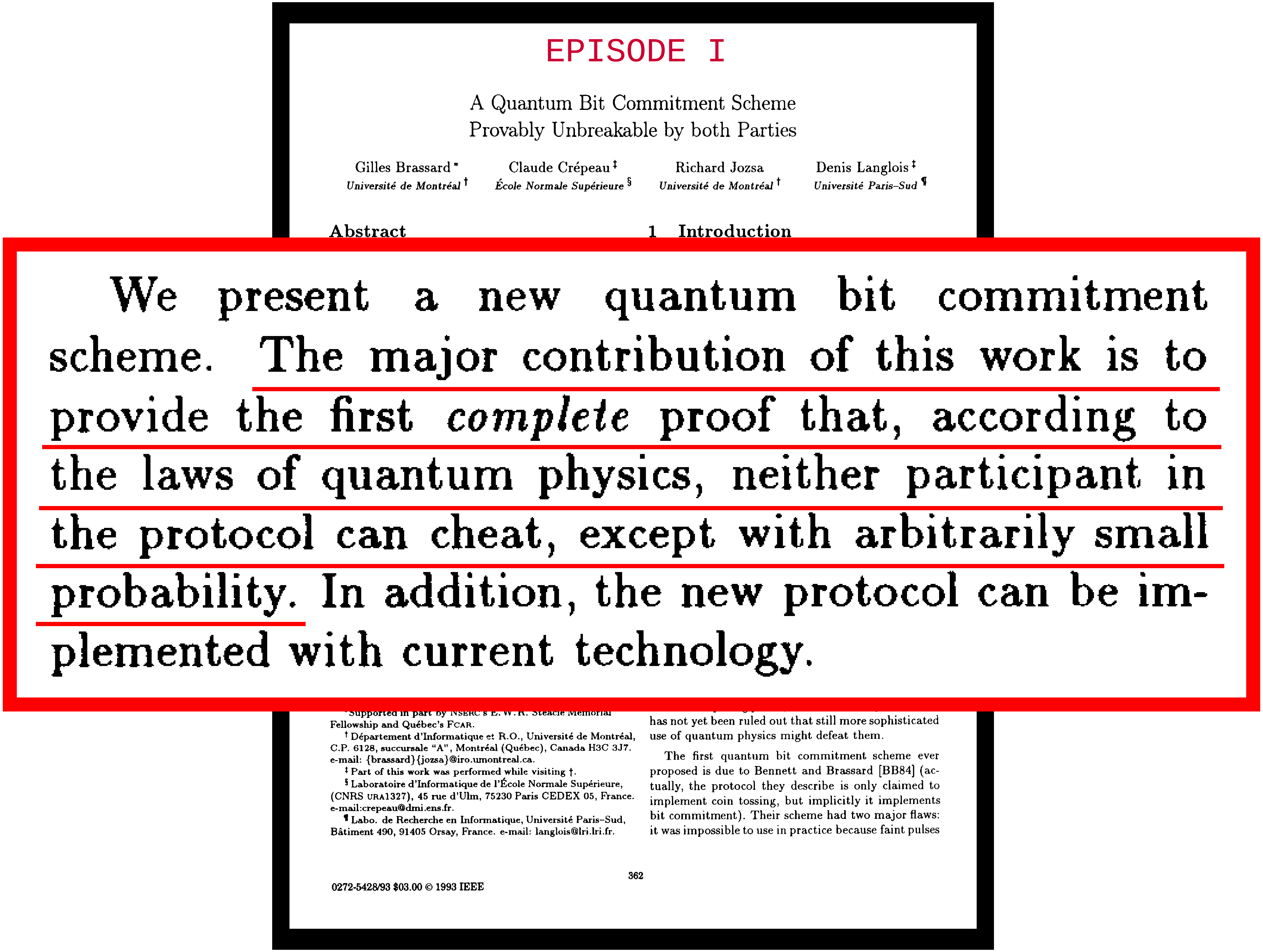
bit commitment scheme ever
nett and Brassard [BB84] (actually, the protocol they describe is only claimed to implement coin tossing, but implicitly it implements bit commitment). Their scheme had two major flaws: it was impossible to use in practice because faint pulses

[§] Laboratoire d'Informatique de l'École Normale Supérieure, (CNRS URA1327), 45 rue d'Ulm, 75230 Paris CEDEX 05, France. e-mail:crepeau@dmi.ens.fr.

[¶] Labo. de Recherche en Informatique, Université Paris–Sud, Bâtiment 490, 91405 Orsay, France. e-mail: langlois@lri.lri.fr.

0272-5428/93 $03.00 © 1993 IEEE

F O C S 1 9 9 3



EPISODE I

A Quantum Bit Commitment Scheme Provably Unbreakable by both Parties

Gilles Brassard[*] Université de Montréal[†]
Claude Crépeau[‡] École Normale Supérieure[§]
Richard Jozsa Université de Montréal[†]
Denis Langlois[‡] Université Paris–Sud[¶]

Abstract

We present a new quantum bit commitment scheme. The major contribution of this work is to provide the first *complete* proof that, according to the laws of quantum physics, neither participant in the protocol can cheat, except with arbitrarily small probability. In addition, the new protocol can be implemented with current technology.

1 Introduction

has not yet been ruled out that still more sophisticated use of quantum physics might defeat them.

The first quantum bit commitment scheme ever proposed is due to Bennett and Brassard [BB84] (actually, the protocol they describe is only claimed to implement coin tossing, but implicitly it implements bit commitment). Their scheme had two major flaws: it was impossible to use in practice because faint pulses

[*] Supported in part by NSERC's E. W. R. Steacie Memorial Fellowship and Québec's FCAR.

[†] Département d'Informatique et R.O., Université de Montréal, C.P. 6128, succursale "A", Montréal (Québec), Canada H3C 3J7. e-mail: {brassard}{jozsa}@iro.umontreal.ca.

[‡] Part of this work was performed while visiting †.

[§] Laboratoire d'Informatique de l'École Normale Supérieure, (CNRS URA1327), 45 rue d'Ulm, 75230 Paris CEDEX 05, France. e-mail:crepeau@dmi.ens.fr.

[¶] Labo. de Recherche en Informatique, Université Paris–Sud, Bâtiment 490, 91405 Orsay, France. e-mail: langlois@lri.lri.fr.

362

0272-5428/93 $03.00 © 1993 IEEE

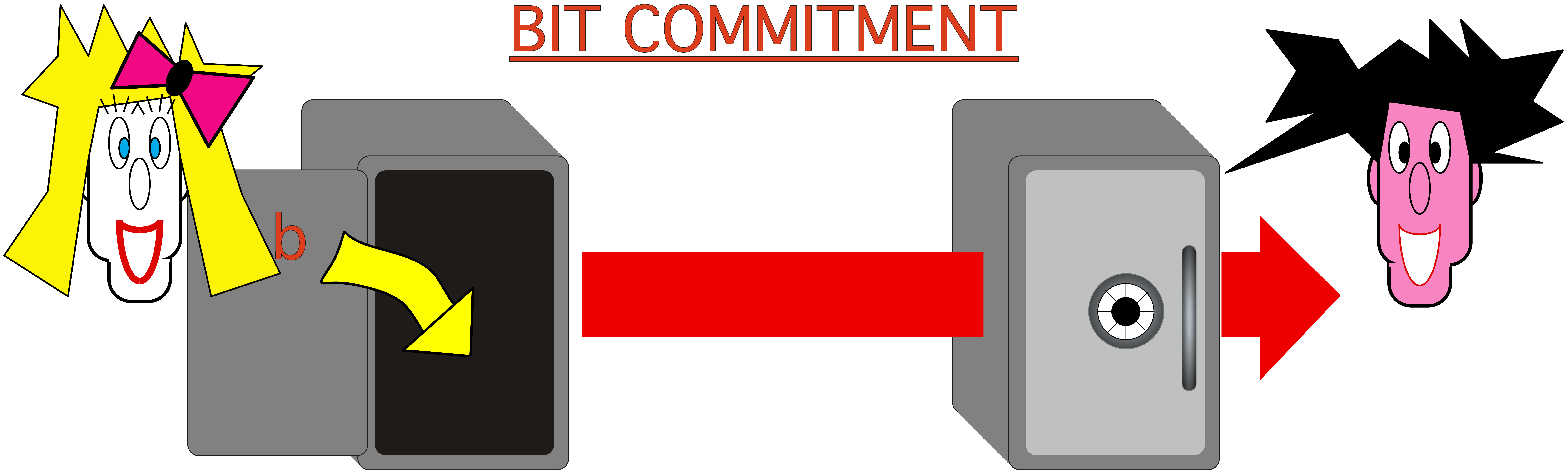
Yoda said:

“Happens to every guy sometimes

. this does”

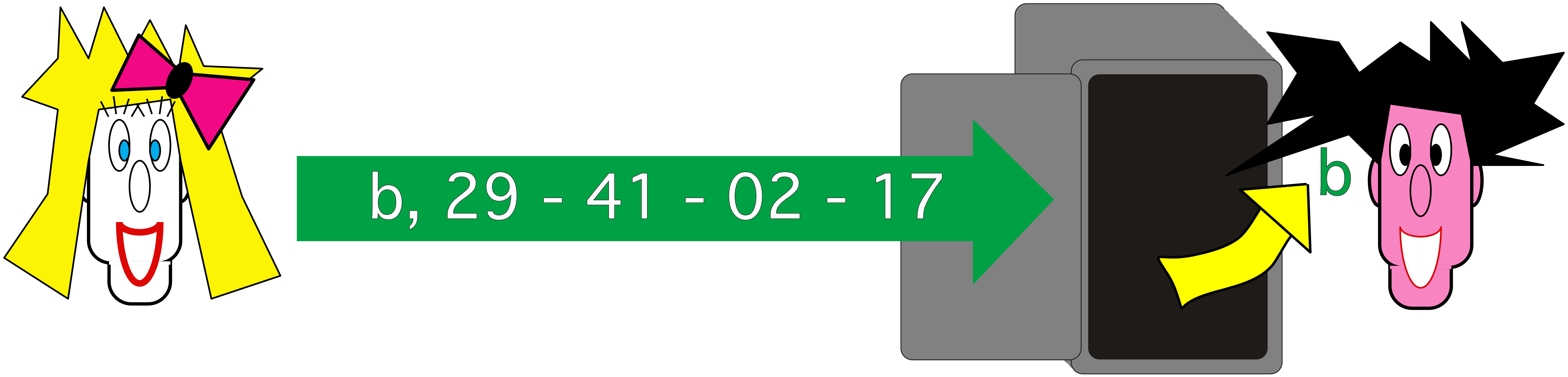
(1) two-party Cryptographic Protocols

BIT COMMITMENT

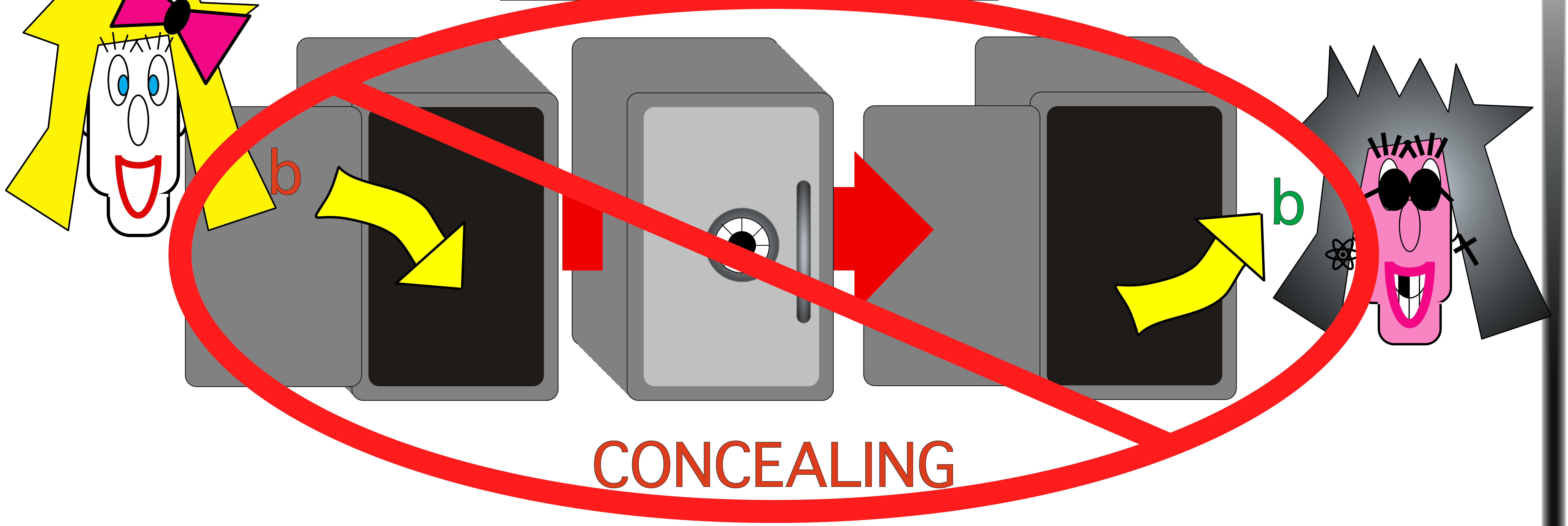


COMMIT

UNVEIL

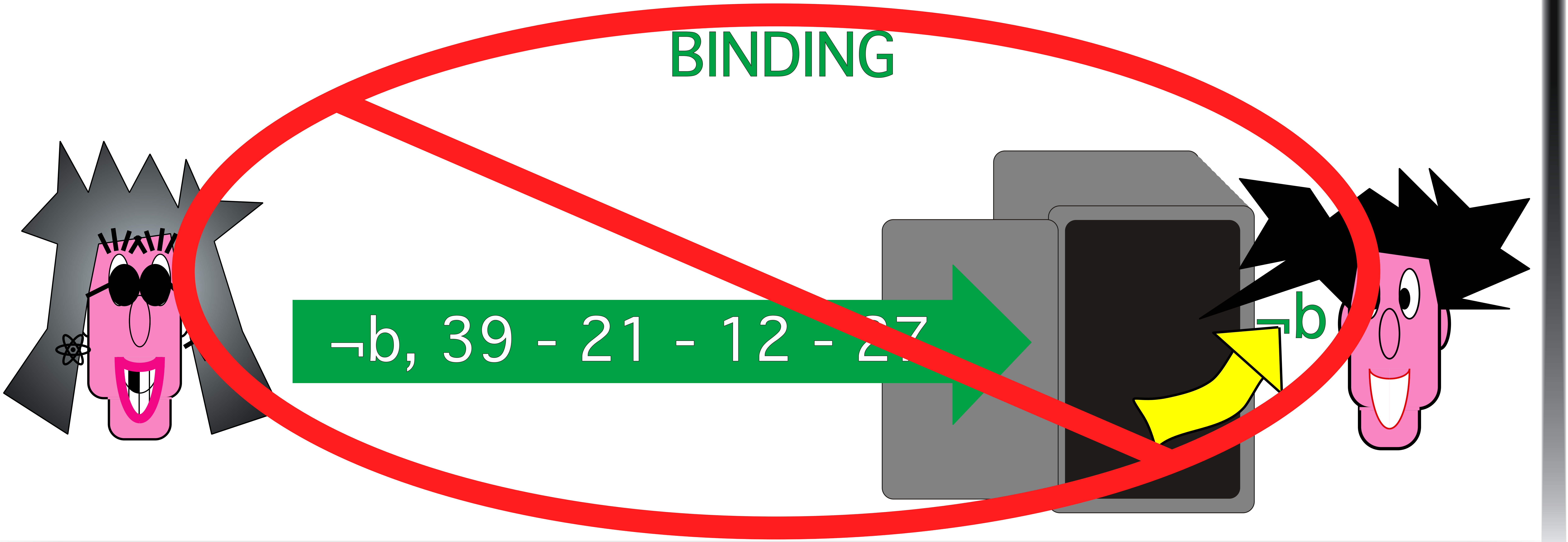


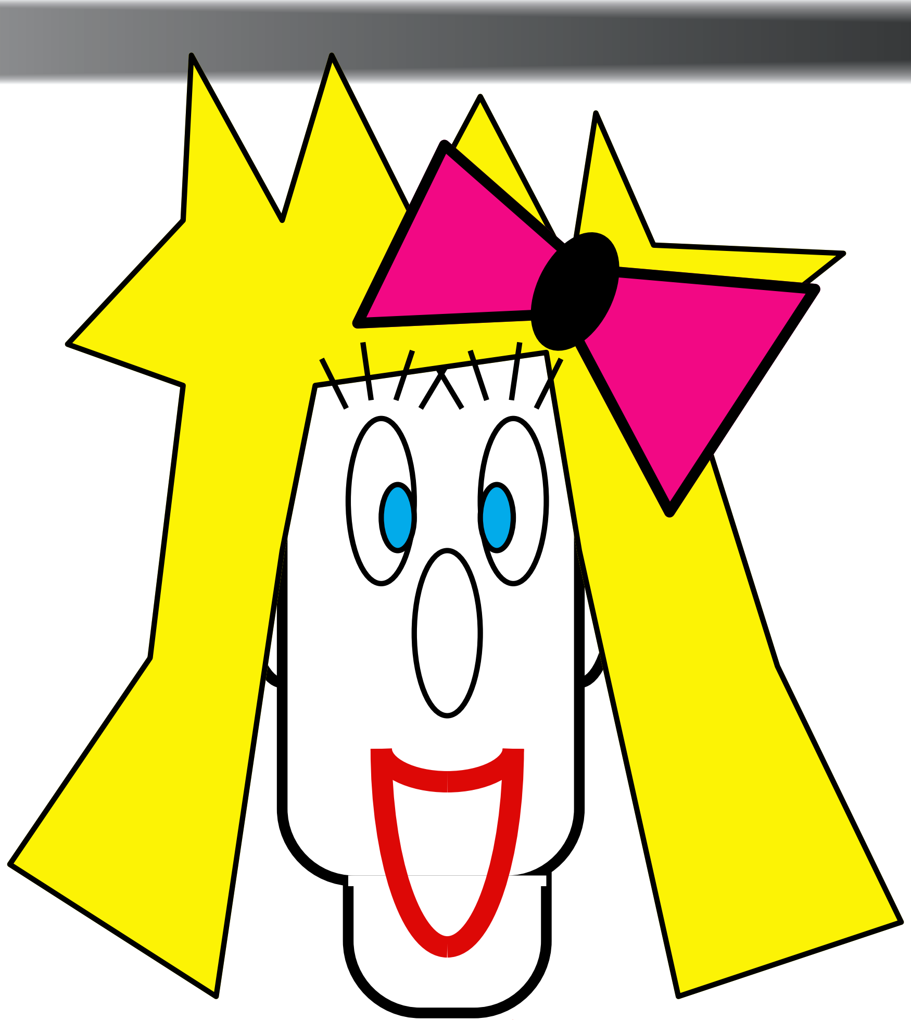
BIT COMMITMENT



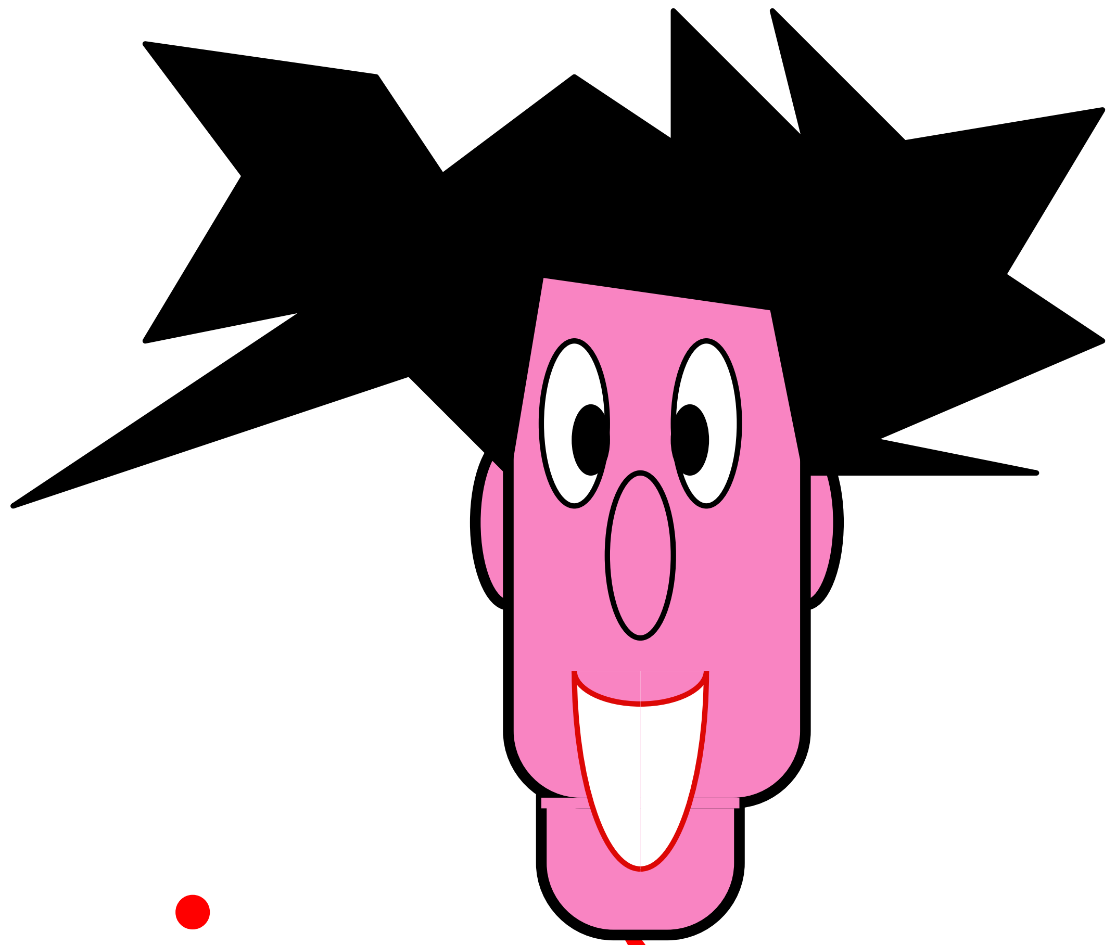
CONCEALING

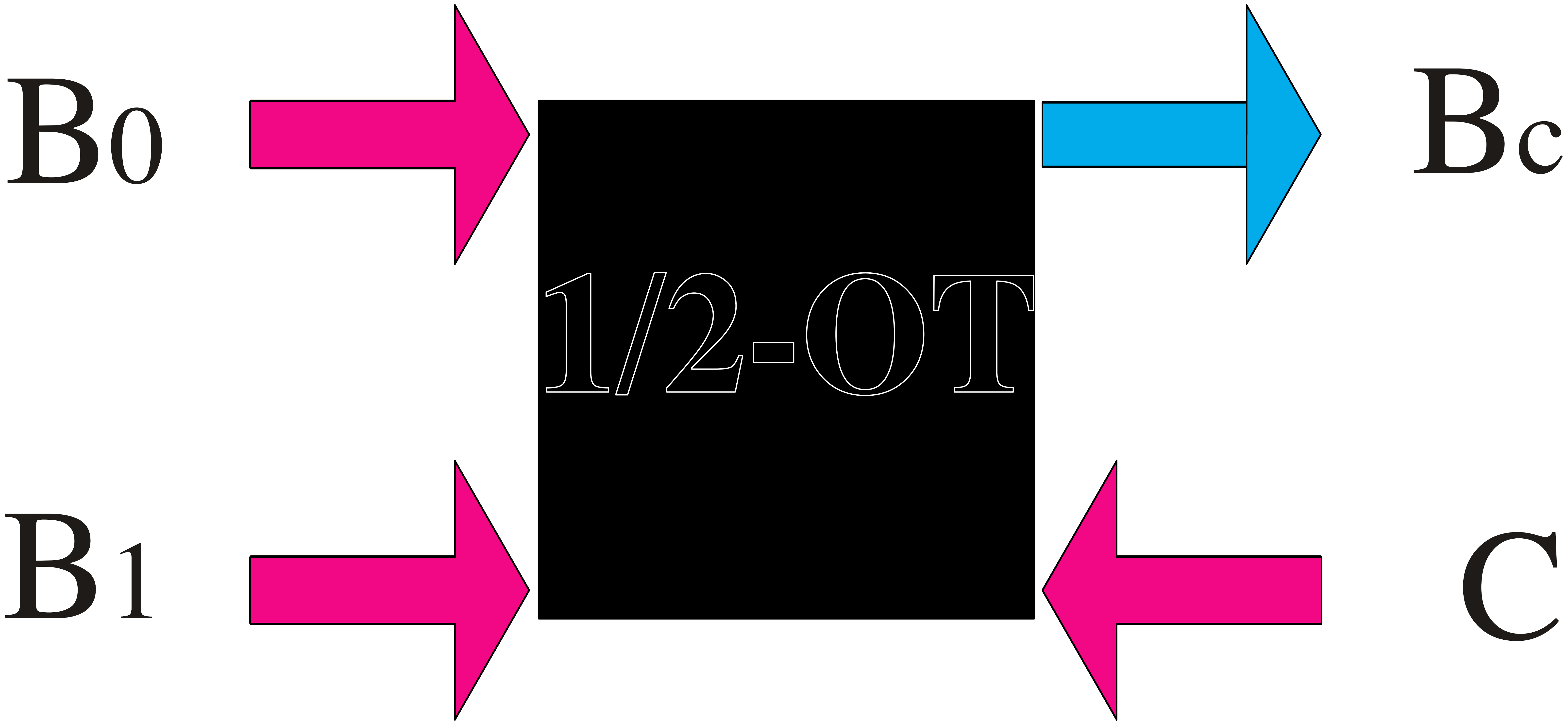
BINDING

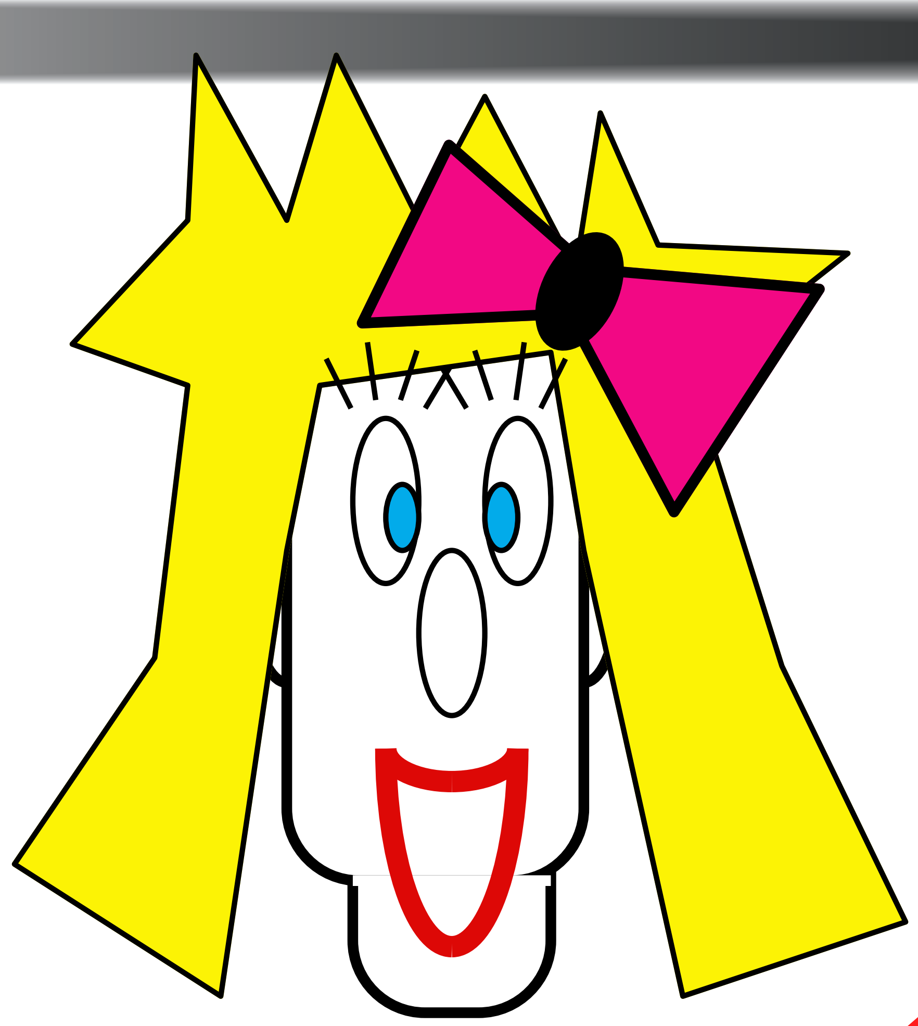




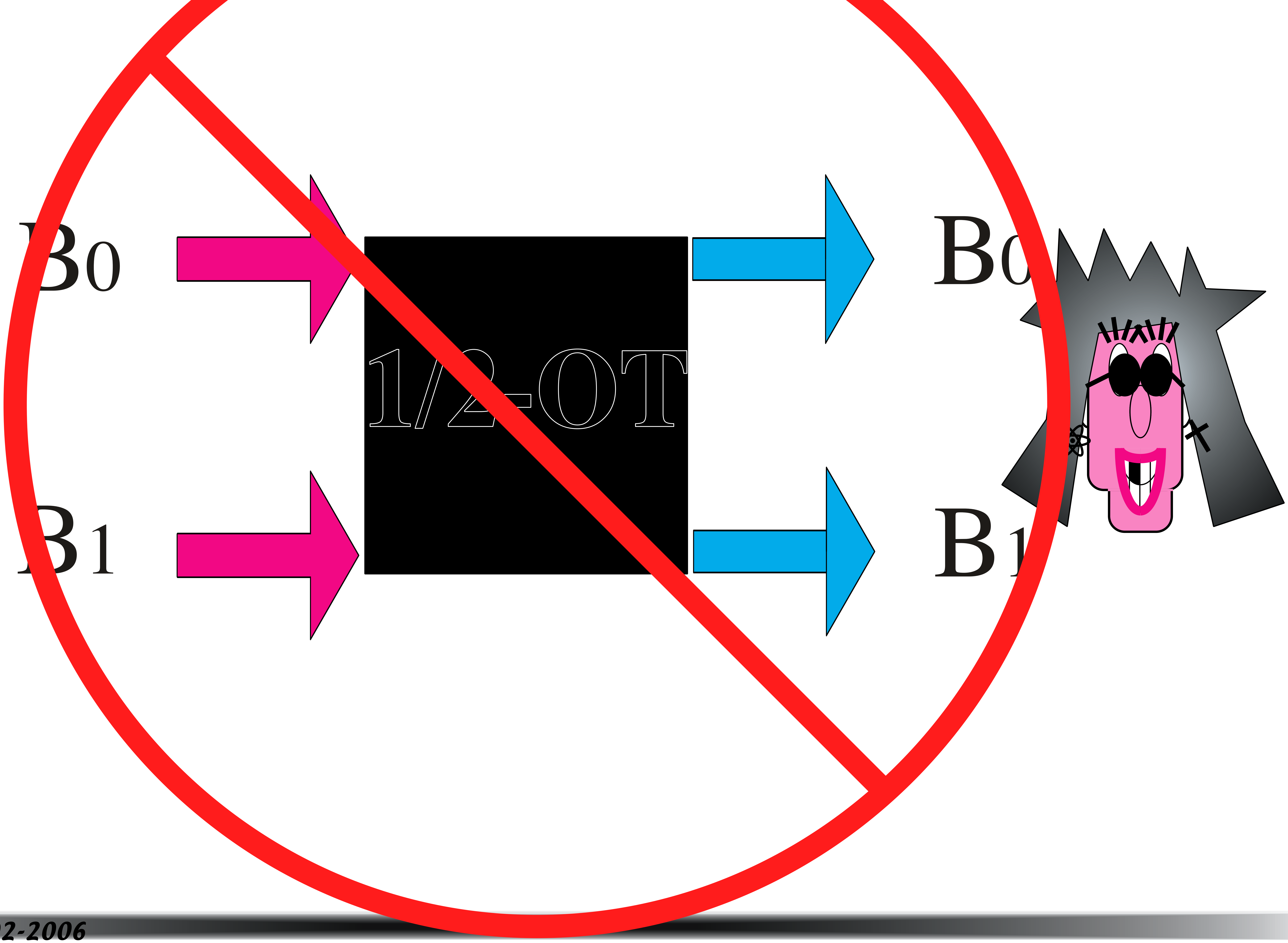
Oblivious Transfer (message multiplexing)



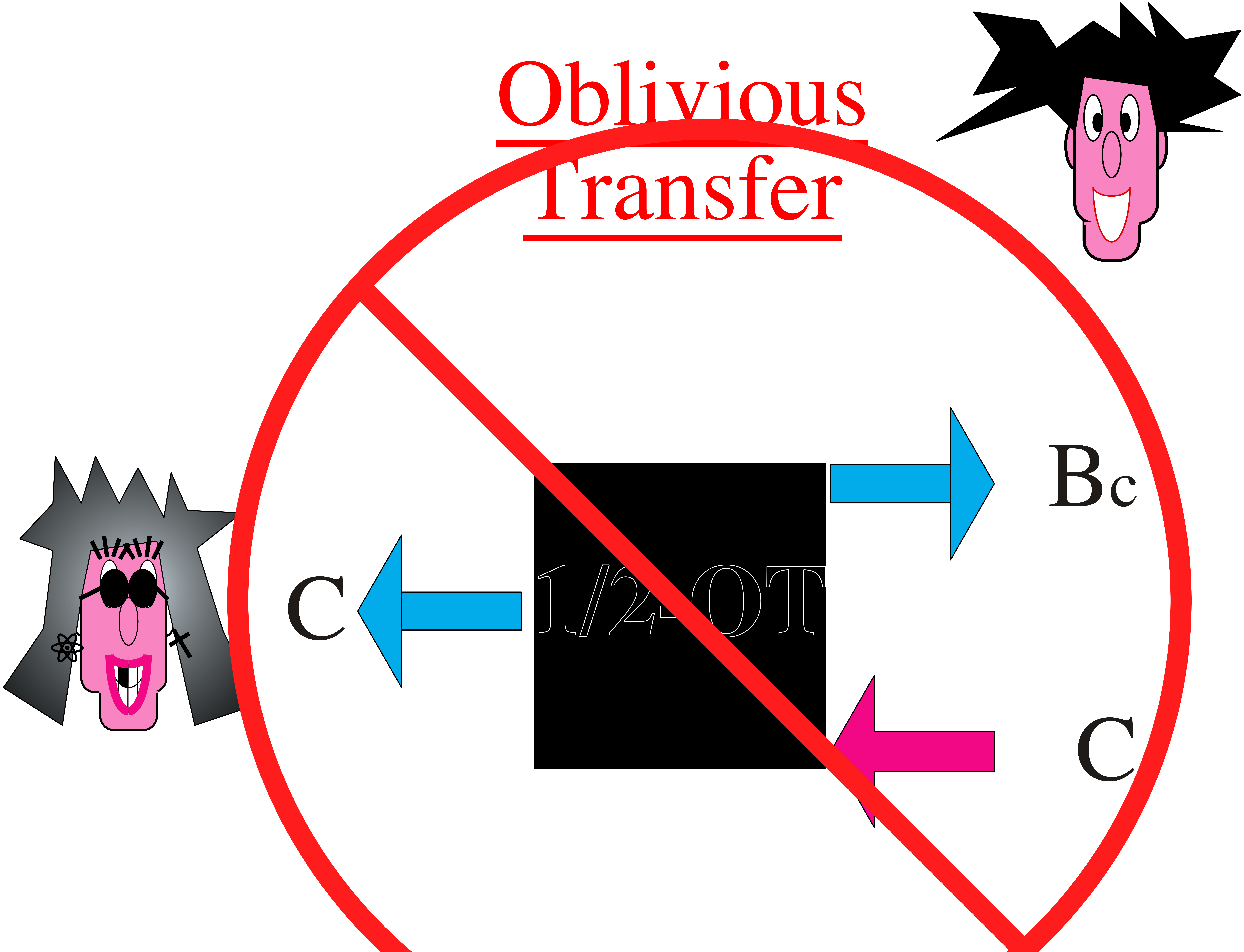


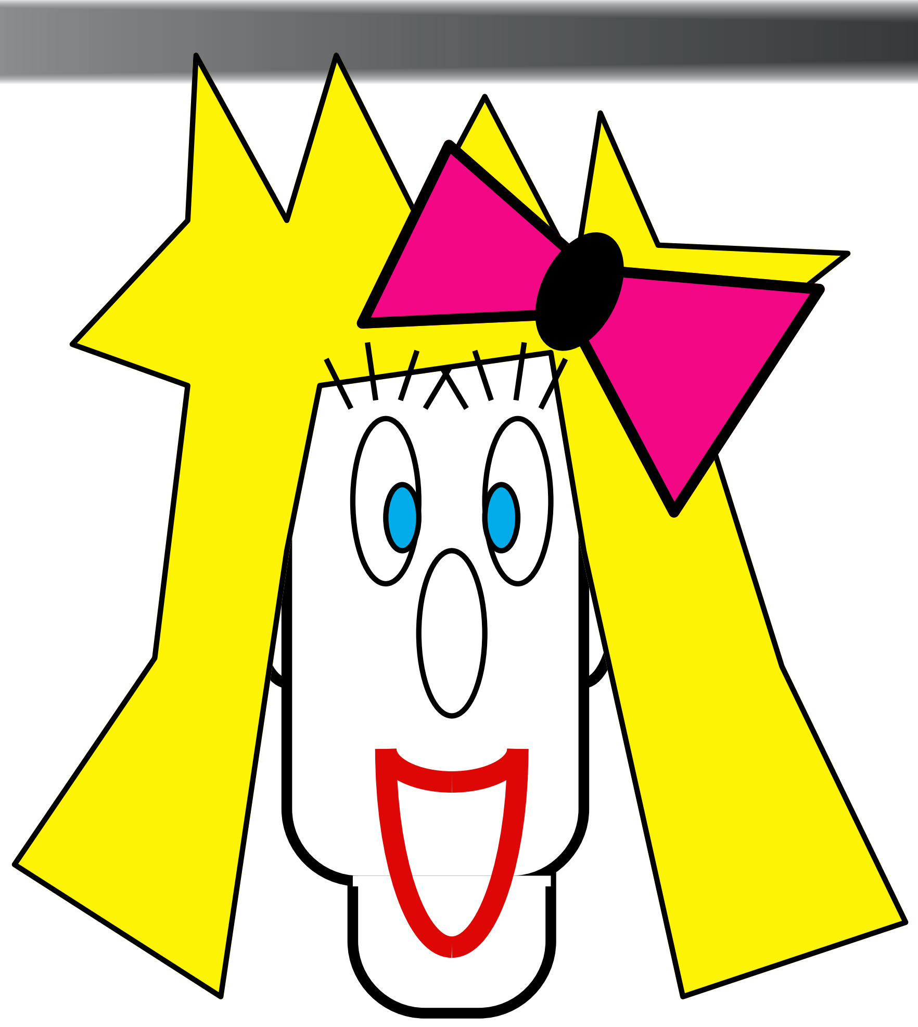


Oblivious Transfer

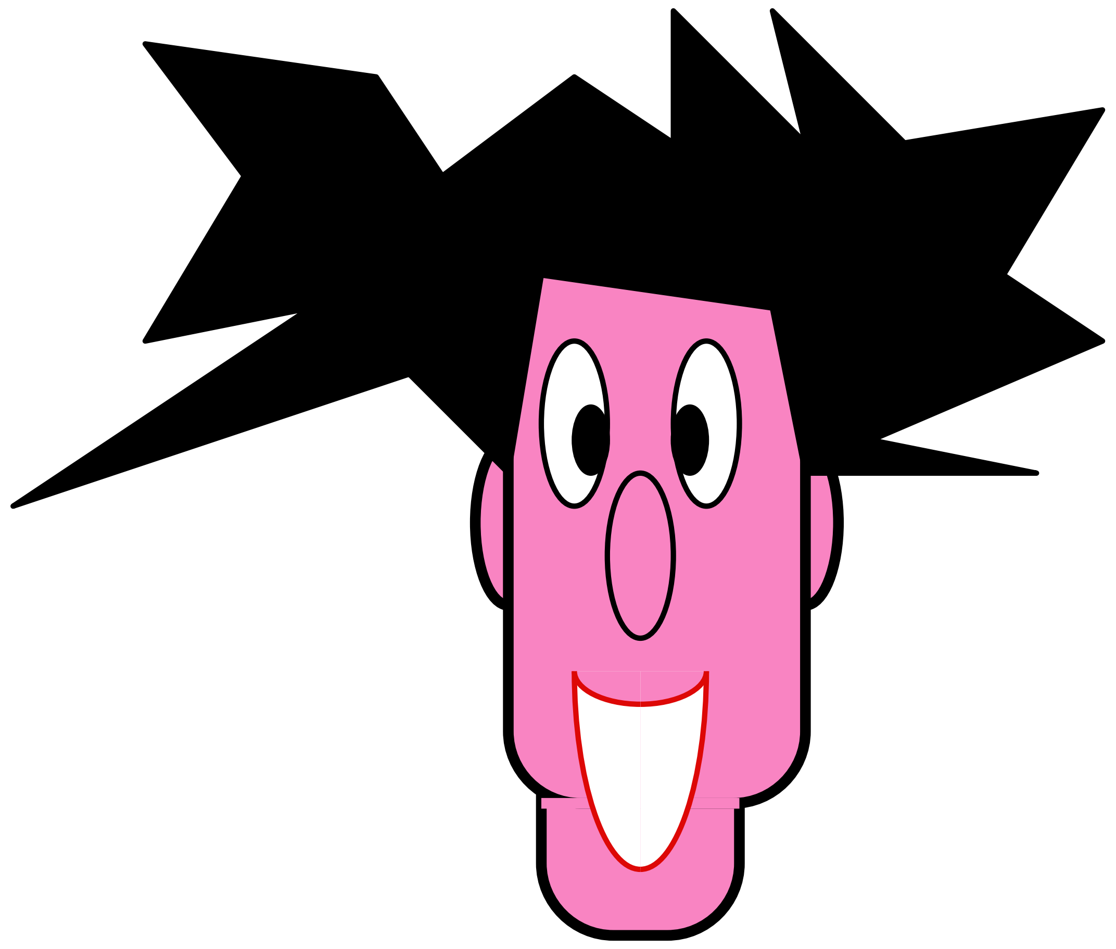


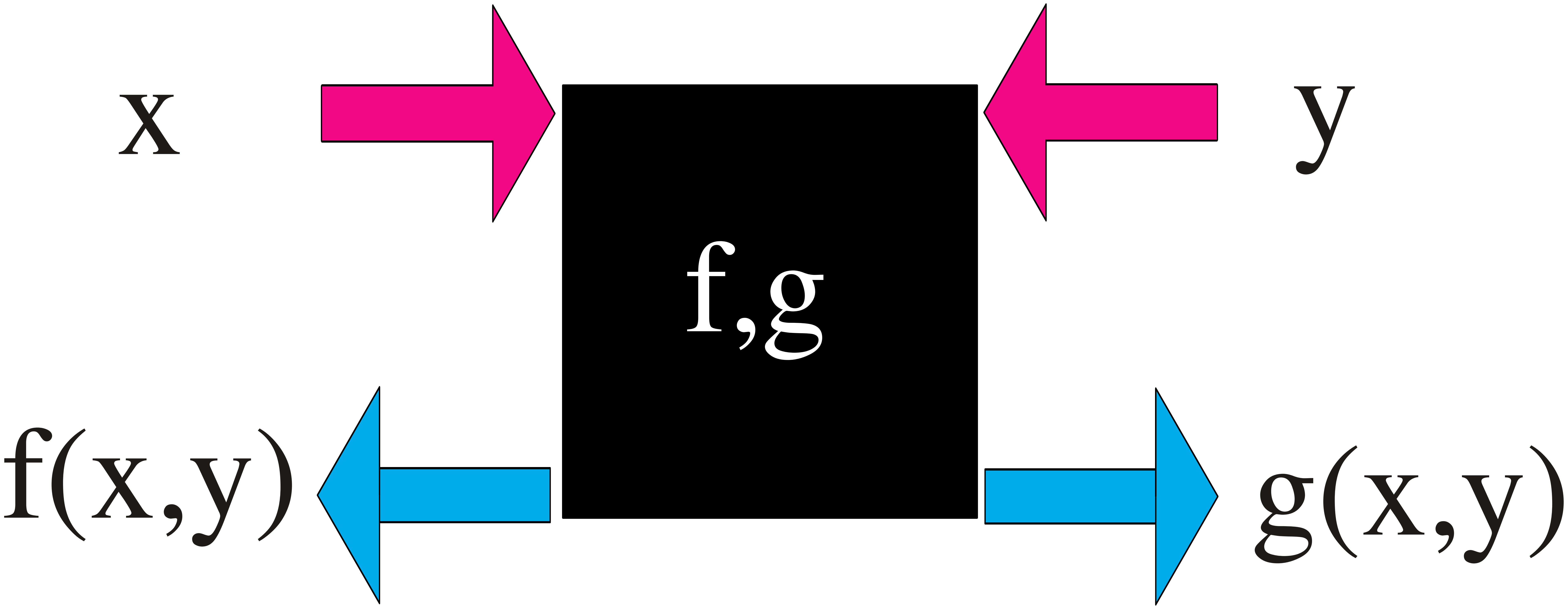
Oblivious Transfer





Oblivious Function Evaluation





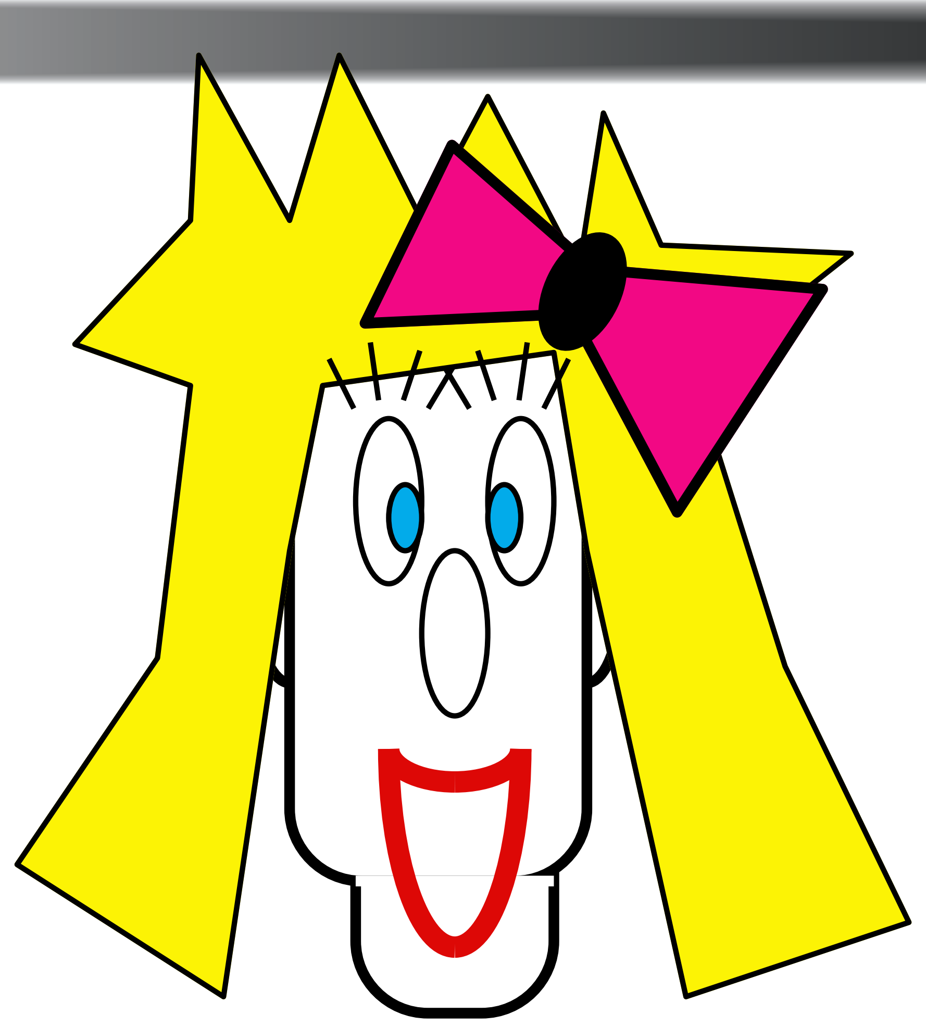
x

y

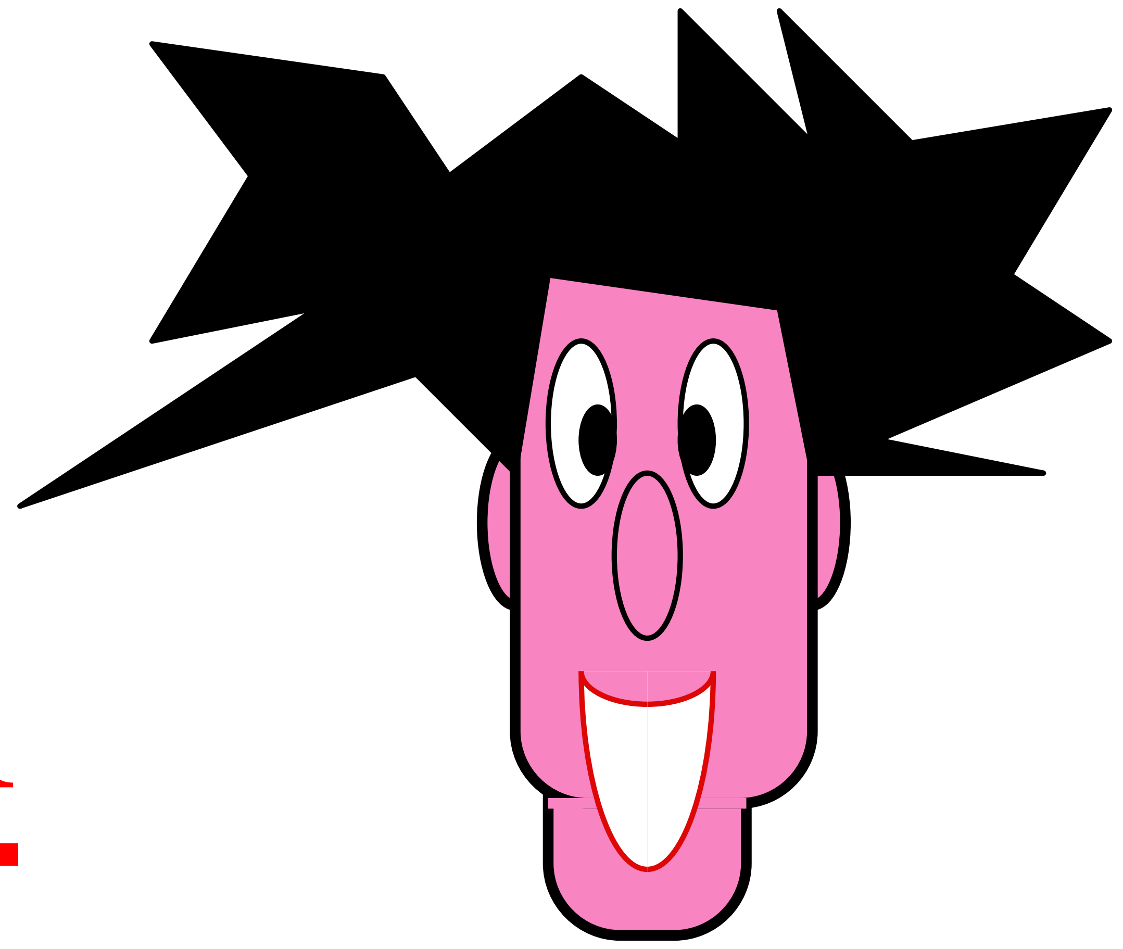
f,g

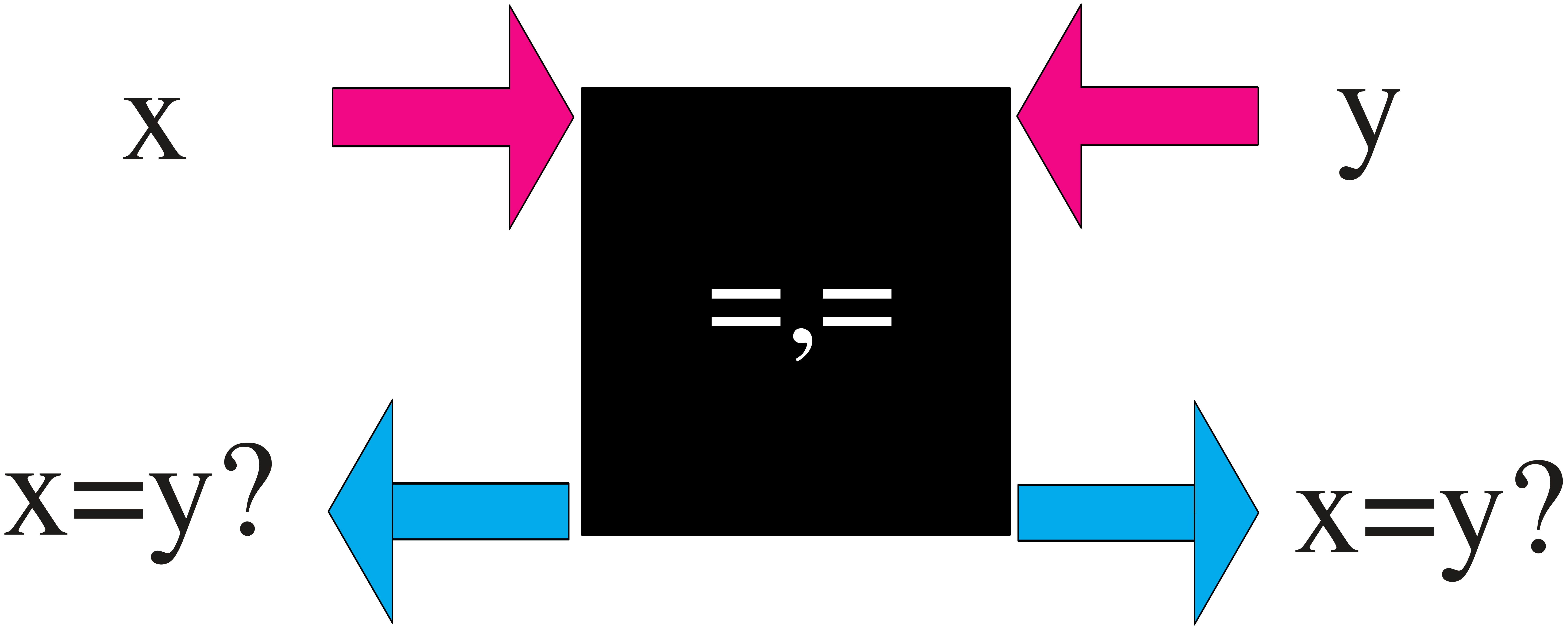
$f(x,y)$

$g(x,y)$



Mutual Identification





x

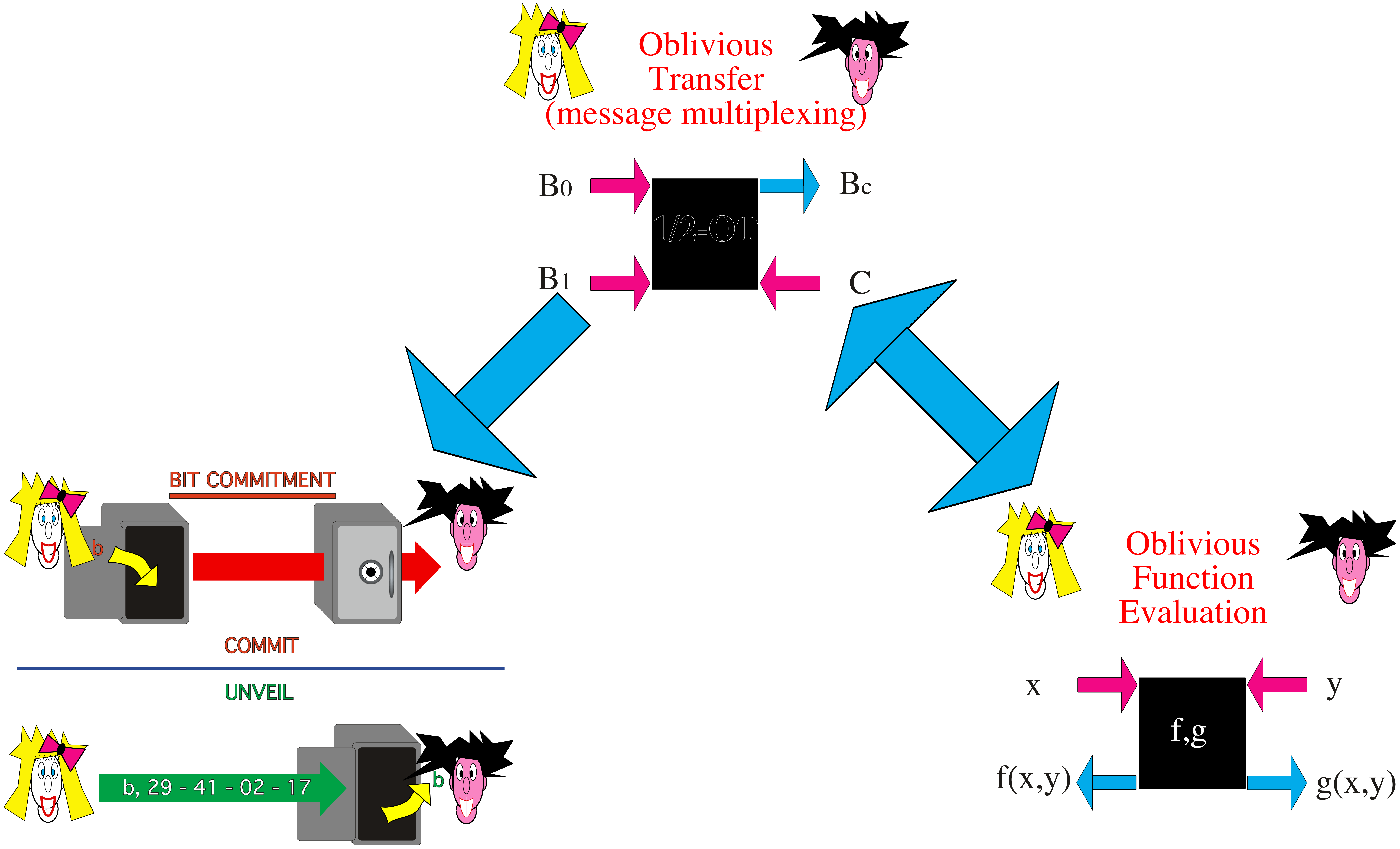
y

=,=

x=y?

x=y?

Classically



Oblivious Transfer (message multiplexing)

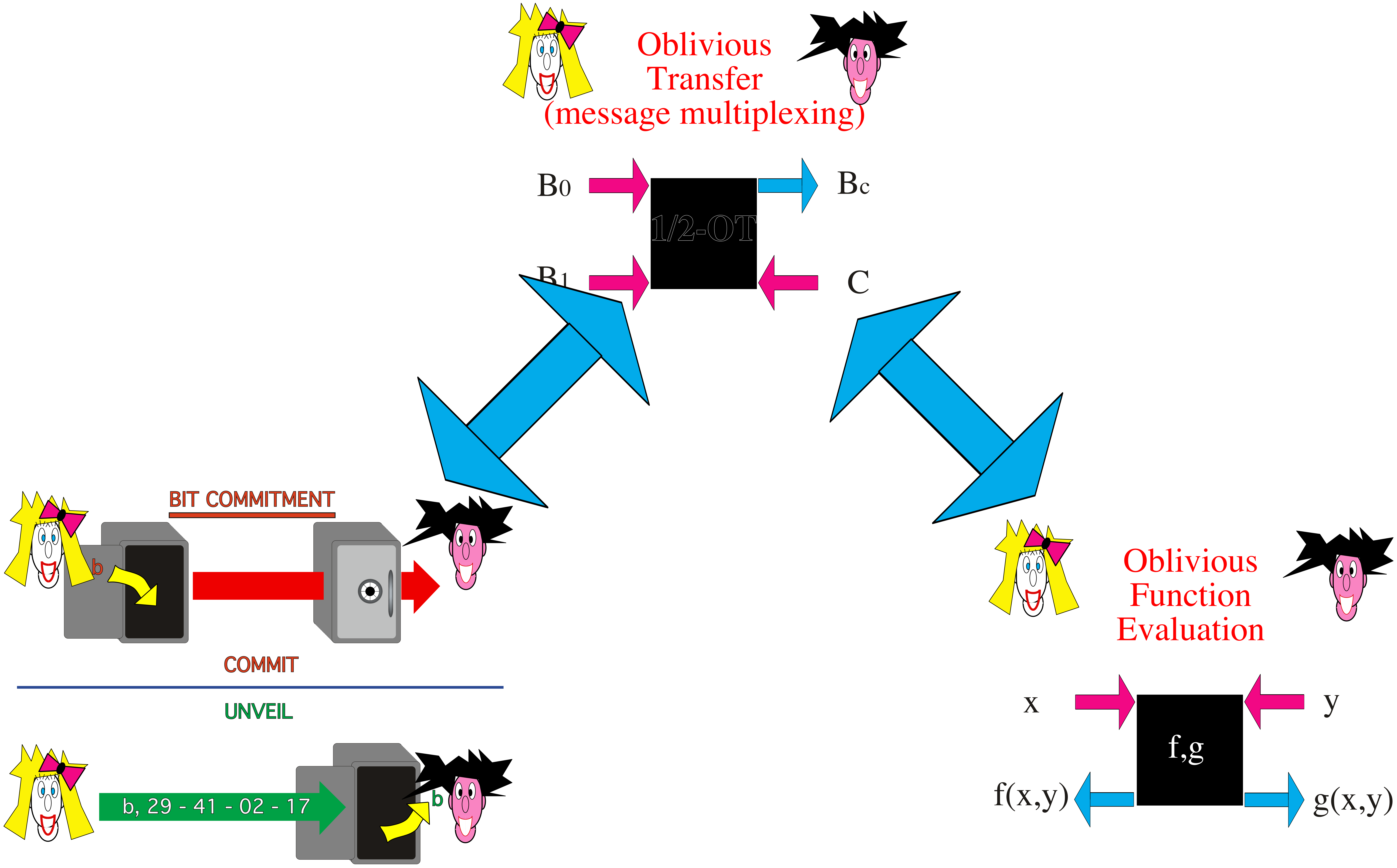
BIT COMMITMENT

COMMIT

UNVEIL

Oblivious Function Evaluation

Quantumly



Oblivious Transfer (message multiplexing)

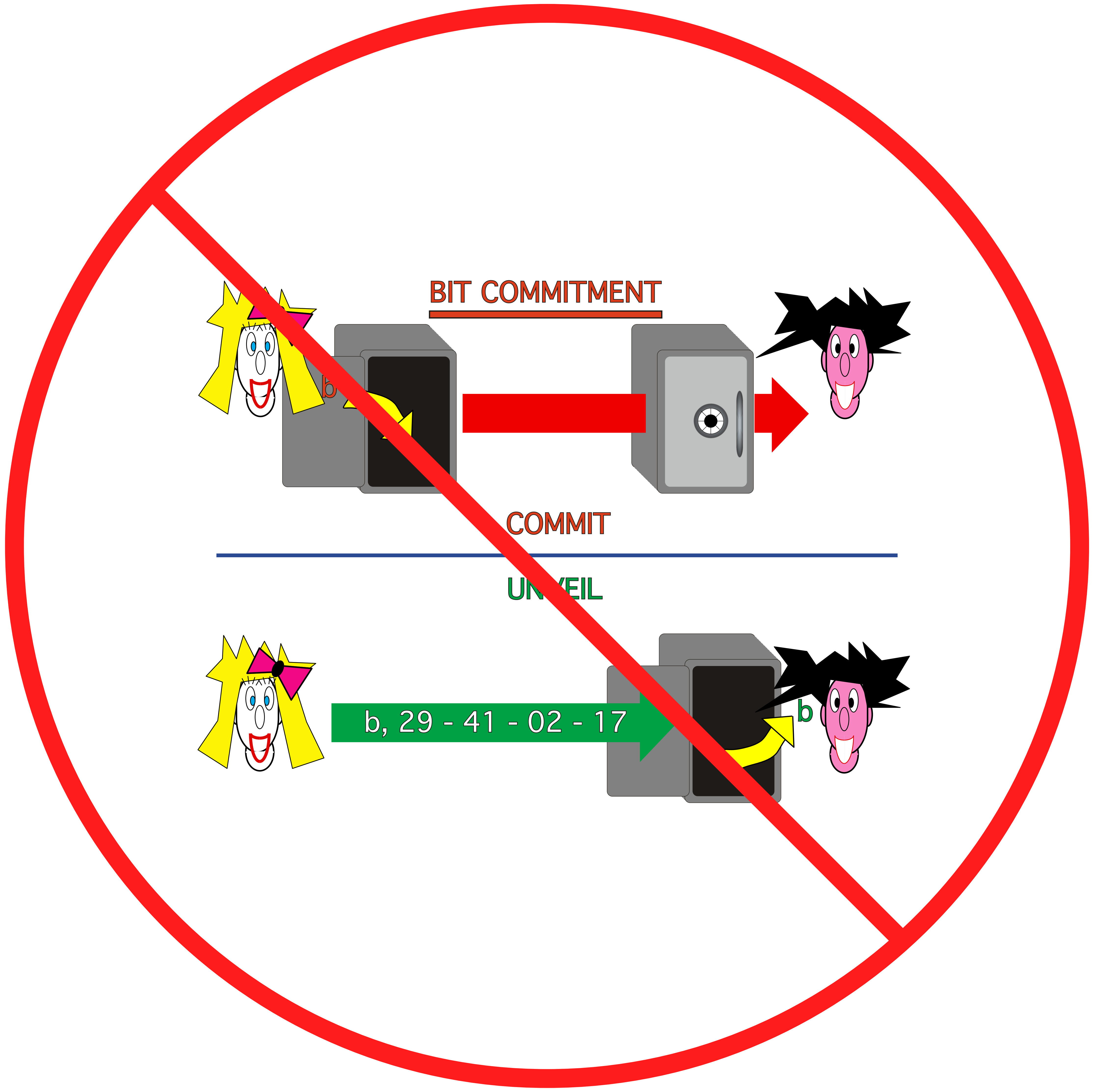
BIT COMMITMENT

COMMIT

UNVEIL

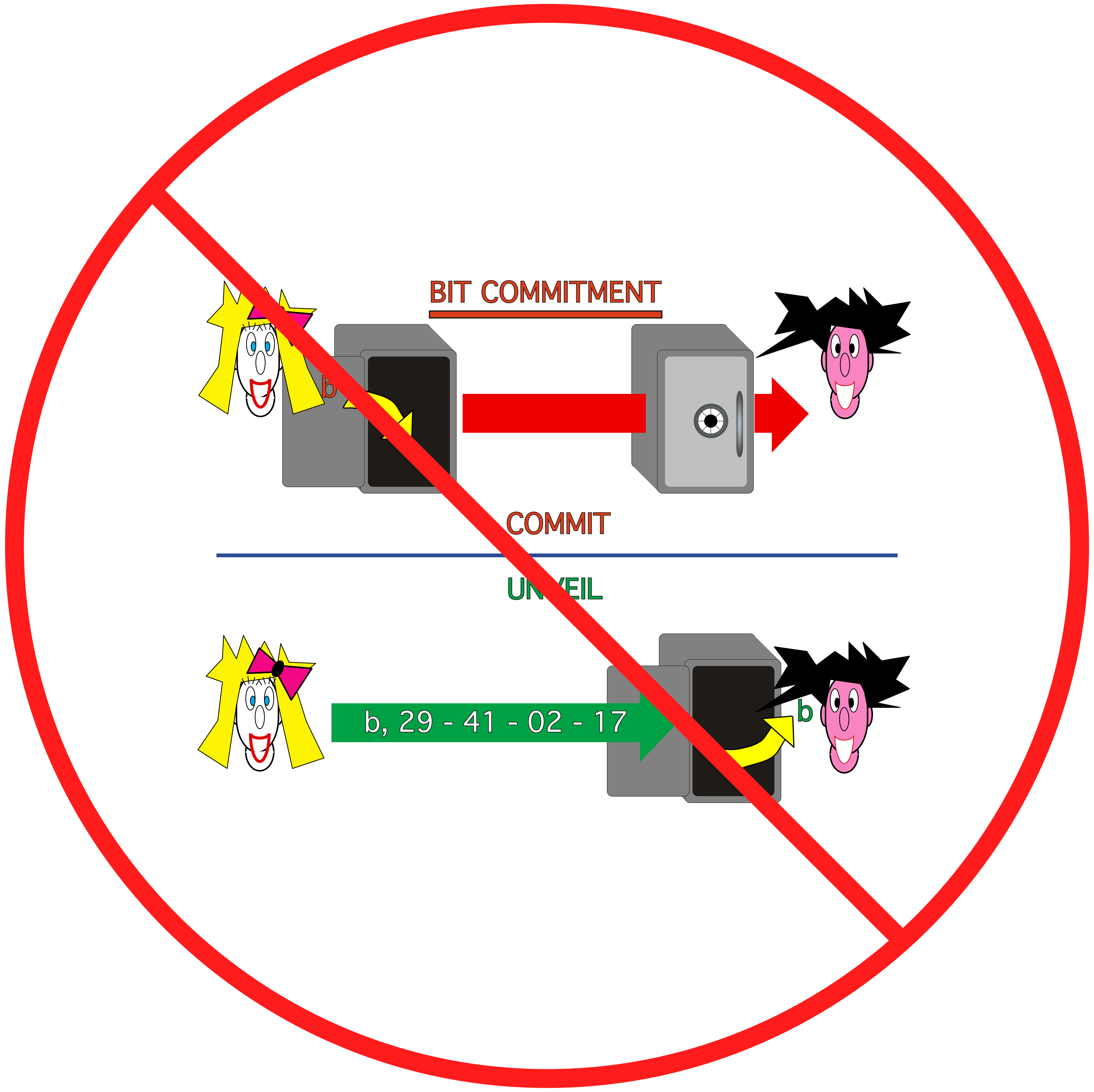
Oblivious Function Evaluation

Classically



Folklore

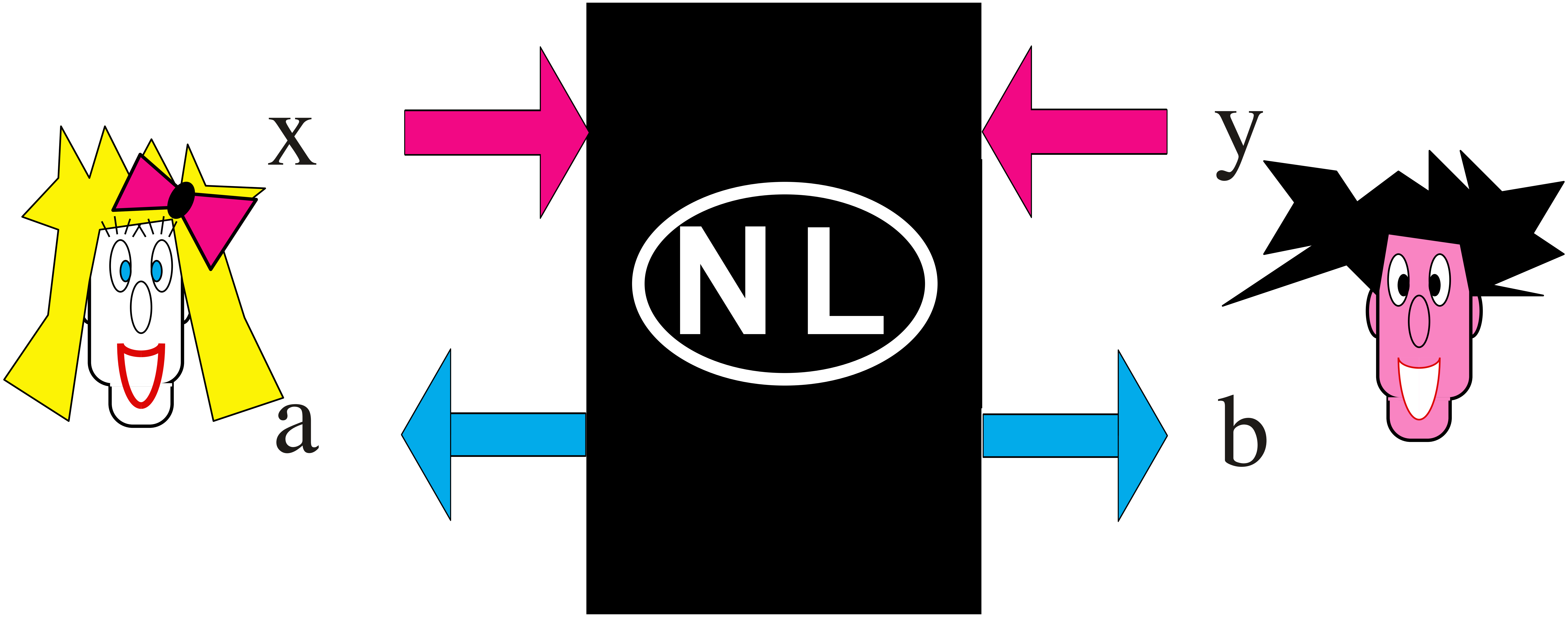
Quantumly



Mayers, Lo-Chau

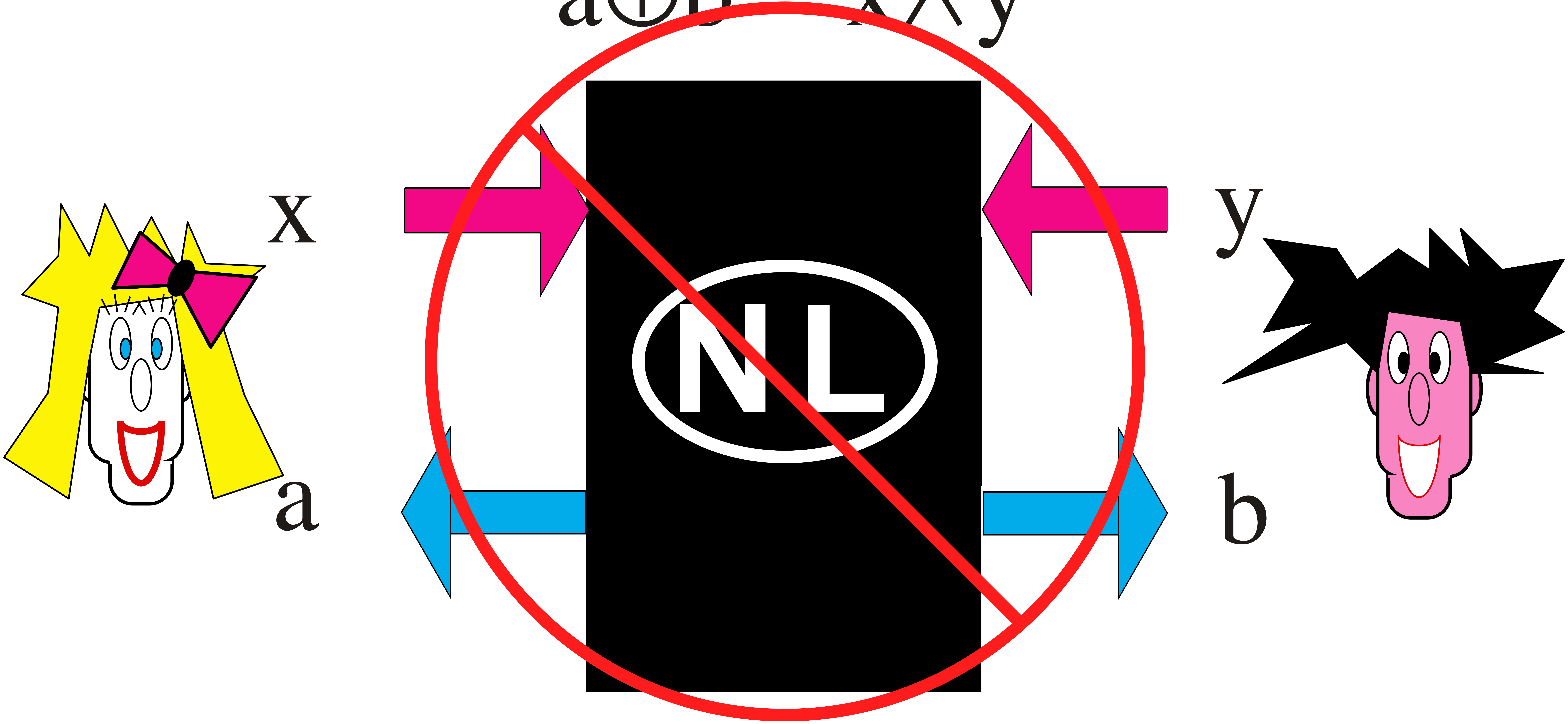
Non-Locality Box

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



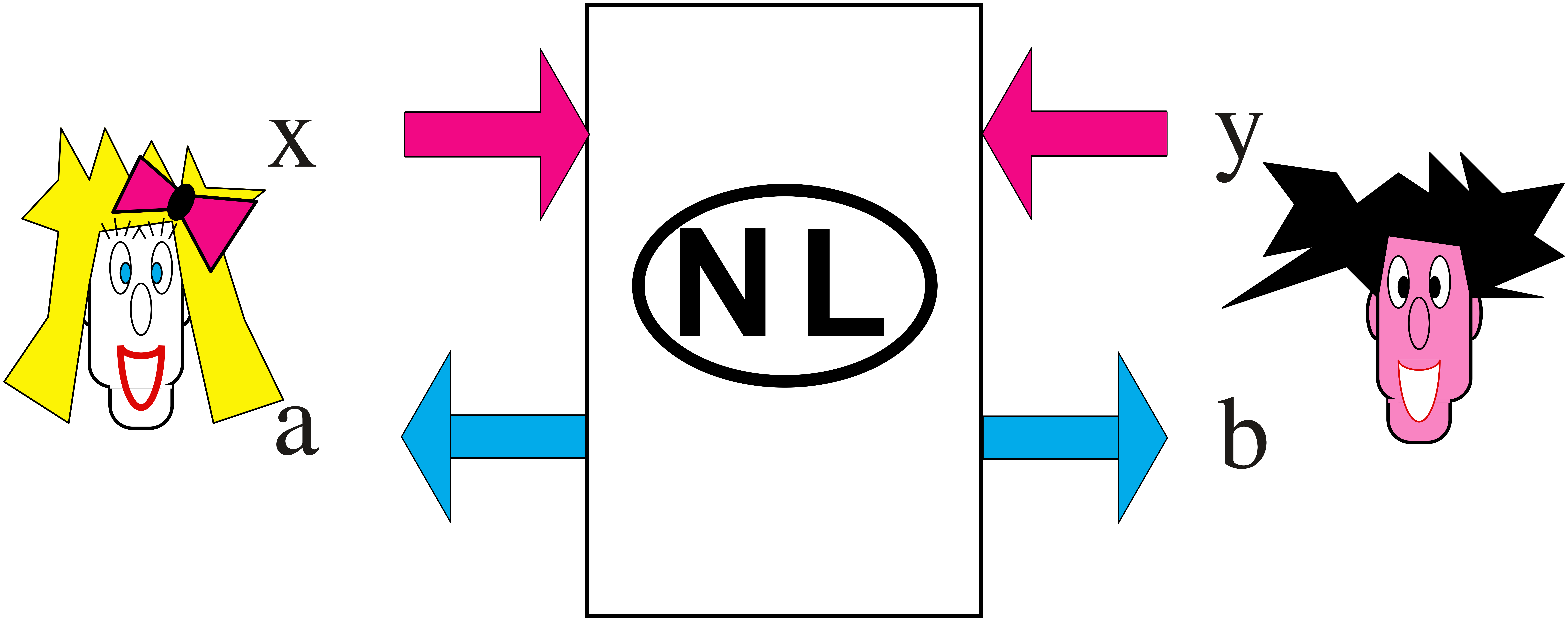
Non-Locality Box

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



Non-Locality Box

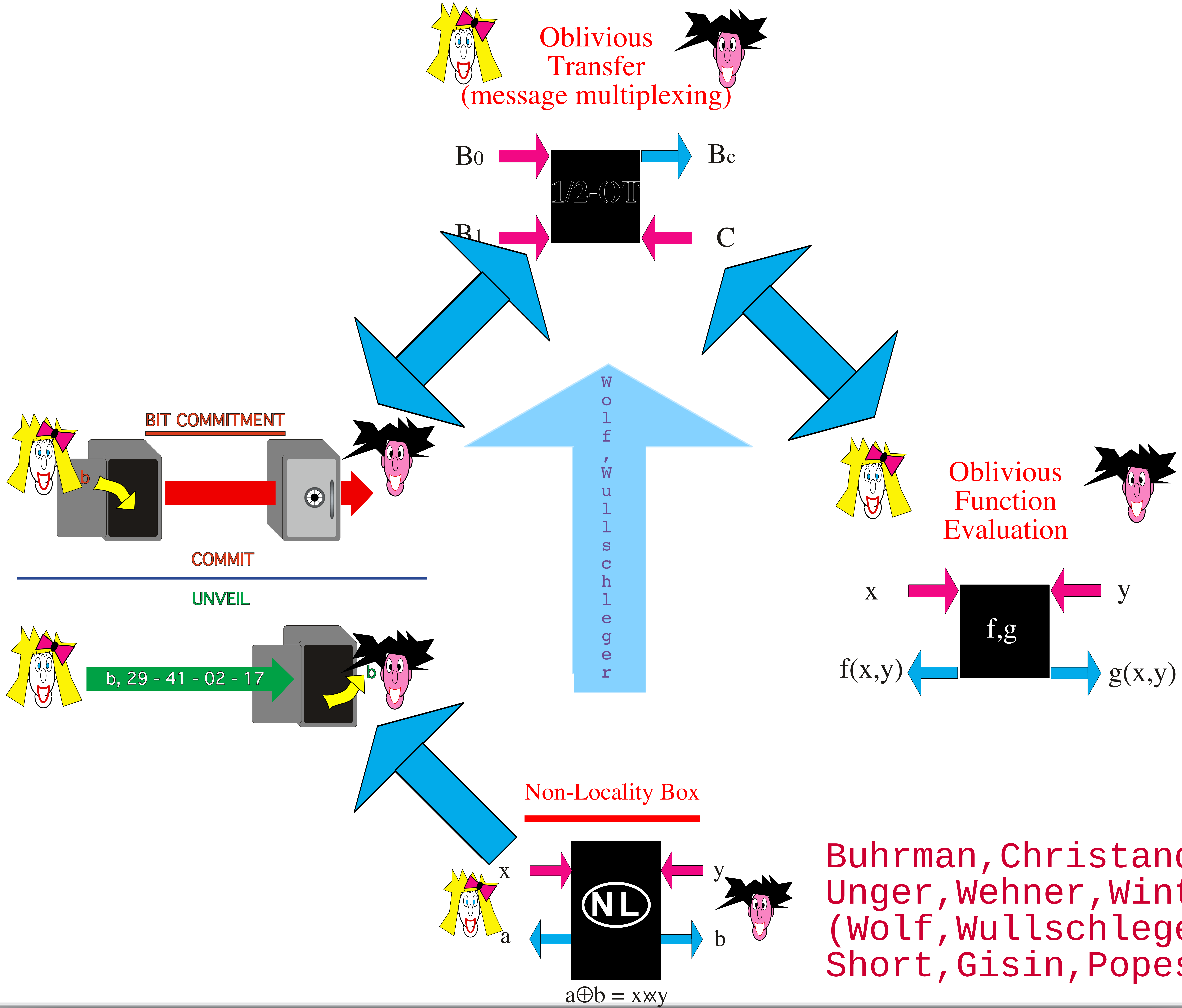
$$\Pr[a \oplus b = x \wedge y] < 1$$



Classical: $\Pr[\ldots] = 75\%$.

Quantum: $\Pr[\ldots] = \cos^2(\pi/8) \approx 85\%$

Quantumly



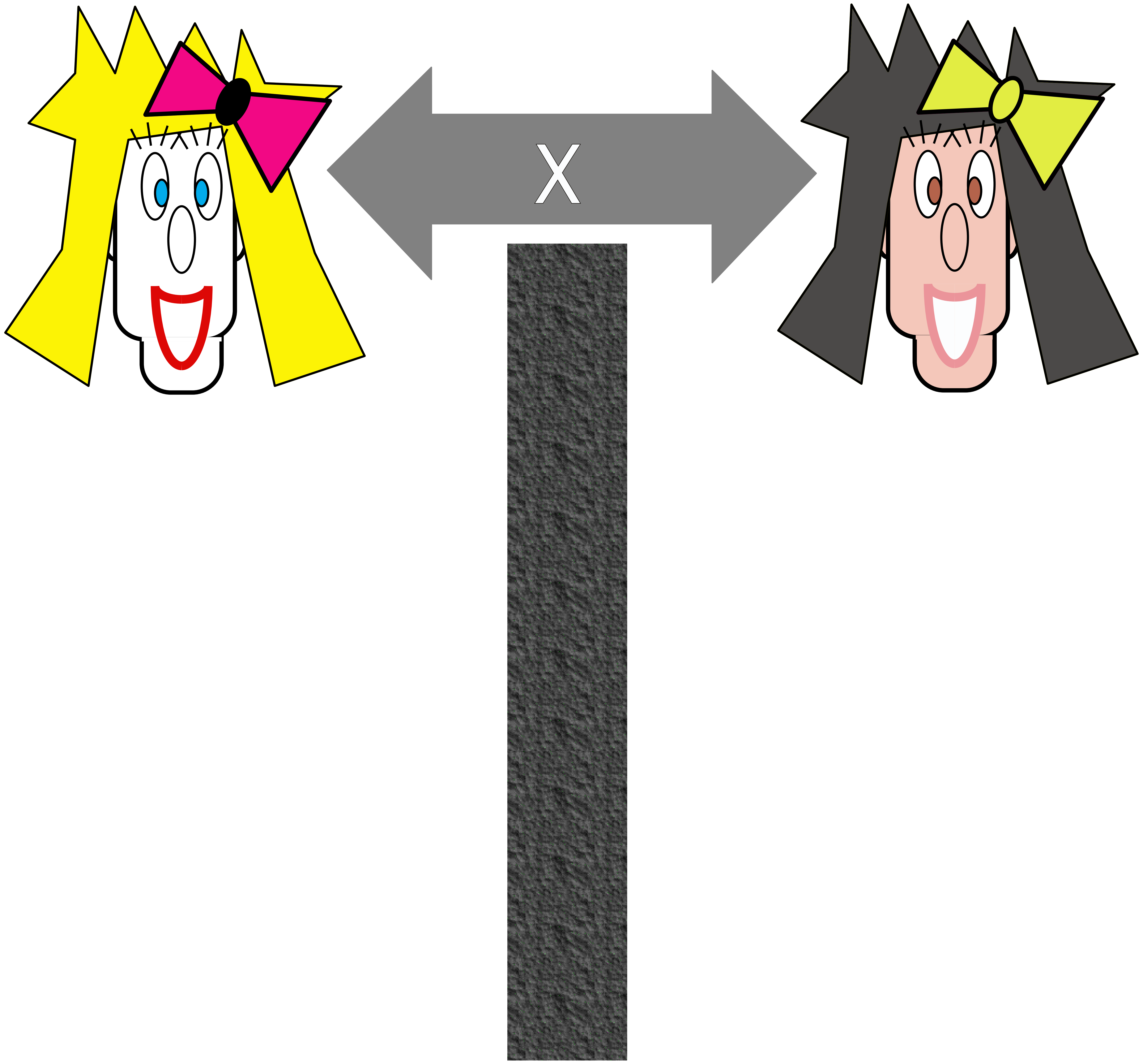
Buhrman, Christandl,
Unger, Wehner, Winter
(Wolf, Wullschleger +
Short, Gisin, Popescu)

(2)
two provers
Cryptographic Protocols

Classically

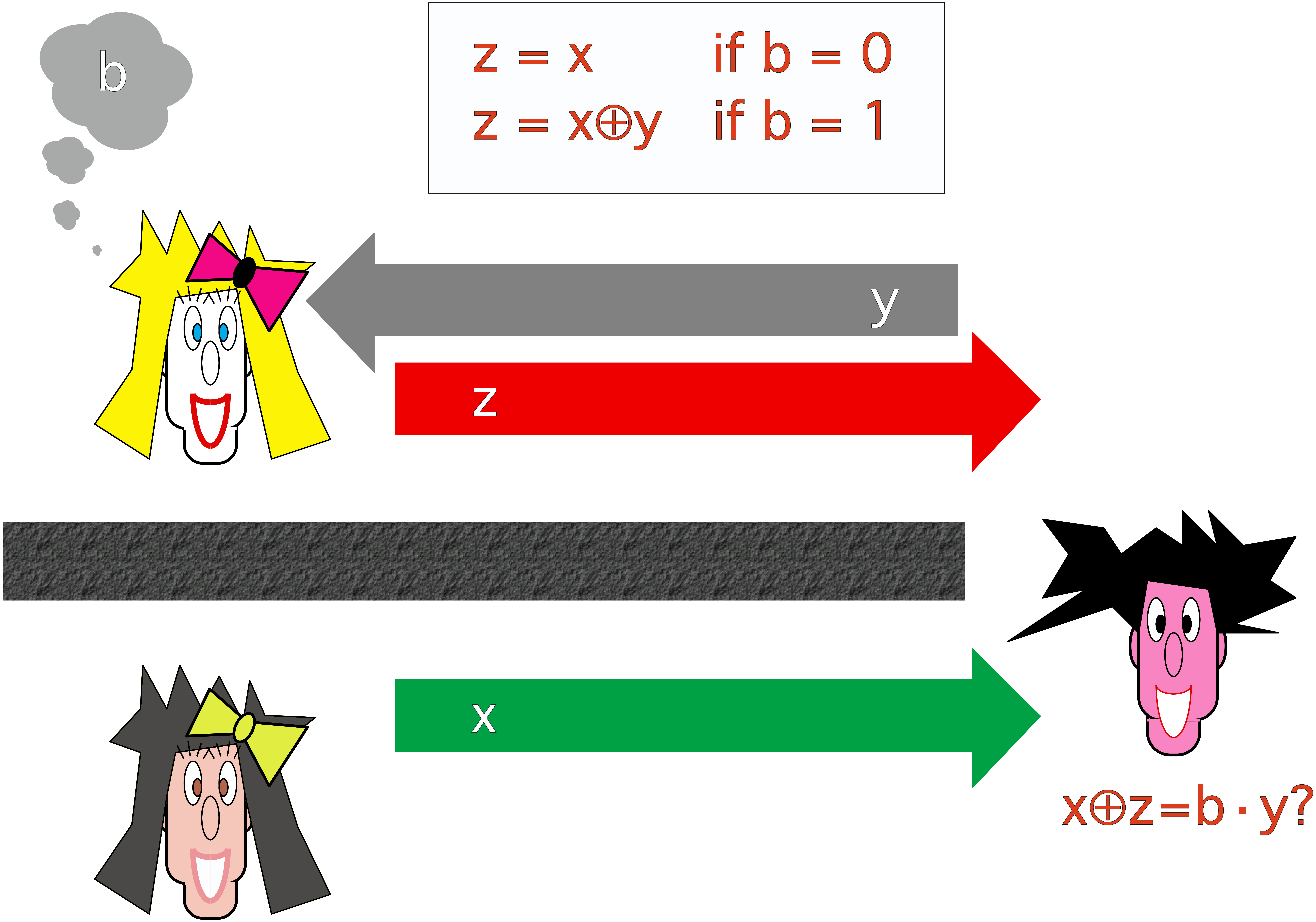
BGKW88

Classically



Ben-Or, Goldwasser, Kilian, Wigderson

$$
\begin{array}{ll}
z = x & \text{if } b = 0 \\
z = x \oplus y & \text{if } b = 1
\end{array}
$$



Ben-Or, Goldwasser, Kilian, Wigderson

SECURE

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

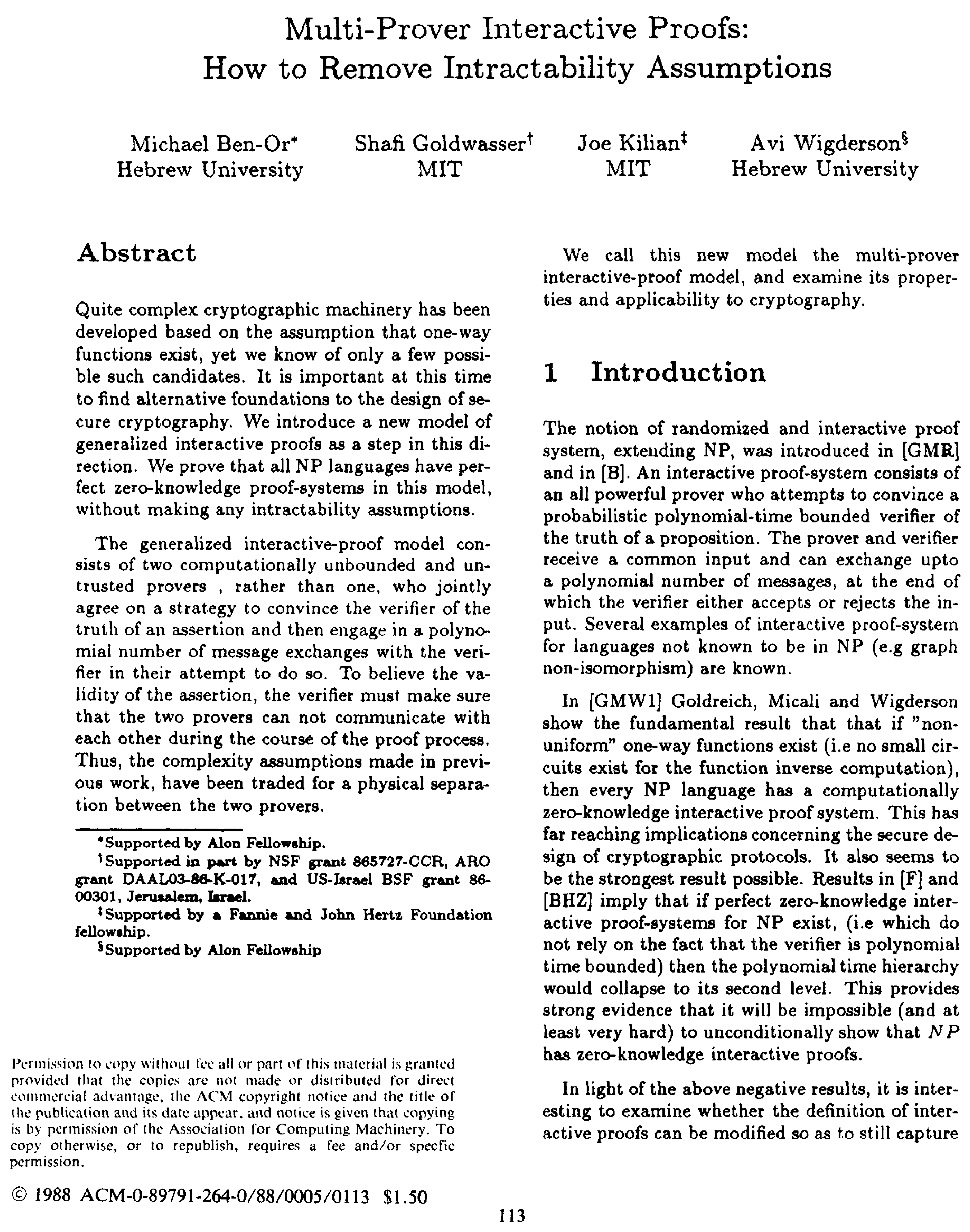
$x_1 \oplus z = 1 \cdot y = y$

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

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

Ben-Or, Goldwasser, Kilian, Wigderson

EPISODE 0



Multi-Prover Interactive Proofs: How to Remove Intractability Assumptions

Michael Ben-Or[*] Hebrew University
Shafi Goldwasser[†] MIT
Joe Kilian[‡] MIT
Avi Wigderson[§] Hebrew University

Abstract

Quite complex cryptographic machinery has been developed based on the assumption that one-way functions exist, yet we know of only a few possible such candidates. It is important at this time to find alternative foundations to the design of secure cryptography. We introduce a new model of generalized interactive proofs as a step in this direction. We prove that all NP languages have perfect zero-knowledge proof-systems in this model, without making any intractability assumptions.

The generalized interactive-proof model consists of two computationally unbounded and untrusted provers , rather than one, who jointly agree on a strategy to convince the verifier of the truth of an assertion and then engage in a polynomial number of message exchanges with the verifier in their attempt to do so. To believe the validity of the assertion, the verifier must make sure that the two provers can not communicate with each other during the course of the proof process. Thus, the complexity assumptions made in previous work, have been traded for a physical separation between the two provers.

We call this new model the multi-prover interactive-proof model, and examine its properties and applicability to cryptography.

1 Introduction

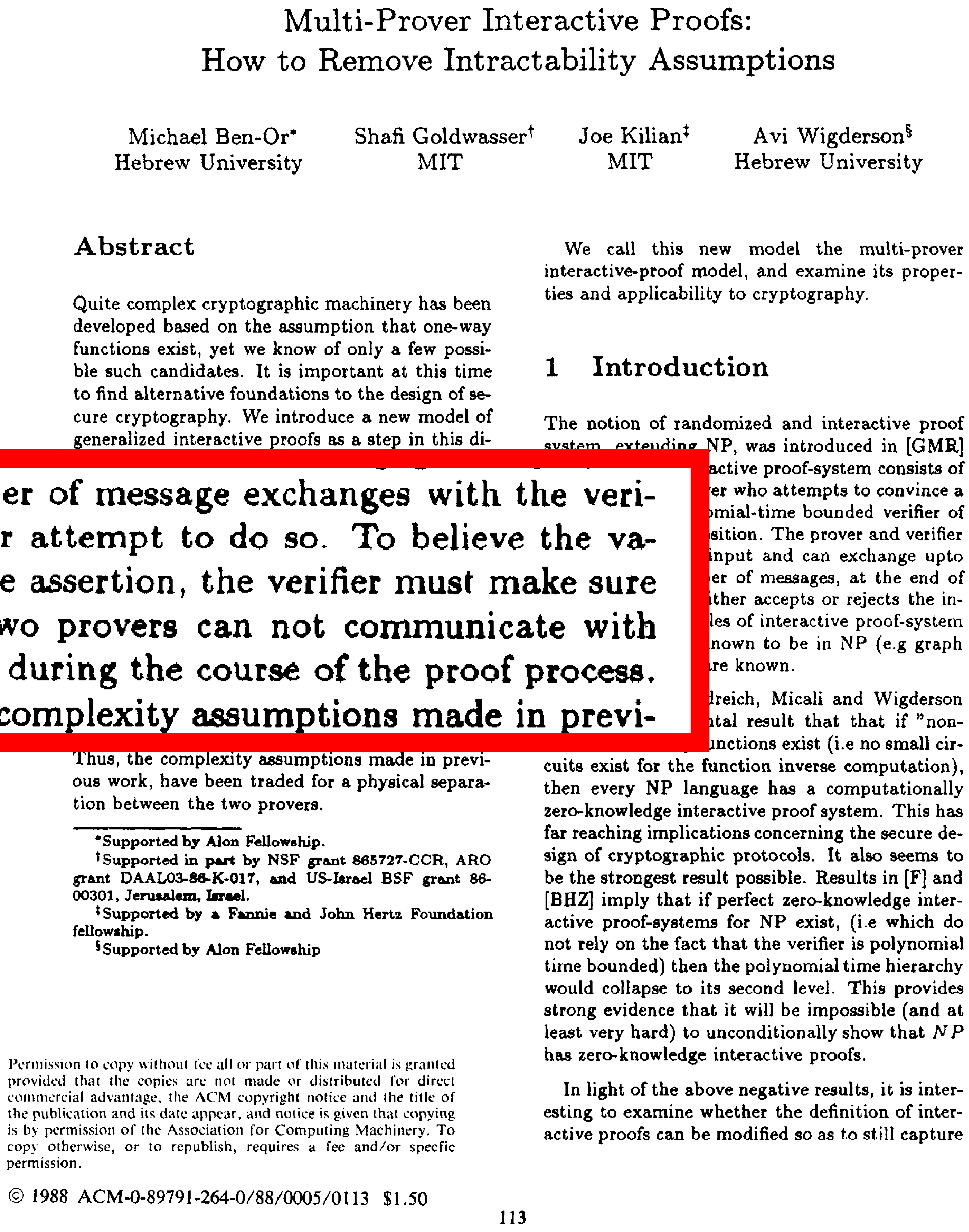
The notion of randomized and interactive proof system, extending NP, was introduced in [GMR] and in [B]. An interactive proof-system consists of an all powerful prover who attempts to convince a probabilistic polynomial-time bounded verifier of the truth of a proposition. The prover and verifier receive a common input and can exchange upto a polynomial number of messages, at the end of which the verifier either accepts or rejects the input. Several examples of interactive proof-system for languages not known to be in NP (e.g graph non-isomorphism) are known.

In [GMW1] Goldreich, Micali and Wigderson show the fundamental result that that if "non-uniform" one-way functions exist (i.e no small circuits exist for the function inverse computation), then every NP language has a computationally zero-knowledge interactive proof system. This has far reaching implications concerning the secure design of cryptographic protocols. It also seems to be the strongest result possible. Results in [F] and [BHZ] imply that if perfect zero-knowledge interactive proof-systems for NP exist, (i.e which do not rely on the fact that the verifier is polynomial time bounded) then the polynomial time hierarchy would collapse to its second level. This provides strong evidence that it will be impossible (and at least very hard) to unconditionally show that NP has zero-knowledge interactive proofs.

In light of the above negative results, it is interesting to examine whether the definition of interactive proofs can be modified so as to still capture

[*] Supported by Alon Fellowship.
[†] Supported in part by NSF grant 865727-CCR, ARO grant DAAL03-86-K-017, and US-Israel BSF grant 86-00301, Jerusalem, Israel.
[‡] Supported by a Fannie and John Hertz Foundation fellowship.
[§] Supported by Alon Fellowship

EPISODE 0



Multi-Prover Interactive Proofs: How to Remove Intractability Assumptions

Michael Ben-Or[*] Hebrew University
Shafi Goldwasser[†] MIT
Joe Kilian[‡] MIT
Avi Wigderson[§] Hebrew University

Abstract

Quite complex cryptographic machinery has been developed based on the assumption that one-way functions exist, yet we know of only a few possible such candidates. It is important at this time to find alternative foundations to the design of secure cryptography. We introduce a new model of generalized interactive proofs as a step in this di-

mial number of message exchanges with the verifier in their attempt to do so. To believe the validity of the assertion, the verifier must make sure that the two provers can not communicate with each other during the course of the proof process. Thus, the complexity assumptions made in previ-

Thus, the complexity assumptions made in previ-

ous work, have been traded for a physical separation between the two provers.

We call this new model the multi-prover interactive-proof model, and examine its properties and applicability to cryptography.

1 Introduction

The notion of randomized and interactive proof system, extending NP, was introduced in [GMR]
active proof-system consists of
er who attempts to convince a
omial-time bounded verifier of
sition. The prover and verifier
input and can exchange upto
er of messages, at the end of
ither accepts or rejects the in-
les of interactive proof-system
nown to be in NP (e.g graph
re known.

dreich, Micali and Wigderson
ntal result that that if "non-
unctions exist (i.e no small circuits exist for the function inverse computation), then every NP language has a computationally zero-knowledge interactive proof system. This has far reaching implications concerning the secure design of cryptographic protocols. It also seems to be the strongest result possible. Results in [F] and [BHZ] imply that if perfect zero-knowledge interactive proof-systems for NP exist, (i.e which do not rely on the fact that the verifier is polynomial time bounded) then the polynomial time hierarchy would collapse to its second level. This provides strong evidence that it will be impossible (and at least very hard) to unconditionally show that NP has zero-knowledge interactive proofs.

In light of the above negative results, it is interesting to examine whether the definition of interactive proofs can be modified so as to still capture

[*] Supported by Alon Fellowship.
[†] Supported in part by NSF grant 865727-CCR, ARO grant DAAL03-86-K-017, and US-Israel BSF grant 86-00301, Jerusalem, Israel.
[‡] Supported by a Fannie and John Hertz Foundation fellowship.
[§] Supported by Alon Fellowship

© 1988 ACM-0-89791-264-0/88/0005/0113 $1.50

EPISODE 0

Multi-Prover Interactive Proofs: How to Remove Intractability Assumptions

Michael Ben-Or[*]
Hebrew University

Shafi Goldwasser[†]
MIT

Joe Kilian[‡]
MIT

Avi Wigderson[§]
Hebrew University

Abstract

We call this new model the multi-prover

mial number of message exchanges with the verifier in their attempt to do so. To believe the validity of the assertion, the verifier must make sure that the two provers can not communicate with each other during the course of the proof process. Thus, the complexity assumptions made in previ-

be the strongest result possible. Results in [F] and [BHZ] imply that if perfect zero-knowledge interactive proof-systems for NP exist, (i.e which do not rely on the fact that the verifier is polynomial time bounded) then the polynomial time hierarchy would collapse to its second level. This provides strong evidence that it will be impossible (and at least very hard) to unconditionally show that NP has zero-knowledge interactive proofs.

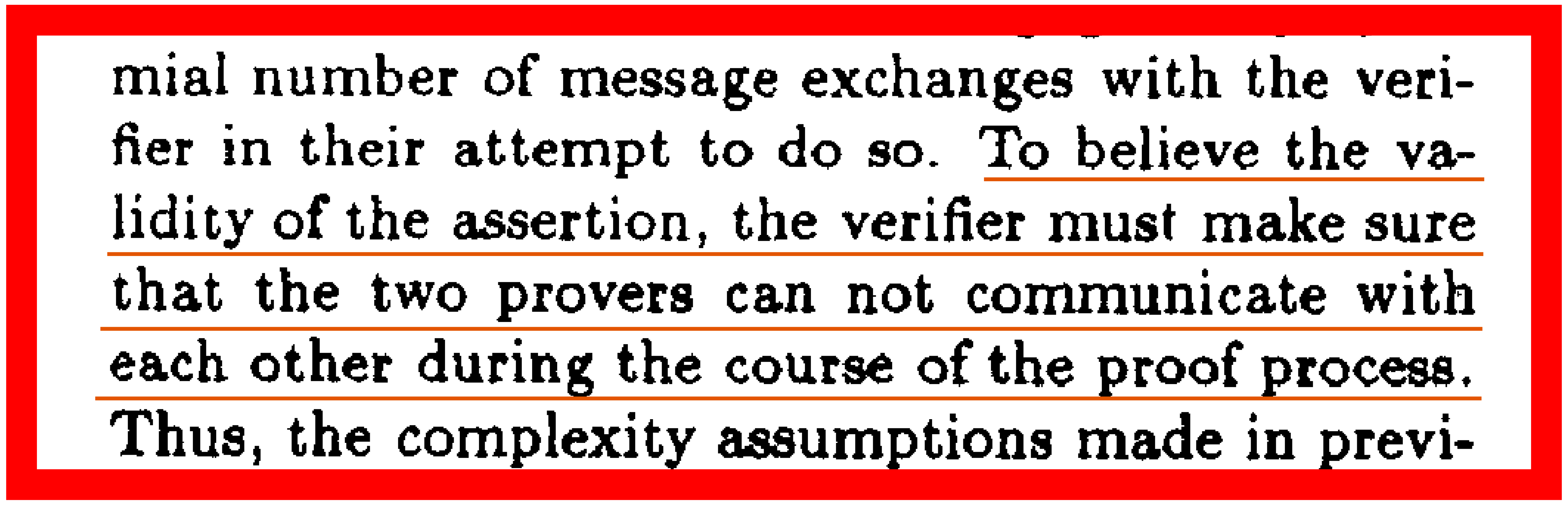
In light of the above negative results, it is interesting to examine whether the definition of interactive proofs can be modified so as to still capture

grant DAAL03-86-K-017, and US-Israel BSF grant 86-00301, Jerusalem, Israel.

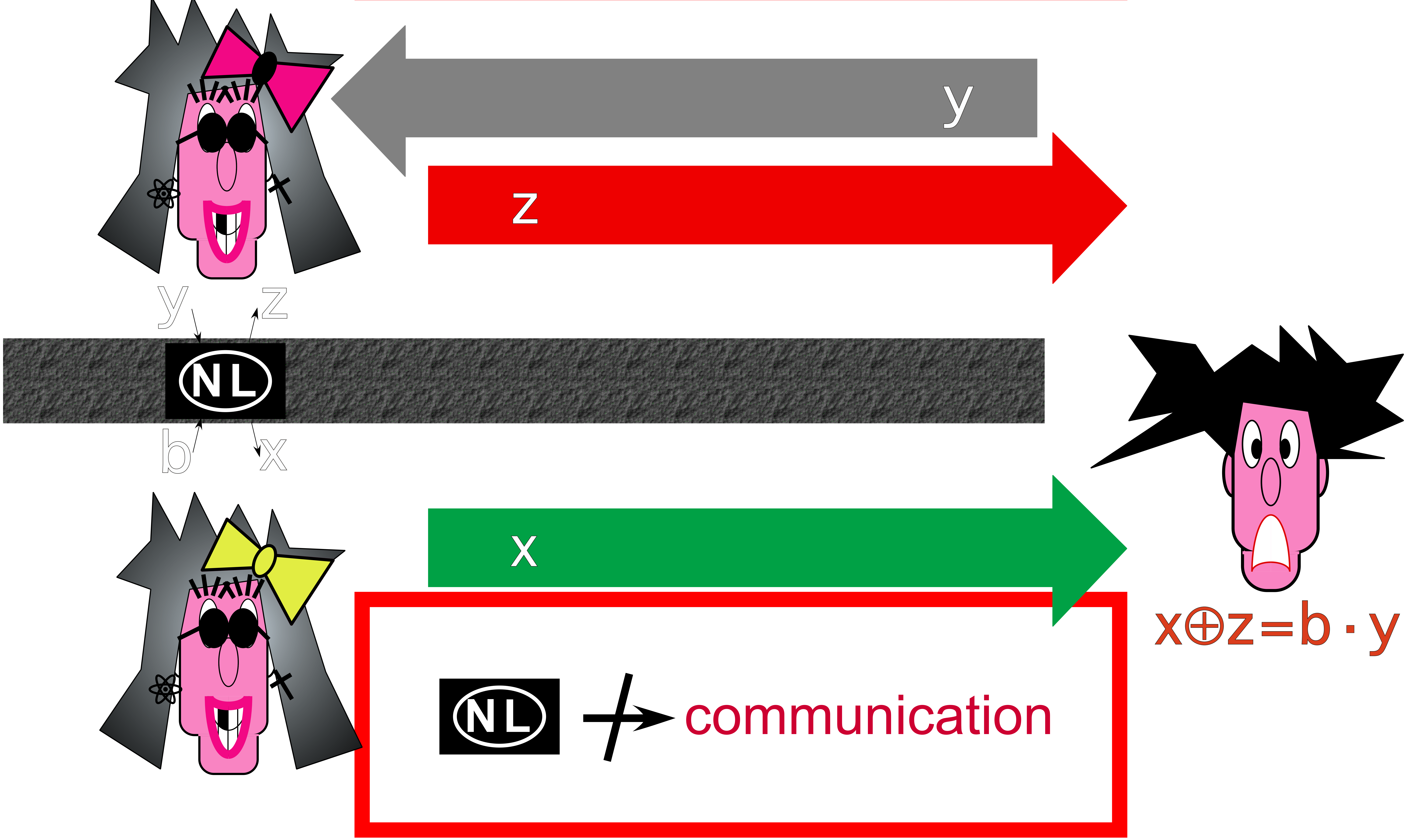
[‡]Supported by a Fannie and John Hertz Foundation fellowship.

[§]Supported by Alon Fellowship

113

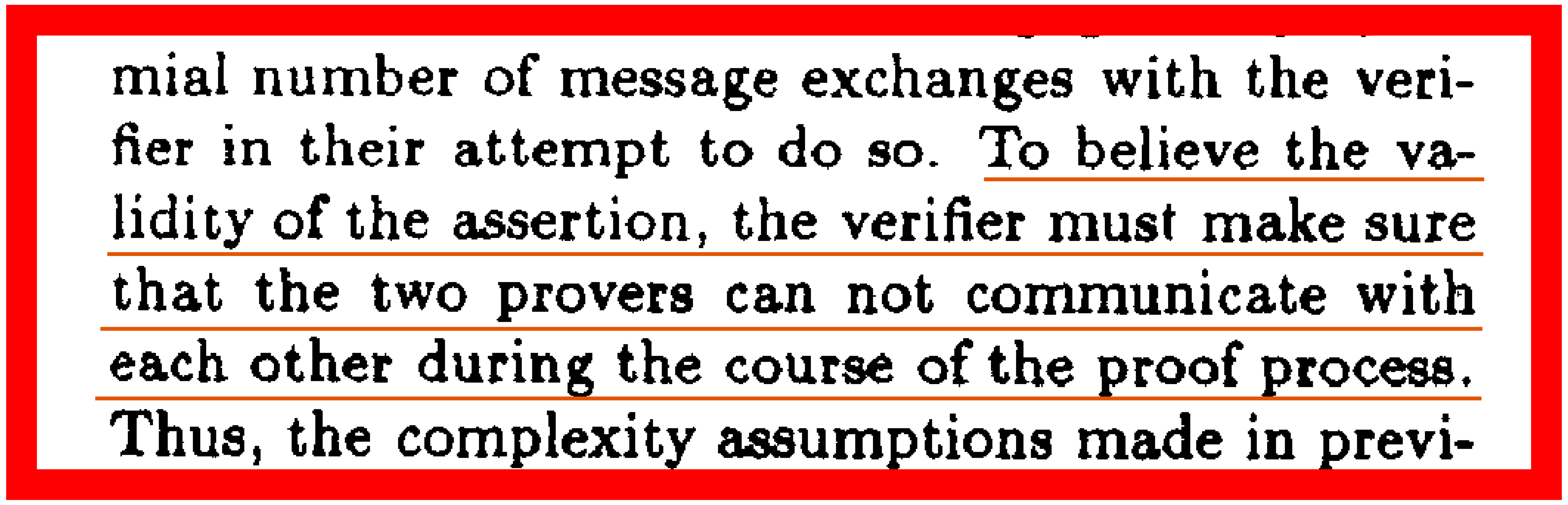


mial number of message exchanges with the verifier in their attempt to do so. To believe the validity of the assertion, the verifier must make sure that the two provers can not communicate with each other during the course of the proof process. Thus, the complexity assumptions made in previ-

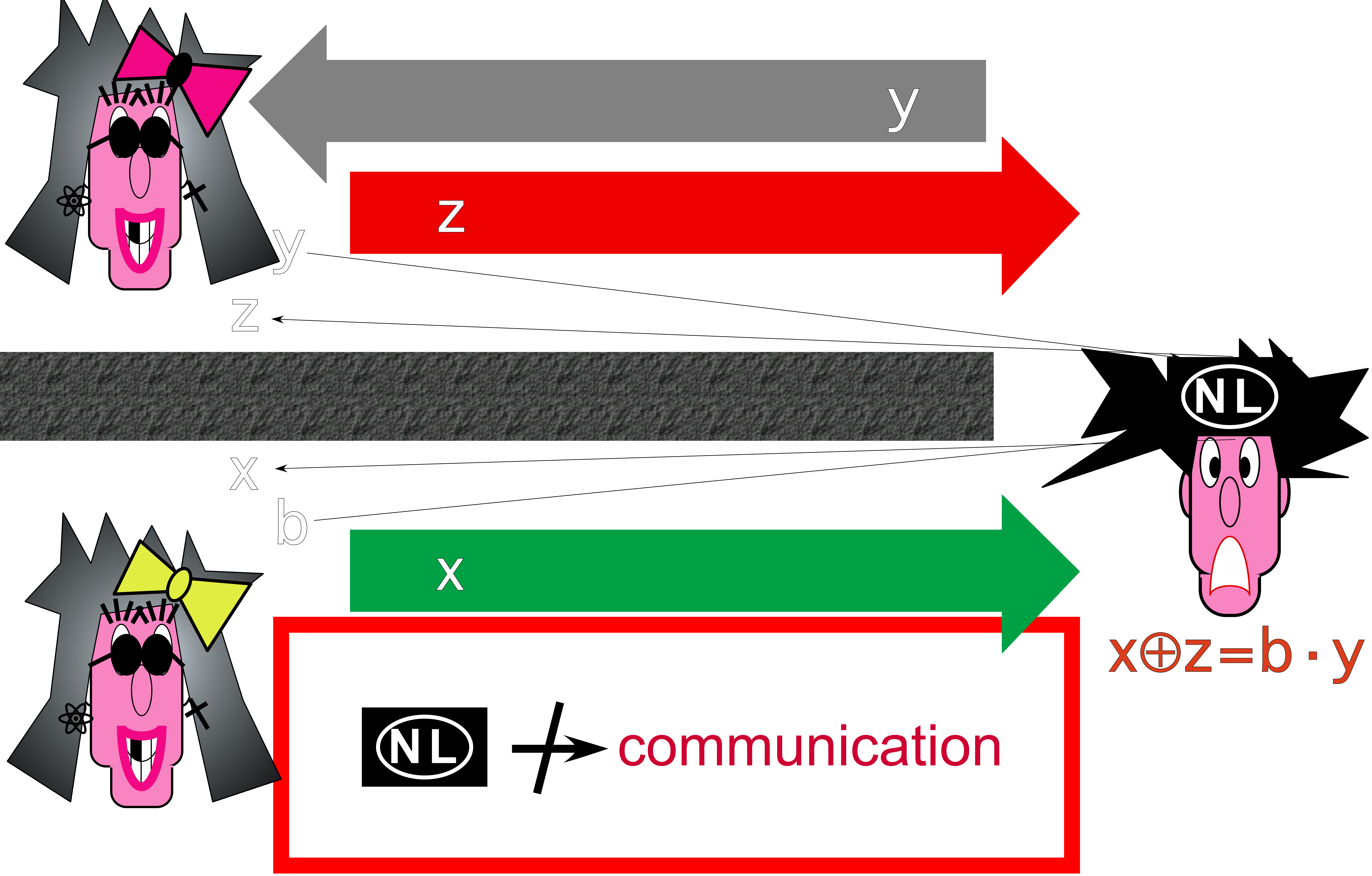


$x \oplus z = b \cdot y$

NL $\not\rightarrow$ communication



mial number of message exchanges with the verifier in their attempt to do so. To believe the validity of the assertion, the verifier must make sure that the two provers can not communicate with each other during the course of the proof process. Thus, the complexity assumptions made in previ-

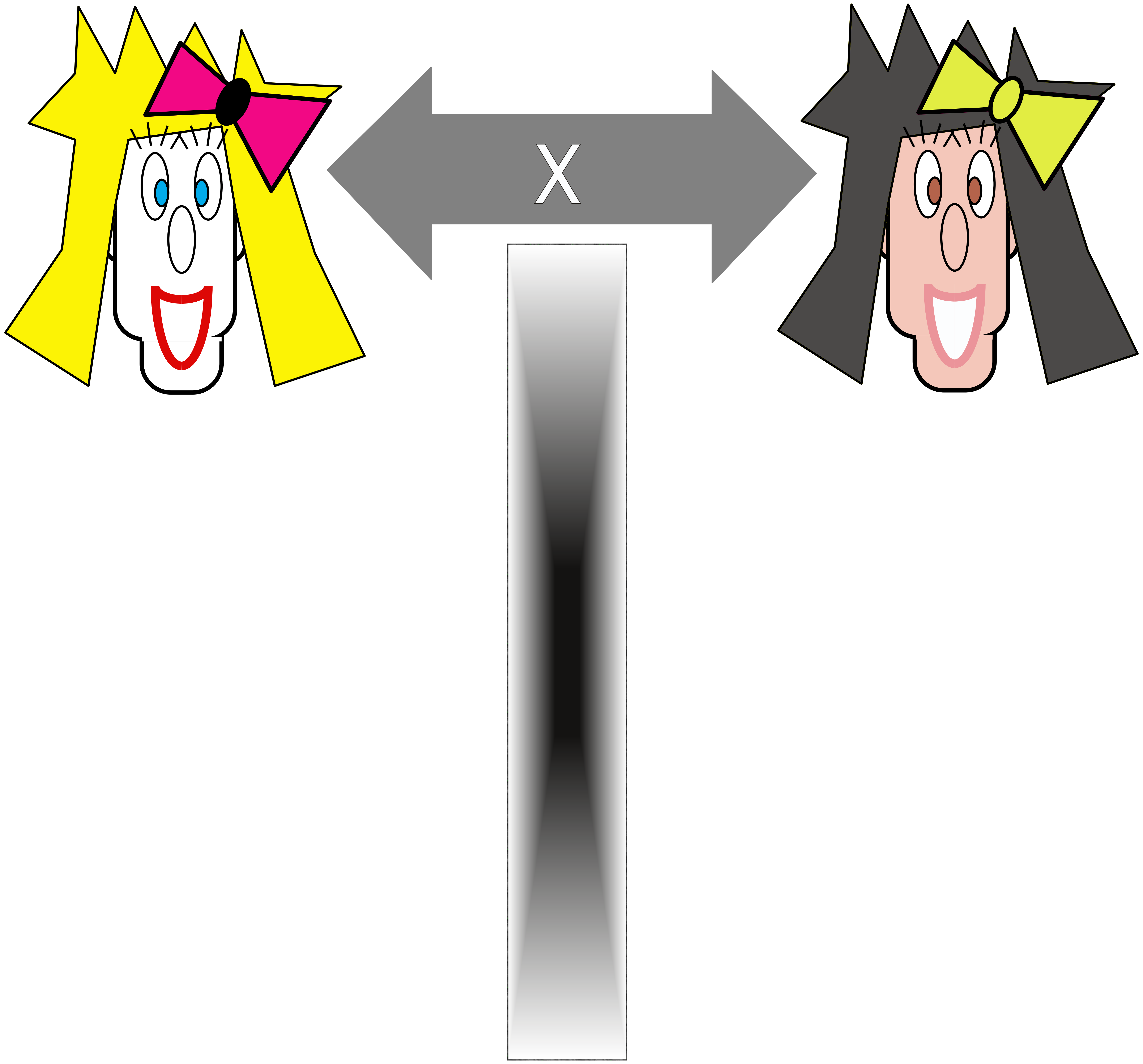


$x \oplus z = b \cdot y$

NL $\not\rightarrow$ communication

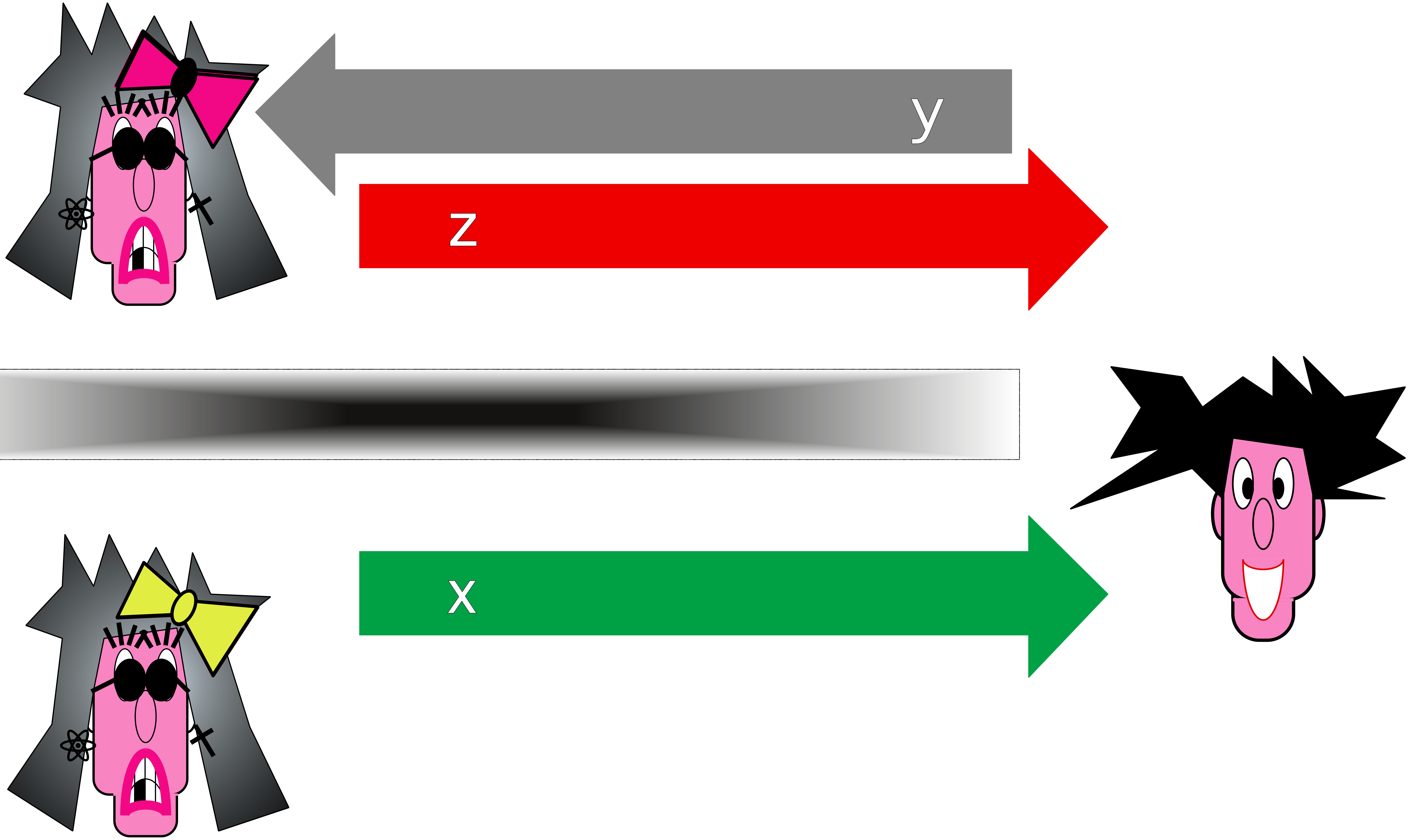
Yoda said:
"Happens to every guy sometimes
. this does"

Classically



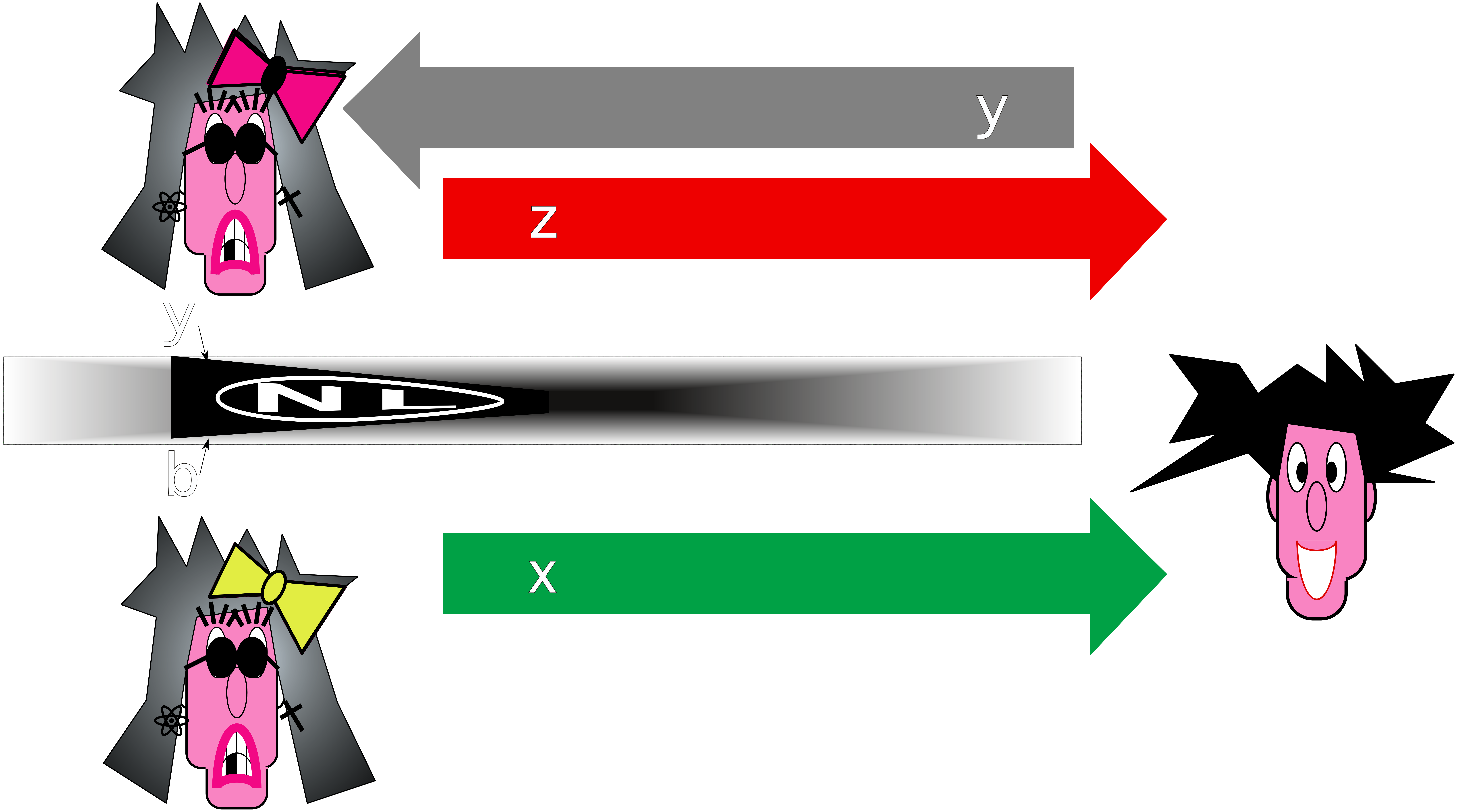
STRONG BGKW

Classically



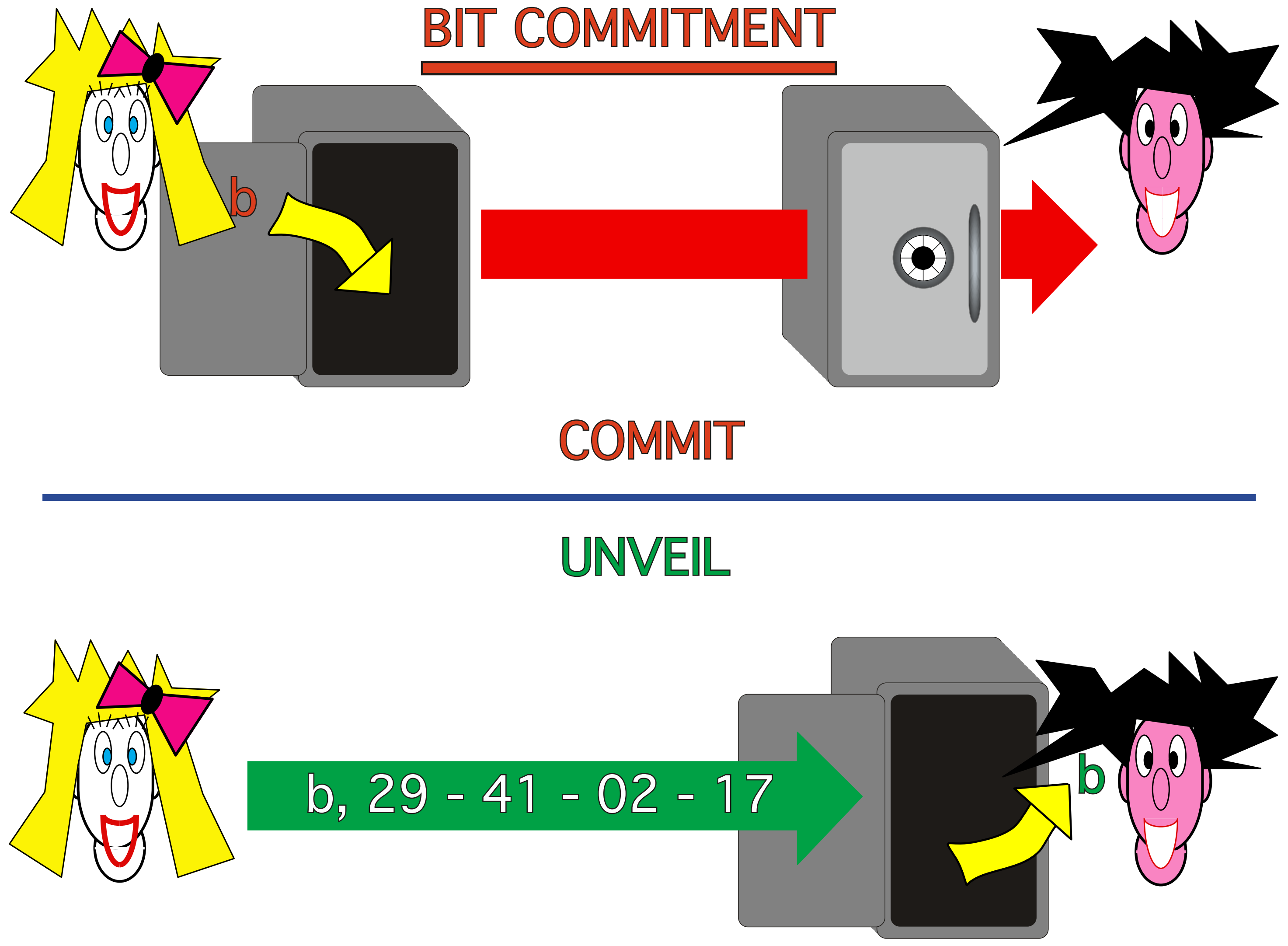
STRONG BGKW

Classically

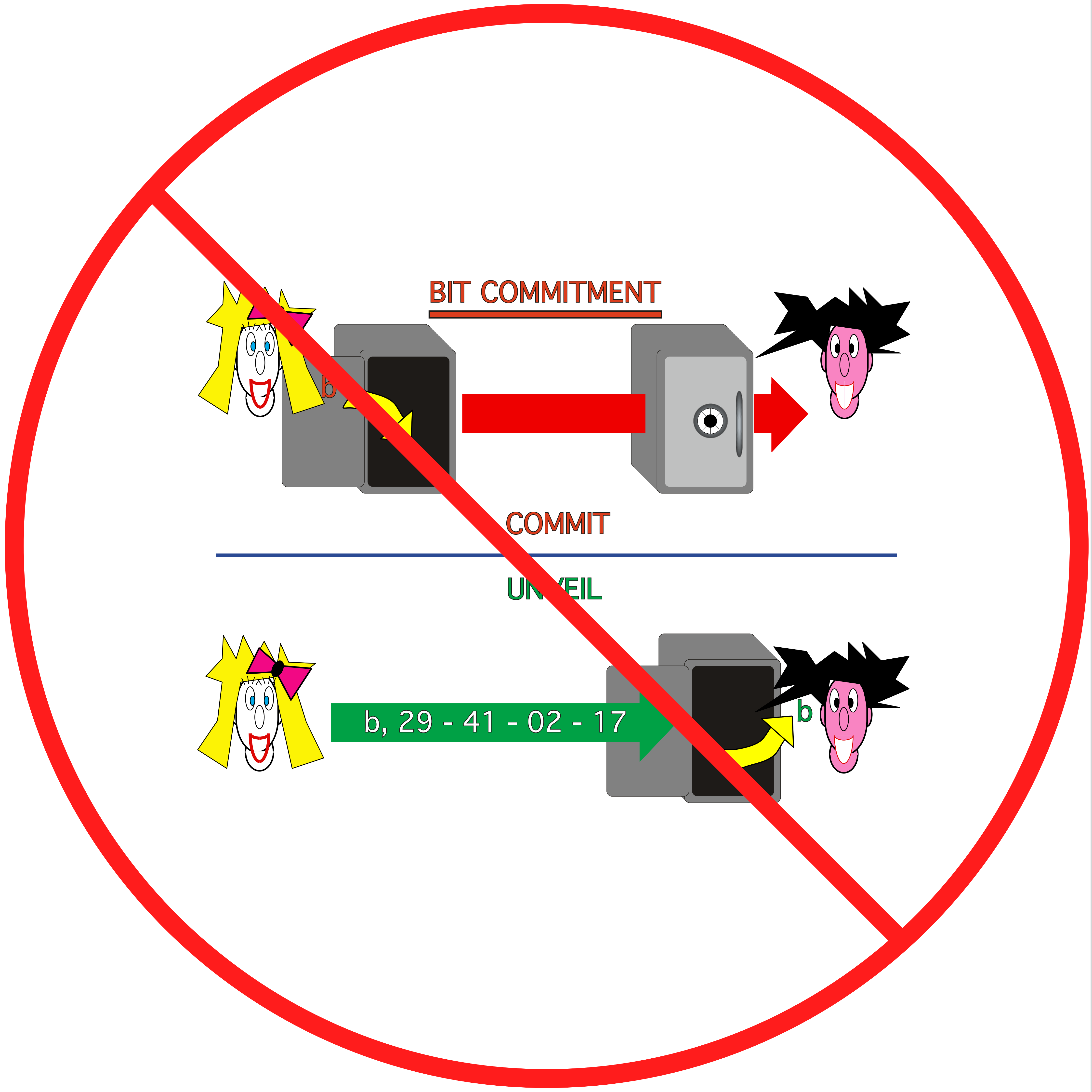


STRONG BGKW

Quantumly



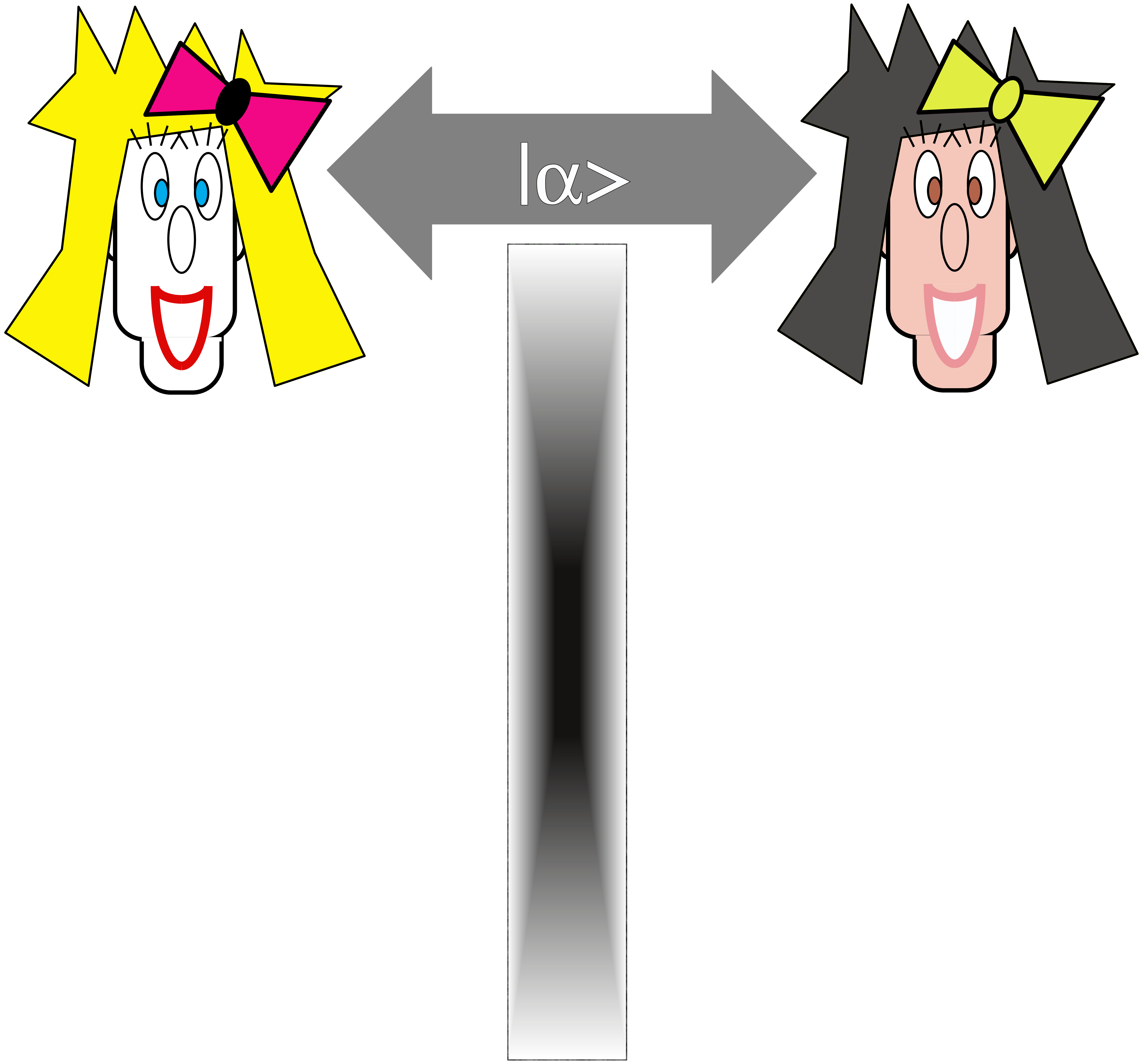
or



???

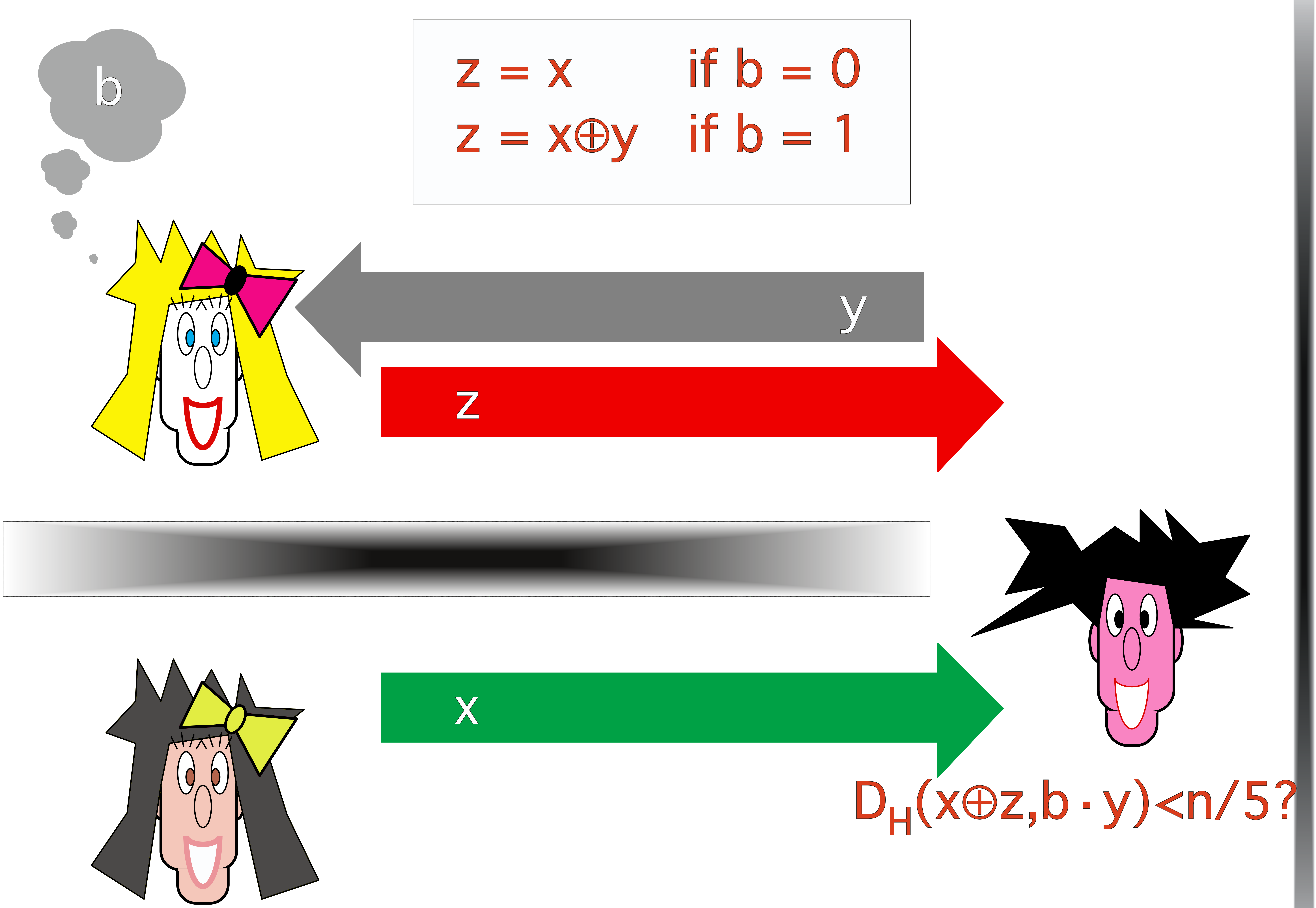
(3)
two provers BC
Classically Secure
Quantumly Insecure

Quantumly



STRONG Q-BGKW

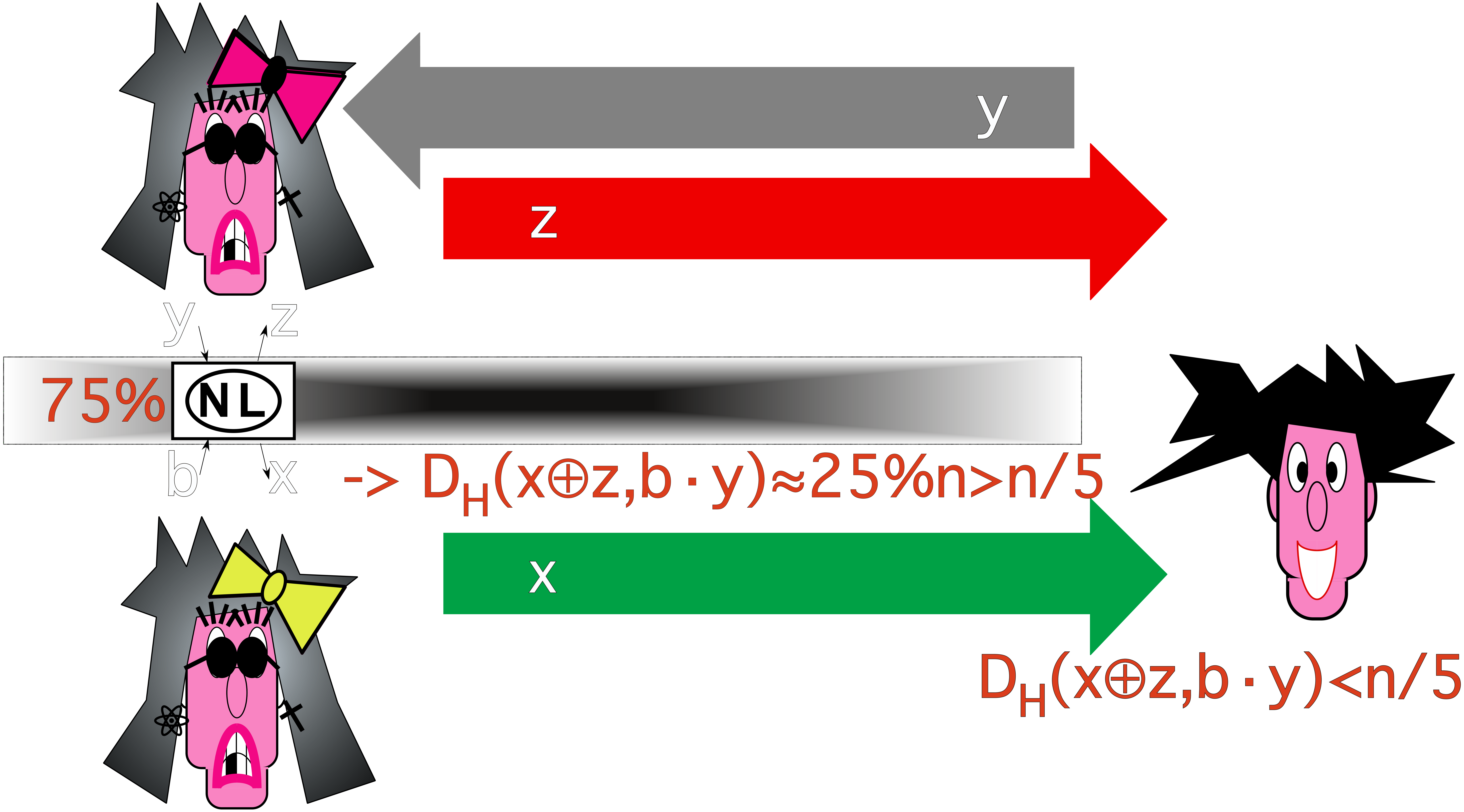
$$z = x \quad \text{if } b = 0$$
$$z = x \oplus y \quad \text{if } b = 1$$



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

STRONG Q-BGKW’

Classically



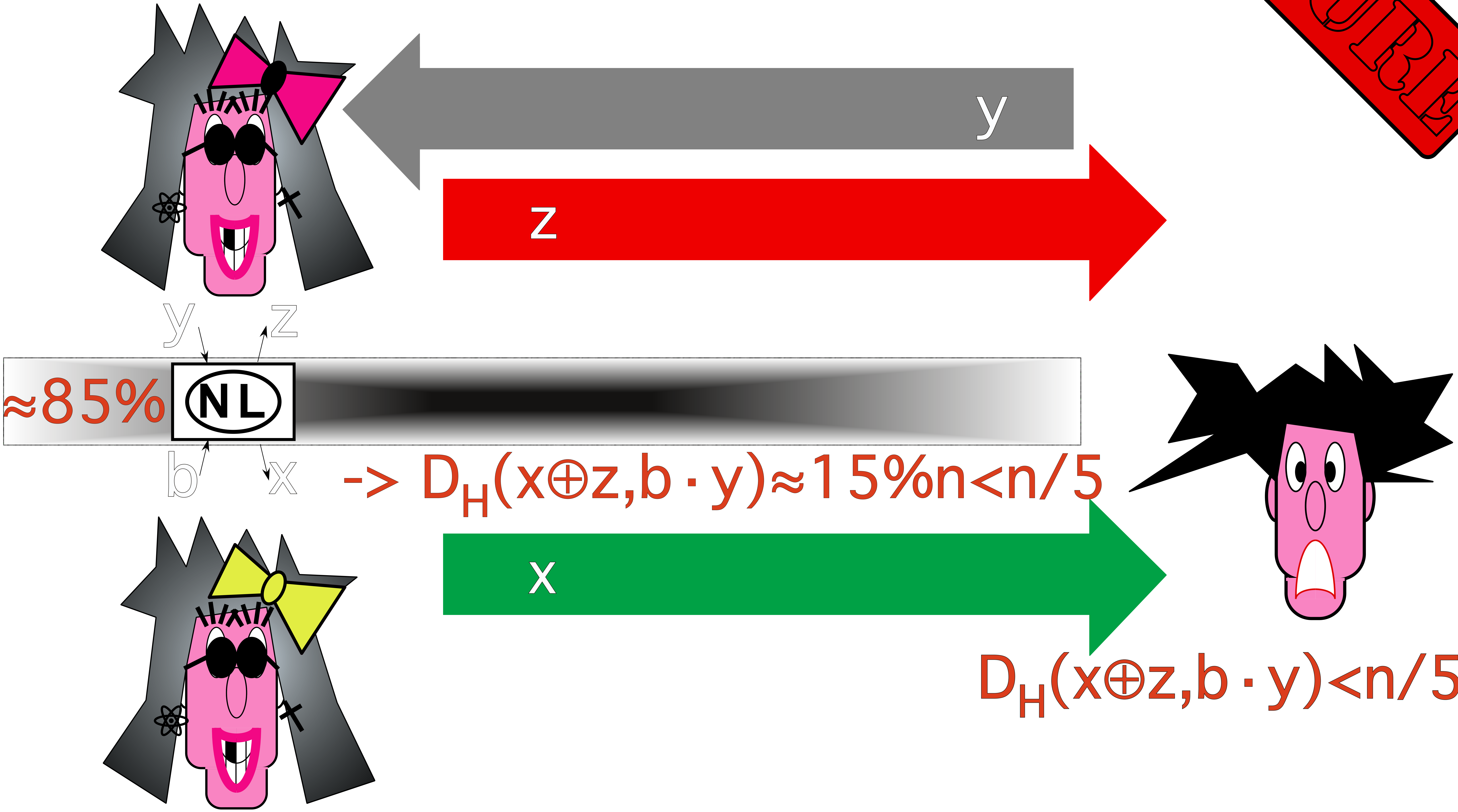
-> $D_H(x \oplus z, b \cdot y) \approx 25\% n > n/5$

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

STRONG Q-BGKW’

Quantumly

INSECURE



$\rightarrow D_H(x \oplus z, b \cdot y) \approx 15\% n < n/5$

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

~~STRONG Q-BGKW'~~

Classically

SECURE

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

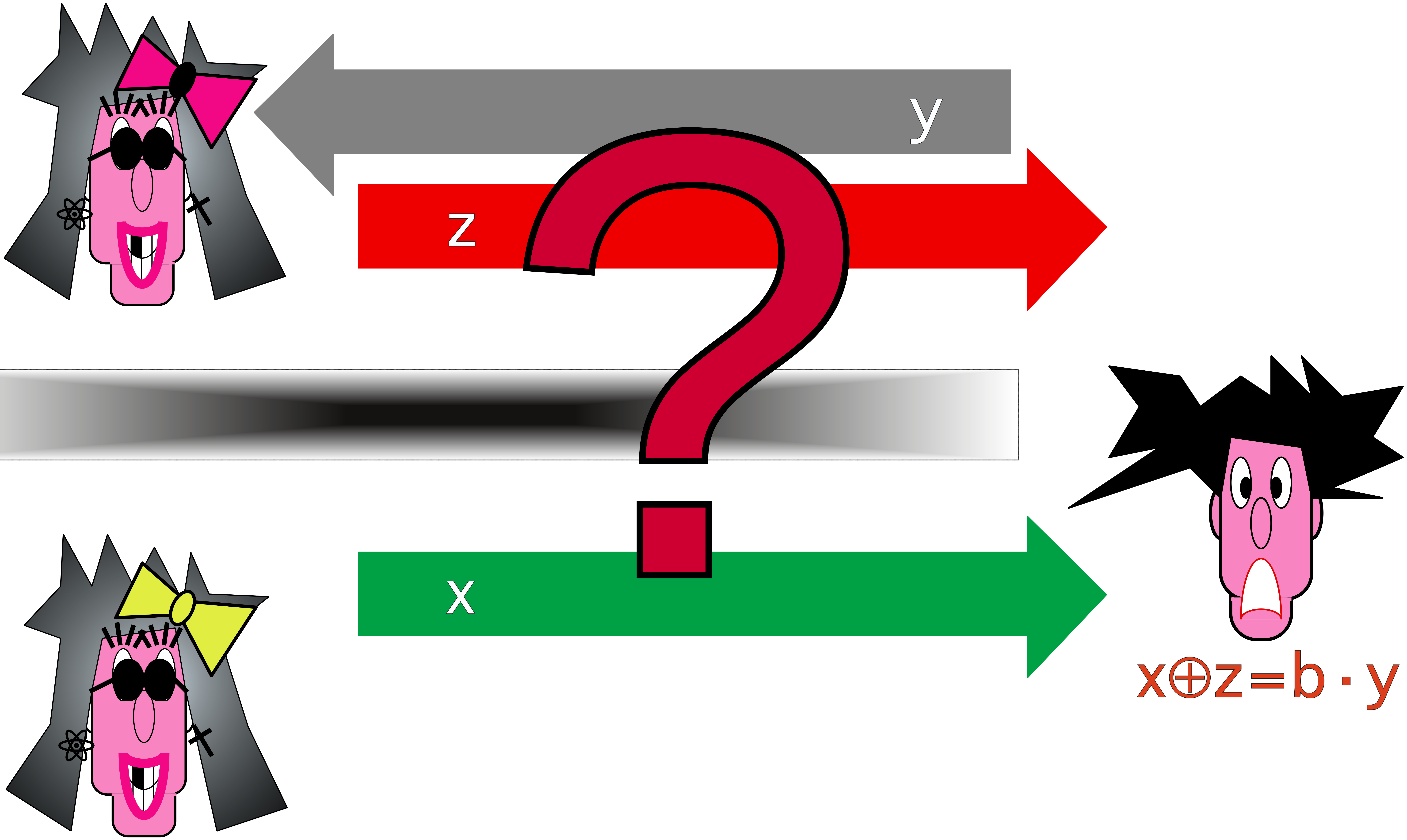
$D_H(x_1 \oplus z, 1 \cdot y) = D_H(x_1 \oplus z, y) < n/5$

$D_H(x_0 \oplus x_1, y) = D_H((x_0 \oplus z) \oplus (x_1 \oplus z), 0 \oplus y) < 2n/5 < n/2$

possible with prob. at most ε^{-n}

STRONG Q-BGKW'

Quantumly

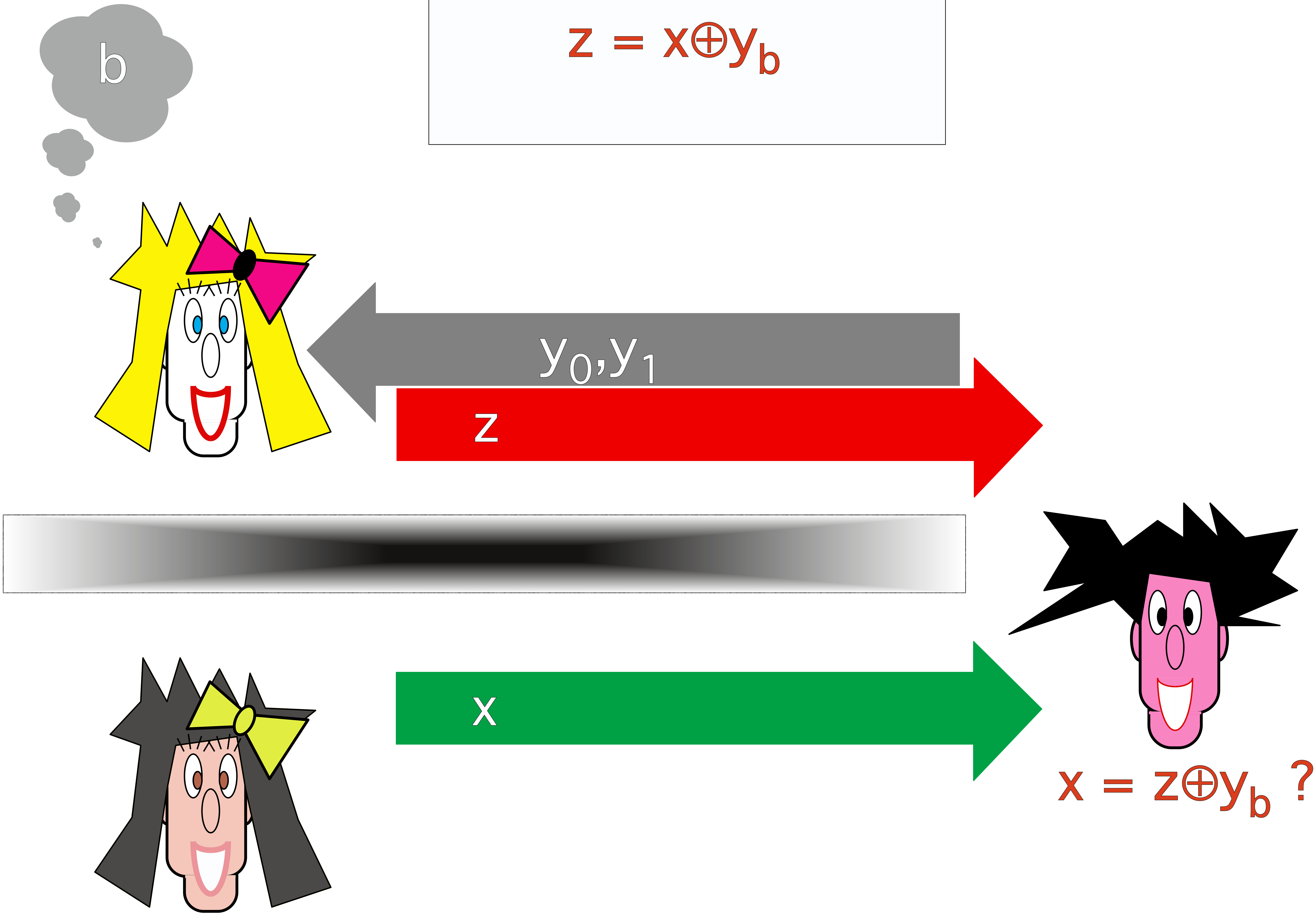


$x \oplus z = b \cdot y$

STRONG Q-BGKW

(4)
two provers BC Classically and Quantumly Secure

$$z = x \oplus y_b$$



$x = z \oplus y_b$?

STRONG Q-BGKW”

Classically

SECURE

$x_0 \oplus z = y_0$

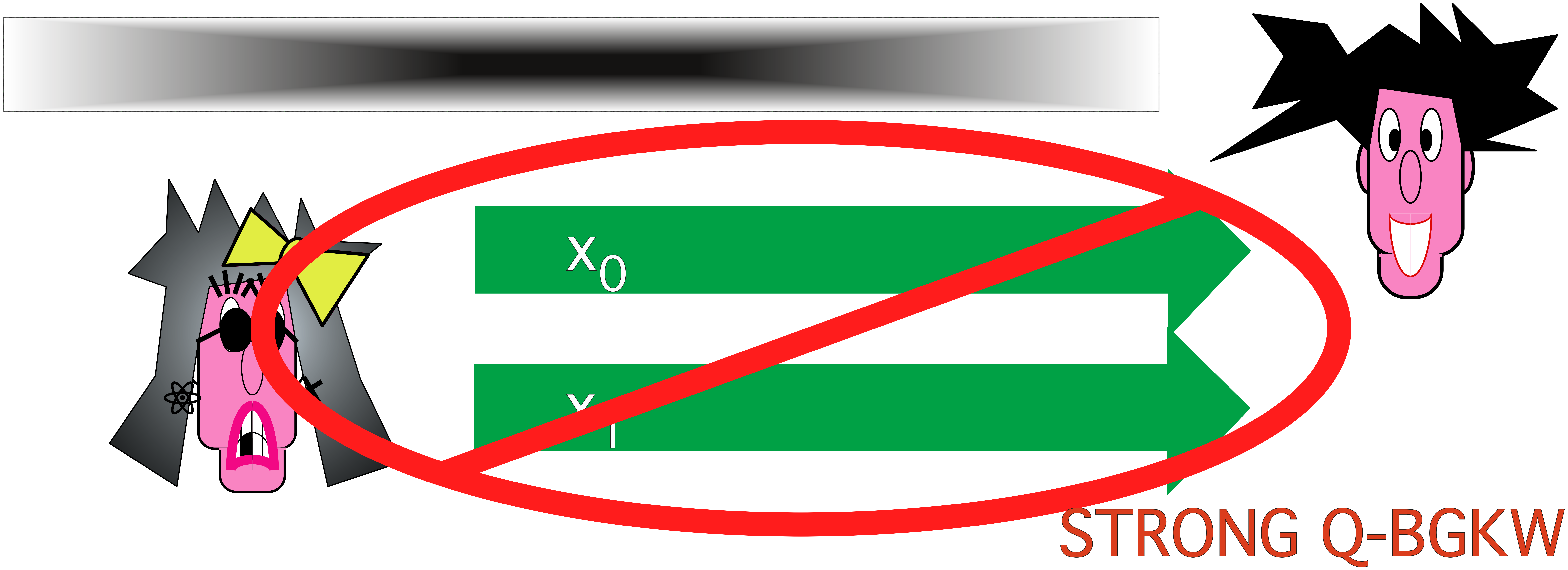
$x_1 \oplus z = y_1$

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

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

STRONG Q-BGKW”

Quantumly



STRONG Q-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 $y_0 \oplus y_1$] > δ.

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.

STRONG Q-BGKW"

Recently

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 $y_0 \oplus y_1$] > δ.

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.

STRONG Q-BGKW”

Yesterday

SECURE

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 $y_0 \oplus y_1$] > poly(δ).

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

STRONG Q-BGKW”

THANK YOU VERY MUCH • TOUSAND TAK • MILLES MERCIS • GRACIAS •

SECURE

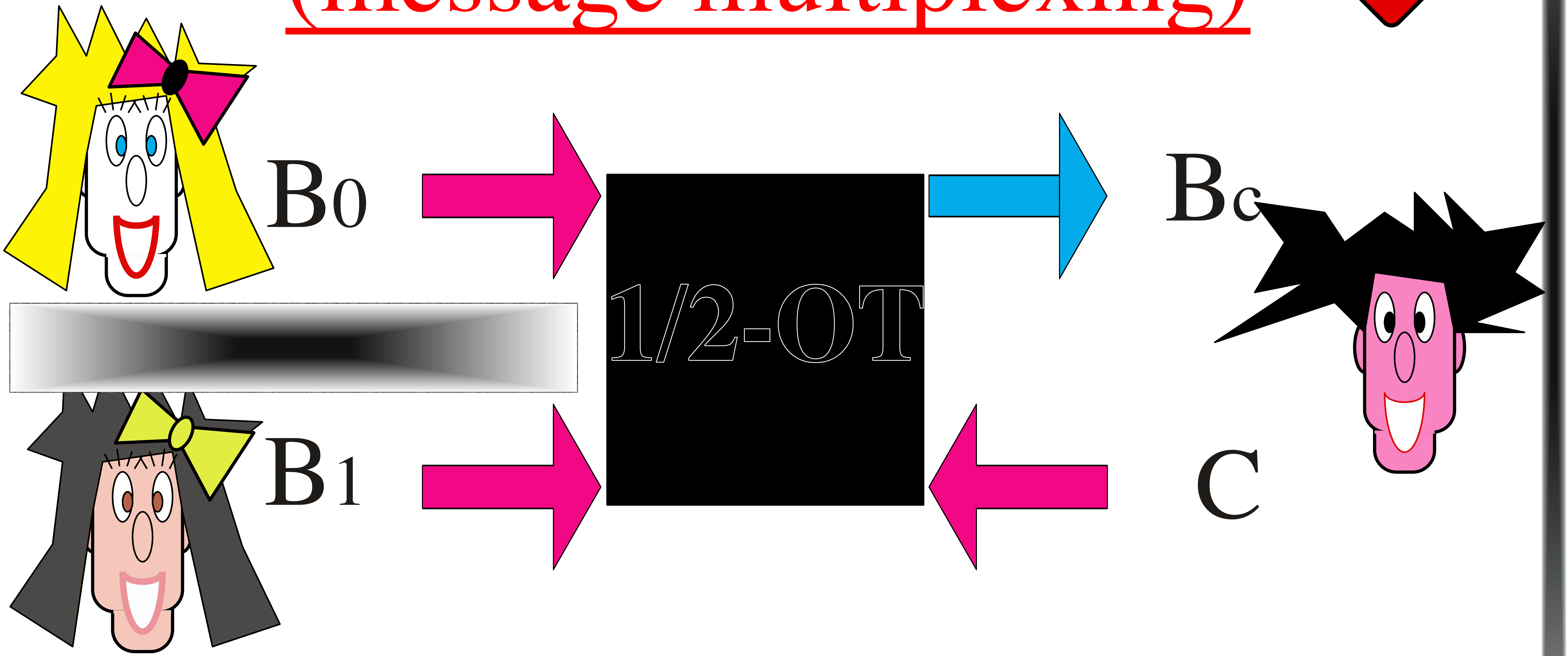
STRONG Q-BGKW”

(5)

WARNING!

Oblivious Transfer (message multiplexing)

SECURE



B0

B1

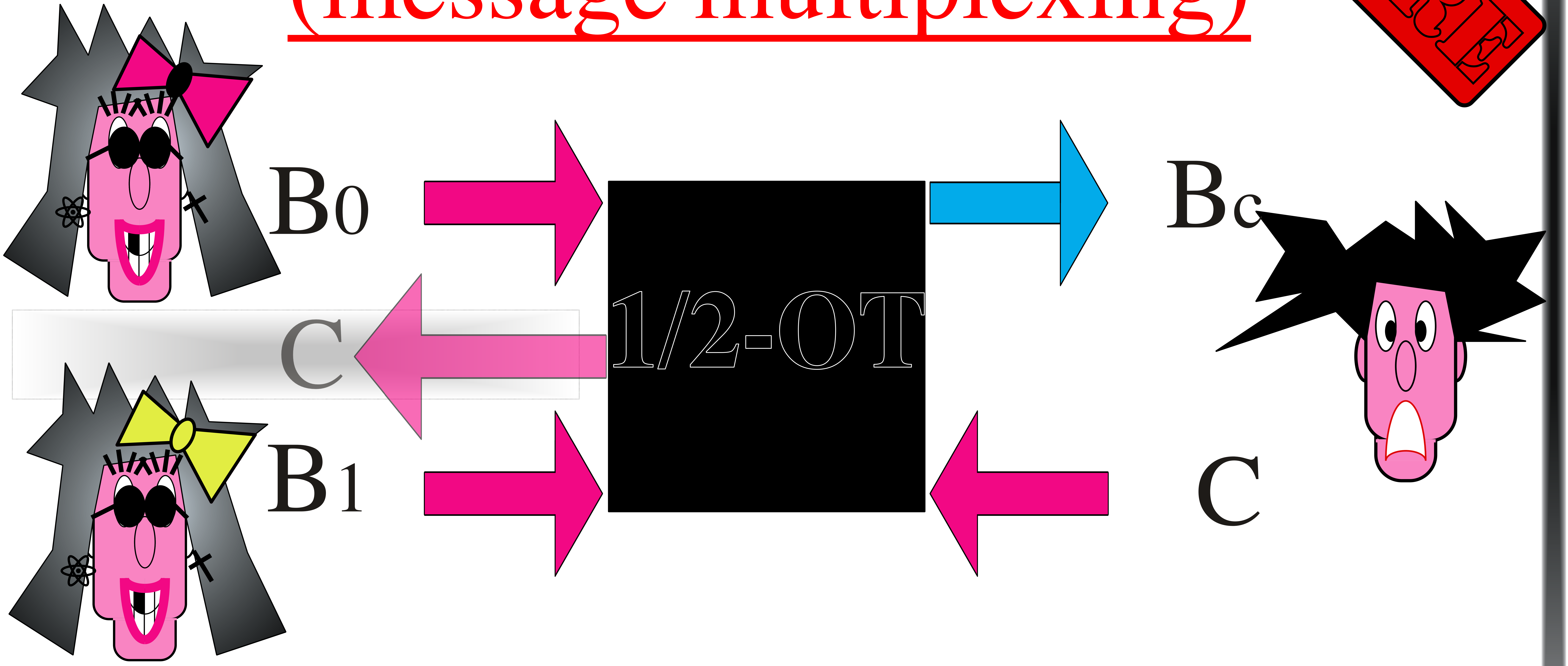
1/2-OT

Bc

C

Oblivious Transfer (message multiplexing)

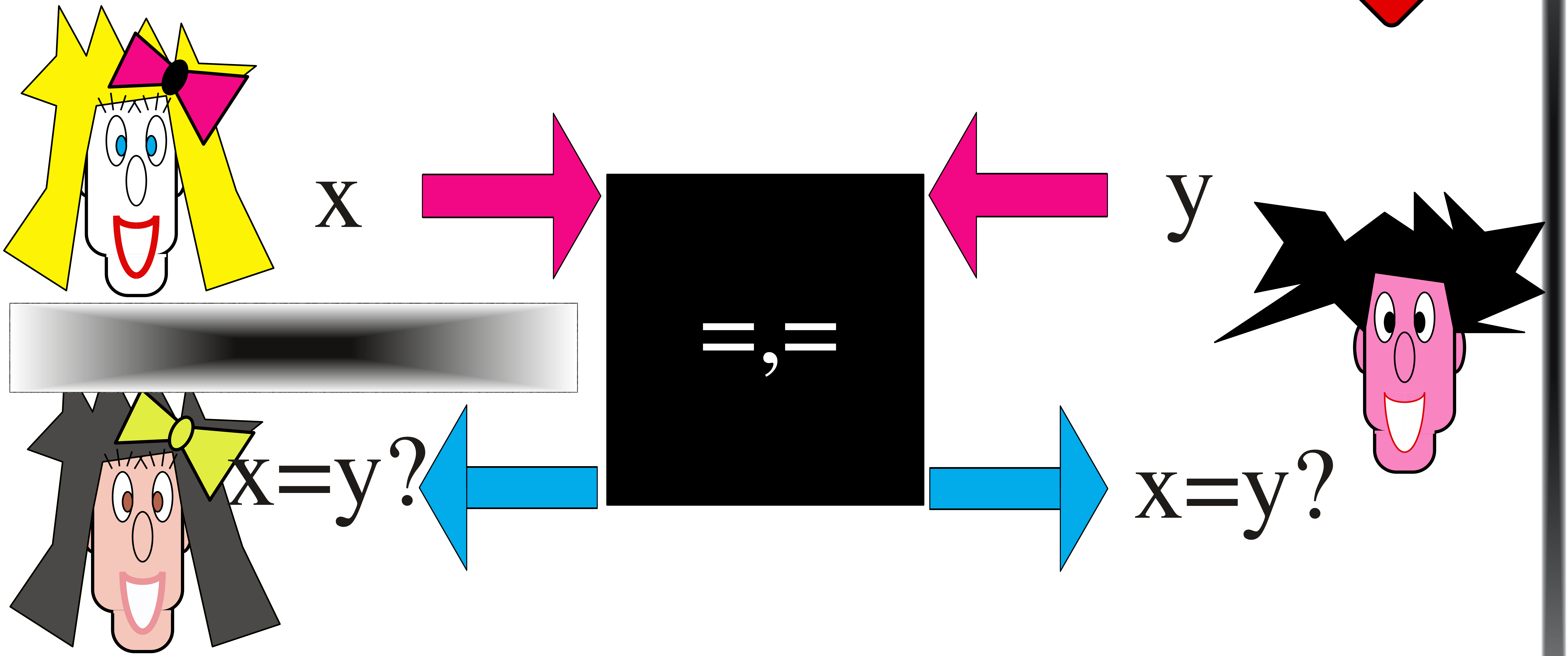
INSECURE



Brassard, Crépeau, Mayers, Salvail 97

Mutual Identification

SECURE



x

y

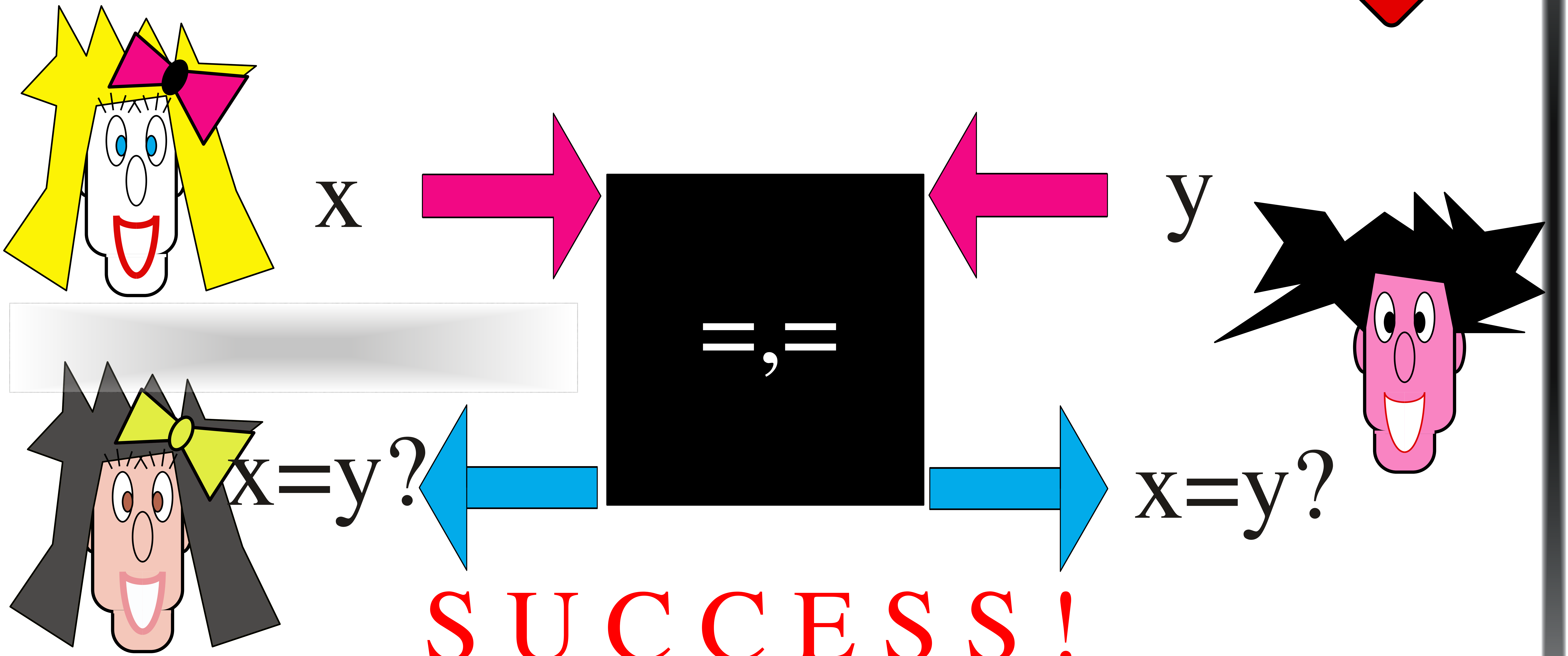
=,=

x=y?

x=y?

Mutual Identification

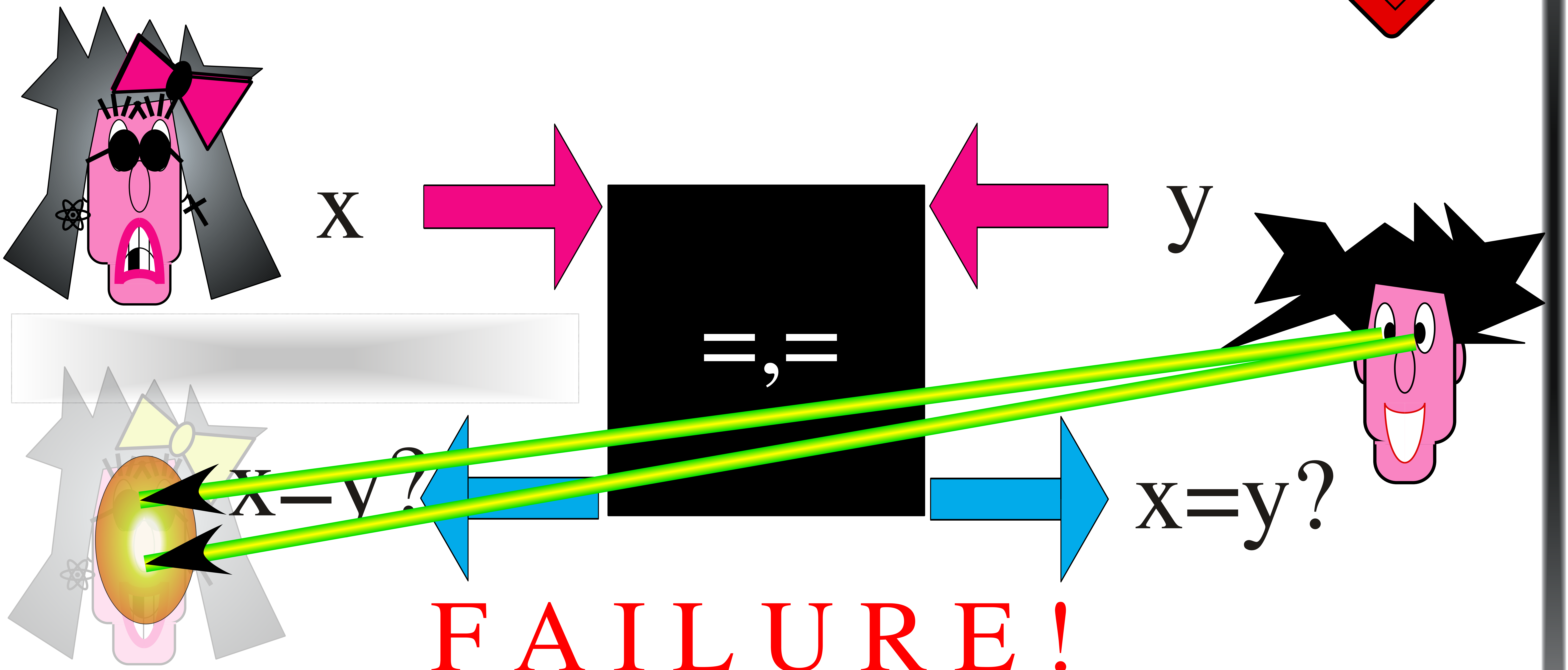
SECURE



SUCCESS!

Mutual Identification

SECURE



FAILURE!

|Bit Commitment⟩ Strikes Back

Claude Crépeau

School of Computer Science
McGill University

Joint work with J-R Simard and A Tapp

L Salvail .