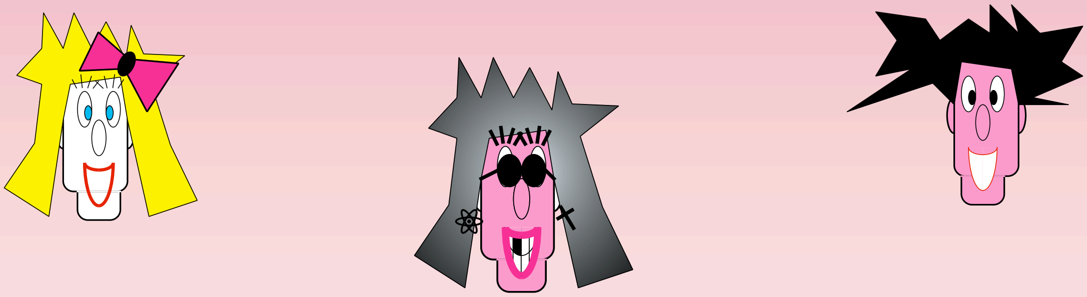
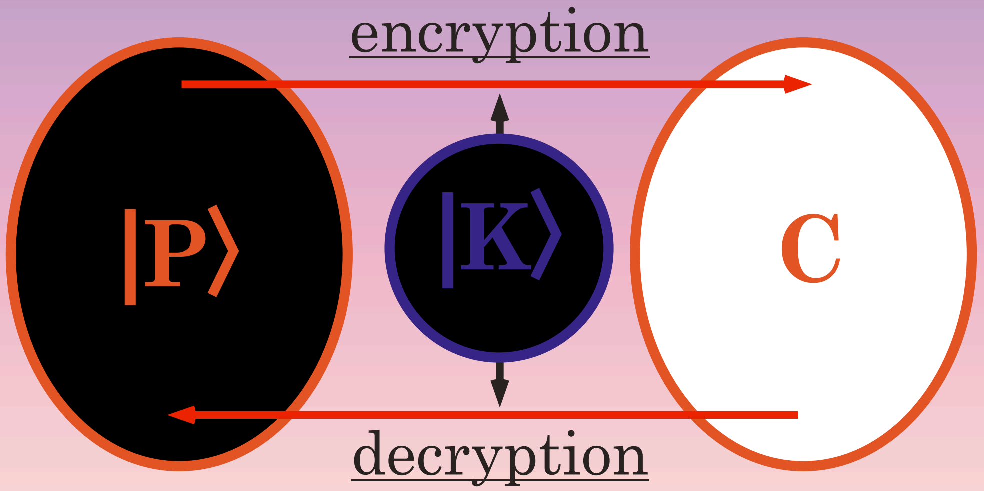
(3.1.2) One-time pad

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

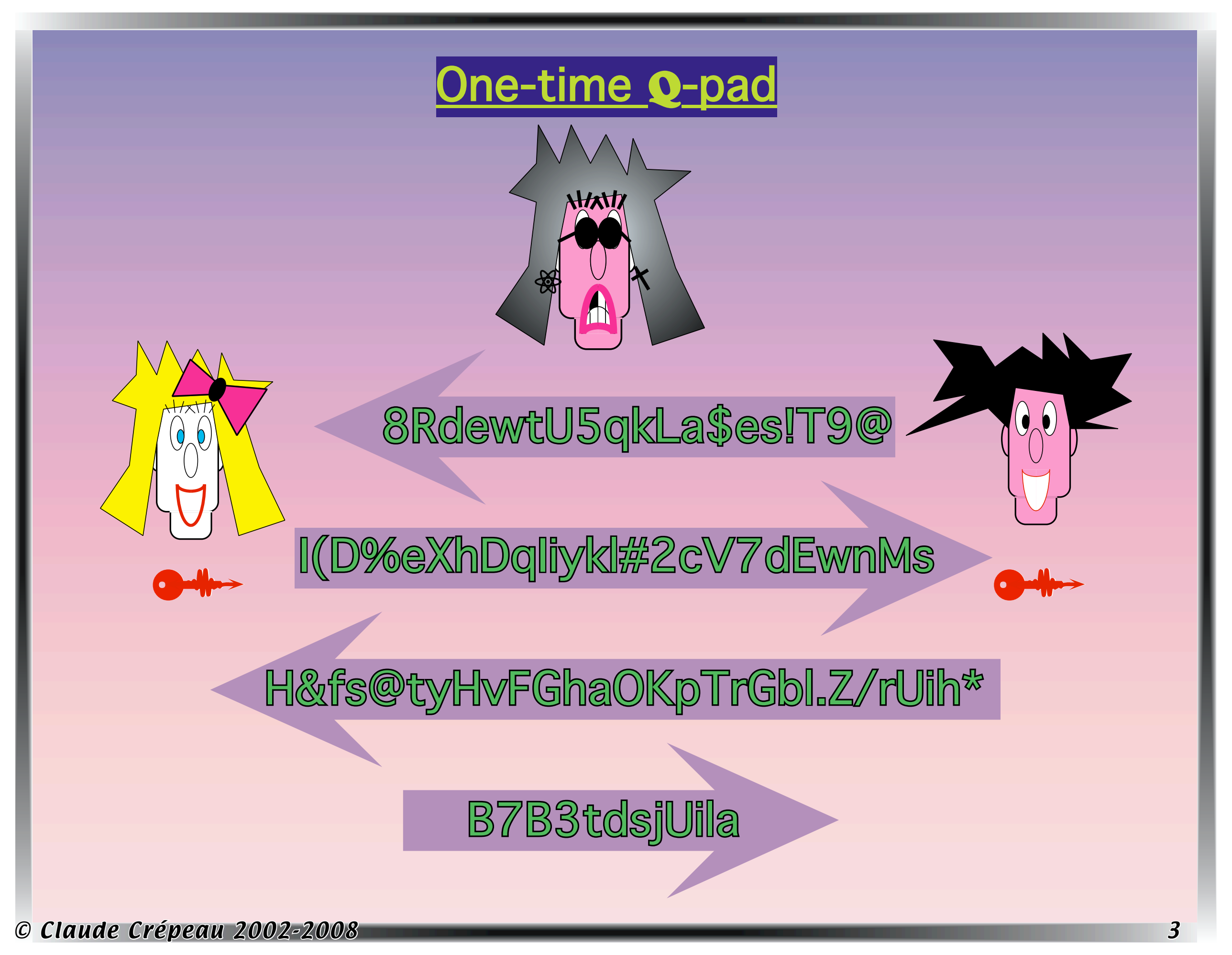
Quantum key : one-time Q-pad (Q-teleportation)
Classical Ciphertext (BBCJPW)



symmetric encryption of Quantum messages



Information Theoretical Security



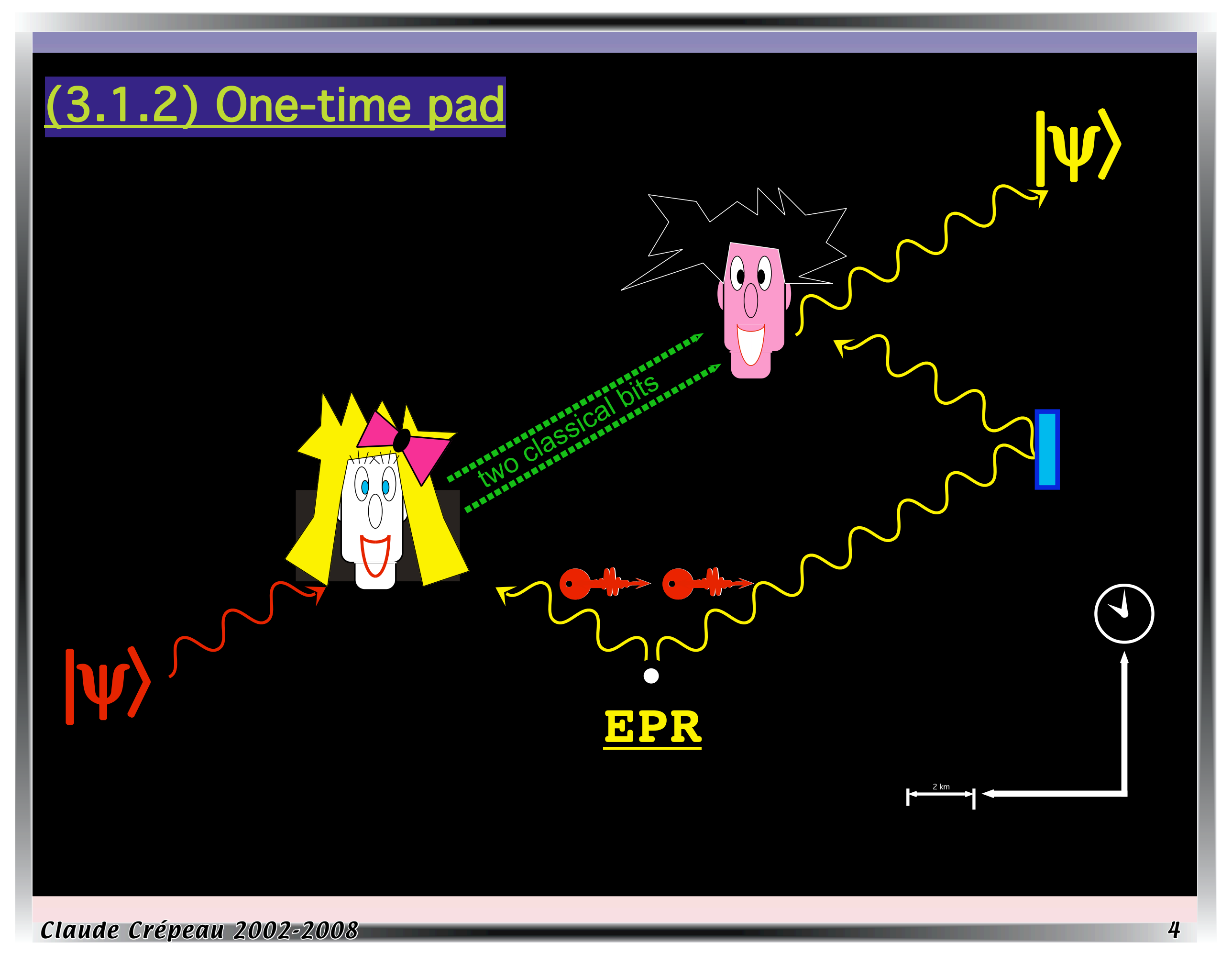
One-time Q-pad

8RdewtU5qkLa$es!T9@

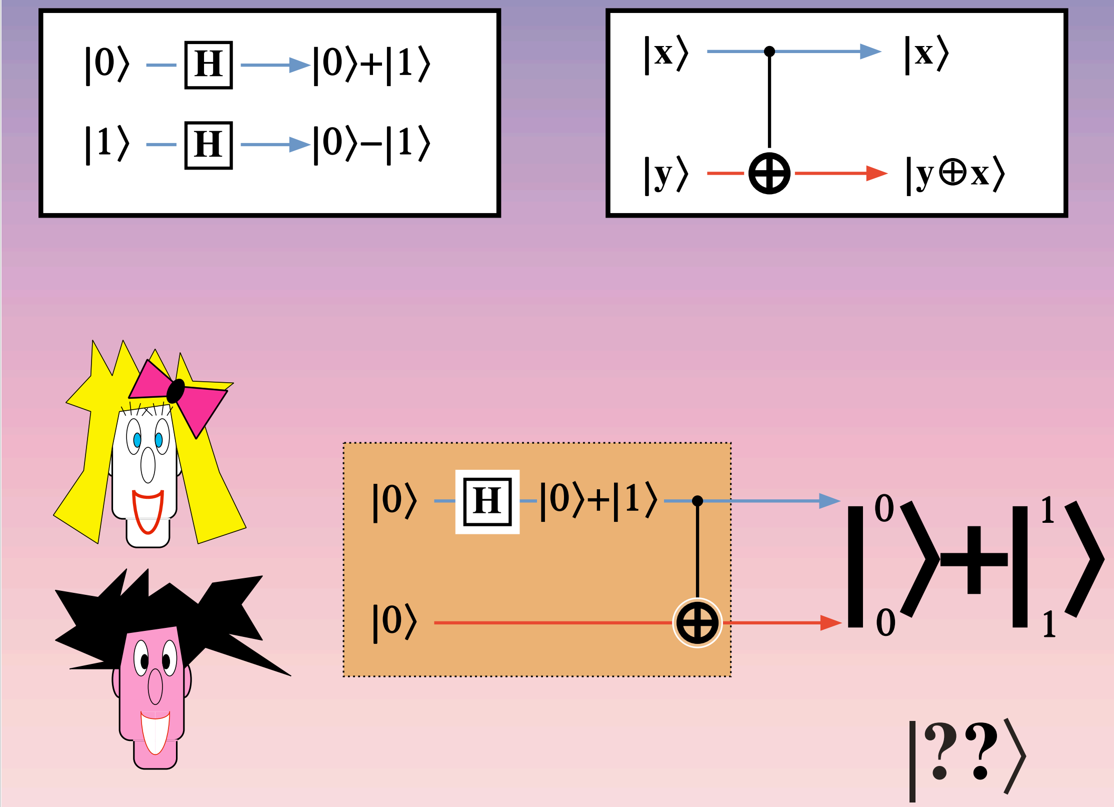
I(D%eXhDqliykl#2cV7dEwnMs

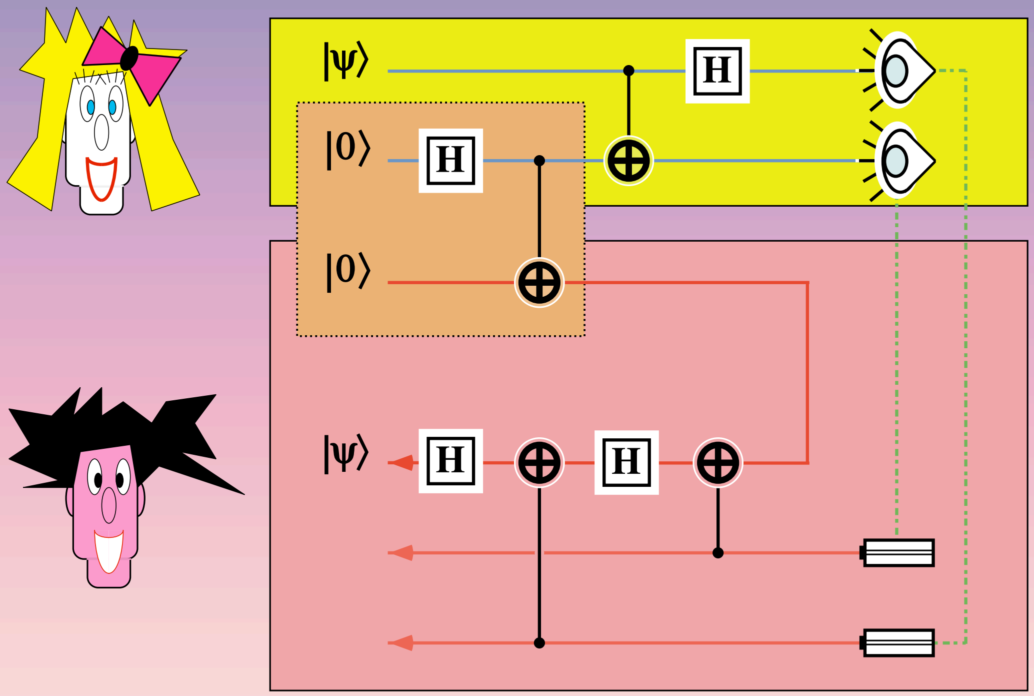
H&fs@tyHvFGhaOKpTrGbl.Z/rUih*

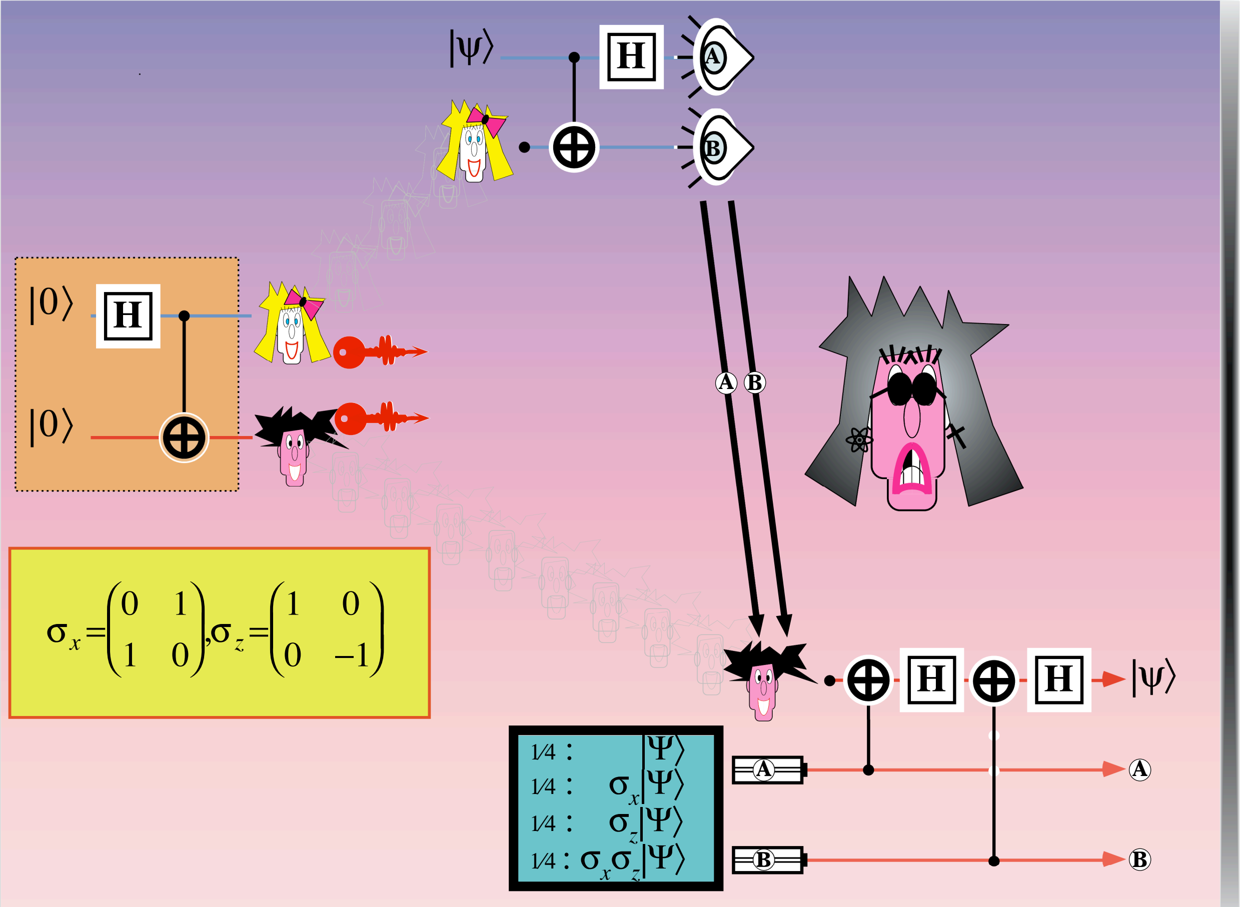
B7B3tdsjUila



(3.1.2) One-time pad


|0⟩ H |0⟩+|1⟩
|1⟩ H |0⟩−|1⟩
|x⟩ |x⟩
|y⟩ ⊕ |y⊕x⟩
|0⟩ H |0⟩+|1⟩
|0⟩ ⊕
|⁰₀⟩+|¹₁⟩
|??⟩


|ψ⟩
H
|0⟩
H
⊕
|0⟩
⊕
|ψ⟩
H
⊕
H
⊕



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

1/4 : $|\Psi\rangle$
1/4 : $\sigma_x|\Psi\rangle$
1/4 : $\sigma_z|\Psi\rangle$
1/4 : $\sigma_x\sigma_z|\Psi\rangle$

(3.1.2b) one-time pad

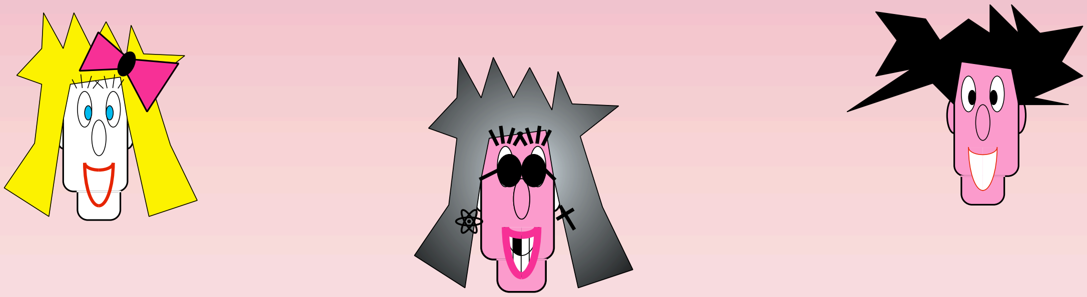
Quantum key : one-time Q-pad
Classical Ciphertext

two random bits
|Ψ⟩

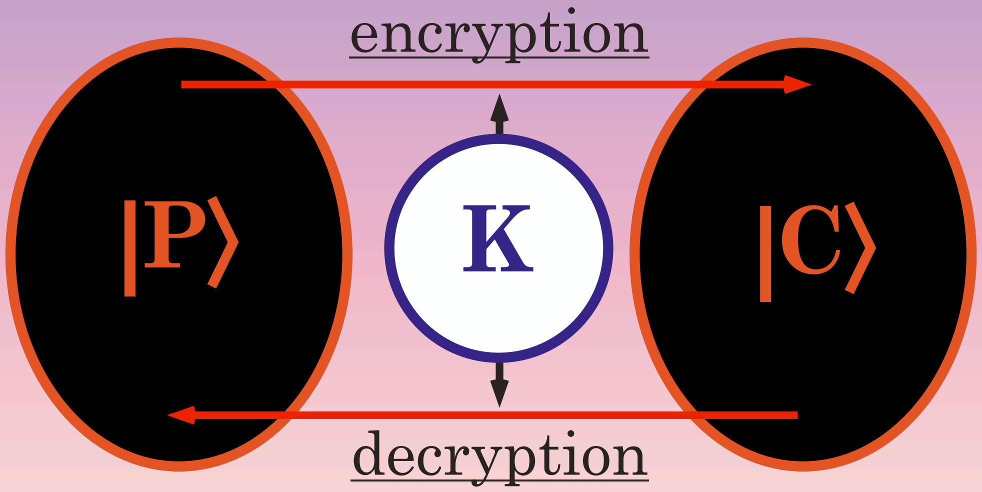
(3.1.2a) One-time pad

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

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



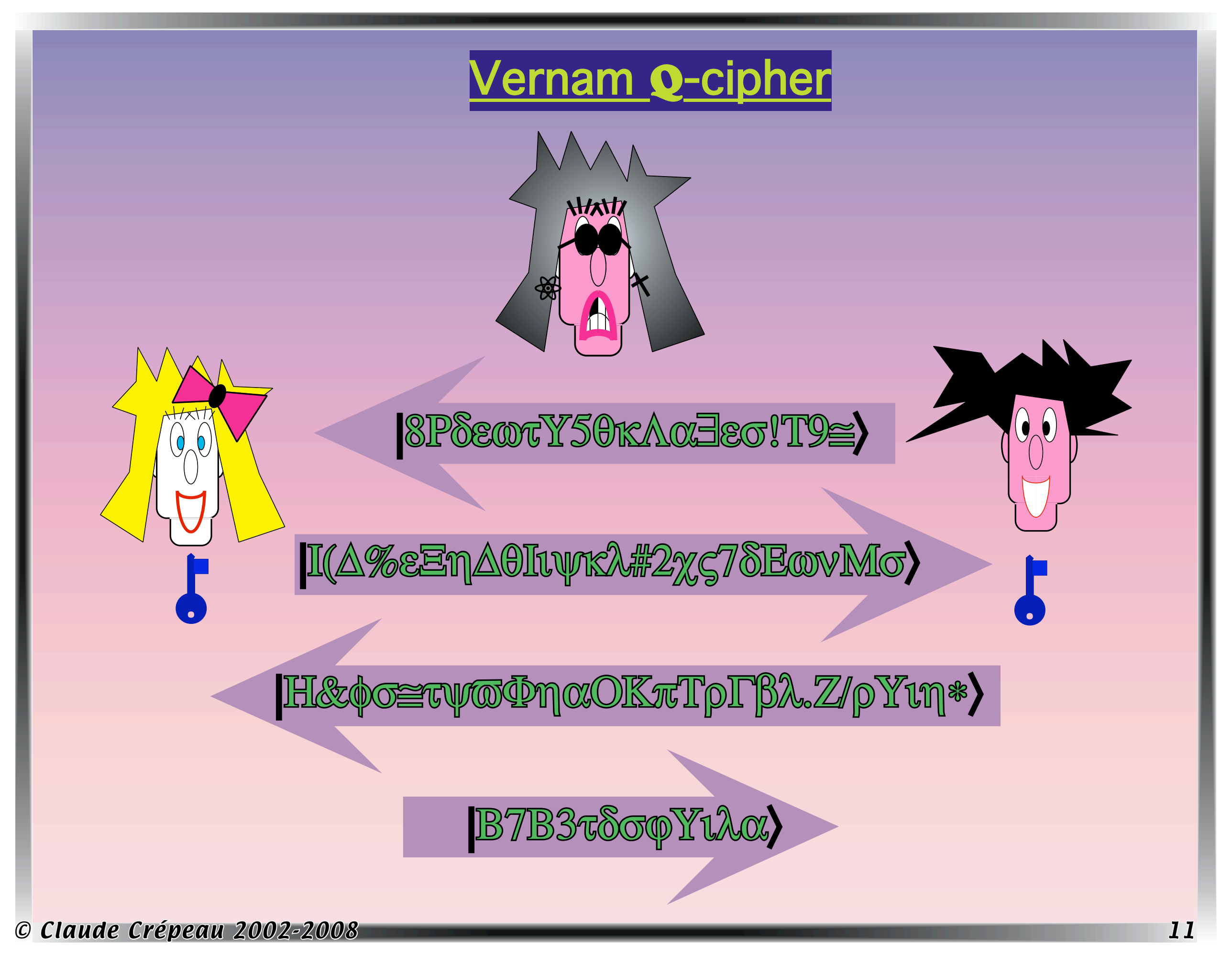
symmetric encryption of Quantum messages



encryption

decryption

Information Theoretical Security



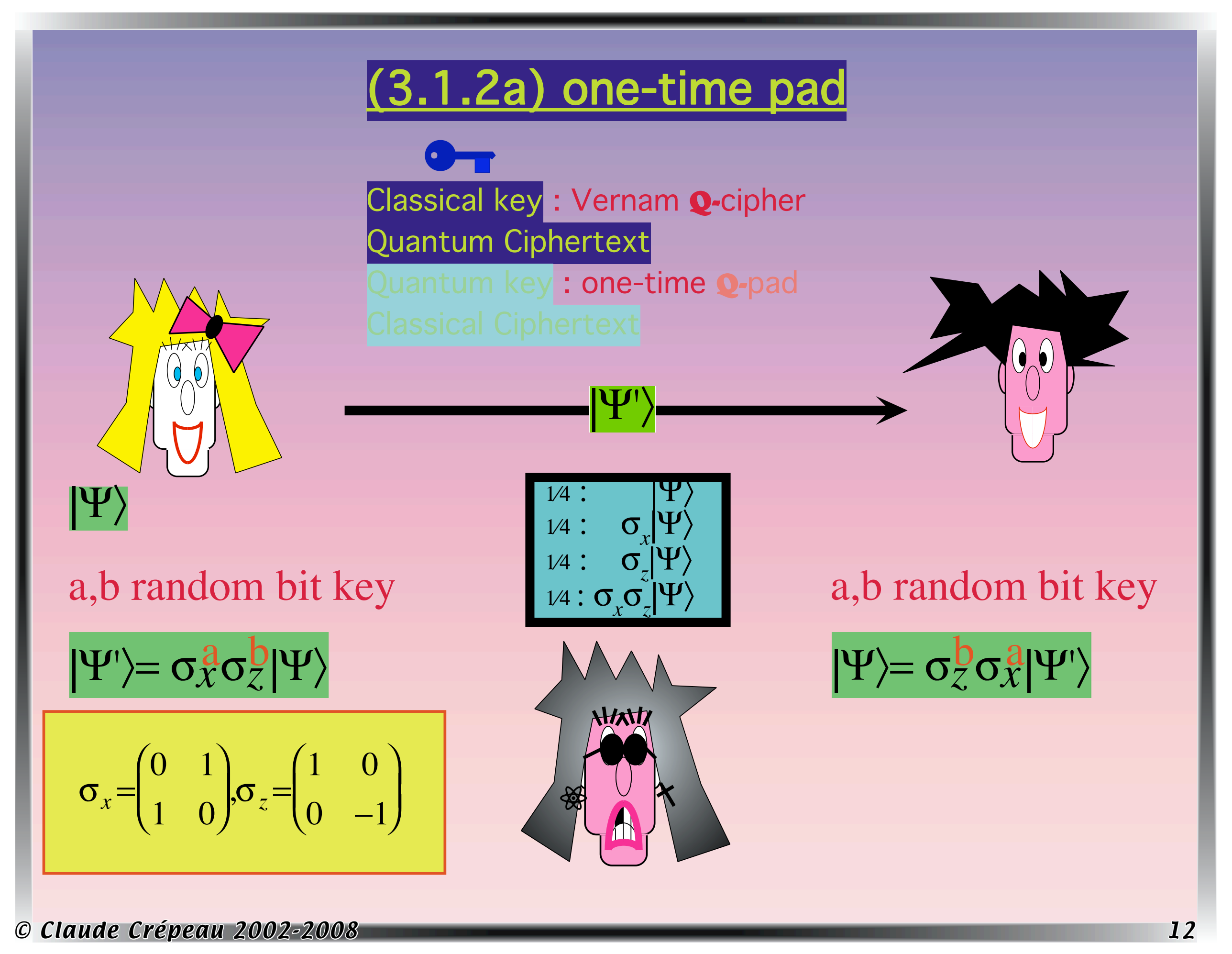
Vernam Q-cipher

|8PδεωτΥ5θκΛα∃εσ!Τ9≅⟩

|Ι(Δ%εΞηΔθΙιψκλ#2χς7δΕωνΜσ⟩

|Η&φσ≅τψϖΦηαΟΚπΤρΓβλ.Ζ/ρΥιη*⟩

|Β7Β3τδσφΥιλα⟩



(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

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

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

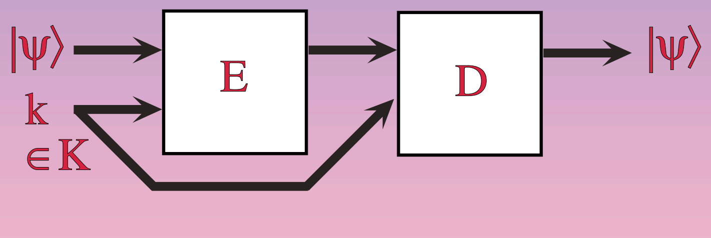
1⁄4 : $|\Psi\rangle$
1⁄4 : $\sigma_x|\Psi\rangle$
1⁄4 : $\sigma_z|\Psi\rangle$
1⁄4 : $\sigma_x\sigma_z|\Psi\rangle$

a,b random bit key

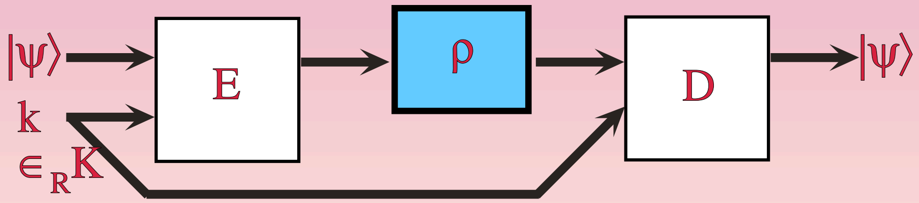
$|\Psi\rangle = \sigma_z^b \sigma_x^a |\Psi'\rangle$

One-time Q-encryption with error ε

Completeness:



Secrecy:



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

One-time Q-encryption with error ε>0

Lower bounds:

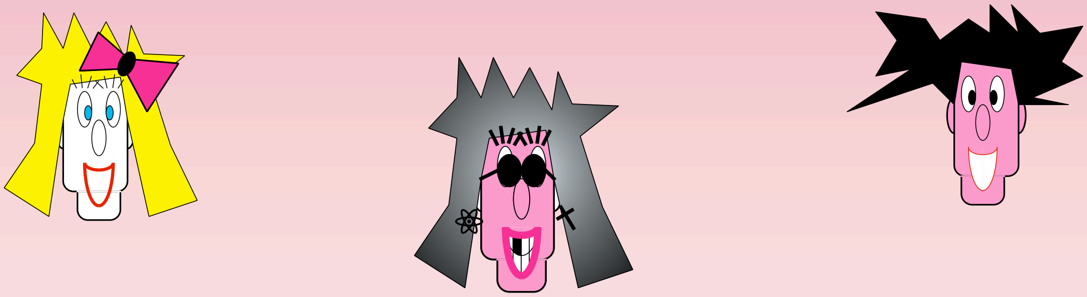
[MTW00]
Arbitrary quantum state = 2 bits / qubit

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

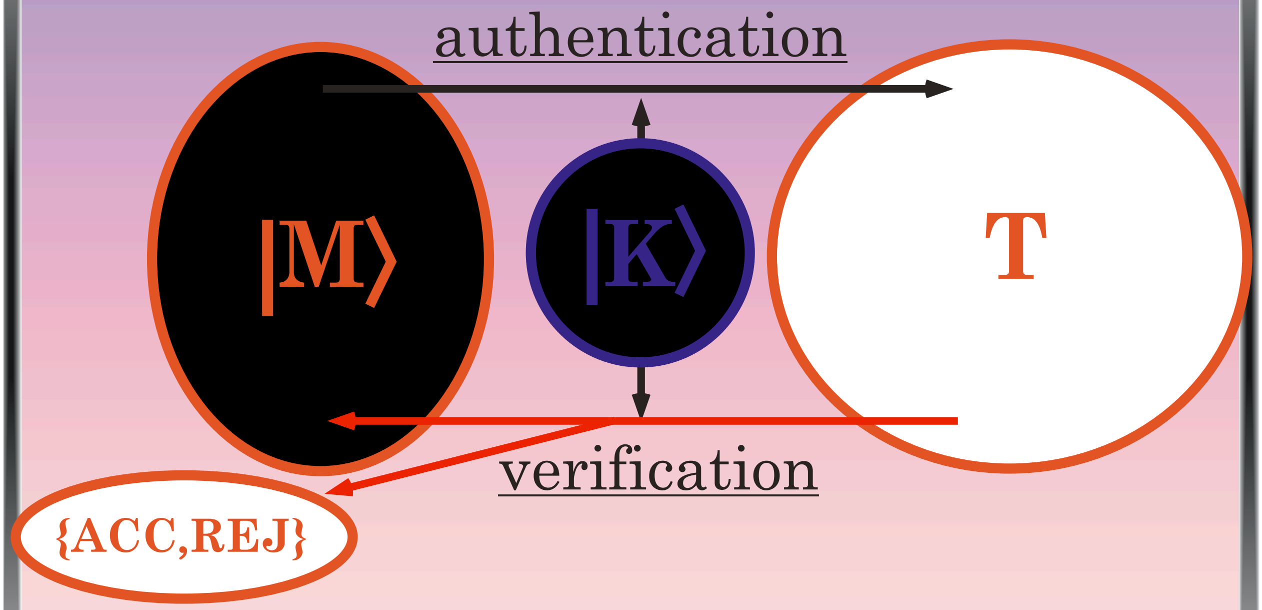
(3.1.3) One-time Q-Authentication

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

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

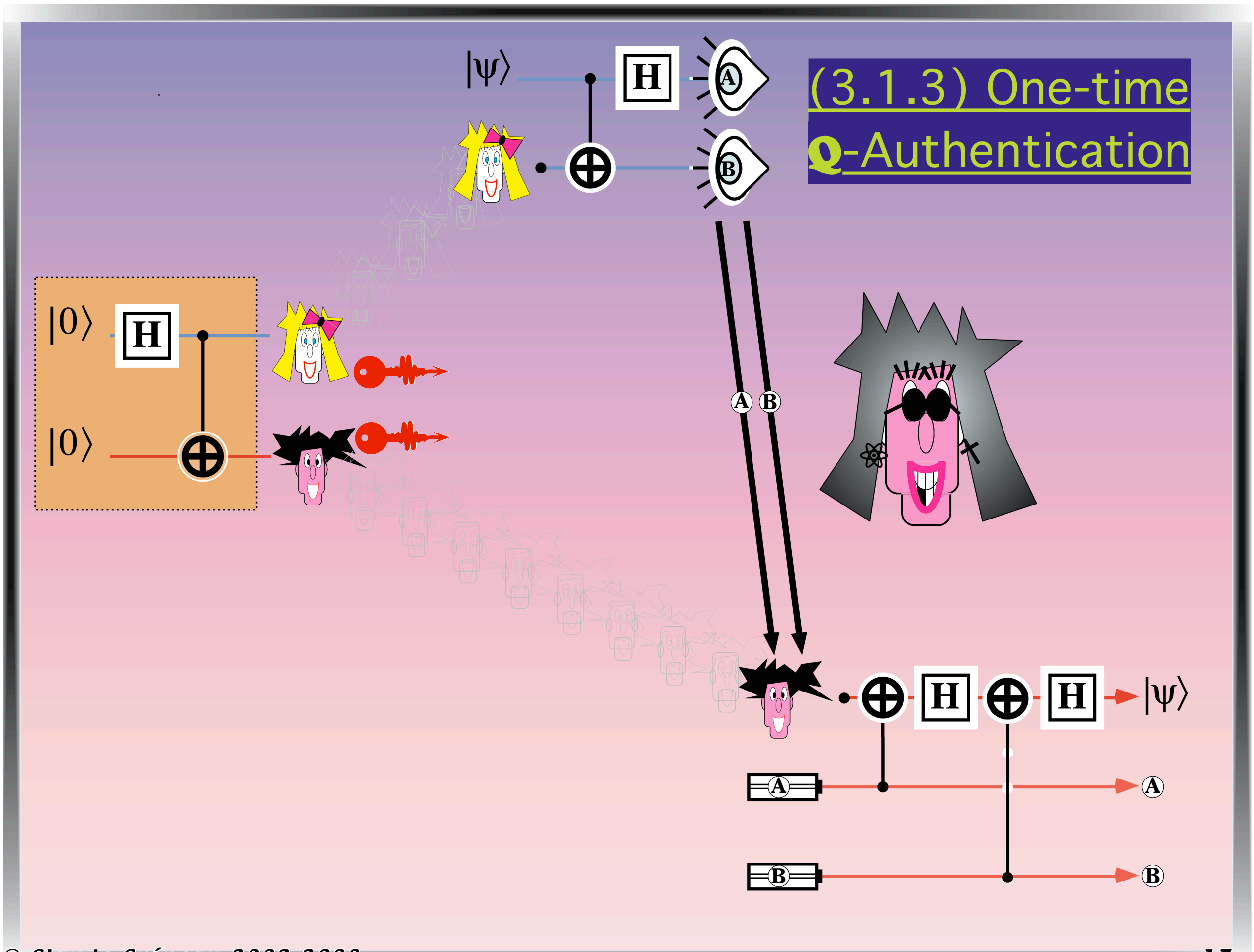


symmetric authentication

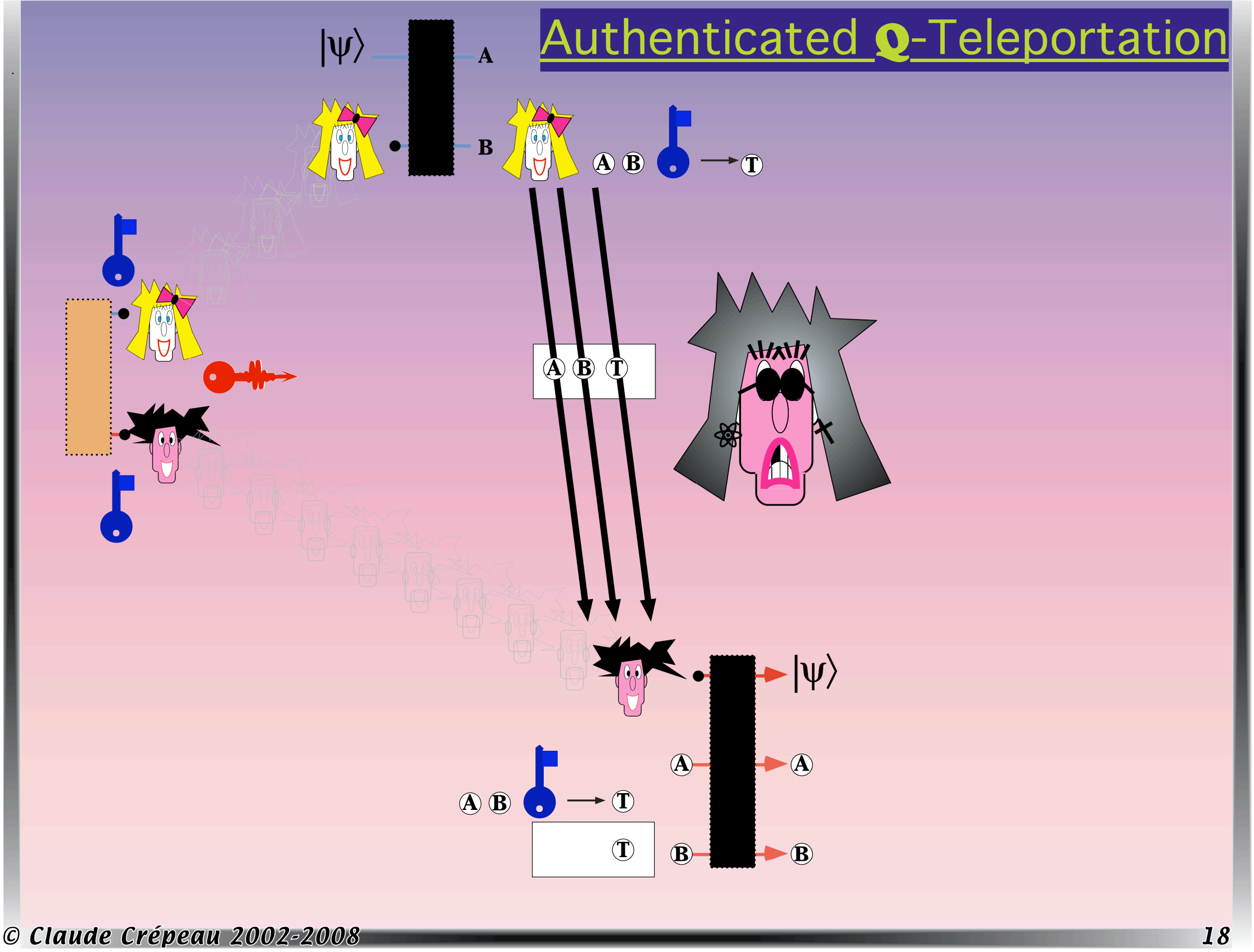


Information Theoretical Security

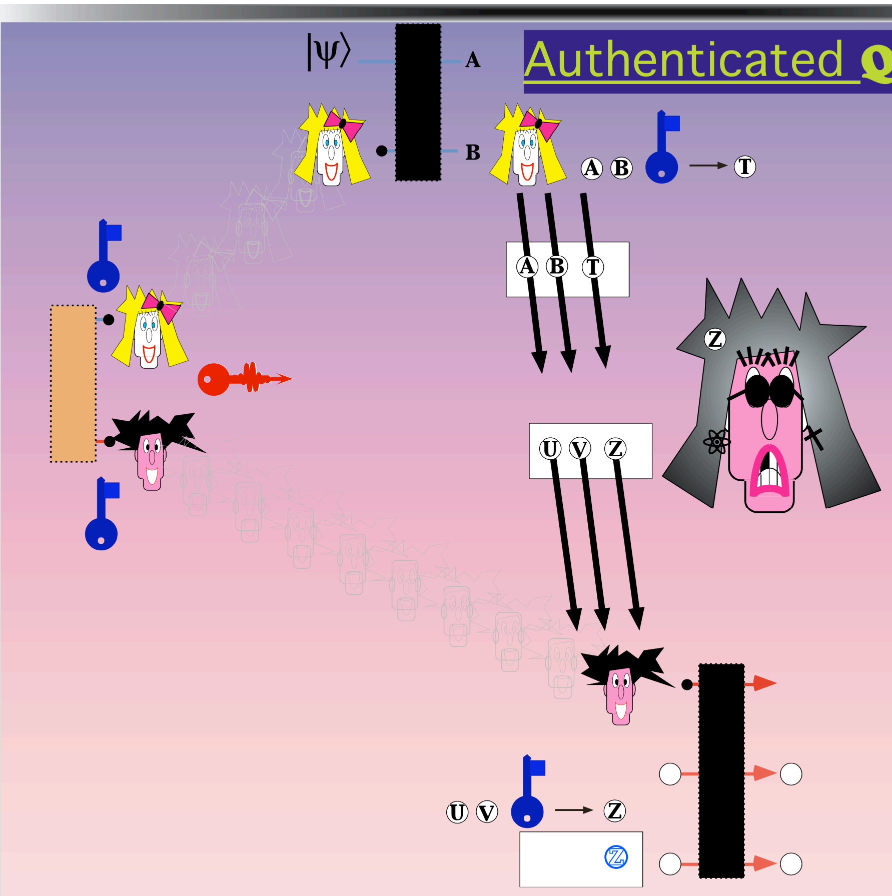
(3.1.3) One-time Q-Authentication



Authenticated Q-Teleportation



Authenticated Q-Teleportation



(3.1.3b) One-time Q-Authentication

Quantum key : 1x Authenticated Q-pad

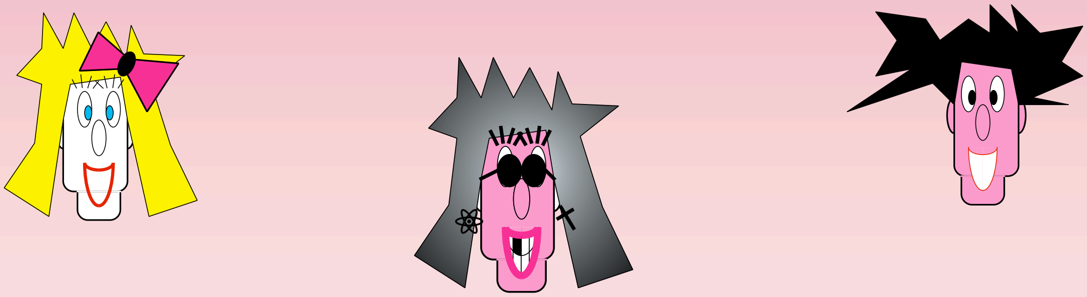
Classical message+tag

two authenticated random bits

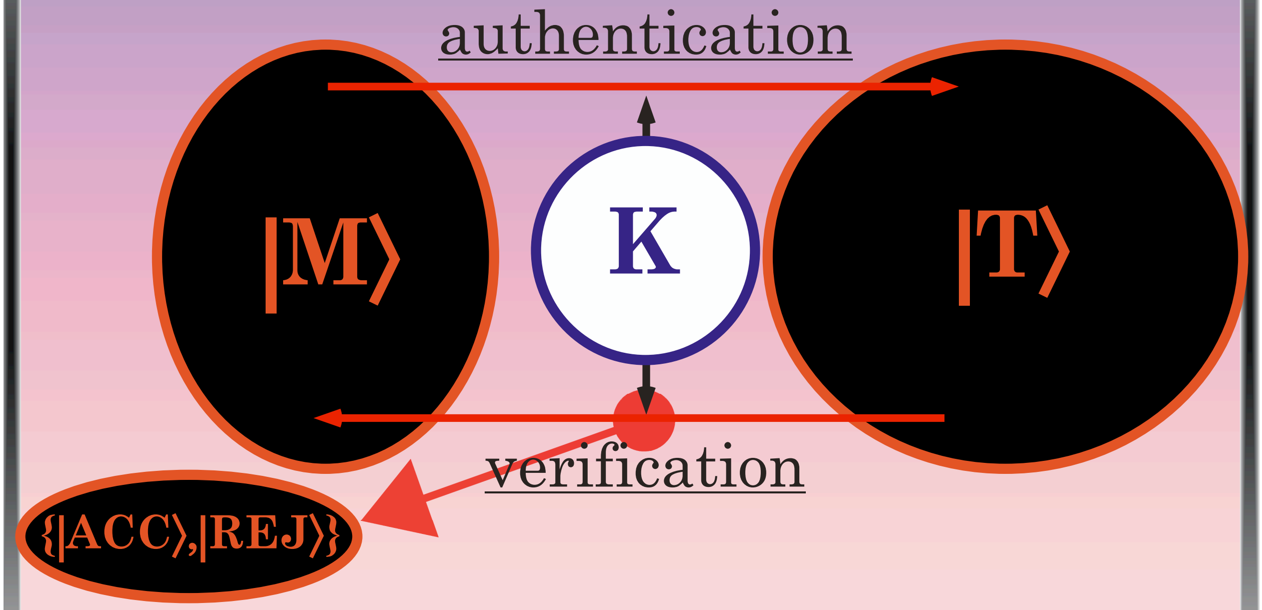
(3.1.3a) One-time Q-Authentication

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

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

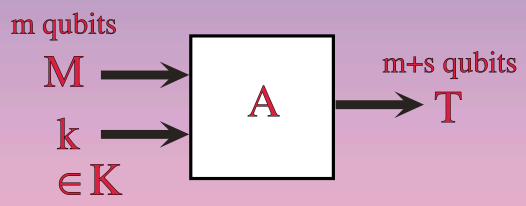


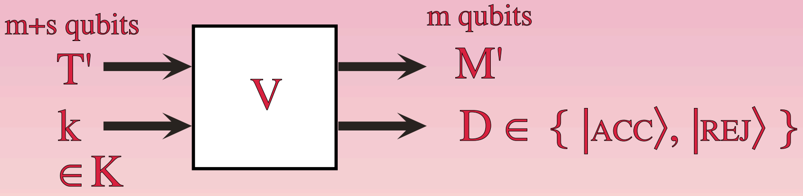
symmetric authentication of Quantum Messages



Information Theoretical Security

One-time Q-Authentication




m+s qubits
T'
k
∈K
V
m qubits
M'
$D \in \{\, |\textsc{acc}\rangle, |\textsc{rej}\rangle \,\}$

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 $D=|\textsc{rej}\rangle$
- output Wrong otherwise

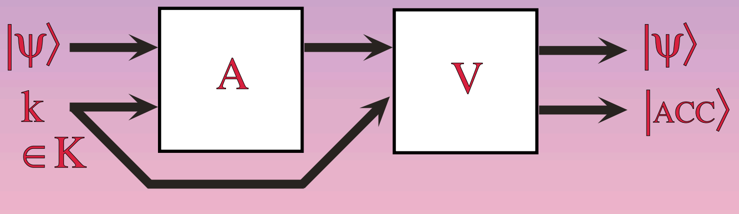
The corresponding projectors are

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

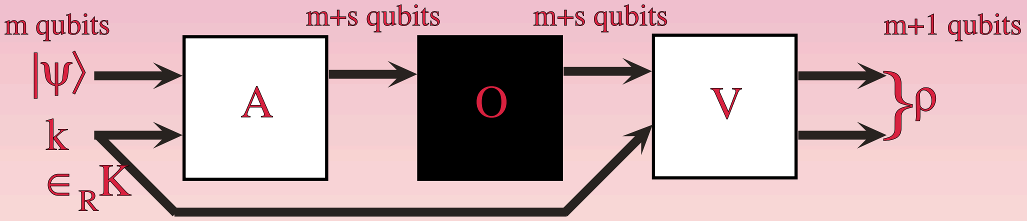
$$W_{|\psi\rangle} = (I_{M'} - |\psi\rangle\langle\psi|) \otimes |\textsc{acc}\rangle\langle\textsc{acc}|$$

One-time Q-Authentication

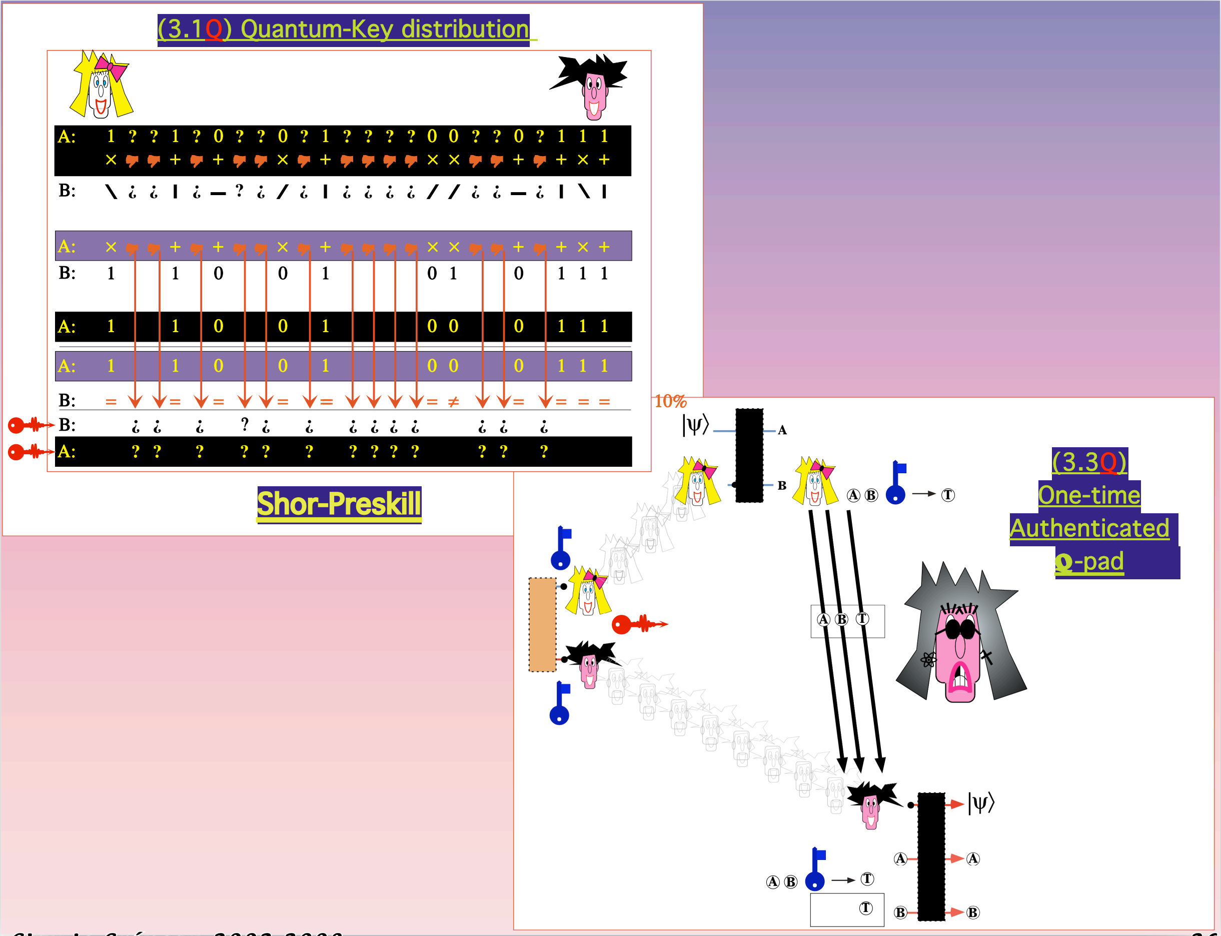
Completeness:



Soundness:



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



(3.1Q) Quantum-Key distribution

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

10%

Shor-Preskill

(3.3Q) One-time Authenticated Q-pad

(3.3C) One-time interactive Q-Authentication

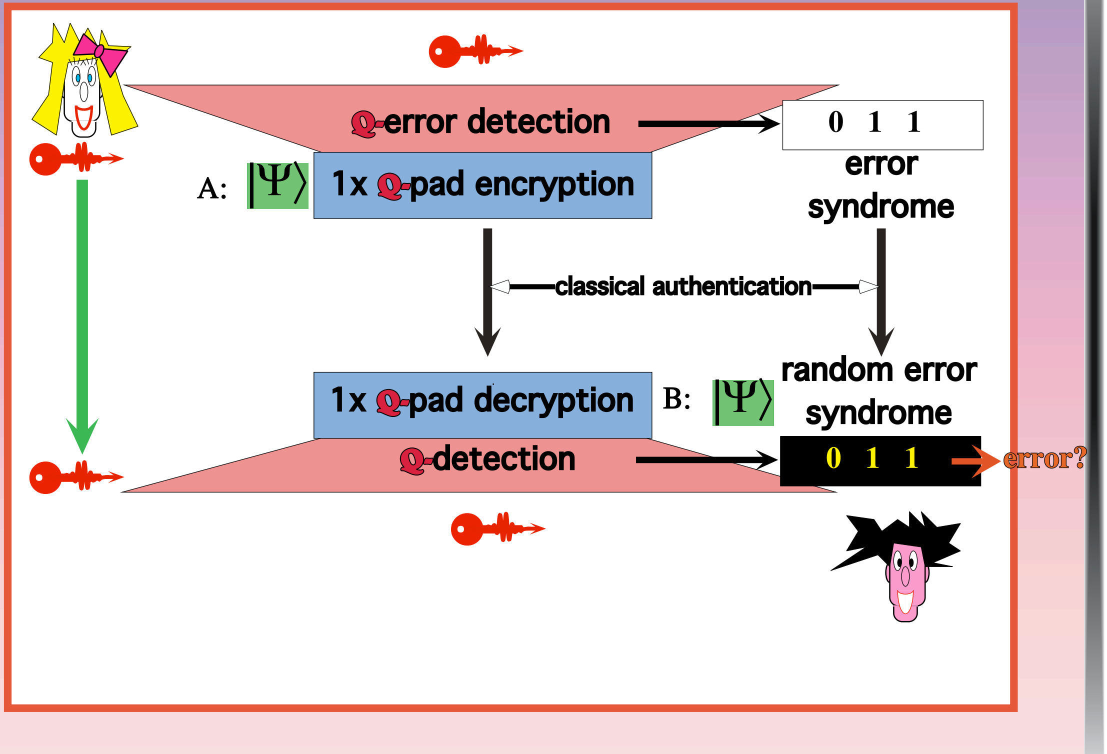
.....

- 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



Q-error detection

0 1 1

error syndrome

A: $|\Psi\rangle$

1x Q-pad encryption

classical authentication

1x Q-pad decryption

B: $|\Psi\rangle$

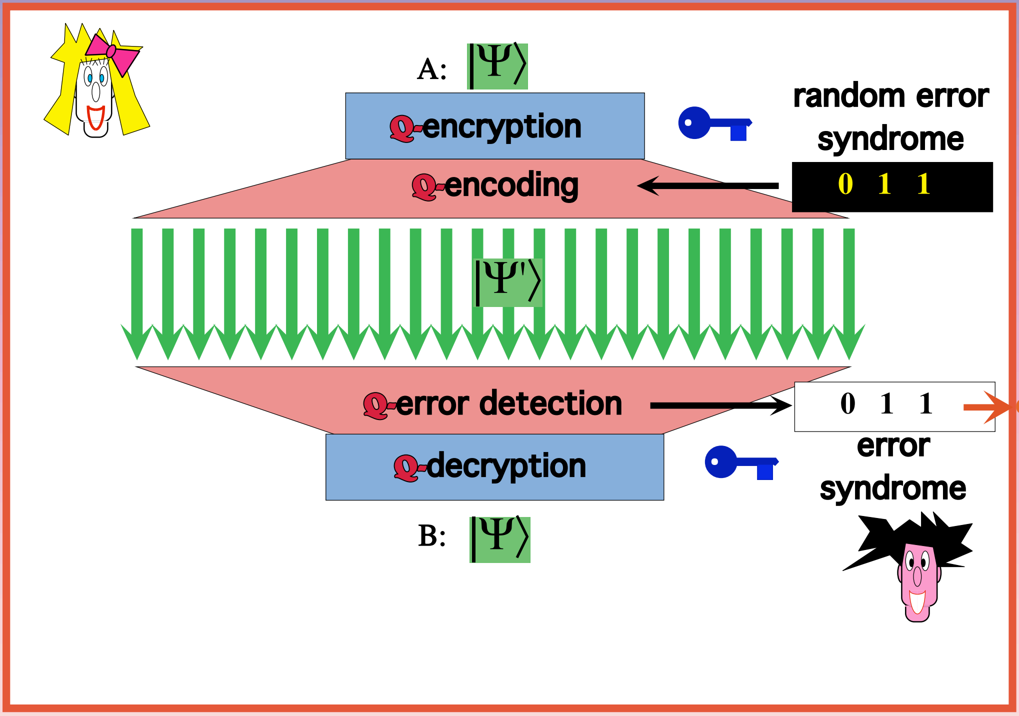
random error syndrome

Q-detection

0 1 1

error?

(3.1.3a) One-time Q-Authentication



A: |Ψ⟩

Q-encryption

random error syndrome

0 1 1

Q-encoding

|Ψ'⟩

Q-error detection

0 1 1

error?

error syndrome

Q-decryption

B: |Ψ⟩

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

|Ψ⟩

|Ψ'⟩

- 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

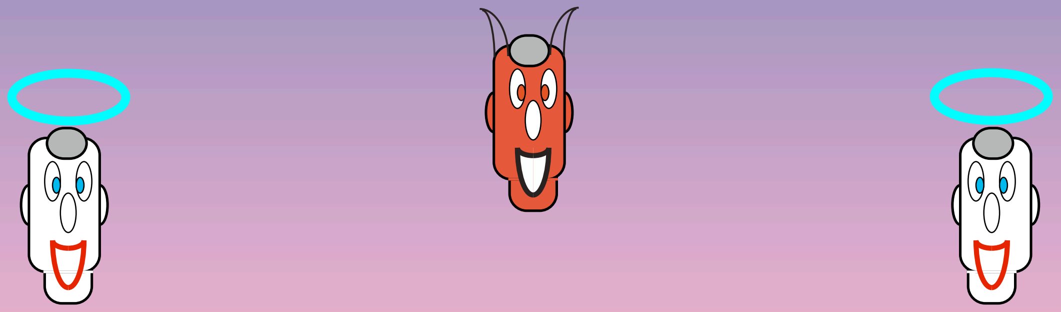
A Quantum Authentication Scheme with error probability ε

is

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

(3.2)
Complexity Theoretical Quantum Cryptography

(3.2) Complexity Theoretical Cryptography



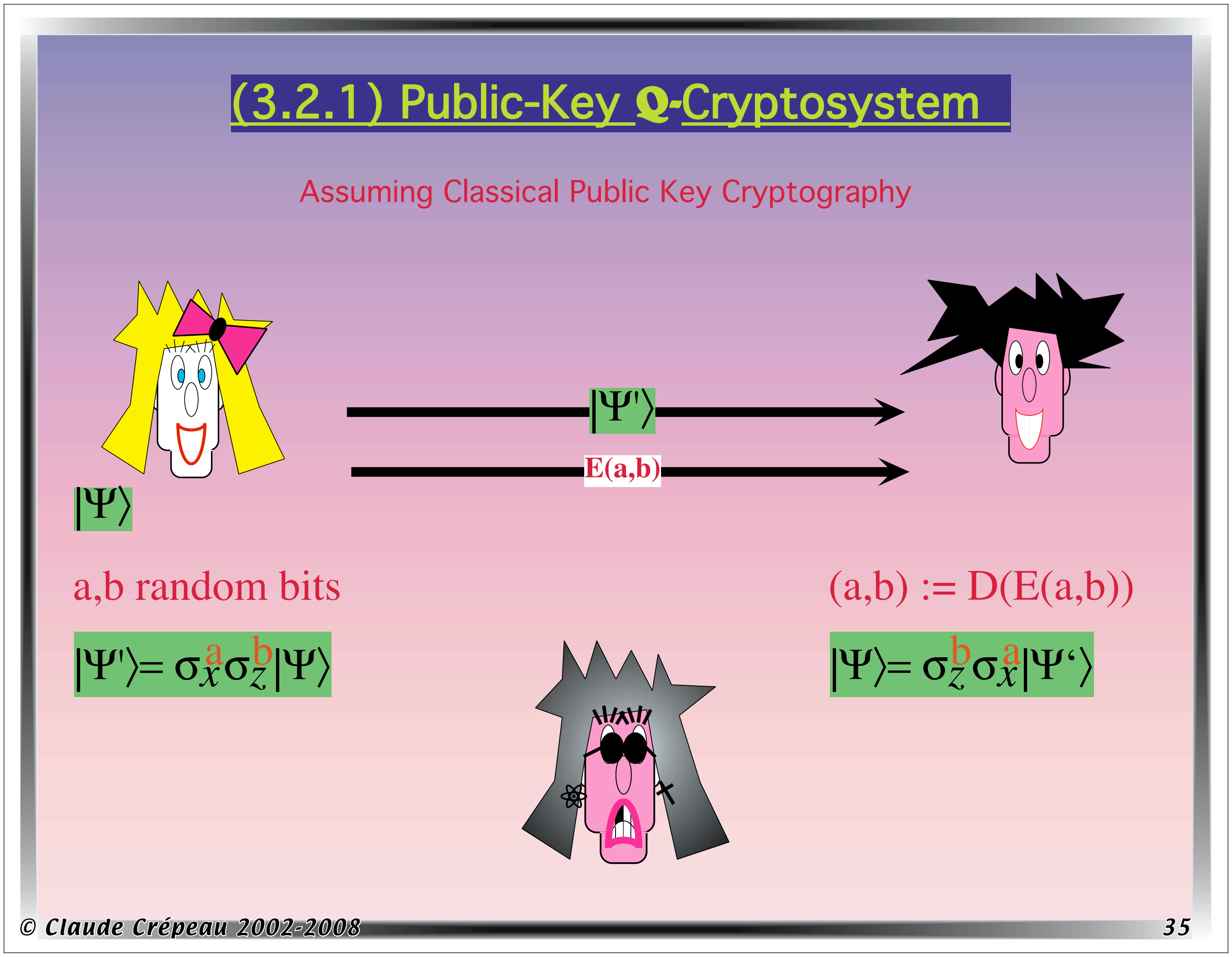
• • • • •

(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

$|\Psi'\rangle$

E(a,b)

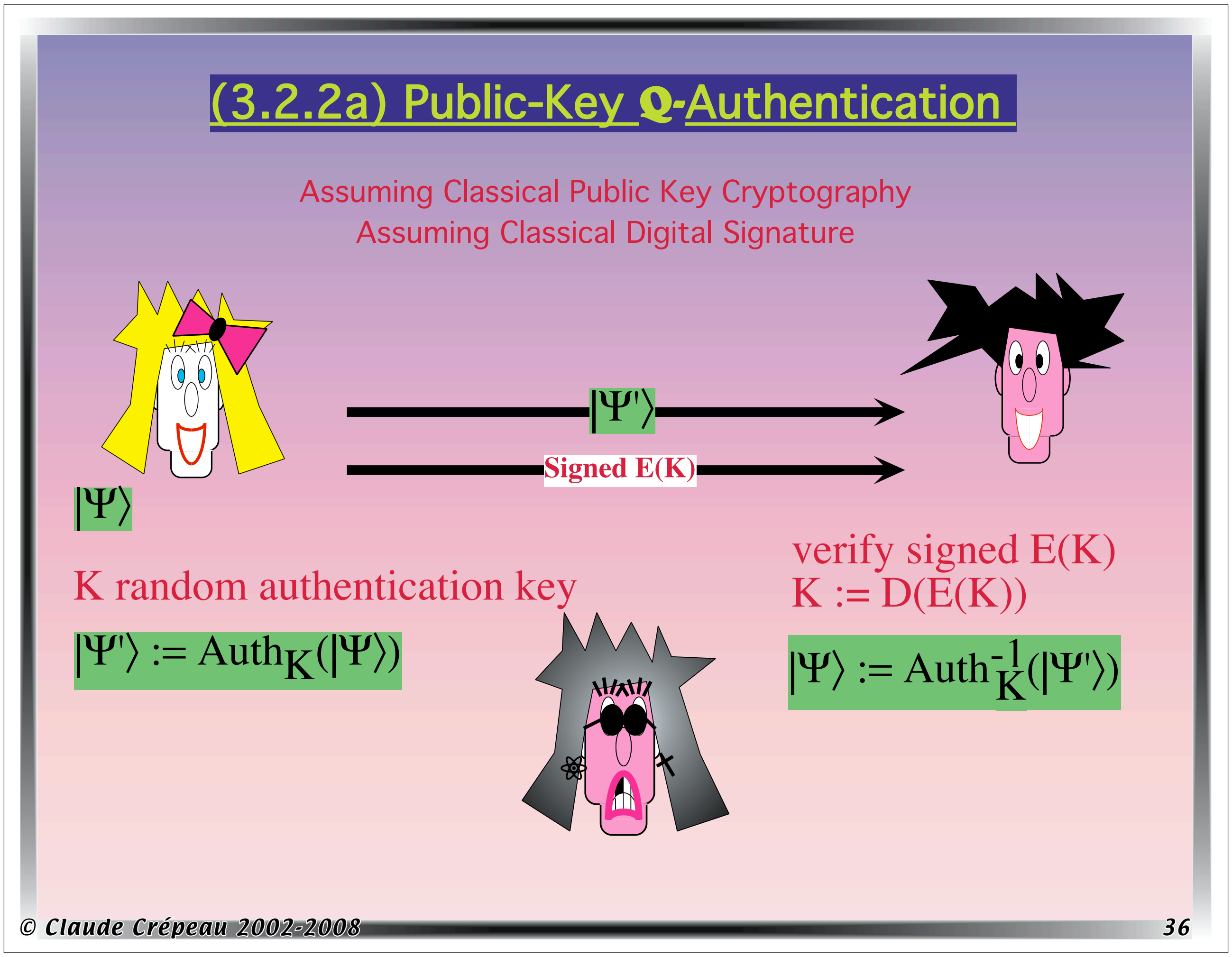
$|\Psi\rangle$

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

$|\Psi'\rangle$

Signed E(K)

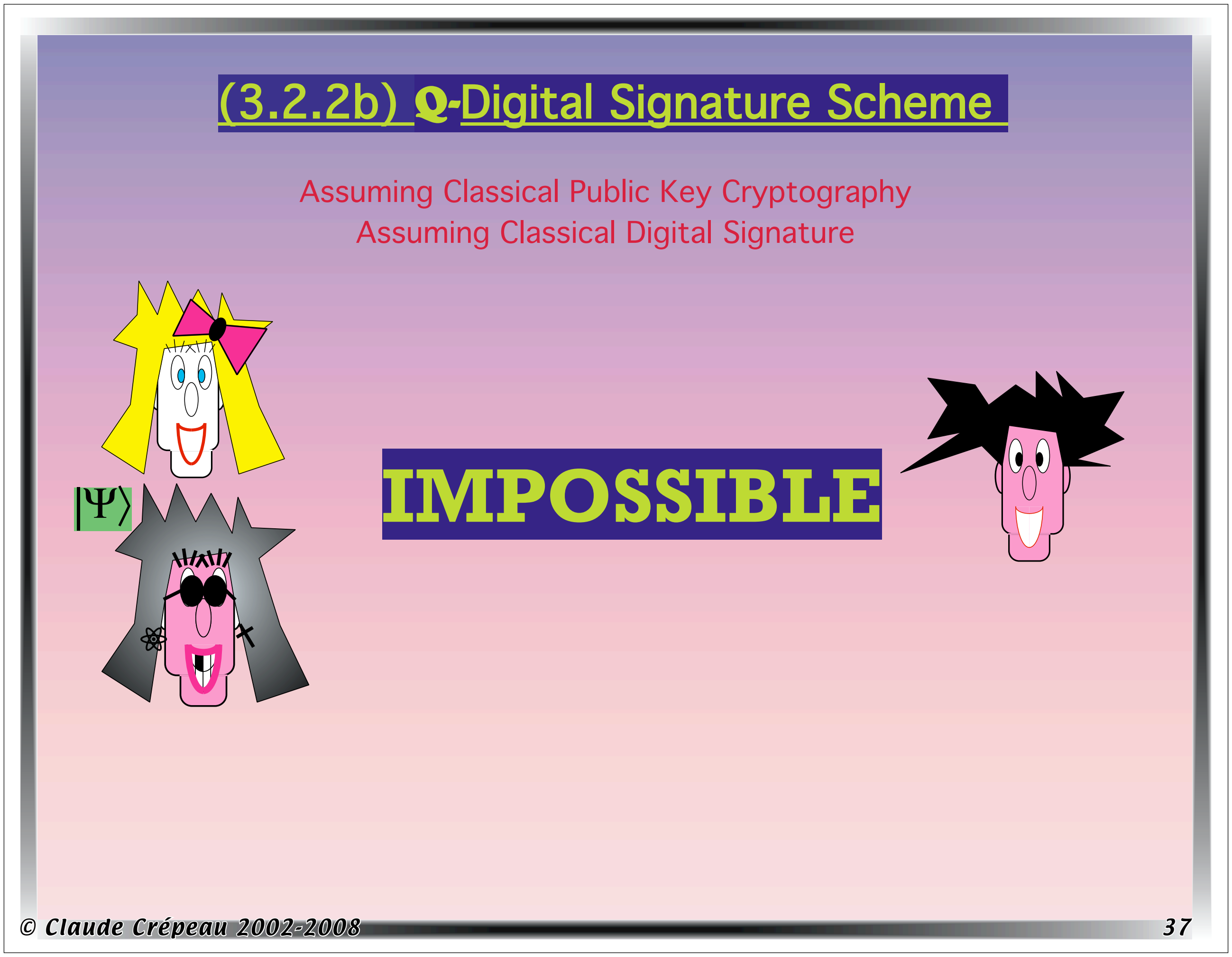
$|\Psi\rangle$

K random authentication key

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

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

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

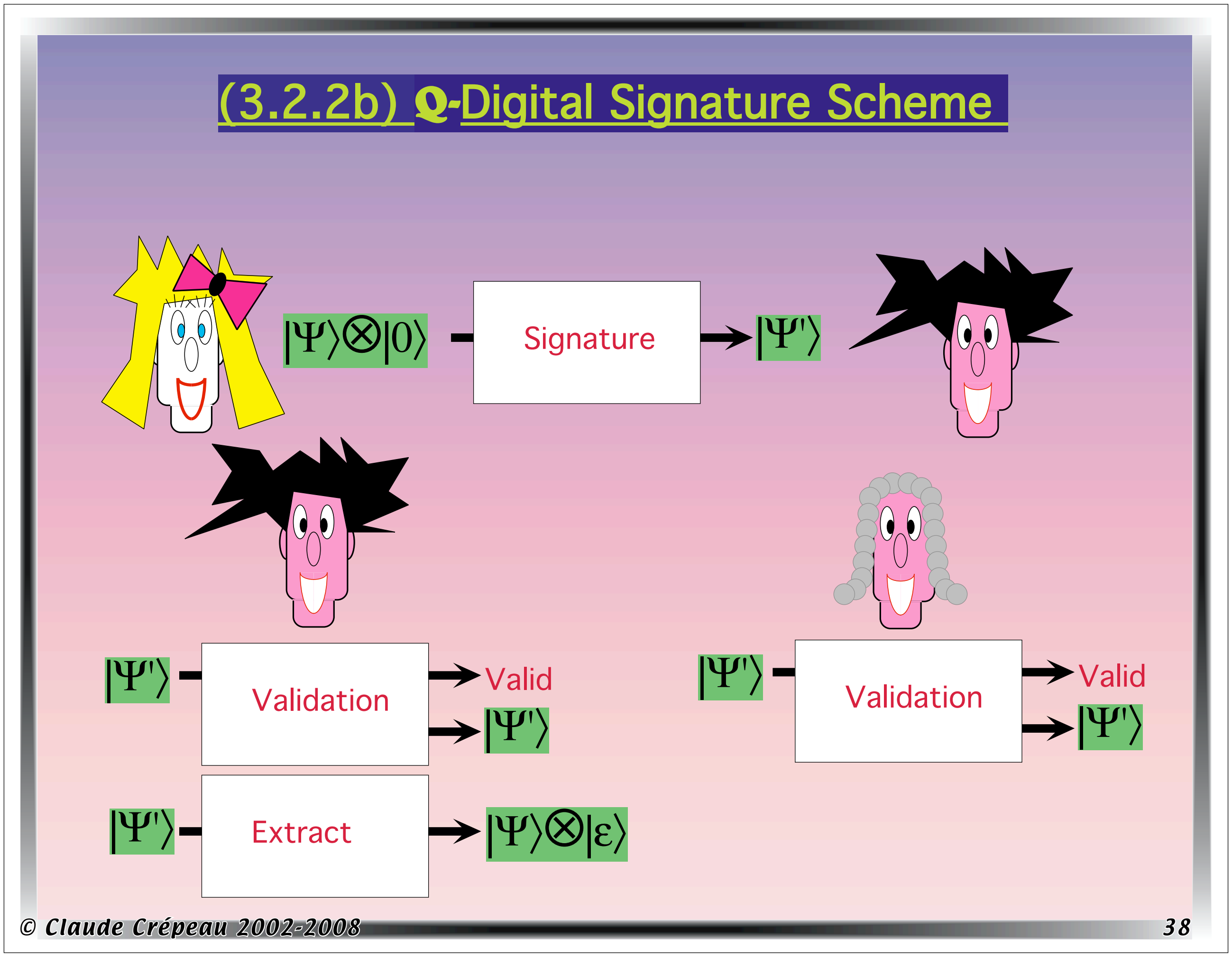


(3.2.2b) Q-Digital Signature Scheme

Assuming Classical Public Key Cryptography
Assuming Classical Digital Signature

$|\Psi\rangle$

IMPOSSIBLE



(3.2.2b) Q-Digital Signature Scheme

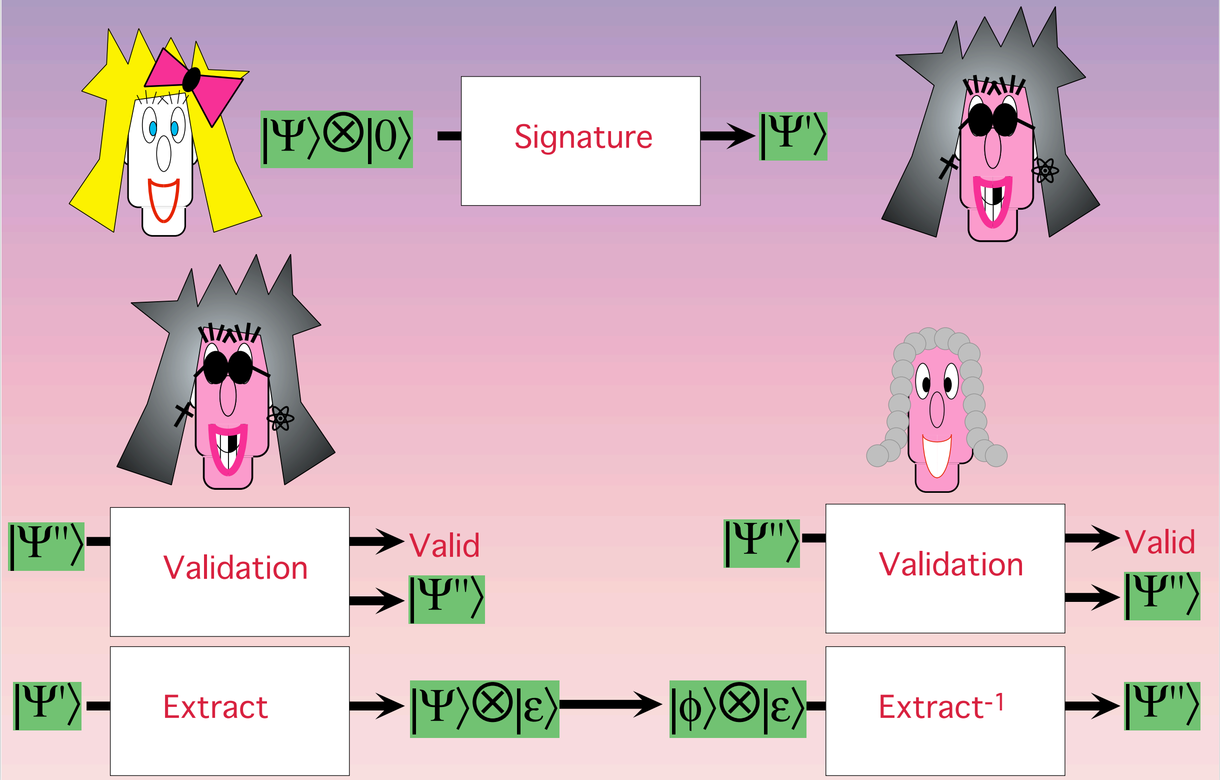
$|\Psi\rangle\otimes|0\rangle$ → Signature → $|\Psi'\rangle$

$|\Psi'\rangle$ → 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 $|\Psi''\rangle$

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

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

(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)

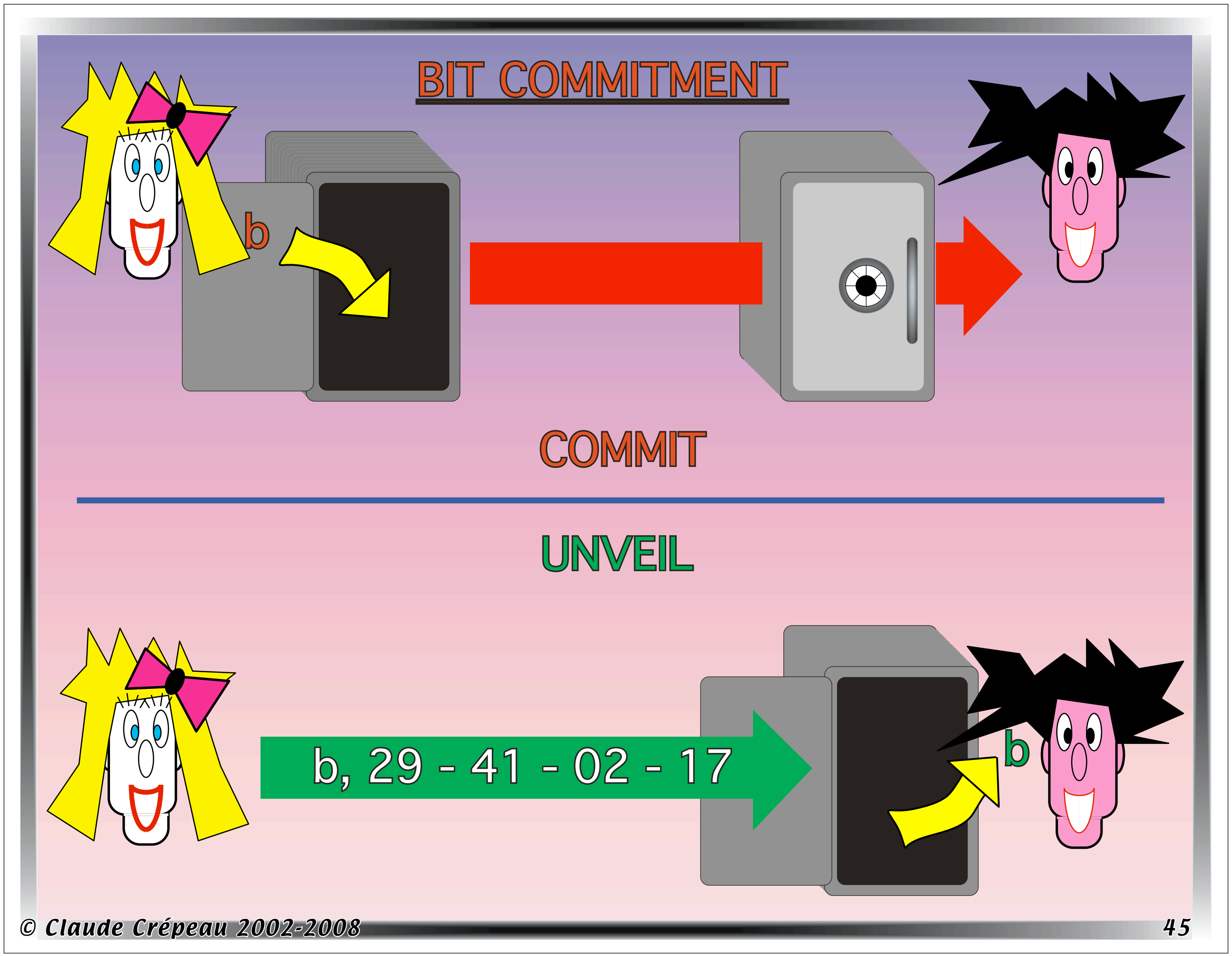
generation : quantum easy
computing f : classical easy
inverting f : classical /quantum hard ???
trapdooring f : classical easy

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

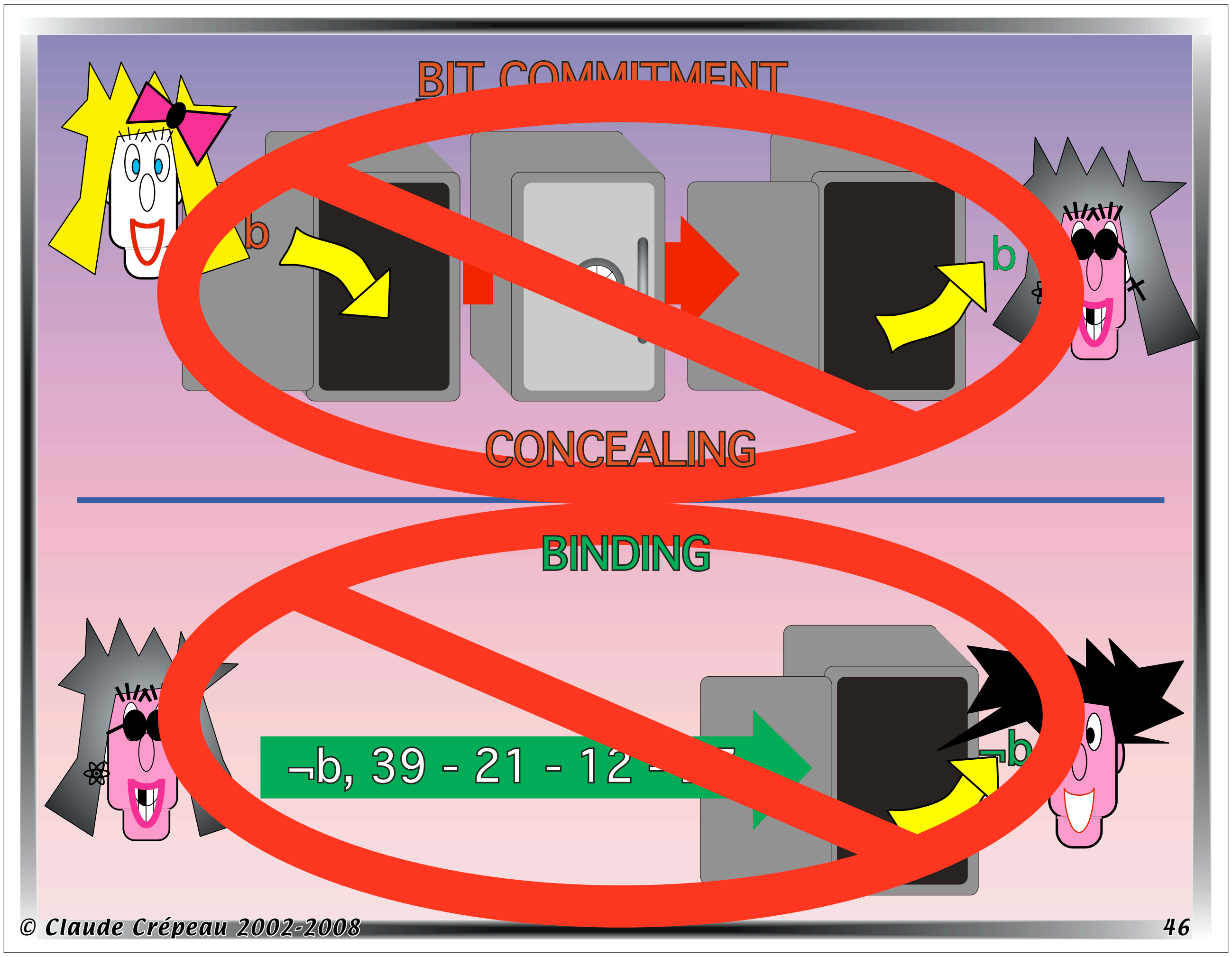
(4)
two-party
Cryptographic Protocols



BIT COMMITMENT

COMMIT

UNVEIL

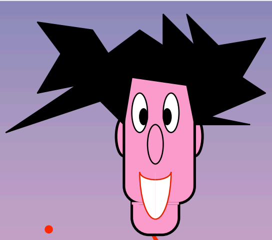


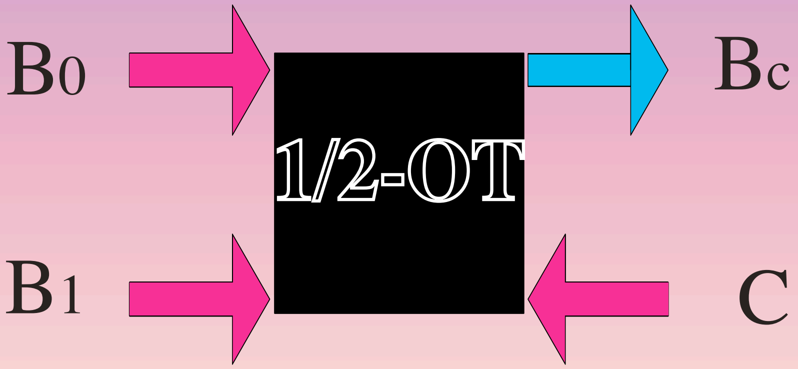
BIT COMMITMENT

CONCEALING

BINDING

Oblivious Transfer (message multiplexing)





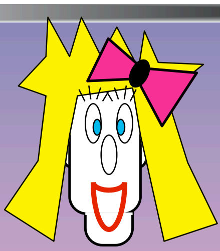
B0

B1

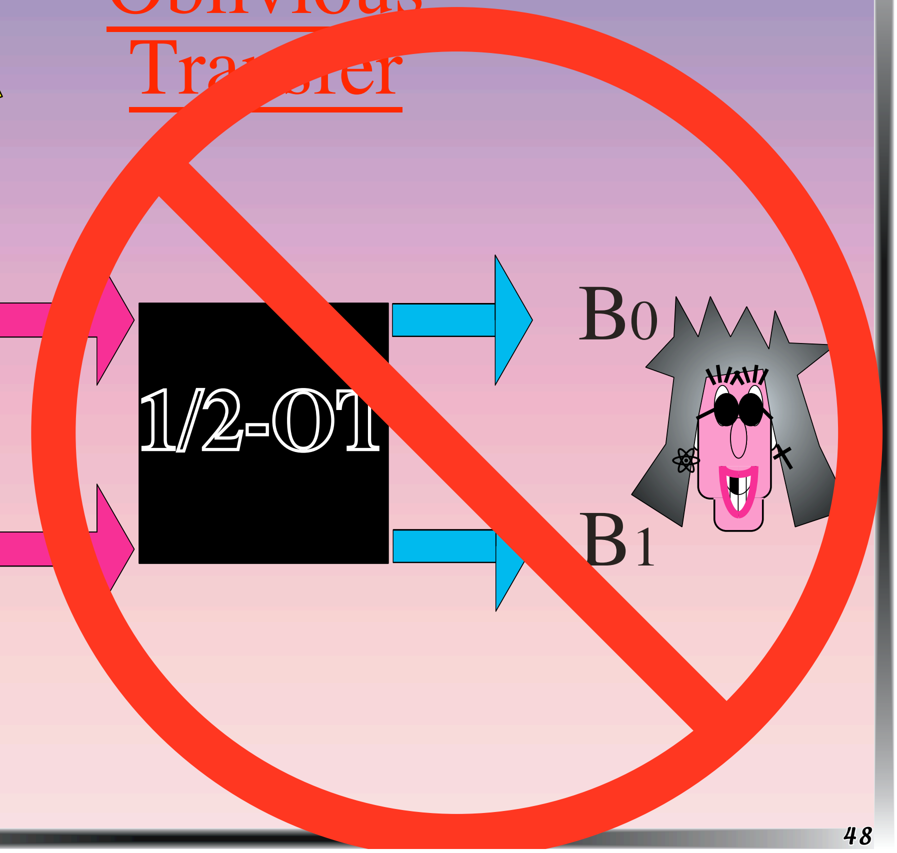
1/2-OT

Bc

C



Oblivious Transfer



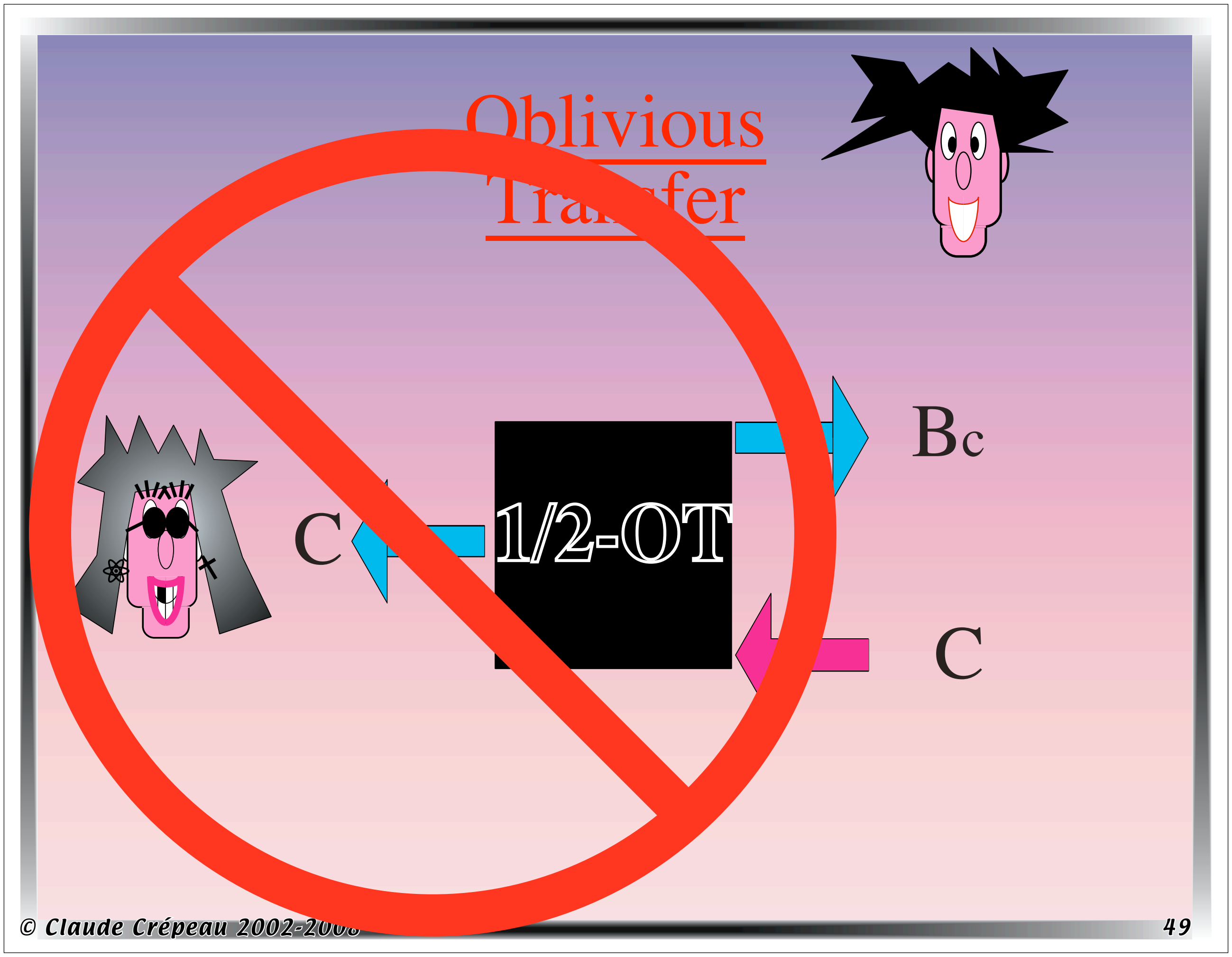
B0

B1

1/2-OT

B0

B1



Oblivious Transfer

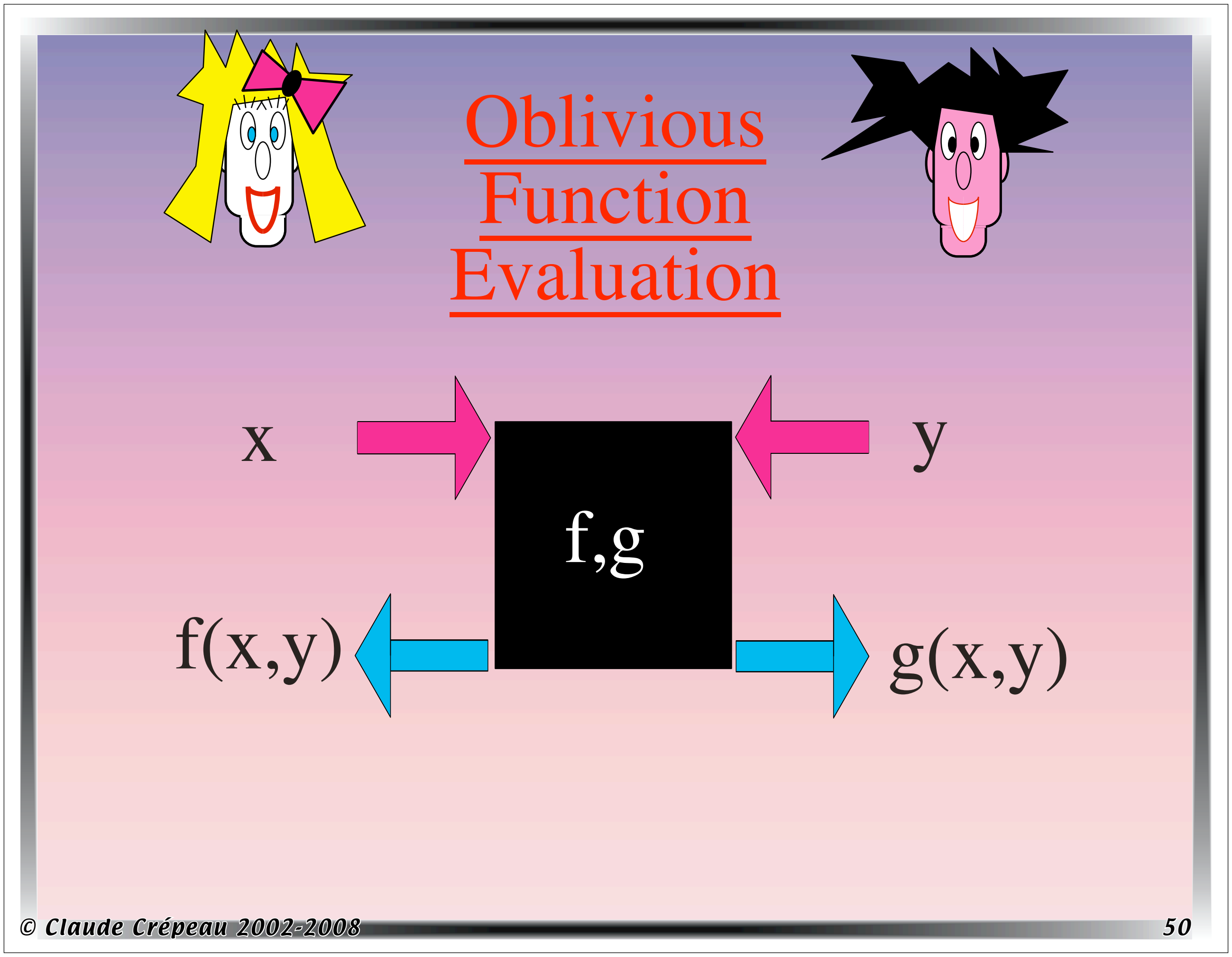
Bc

C

1/2-OT

C

© Claude Crépeau 2002-2008



Oblivious Function Evaluation

x

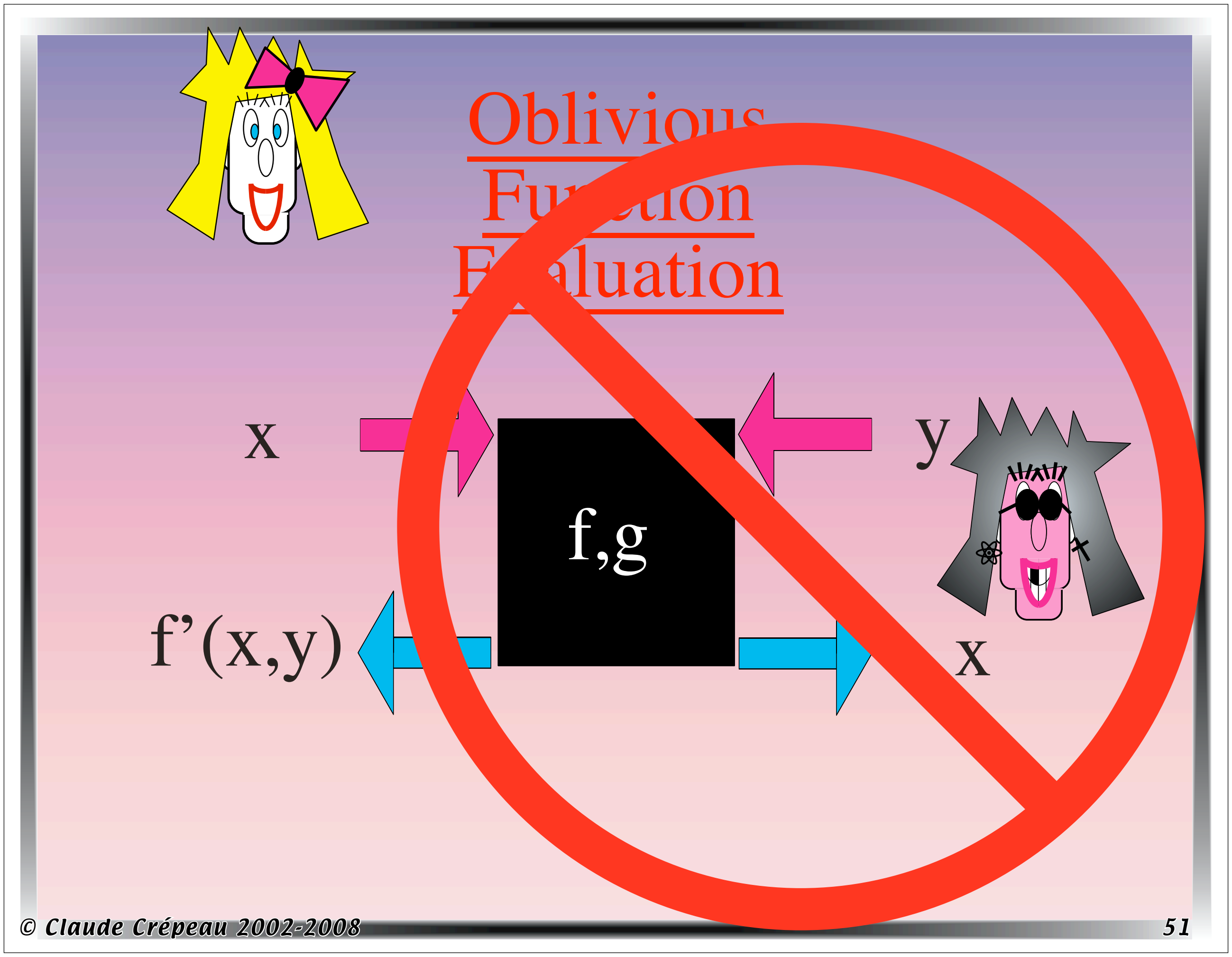
y

f,g

f(x,y)

g(x,y)

© Claude Crépeau 2002-2008



Oblivious Function Evaluation

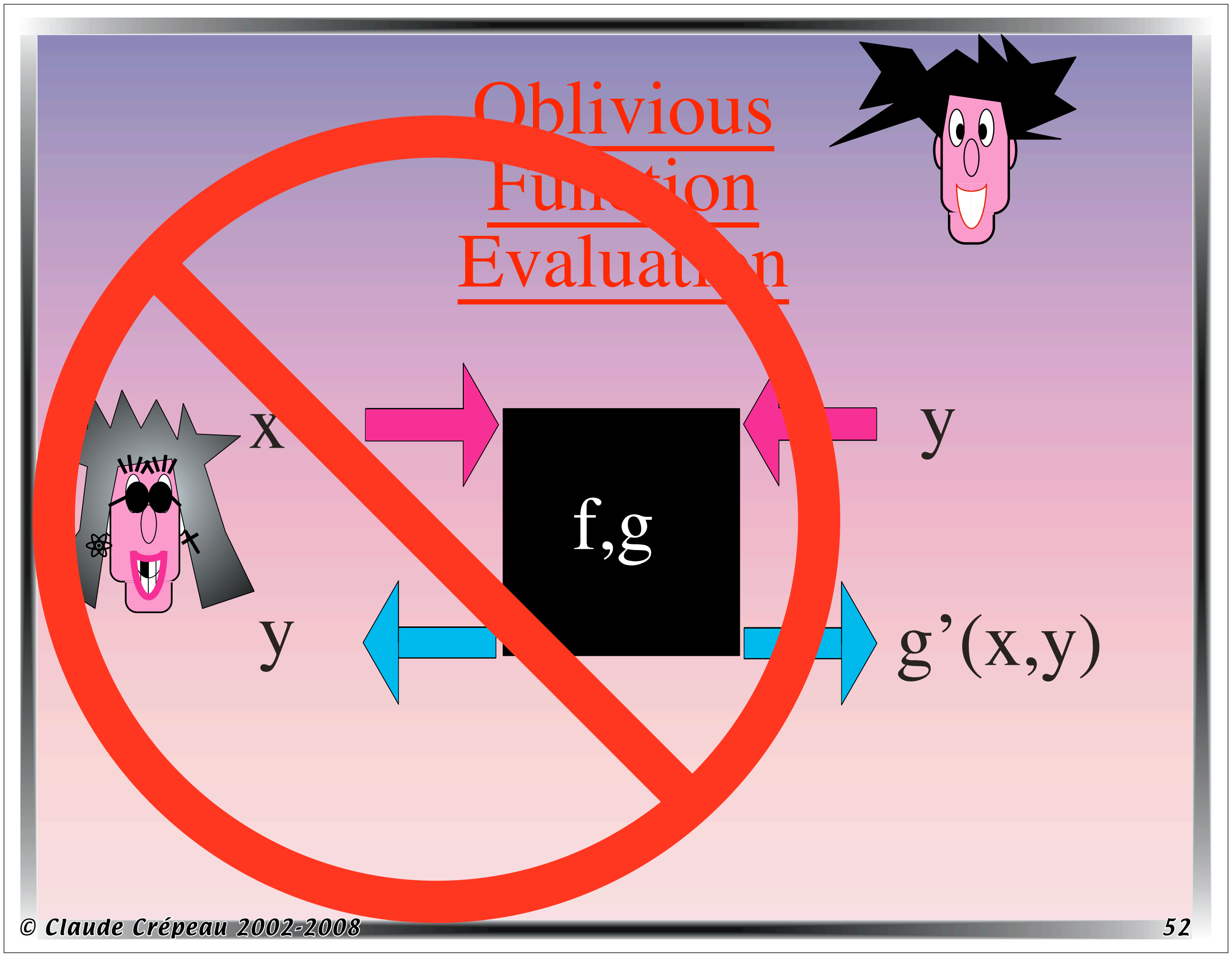
x

y

f,g

f’(x,y)

x



Oblivious Function Evaluation

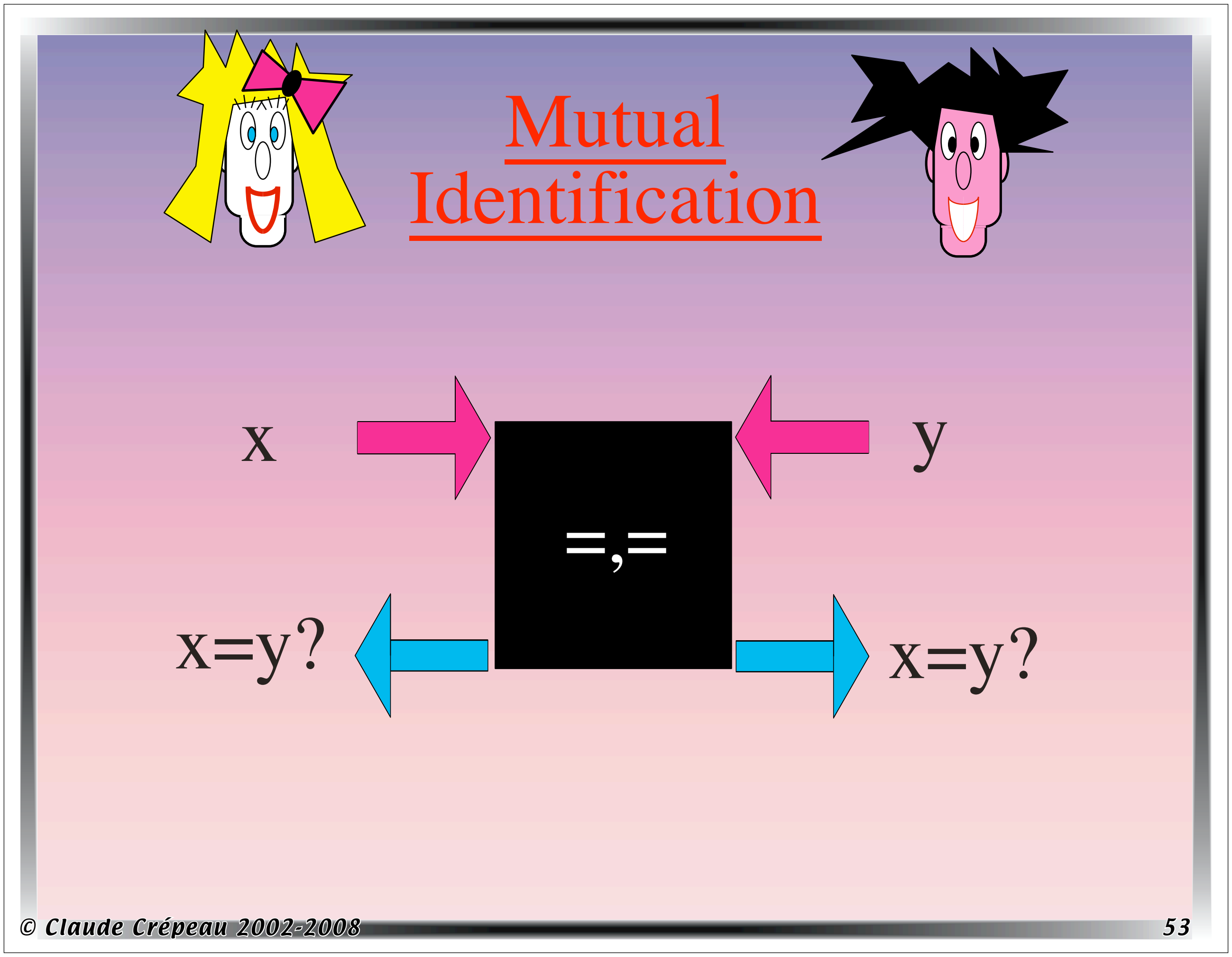
x

y

f,g

y

g’(x,y)



Mutual Identification

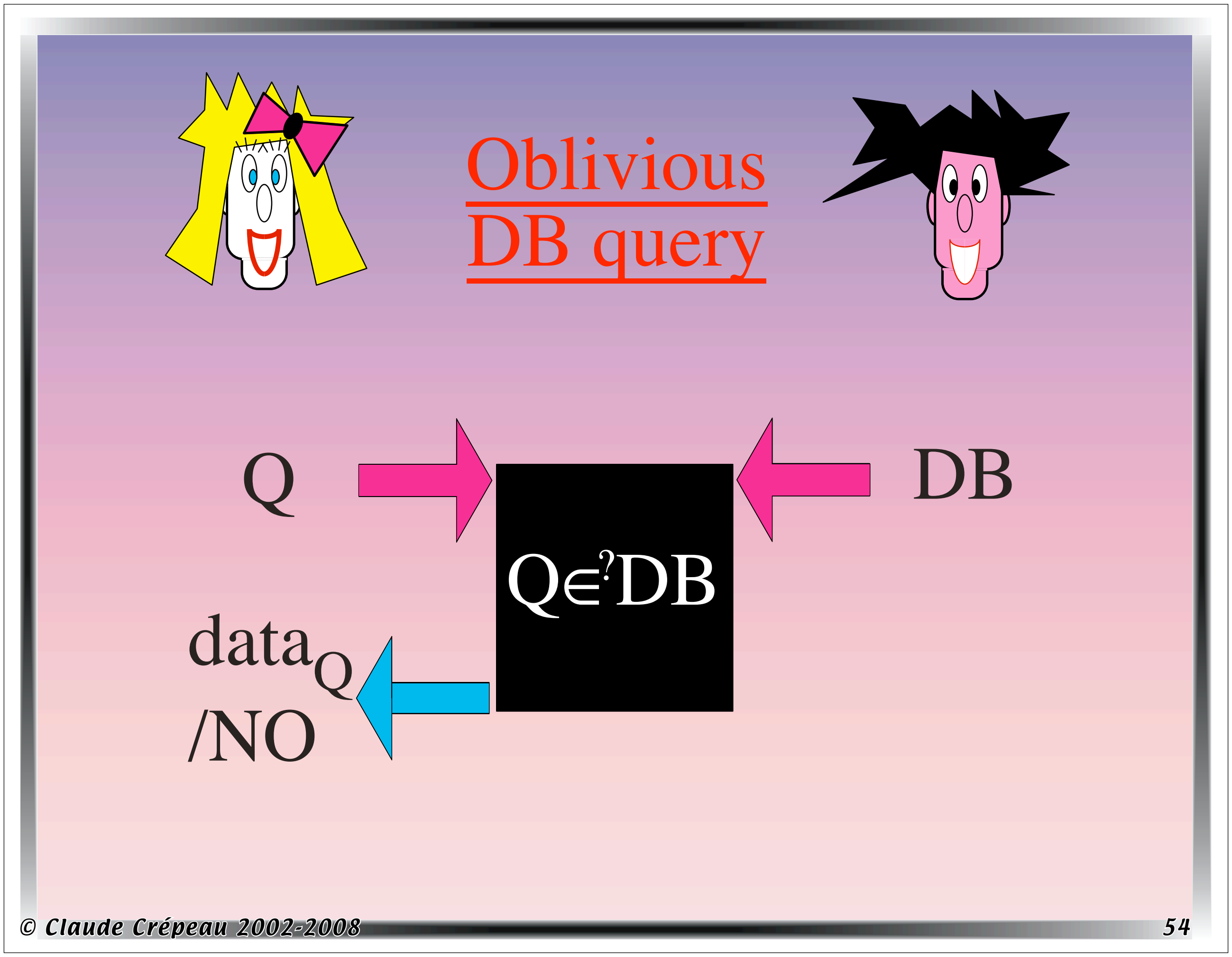
x

y

=,=

x=y?

x=y?



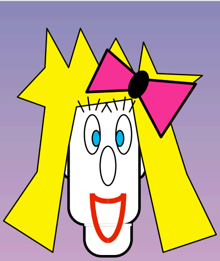
Oblivious DB query

Q

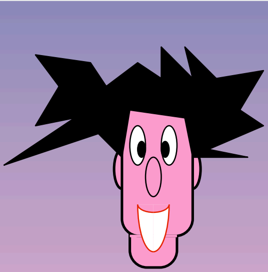
DB

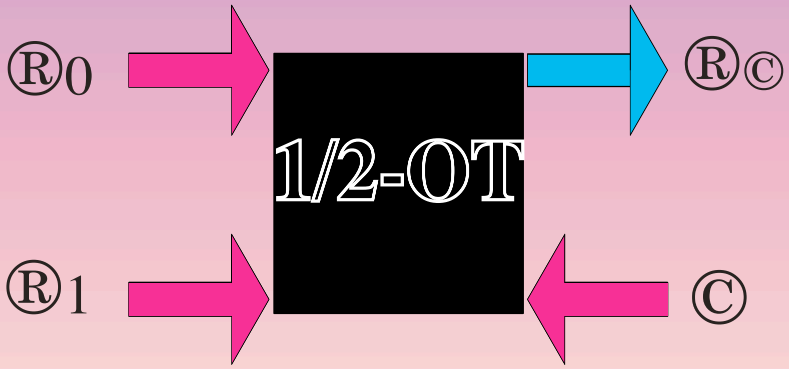
$Q \overset{?}{\in} DB$

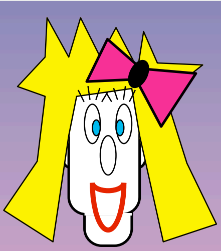
data_Q /NO



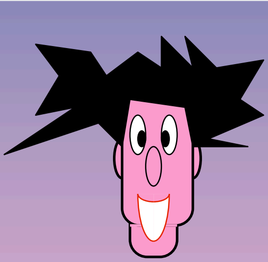
Randomized Oblivious Transfer

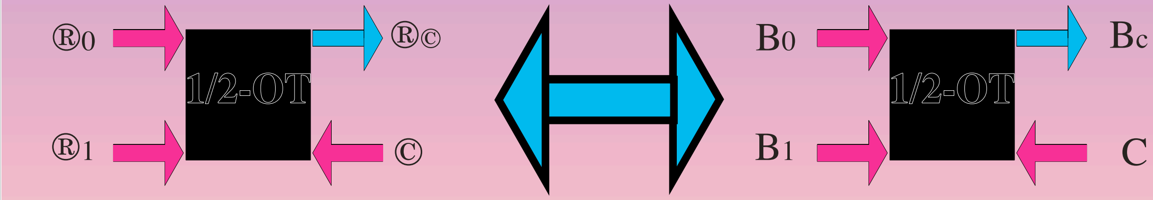




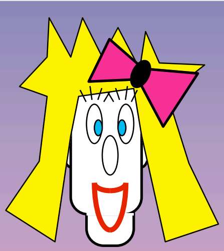


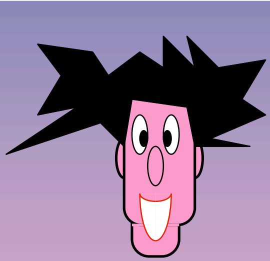
Randomized Oblivious Transfer

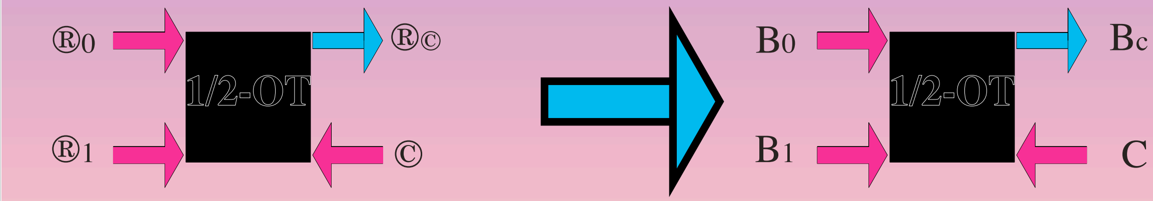




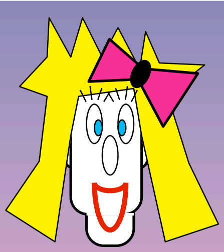
Randomized Oblivious Transfer

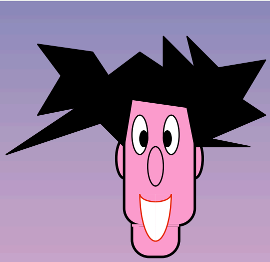


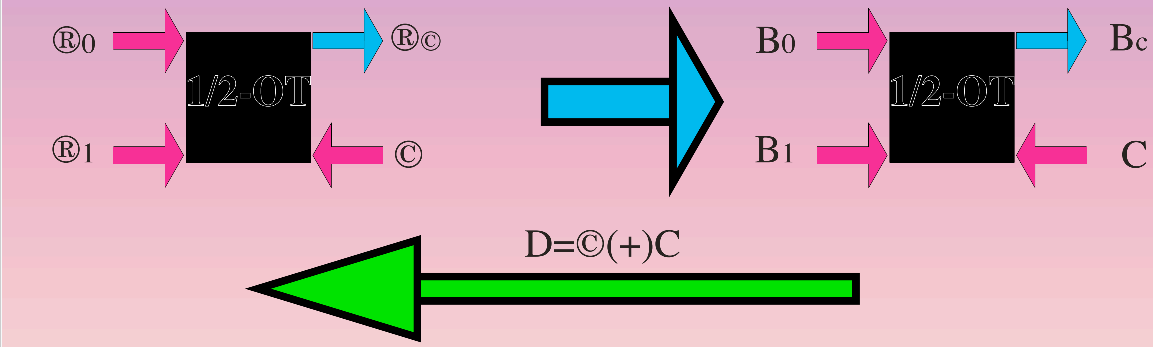


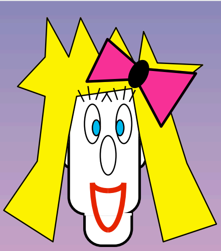


Randomized Oblivious Transfer

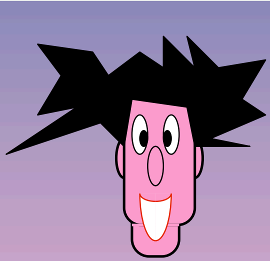


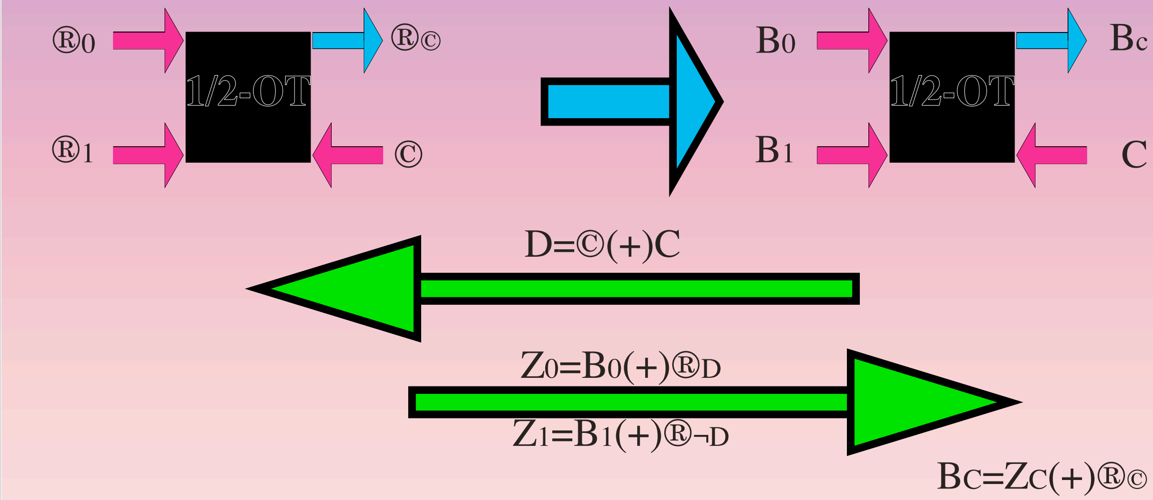


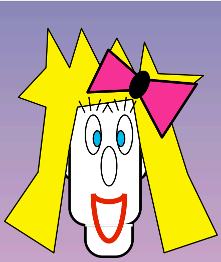




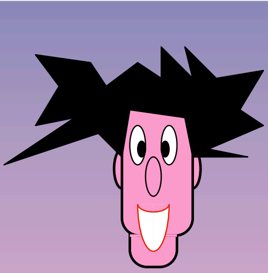
Randomized Oblivious Transfer

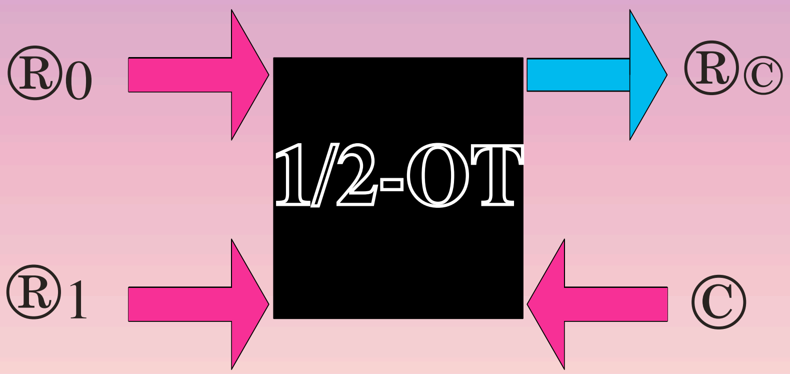




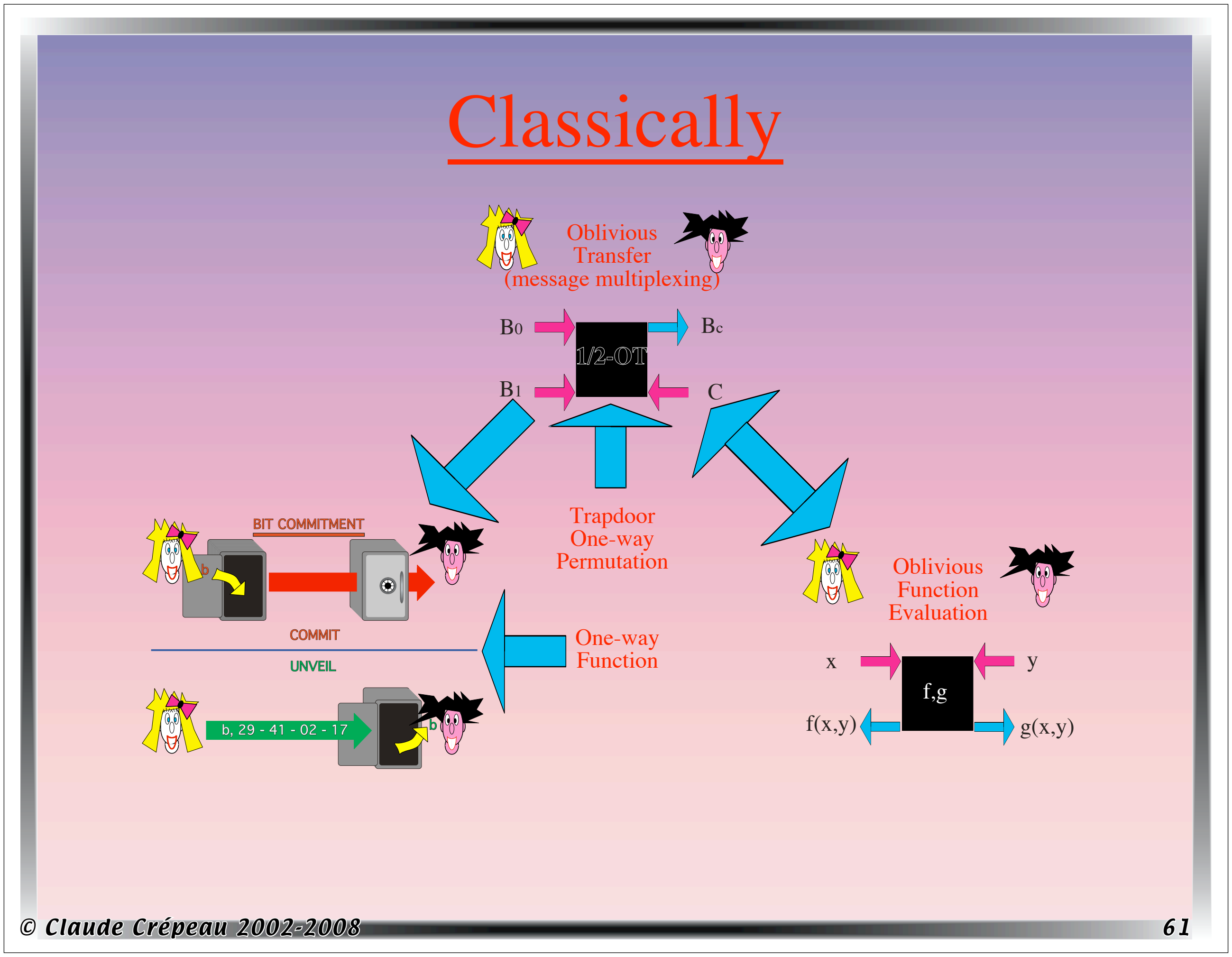


Randomized Oblivious Transfer





IS AN INVESTMENT IN THE FUTURE



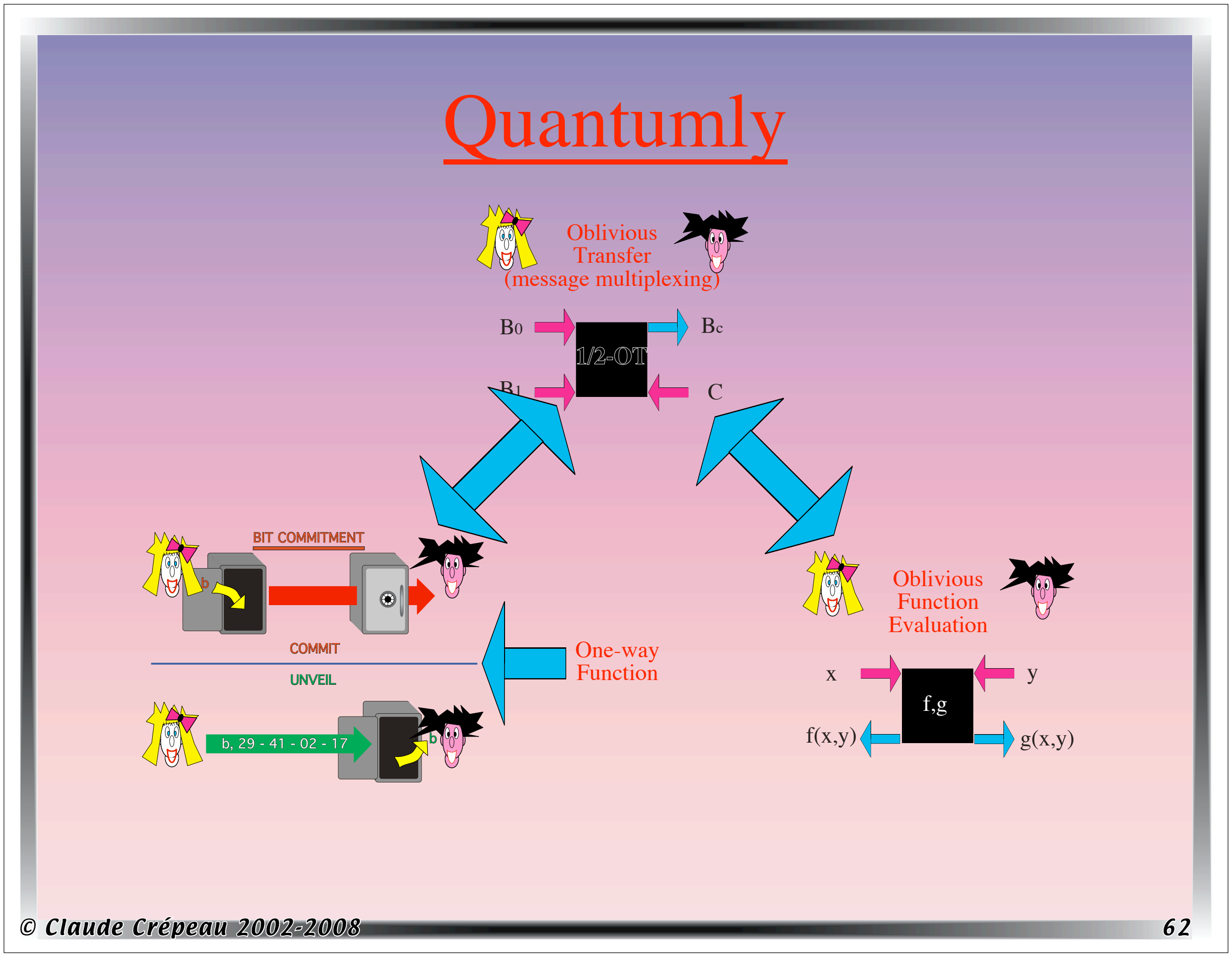
Classically

Oblivious Transfer (message multiplexing)

Trapdoor One-way Permutation

One-way Function

Oblivious Function Evaluation



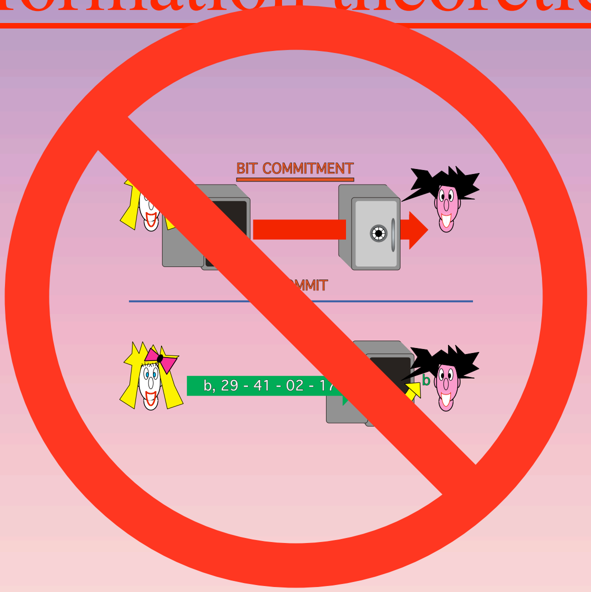
Quantumly

Oblivious Transfer (message multiplexing)

One-way Function

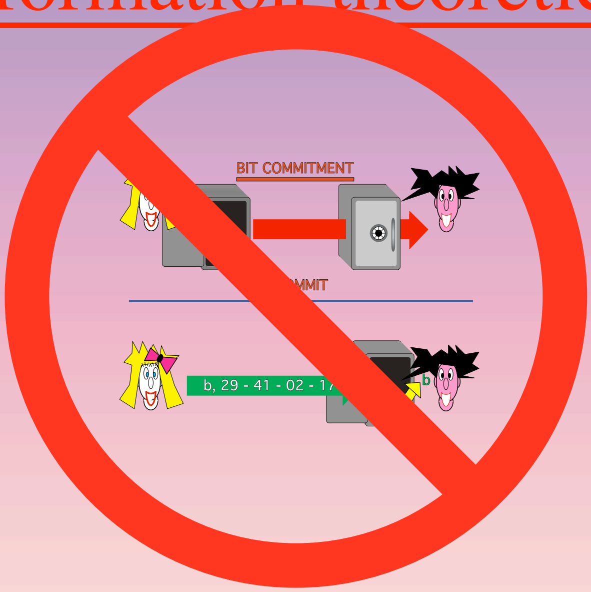
Oblivious Function Evaluation

Classically (information theoretical)



Folklore

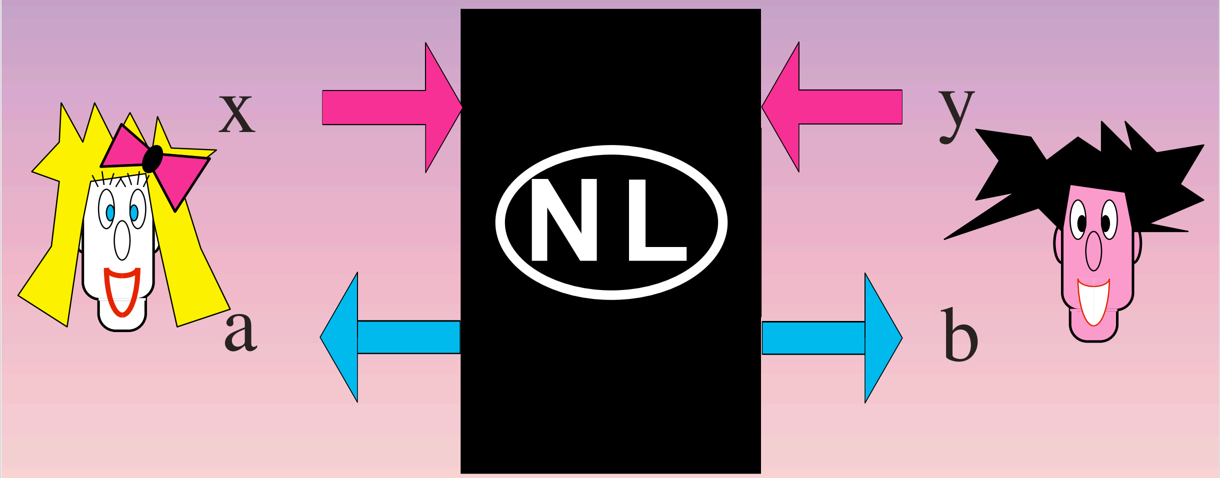
Quantumly (information theoretical)



Mayers, Lo-Chau

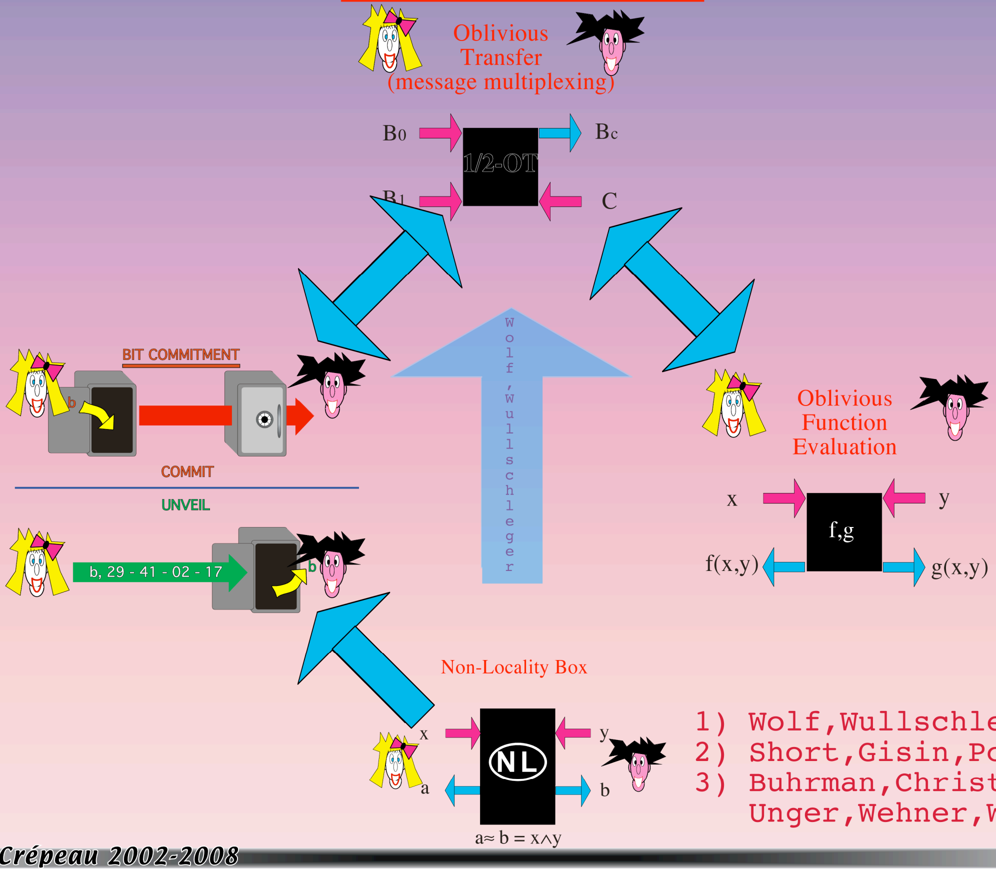
Non-Locality Box

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



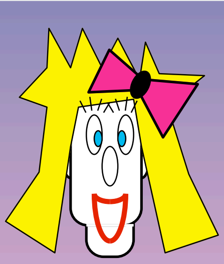
C: 3/4 Q: $\cos^2(\pi/8) \approx 85\%$

Quantumly

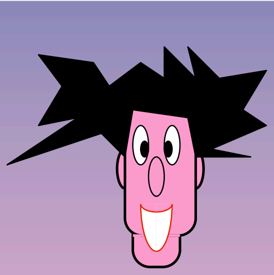


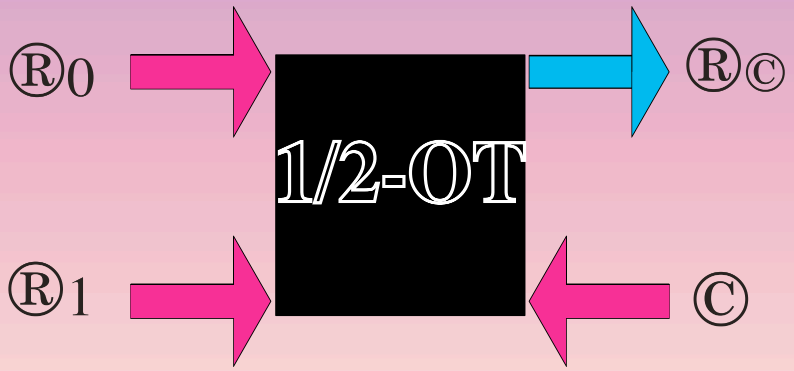
1) Wolf,Wullschleger ?
2) Short,Gisin,Popescu
3) Buhrman,Christandl,
   Unger,Wehner,Winter

(5) Quantum Oblivious Transfer

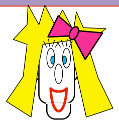


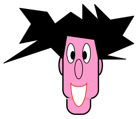
Randomized Oblivious Transfer





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 👎 👎 👎 👎 👎 👎 👎 👎 👎 👎 👎 👎 👎

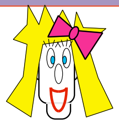
A: 0 0 1 1 0 1 0 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 0 1

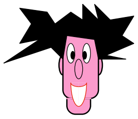
B: 0 0 1 1 0 1 0 1 = 0 👎 = 👎 👎 👎 👎 👎 👎 👎 👎

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

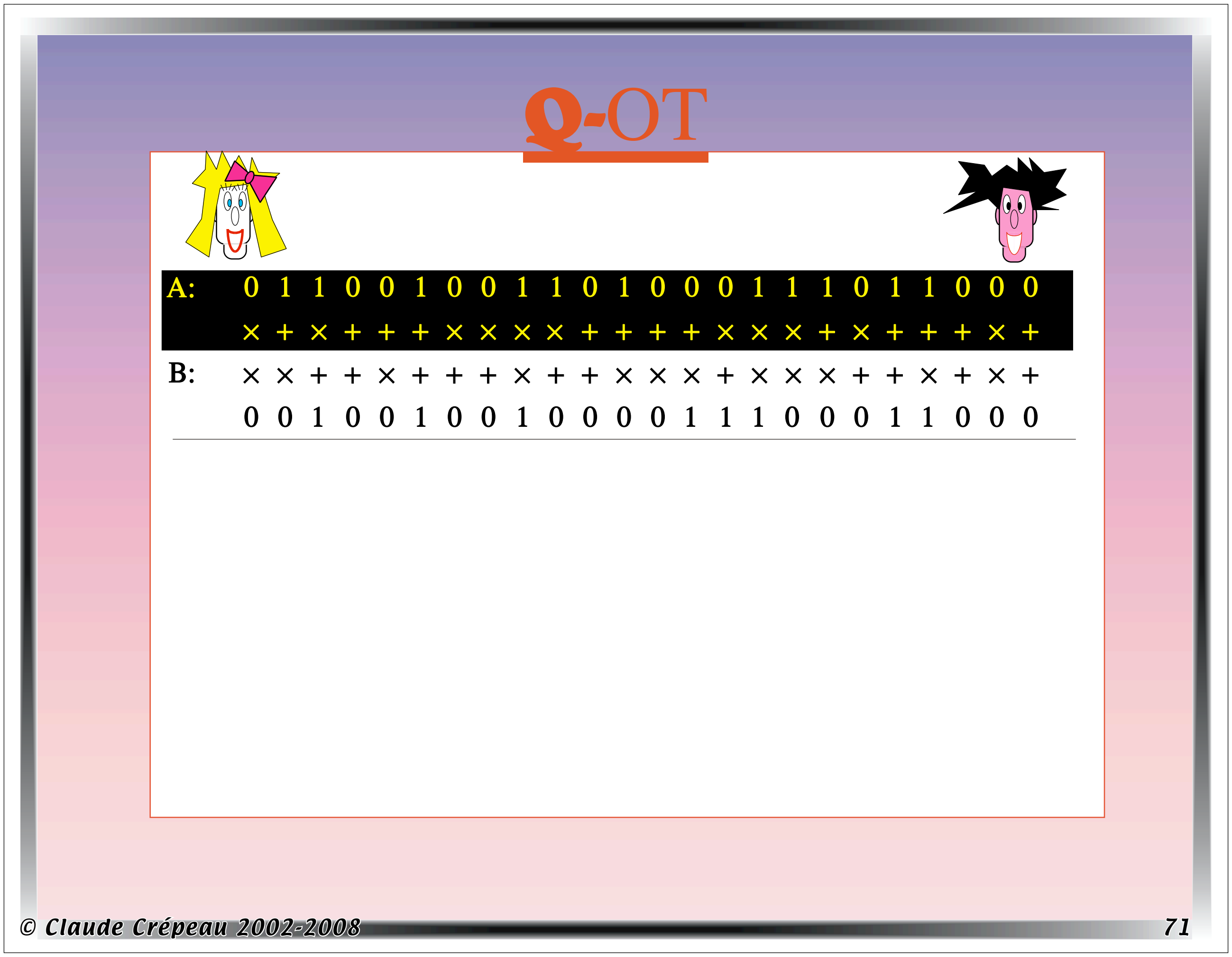
Crépeau-Kilian

Q-OT



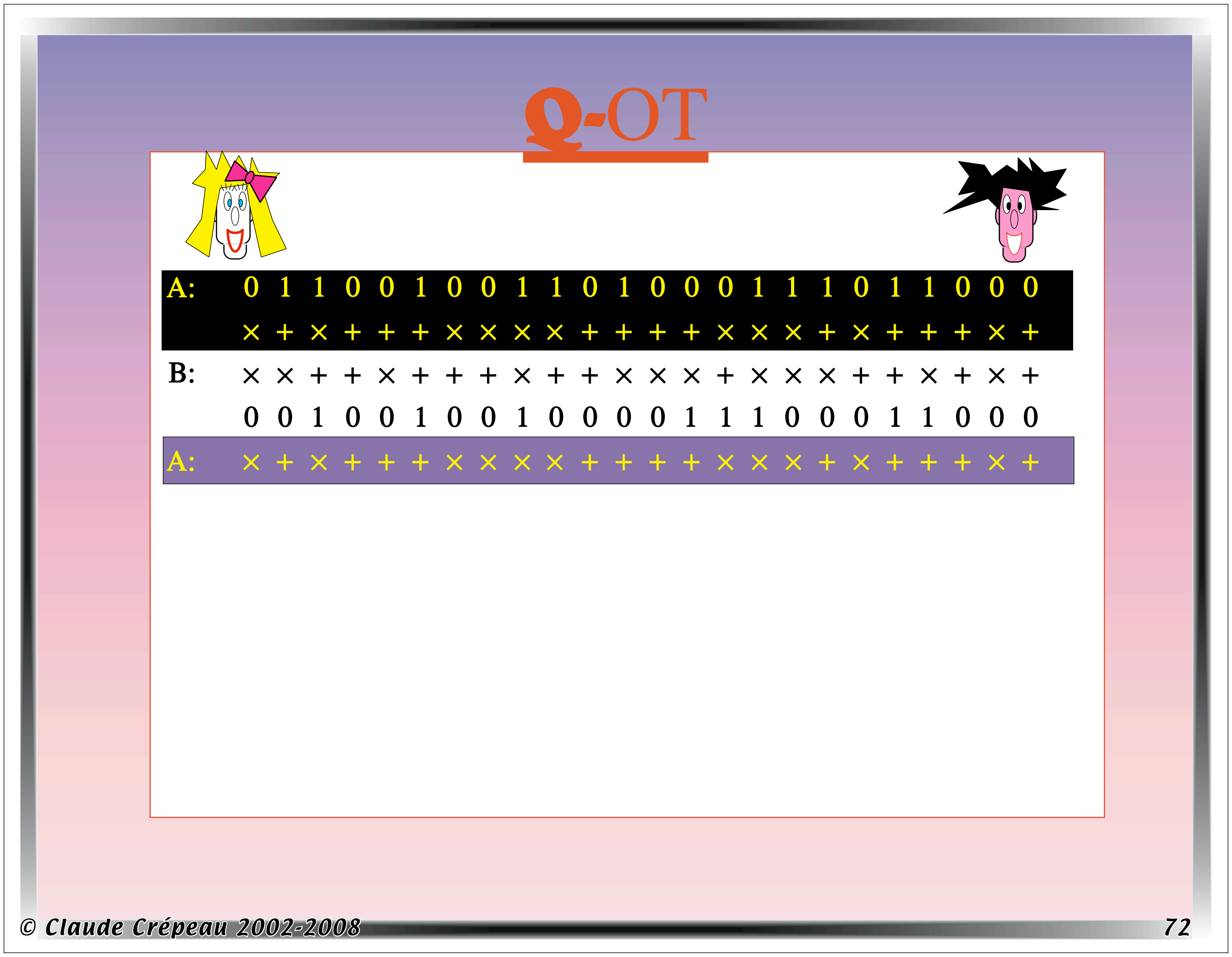


A: 0 1 1 0 0 1 0 0 1 1 0 1 0 0 0 1 1 1 0 1 1 0 0 0
× + × + + + × × × × + + + + × × × + × + + + × +



Q-OT

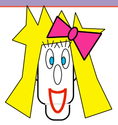
A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	×	×	+	+	×	+	+	+	×	+	+	×	×	×	+	×	×	×	+	+	×	+	×	+
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0

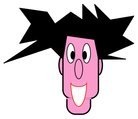


Q-OT

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

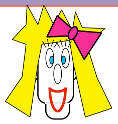
Q-OT

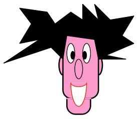




B:	×	×	+	+	×	+	+	+	×	+	+	×	×	×	+	×	×	×	+	+	×	+	×	+
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0
A:	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	0	👎	👎	0	👎	1	👎	👎	1	👎	0	👎	👎	👎	👎	1	0	👎	👎	1	👎	0	0	0

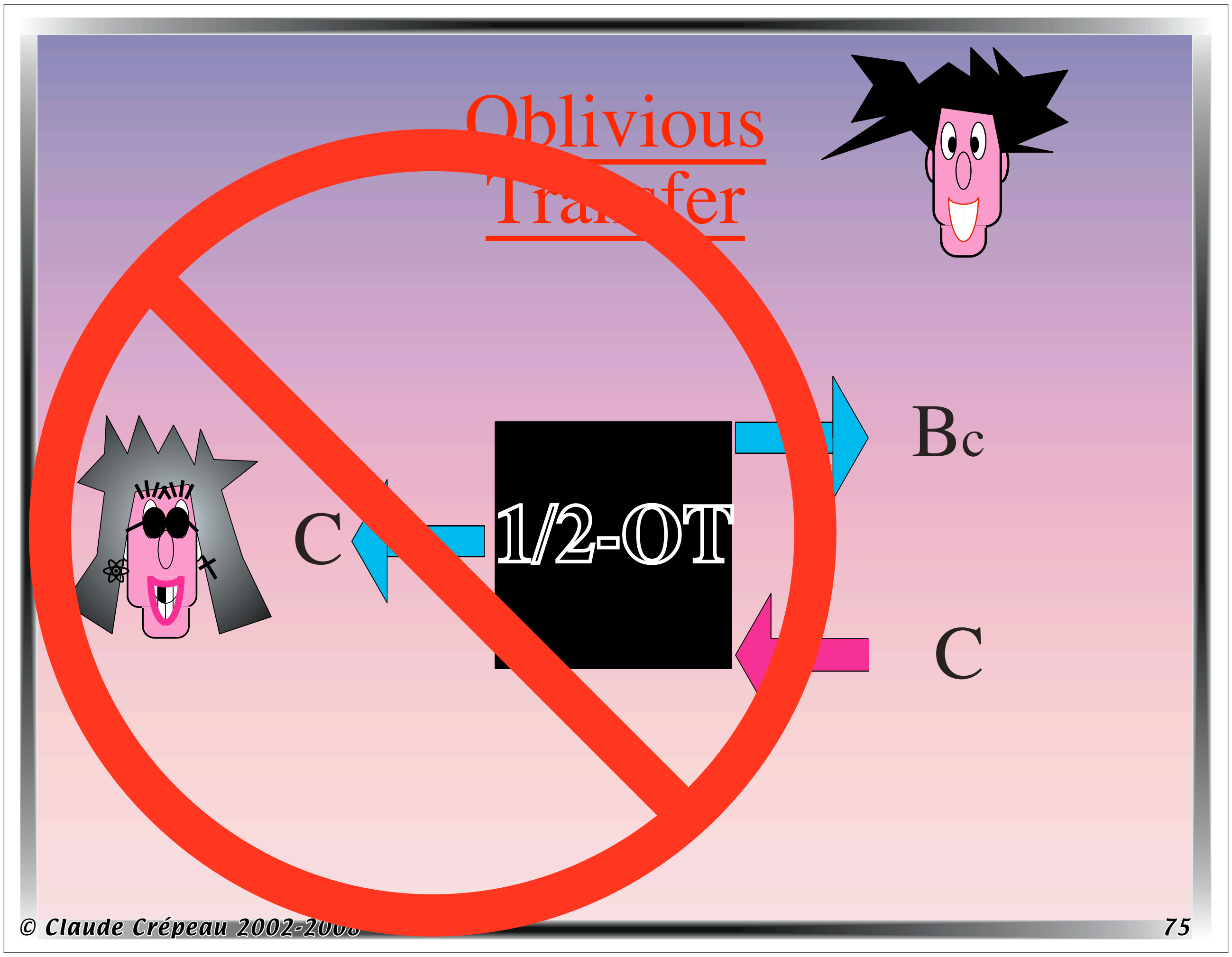
Q-OT



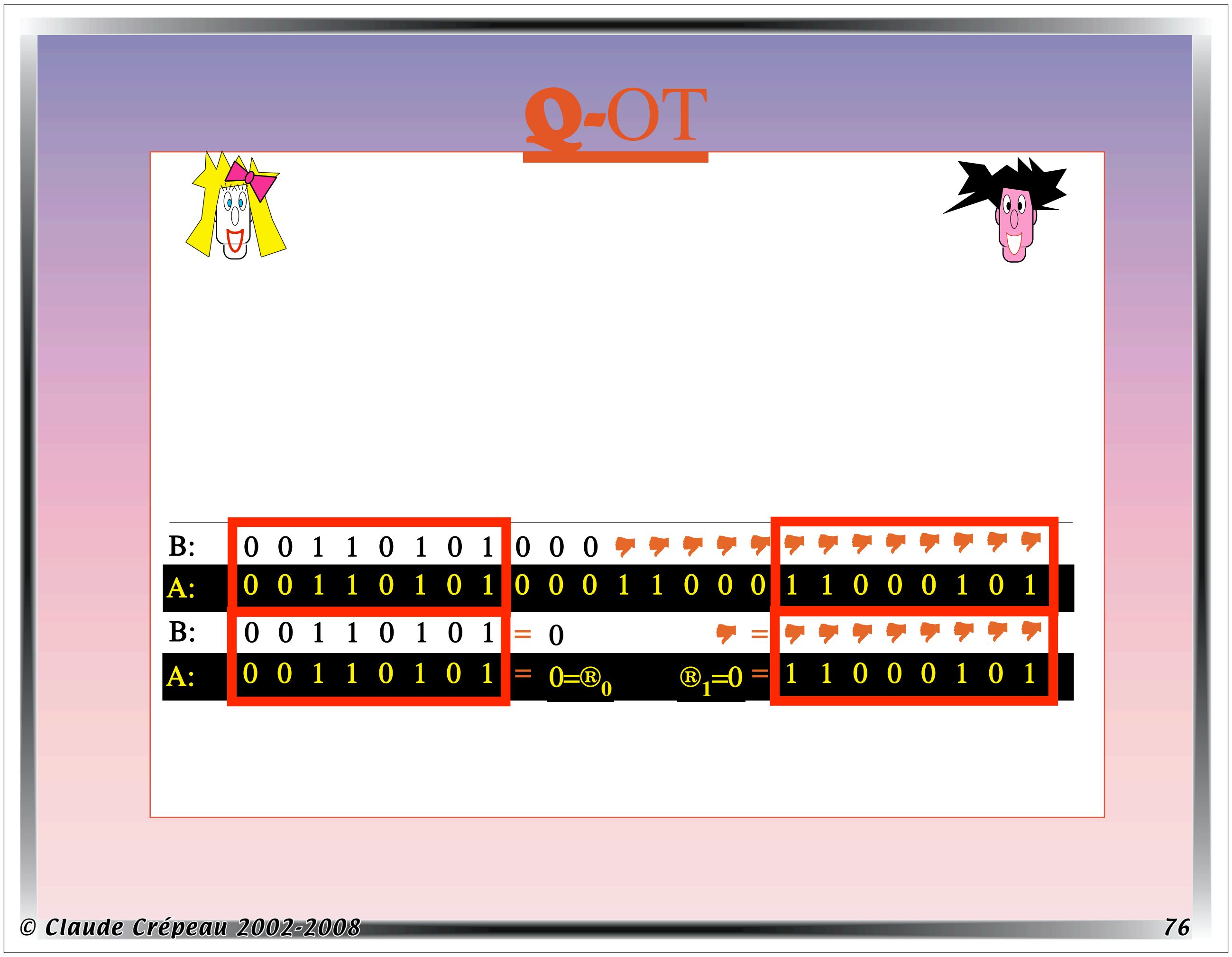


A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0

B:	0	👎	👎	0	👎	1	👎	👎	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

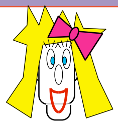
B: 0 0 1 1 0 1 0 1 0 0 0 👎 👎 👎 👎 👎 👎 👎 👎 👎 👎 👎 👎 👎

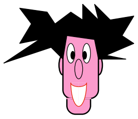
A: 0 0 1 1 0 1 0 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 0 1

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

Q-OT

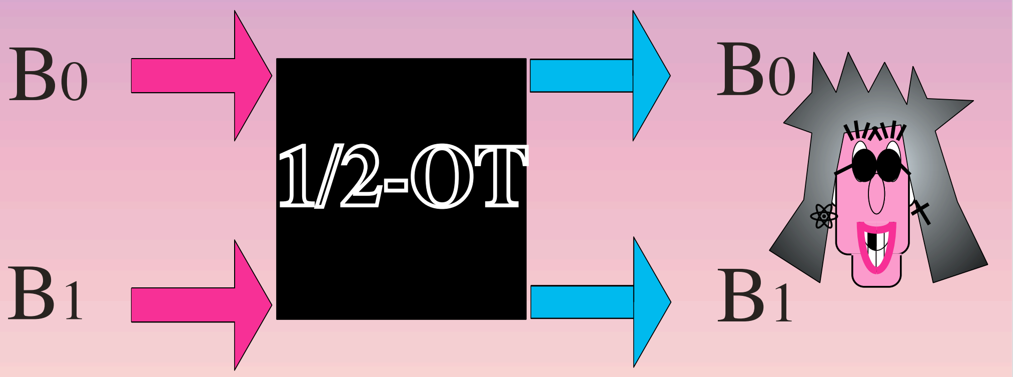


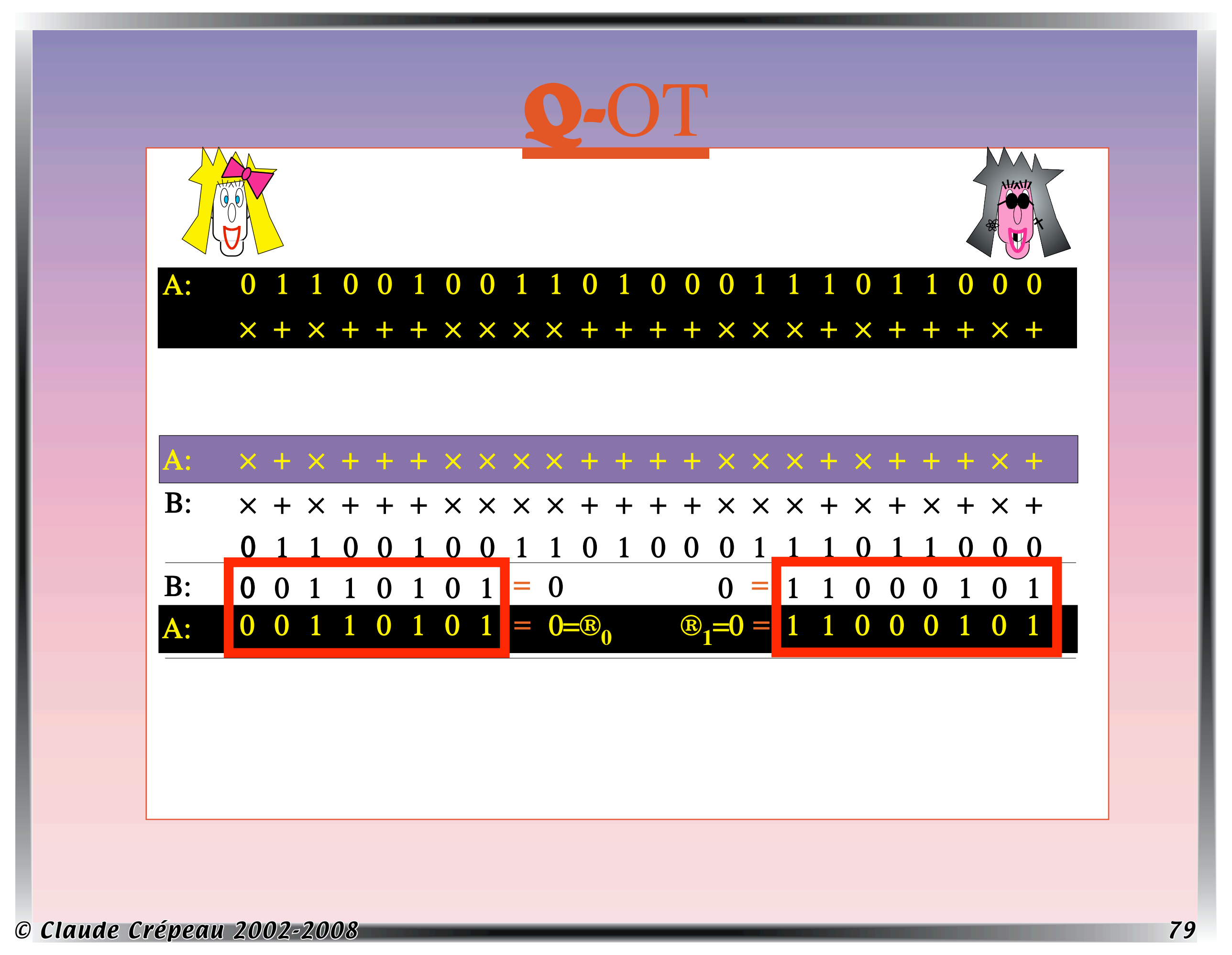


B: 0 0 1 1 0 1 0 1 = 0 👎 = 👎 👎 👎 👎 👎 👎 👎 👎

A: 0 0 1 1 0 1 0 1 = $0=\circledR_0$ $\circledR_1=0$ = 1 1 0 0 0 1 0 1

Oblivious Transfer

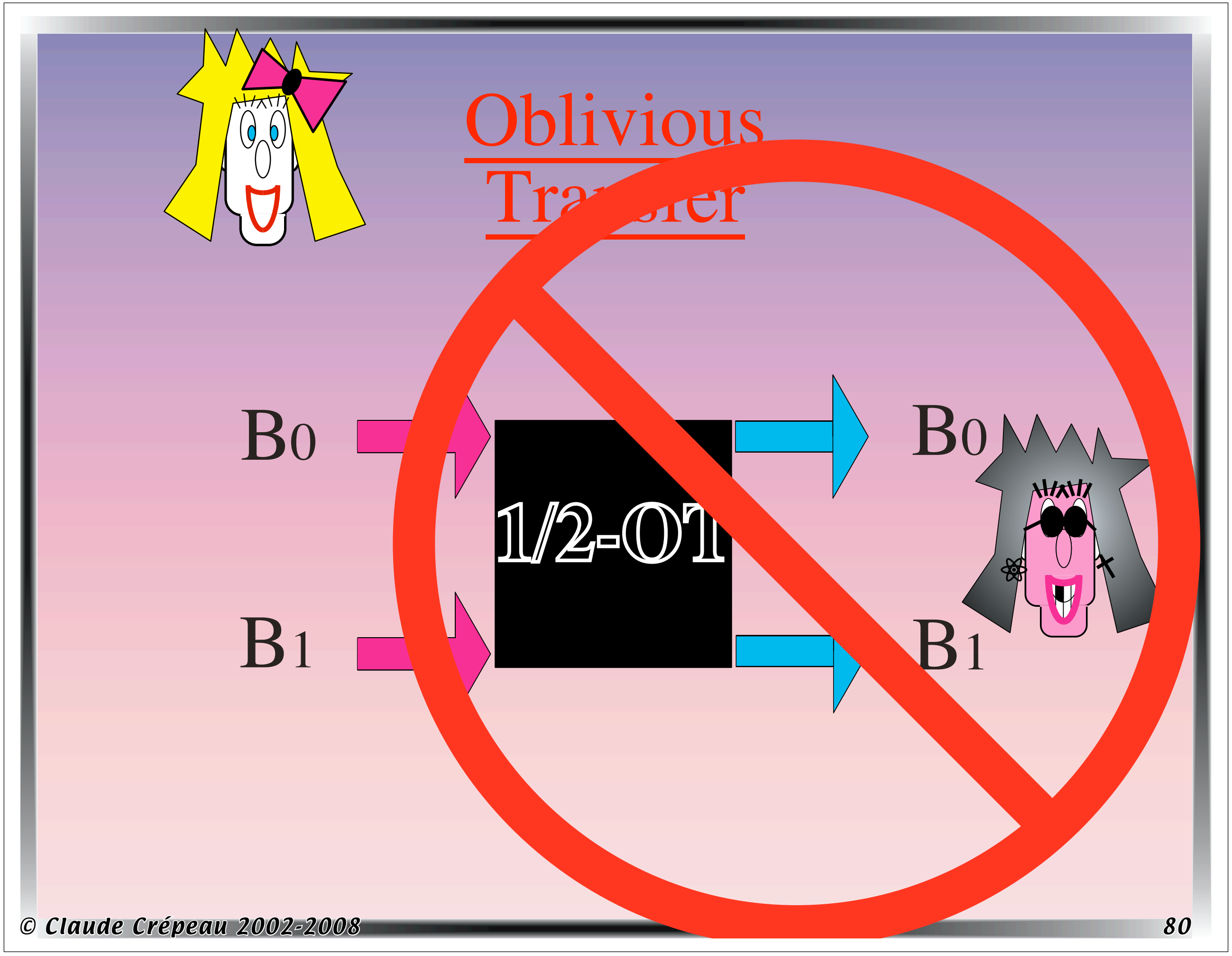




Q-OT

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

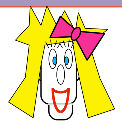
A:	× + × + + + × × × × + + + + × × × + × + + + × +			
B:	× + × + + + × × × × + + + + × × × + × + × + × +			
	0 1 1 0 0 1 0 0 1 1 0 1 0 0 0 1 1 1 0 1 1 0 0 0			
B:	0 0 1 1 0 1 0 1	= 0	0 =	1 1 0 0 0 1 0 1
A:	0 0 1 1 0 1 0 1	= 0=®$_0$	®$_1$=0 =	1 1 0 0 0 1 0 1



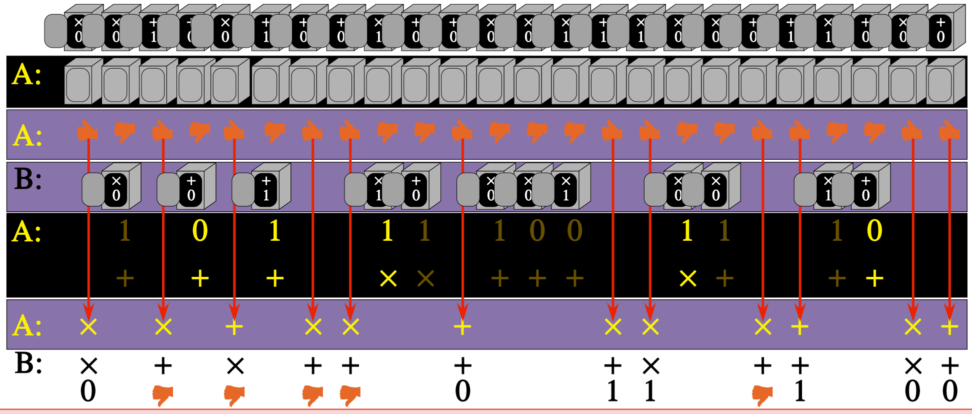
Oblivious Transfer

Q-OT

from Q-BC

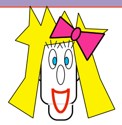


A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	×	×	+	+	×	+	+	+	×	+	+	×	×	×	+	×	×	×	+	+	×	+	×	+
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0

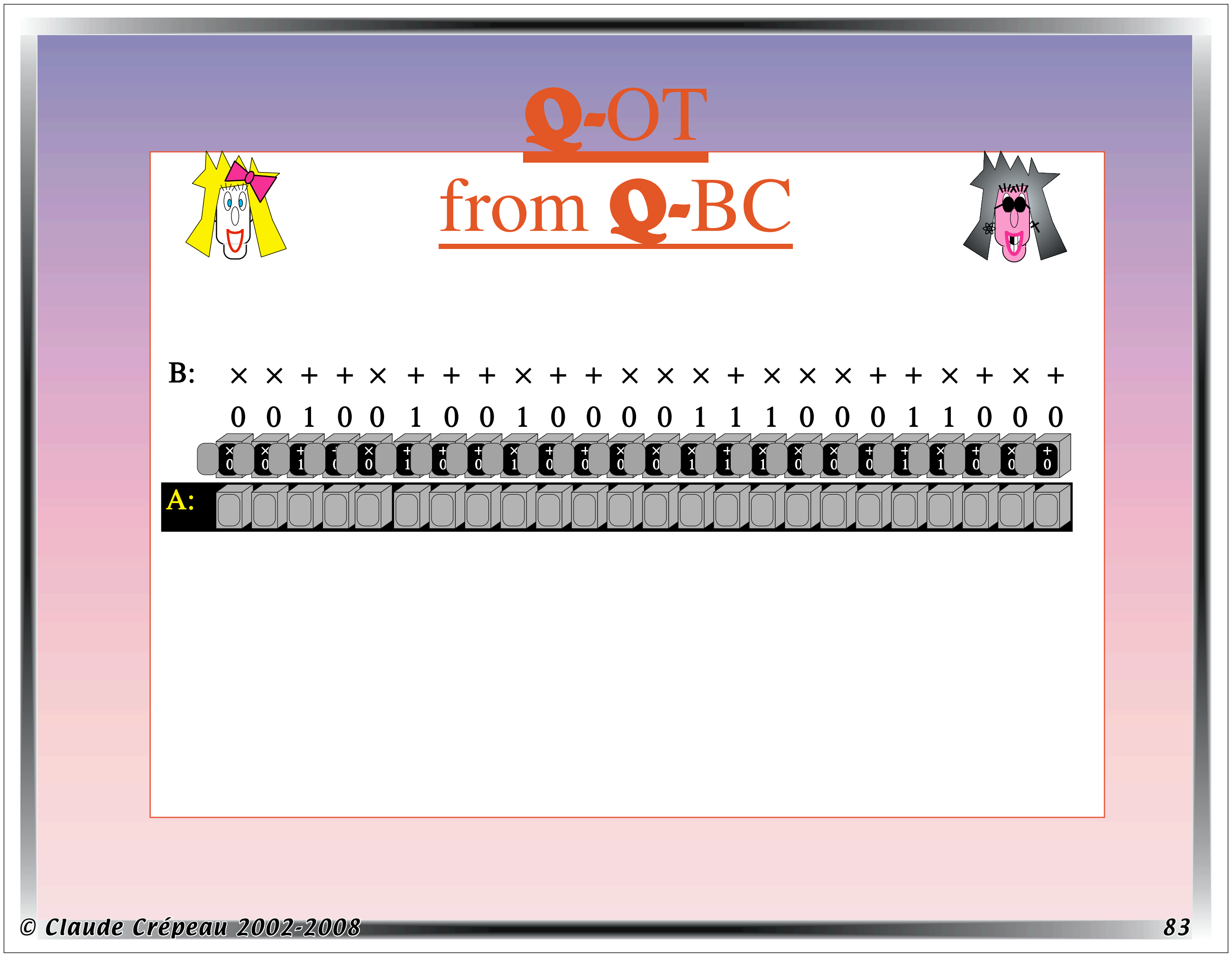

A:
A:
B:
A: 1 0 1 1 1 1 0 0 1 1 1 0
+ + + × × + + + × + + +
A: × × + × × + × × × + × +
B: × + × + + + + × + + × +
0 0 1 1 1 0 0

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

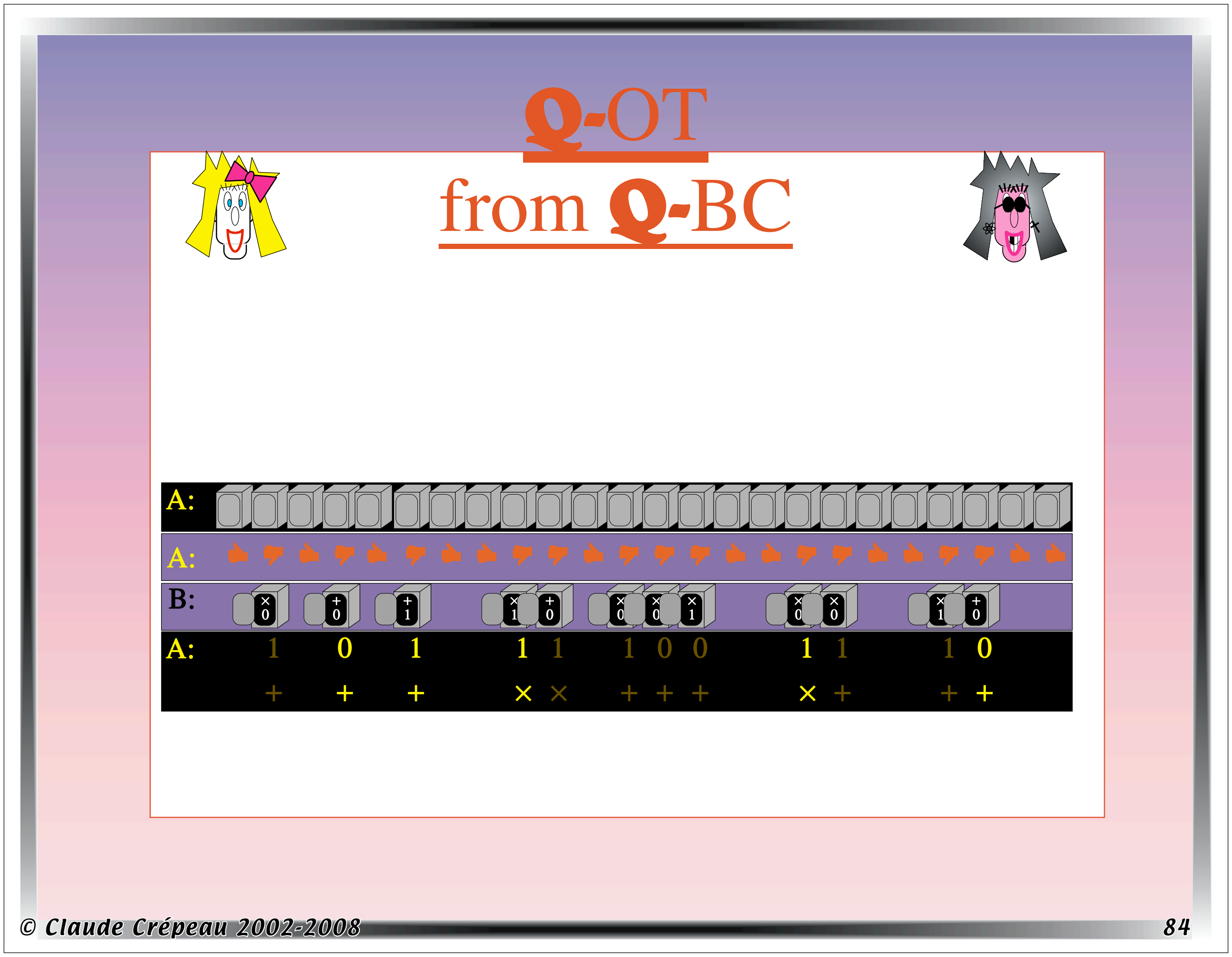


Q-OT from Q-BC

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 from Q-BC

A:

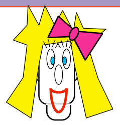
A:

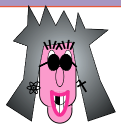
B:

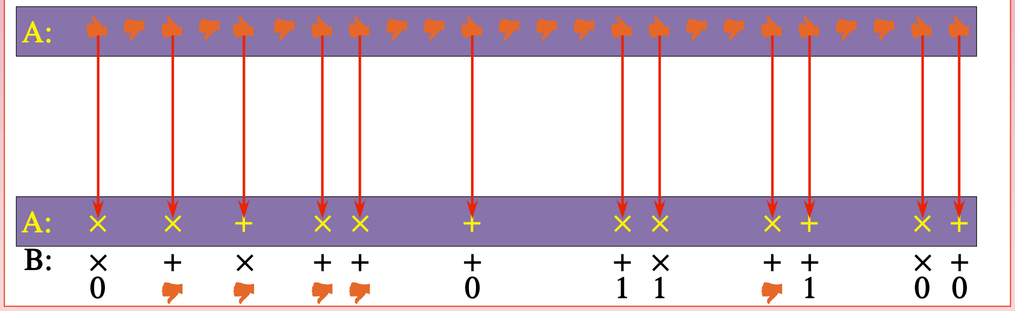
A: 1 0 1 1 1 1 0 0 1 1 1 0

+ + + × × + + + × + + +

Q-OT
from Q-BC

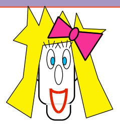


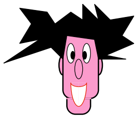




A:	👍	👎	👍	👎	👍	👎	👍	👍	👎	👎	👍	👎	👎	👎	👍	👍	👎	👎	👍	👍	👎	👎	👍	👍
A:	×		×		+		×	×			+				×	×			×	+			×	+
B:	×		+		×		+	+			+				+	×			+	+			×	+
	0		👎		👎		👎	👎			0				1	1			👎	1			0	0

Q-OT





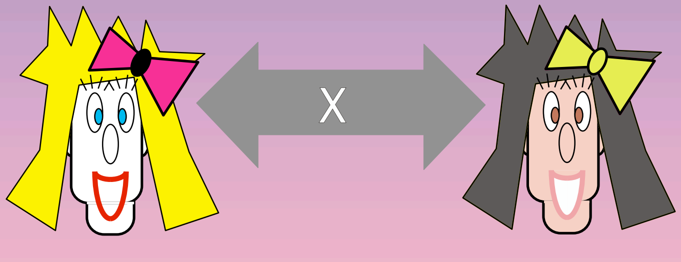
A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	×	×	+	+	×	+	+	+	×	+	+	×	×	×	+	×	×	×	+	+	×	+	×	+
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0
A:	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	0	👎	👎	0	👎	1	👎	👎	1	👎	0	👎	👎	👎	👎	1	0	👎	👎	1	👎	0	0	0

(6)
two provers
Cryptographic Protocols

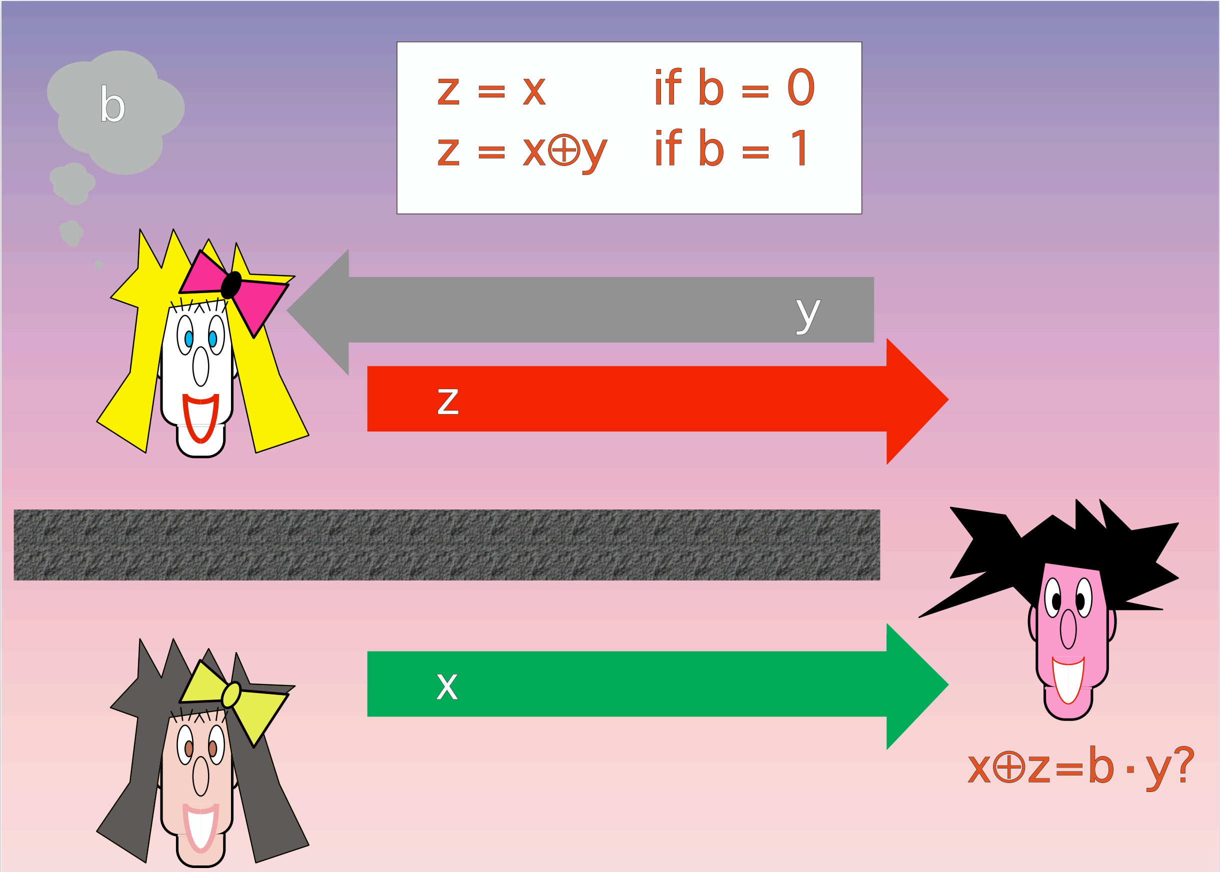
Classically

BGKW88

Classically



Ben-Or, Goldwasser, Kilian, Wigderson

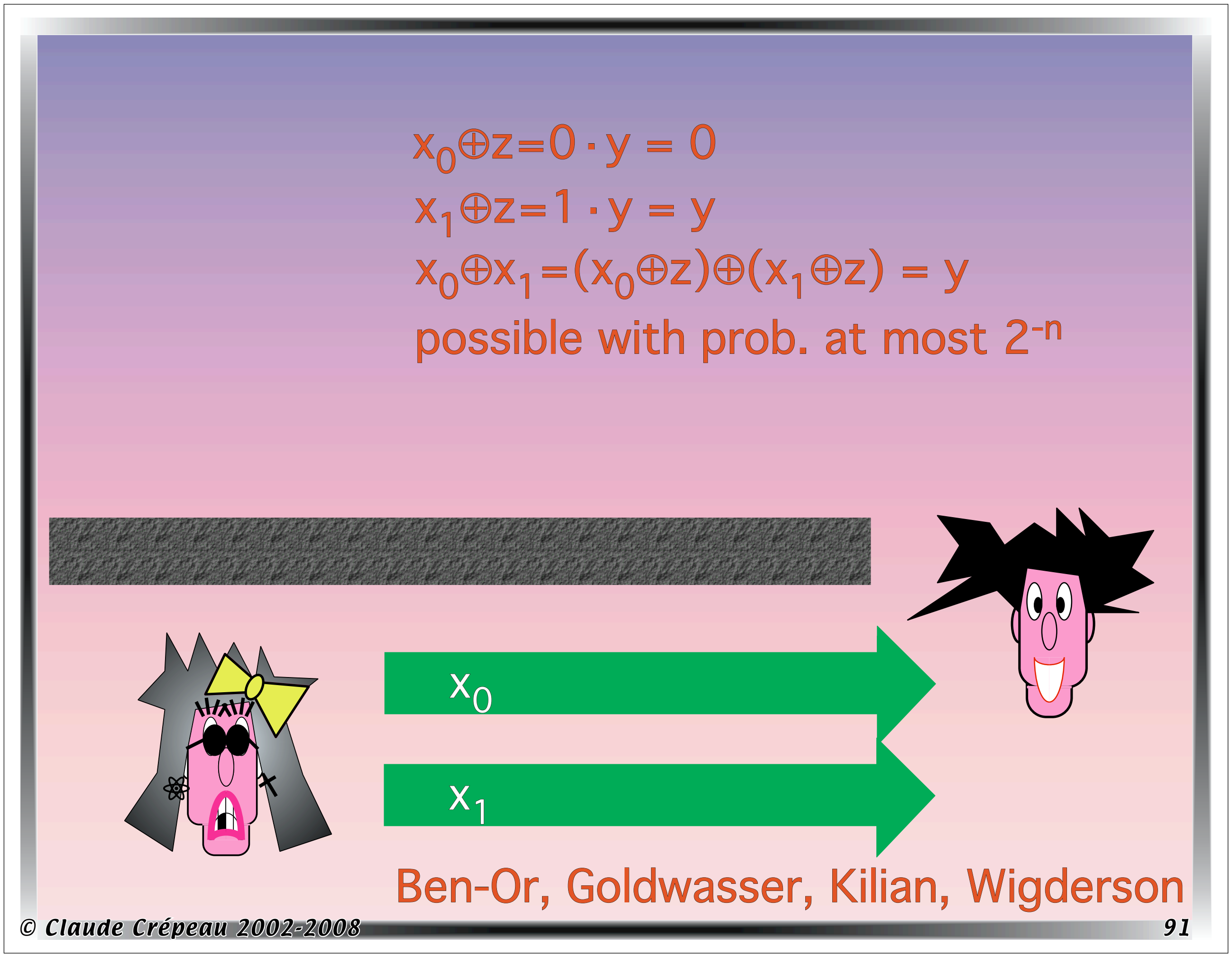


$z = x$ if $b = 0$

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

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

Ben-Or, Goldwasser, Kilian, Wigderson



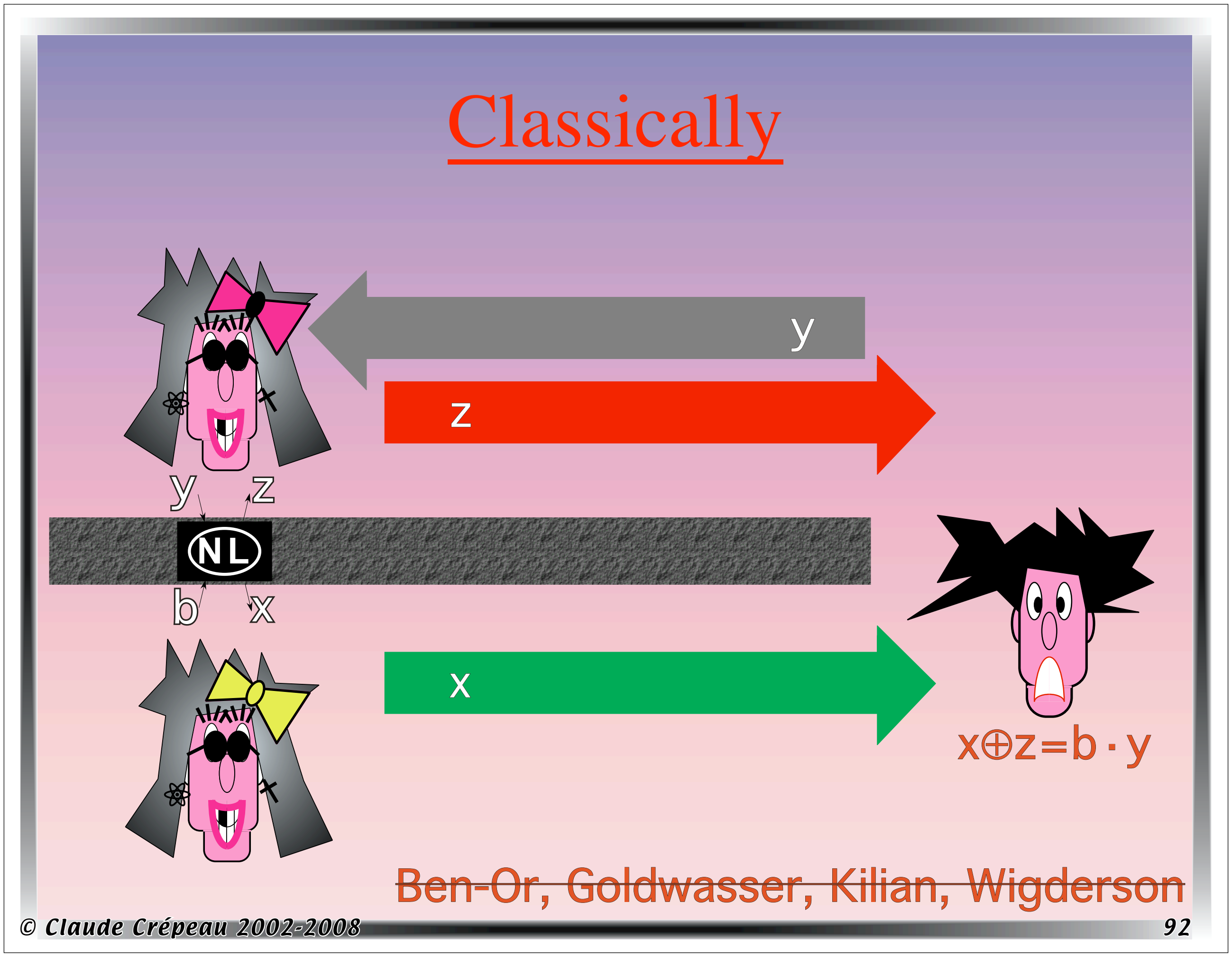
$x_0 \oplus z = 0 \cdot y = 0$

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

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

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

Ben-Or, Goldwasser, Kilian, Wigderson

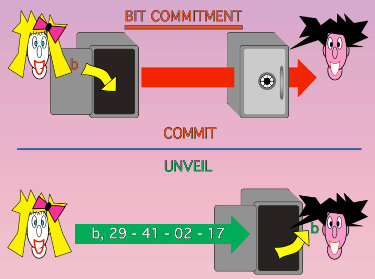


Classically

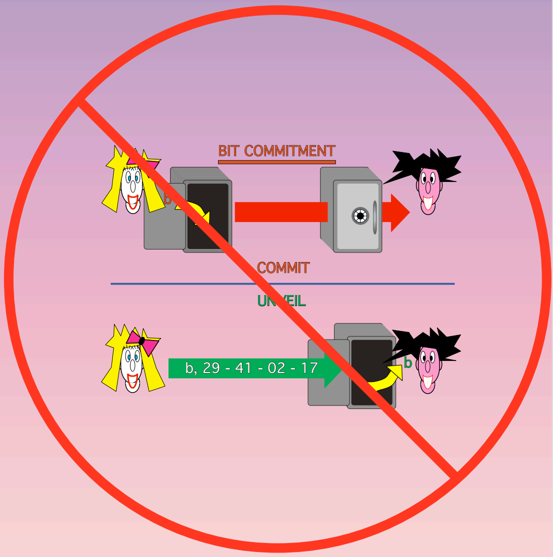
$x \oplus z = b \cdot y$

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

Quantumly

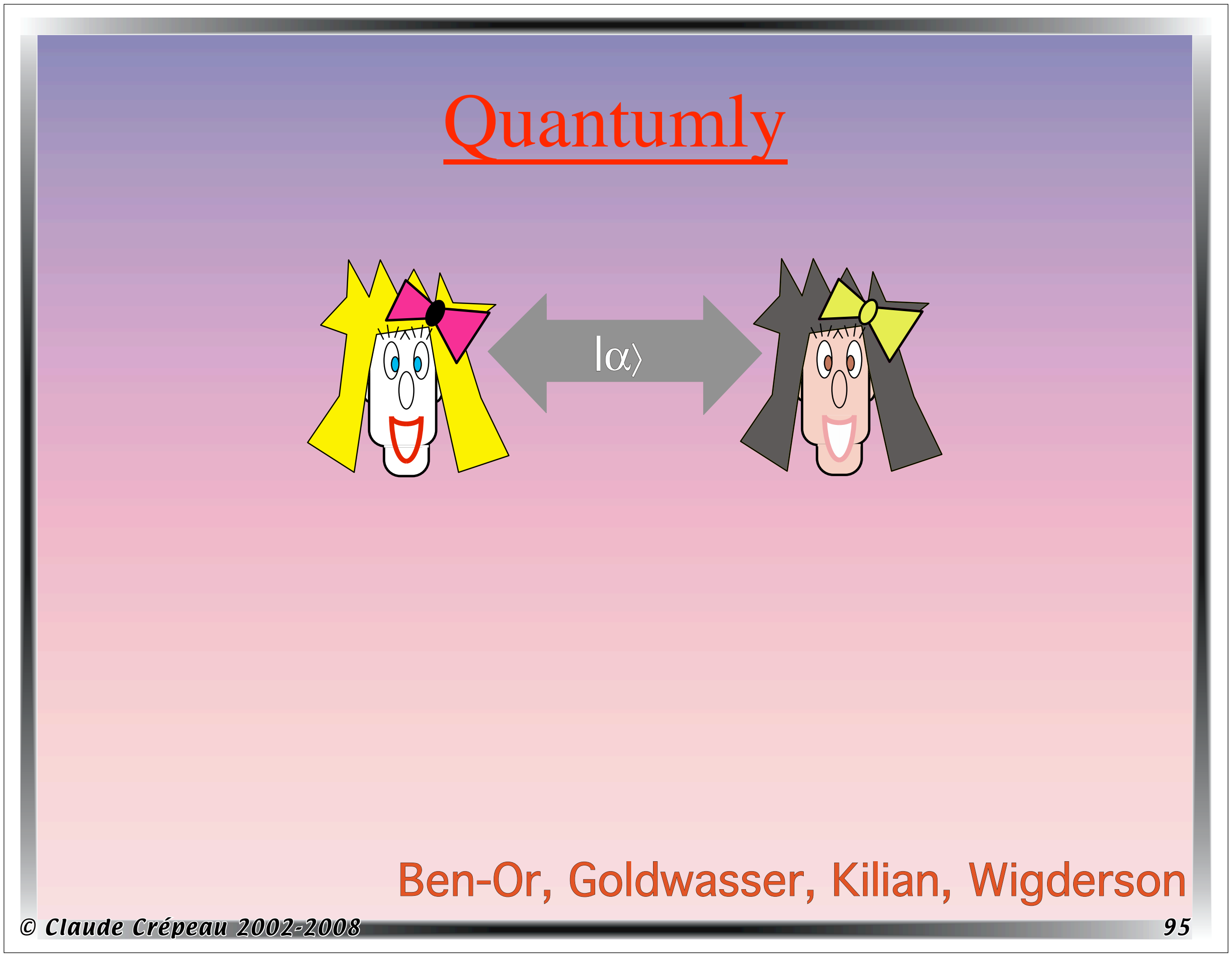


or



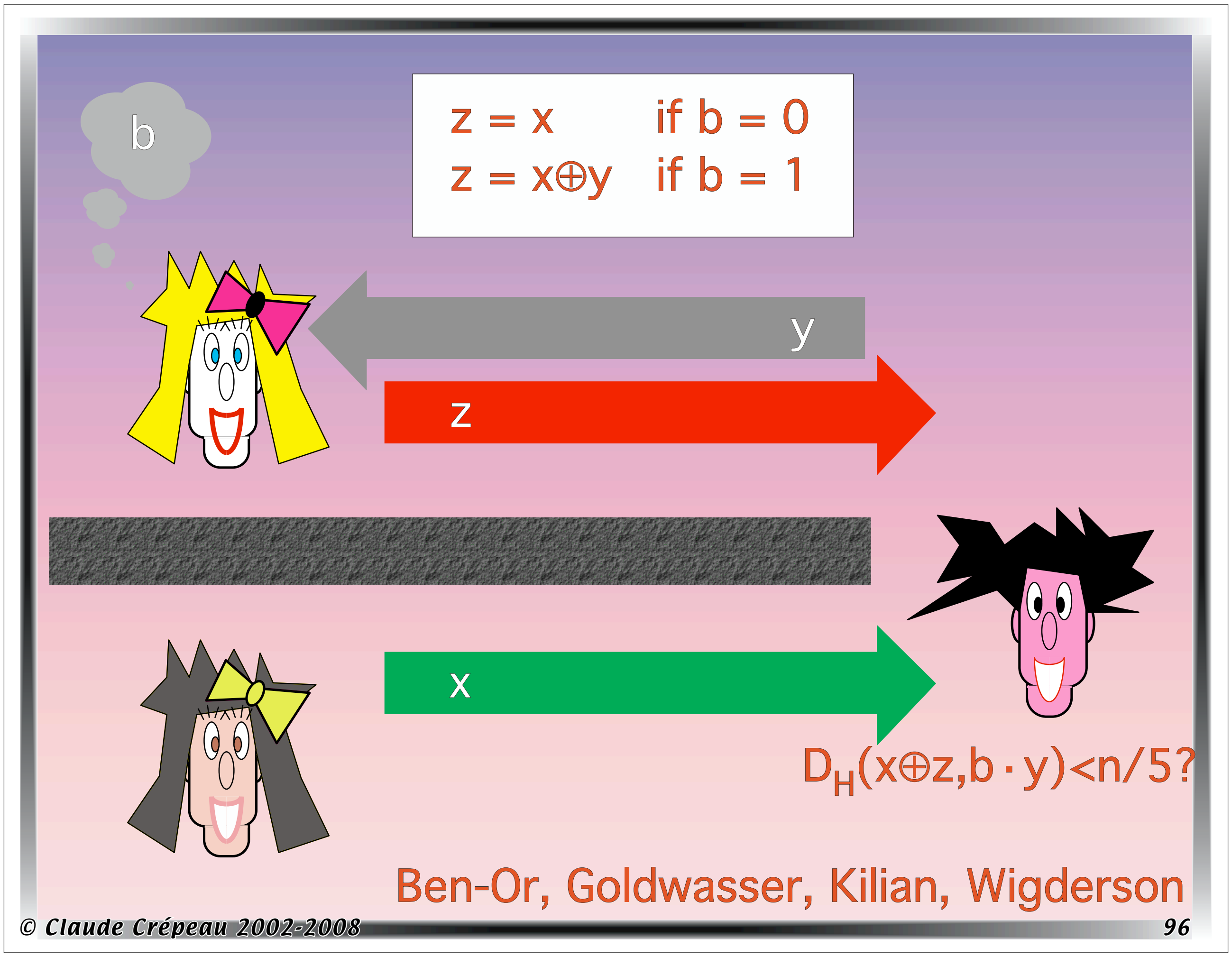
???

(7)
two provers BC
Classically Secure
Quantumly Insecure



Quantumly

Ben-Or, Goldwasser, Kilian, Wigderson

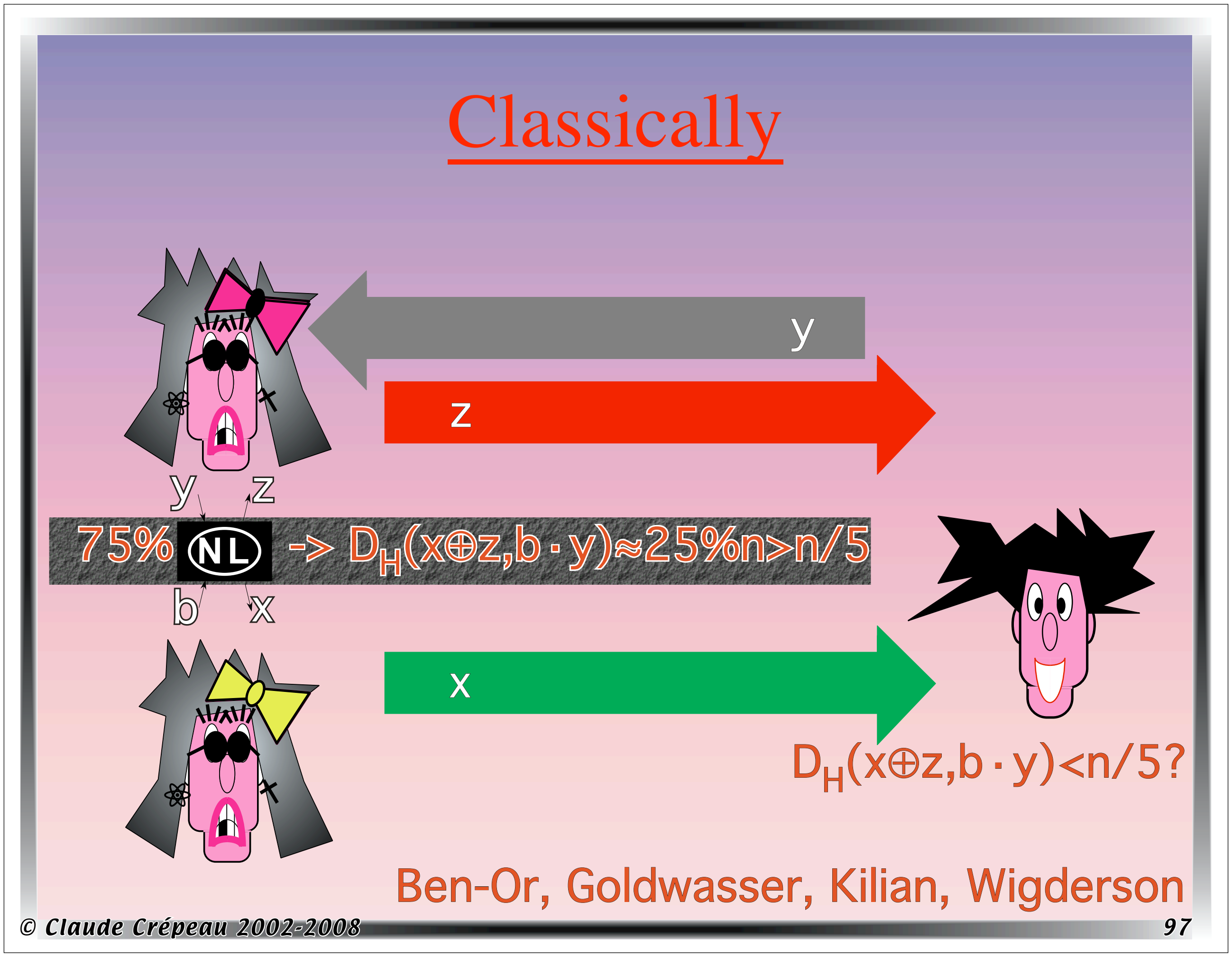


$z = x$ if $b = 0$

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

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

Ben-Or, Goldwasser, Kilian, Wigderson

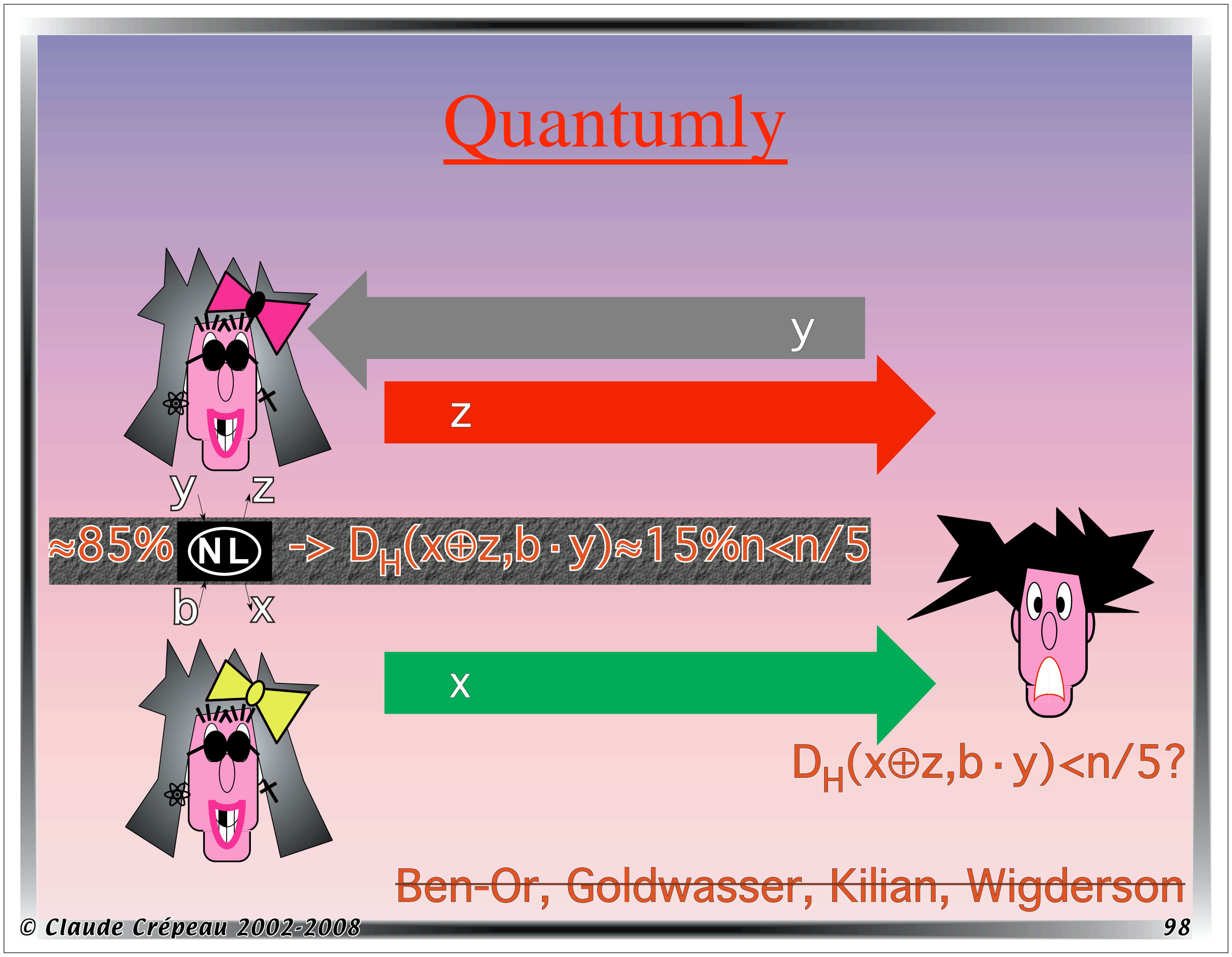


Classically

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

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

Ben-Or, Goldwasser, Kilian, Wigderson



Quantumly

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

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

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

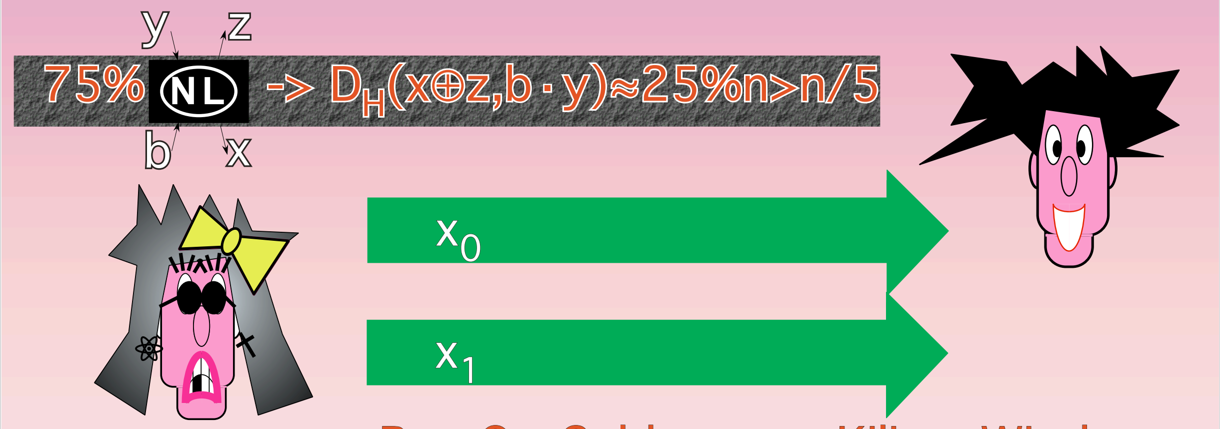
Classically

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

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

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

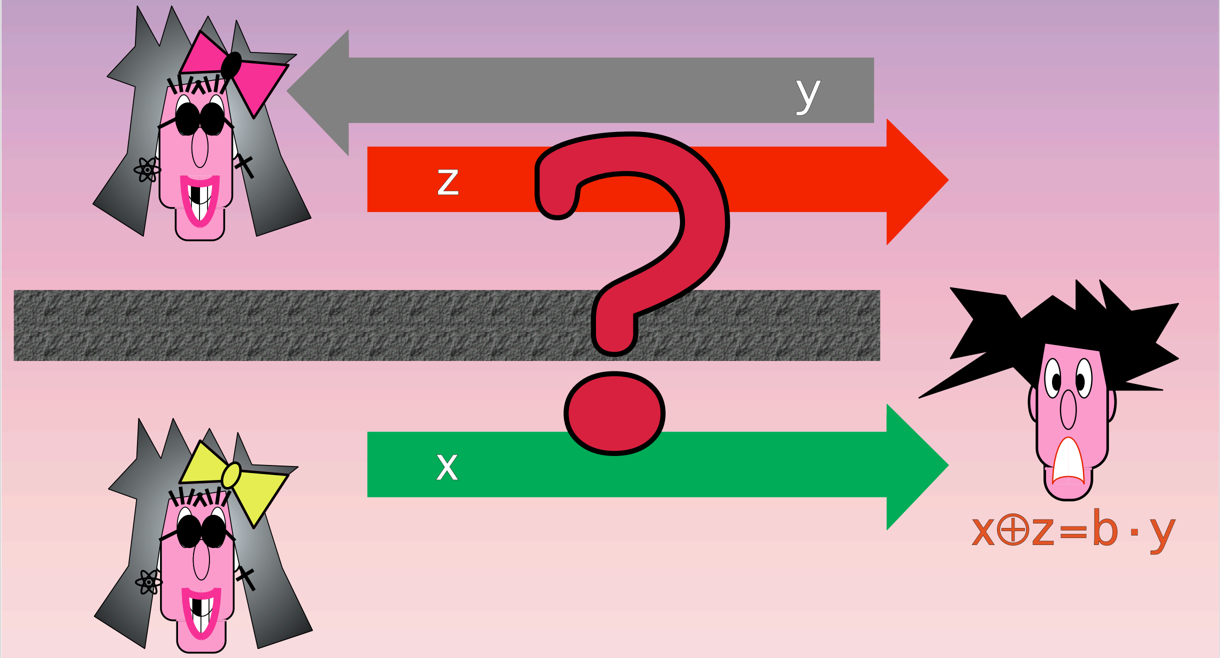
possible with prob. at most c^{-n}



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

Ben-Or, Goldwasser, Kilian, Wigderson

Quantumly

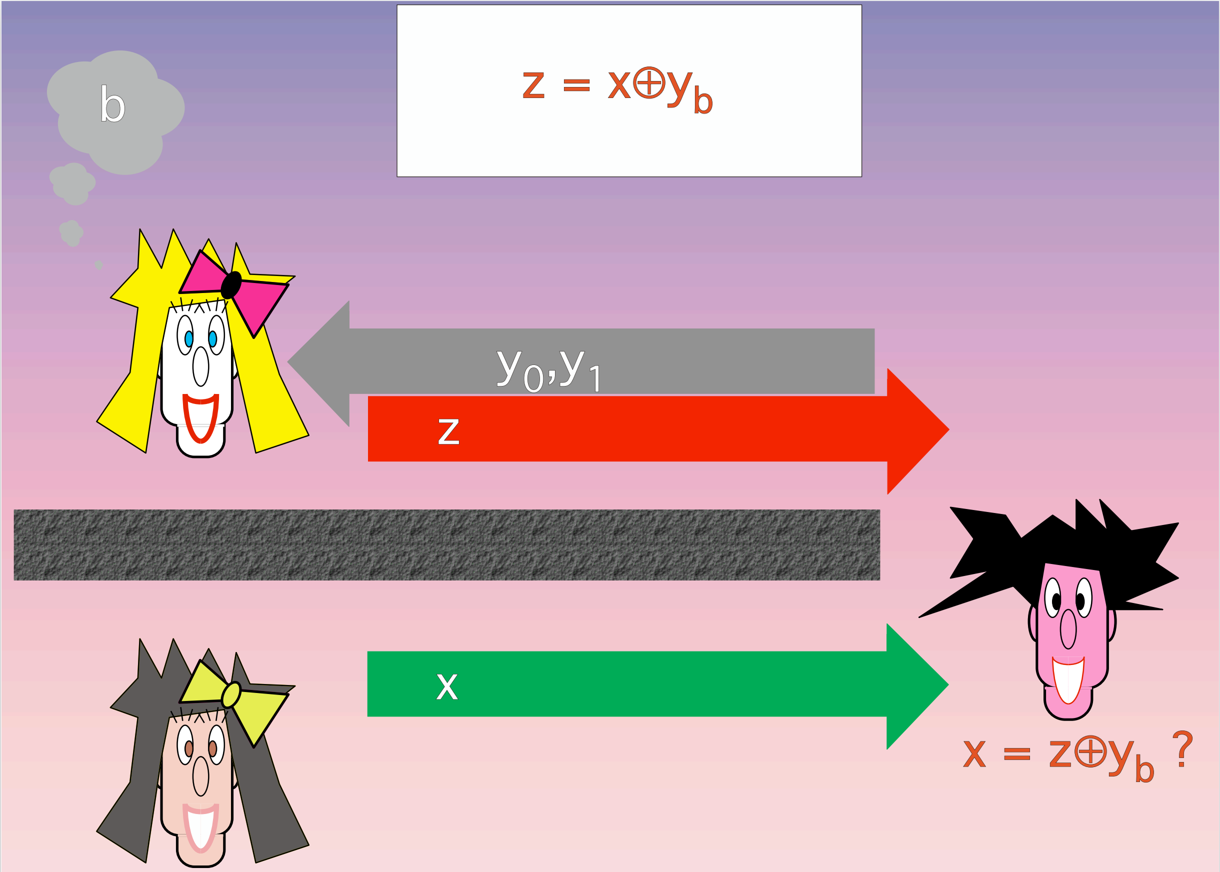


$x \oplus z = b \cdot y$

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

(8) two provers BC Classically and Quantumly Secure

$z = x \oplus y_b$



modified BGKW

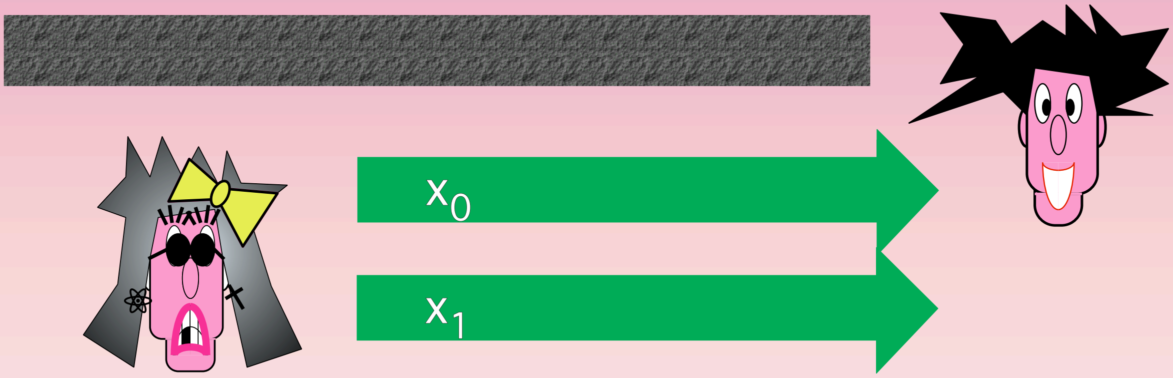
Classically

$x_0 \oplus z = y_0$

$x_1 \oplus z = y_1$

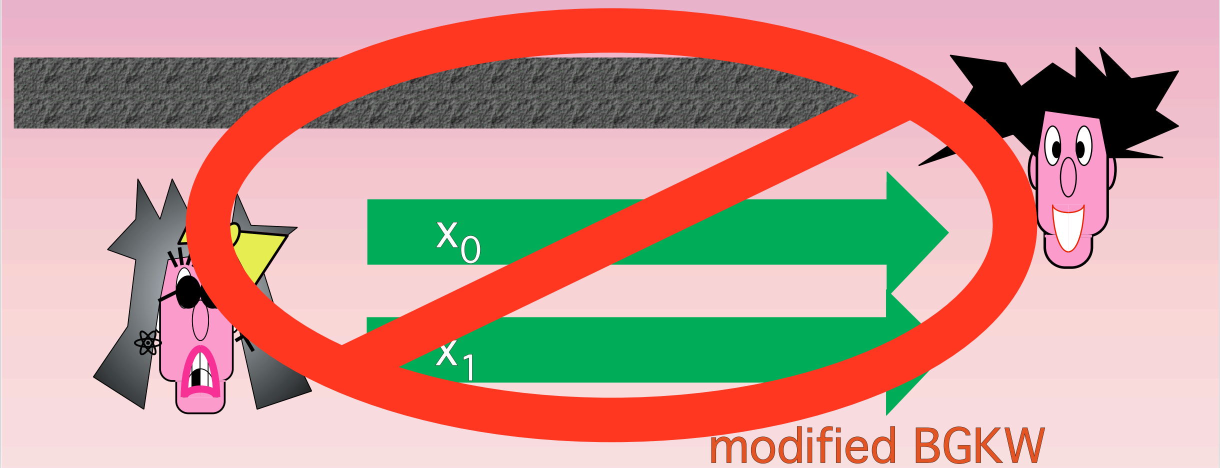
$x_0 \oplus x_1 = (x_0 \oplus z) \oplus (x_1 \oplus z) = y_0 \oplus y_1$

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



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.

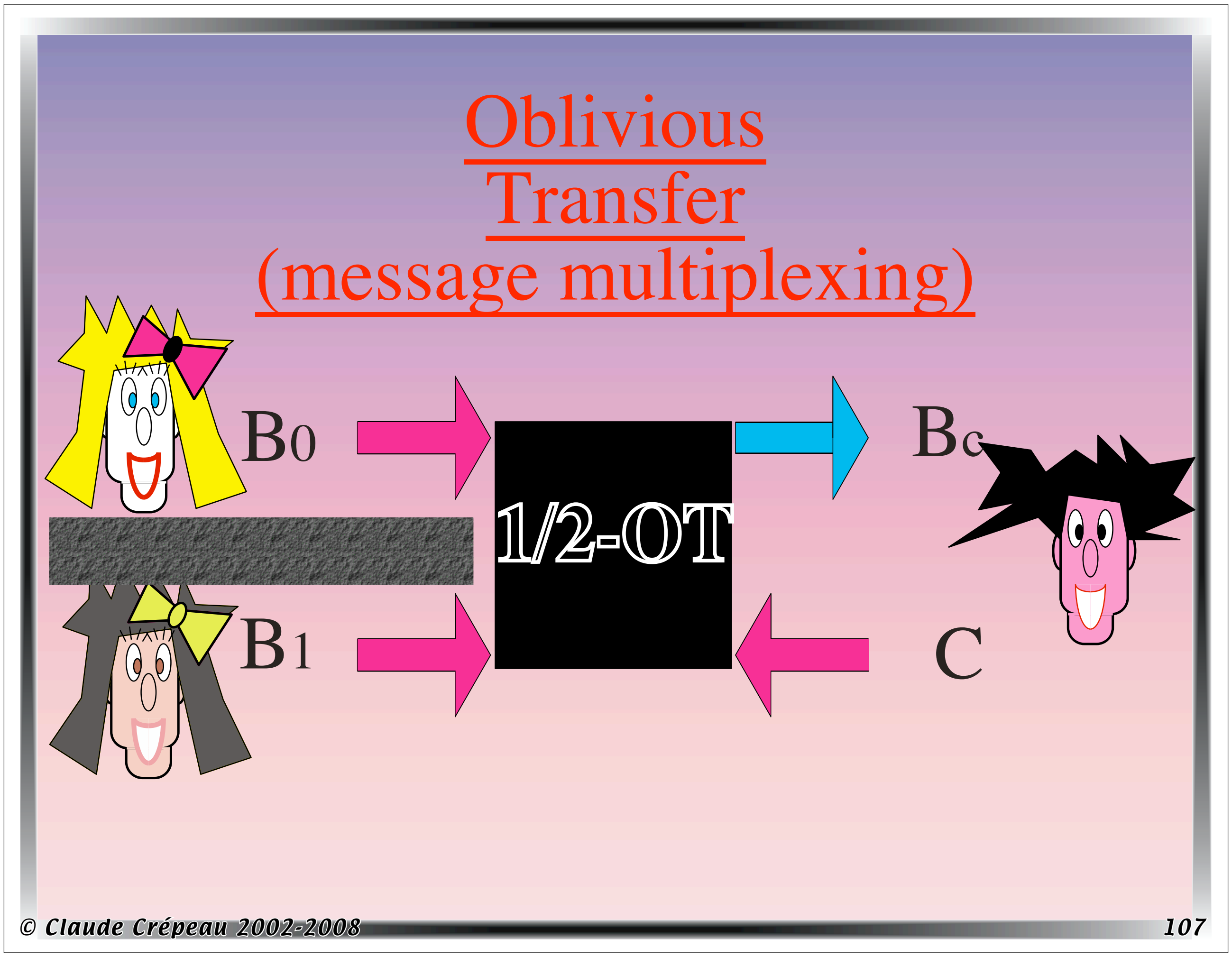
Suppose the success probability of unveiling is

$$p_0+p_1 > 1+\delta,$$

then the (prediction probability of $y_0 \oplus y_1$) > 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.

(9)
WARNING !



Oblivious Transfer (message multiplexing)

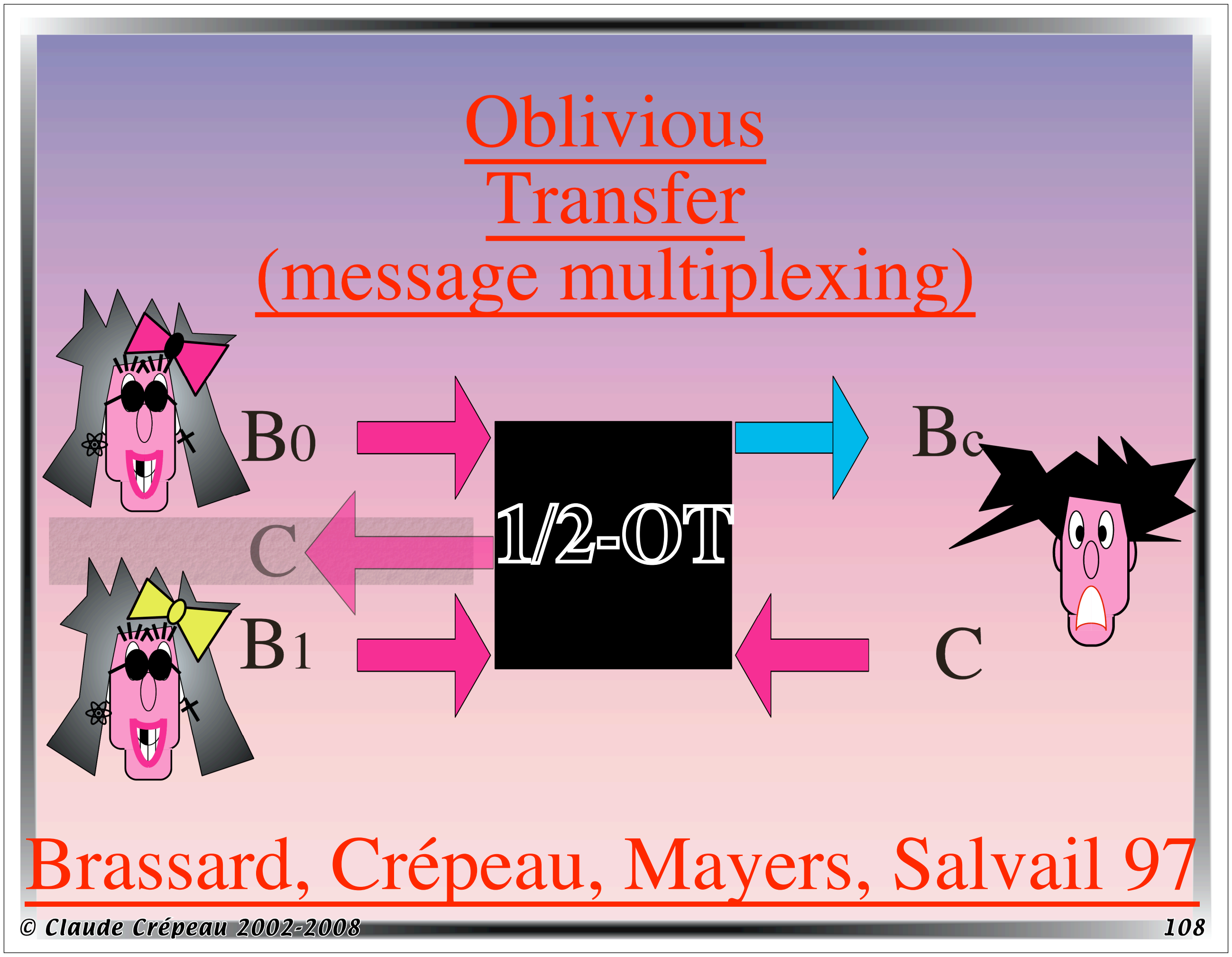
B_0

B_1

1/2-OT

B_c

C



Oblivious Transfer (message multiplexing)

B_0

C

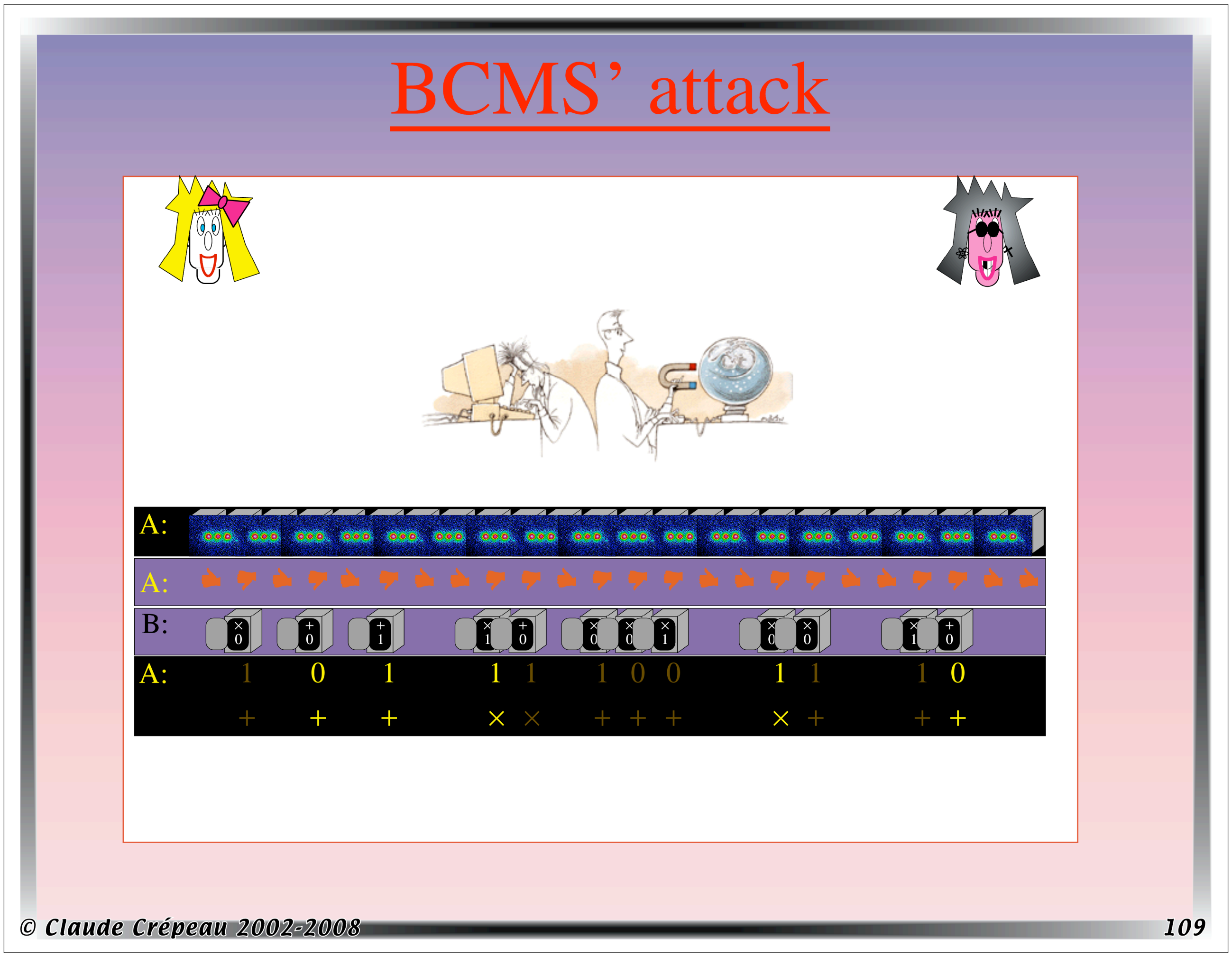
B_1

1/2-OT

B_c

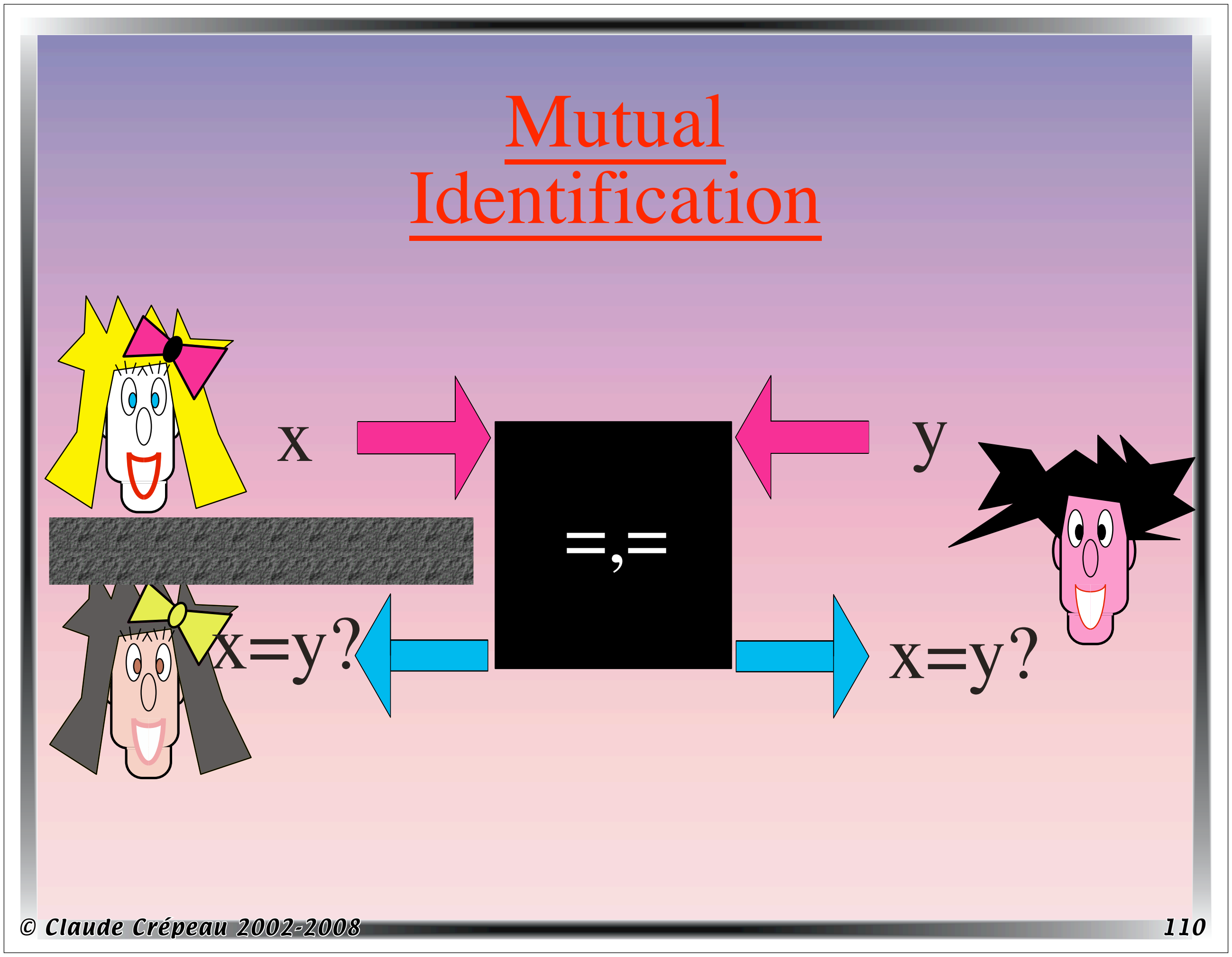
C

Brassard, Crépeau, Mayers, Salvail 97



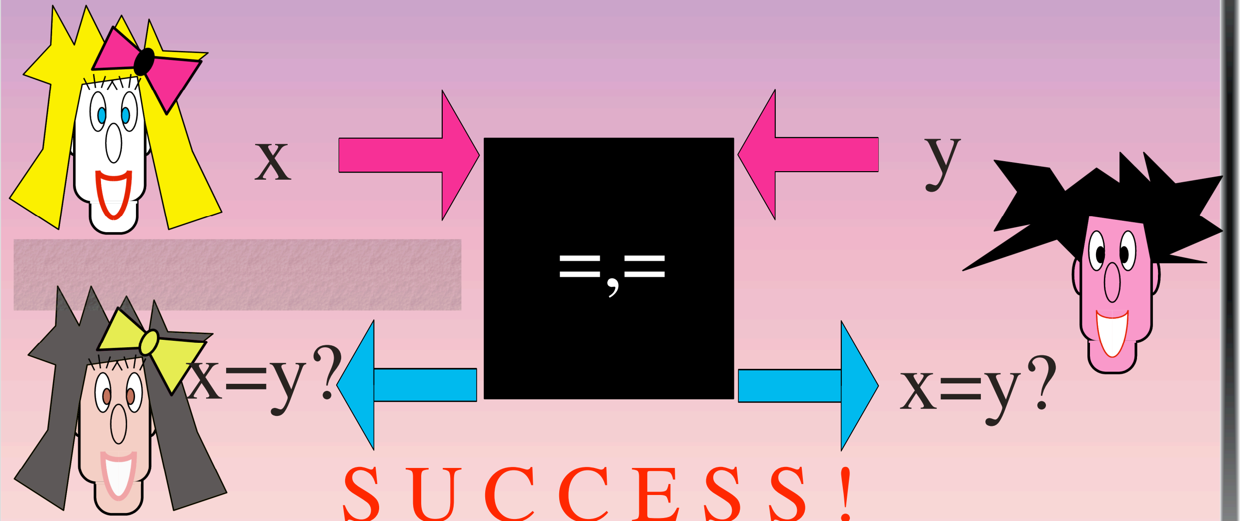
BCMS' attack

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



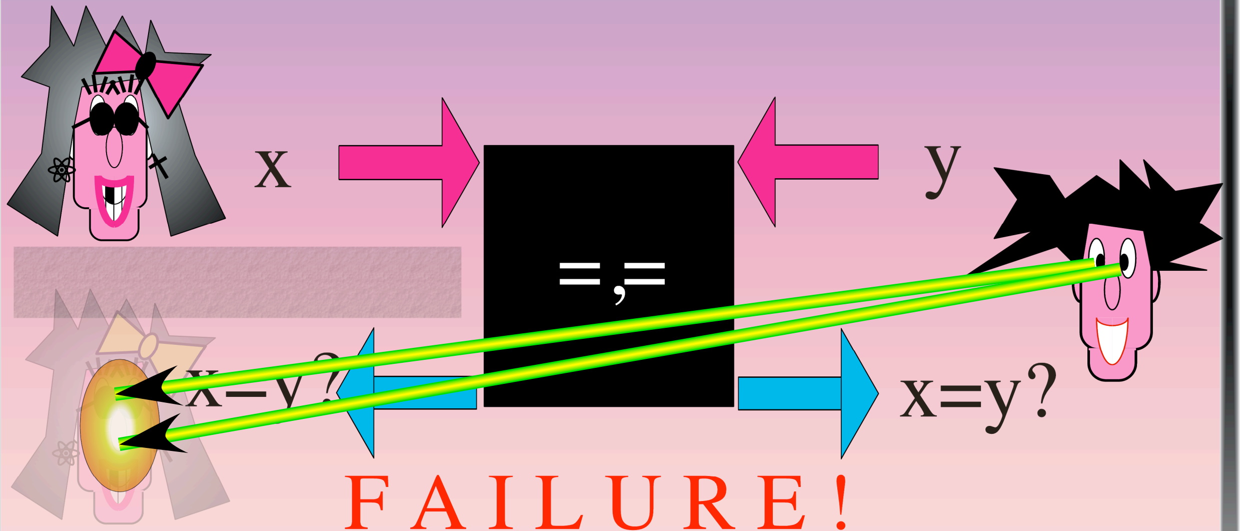
Mutual Identification

Mutual Identification

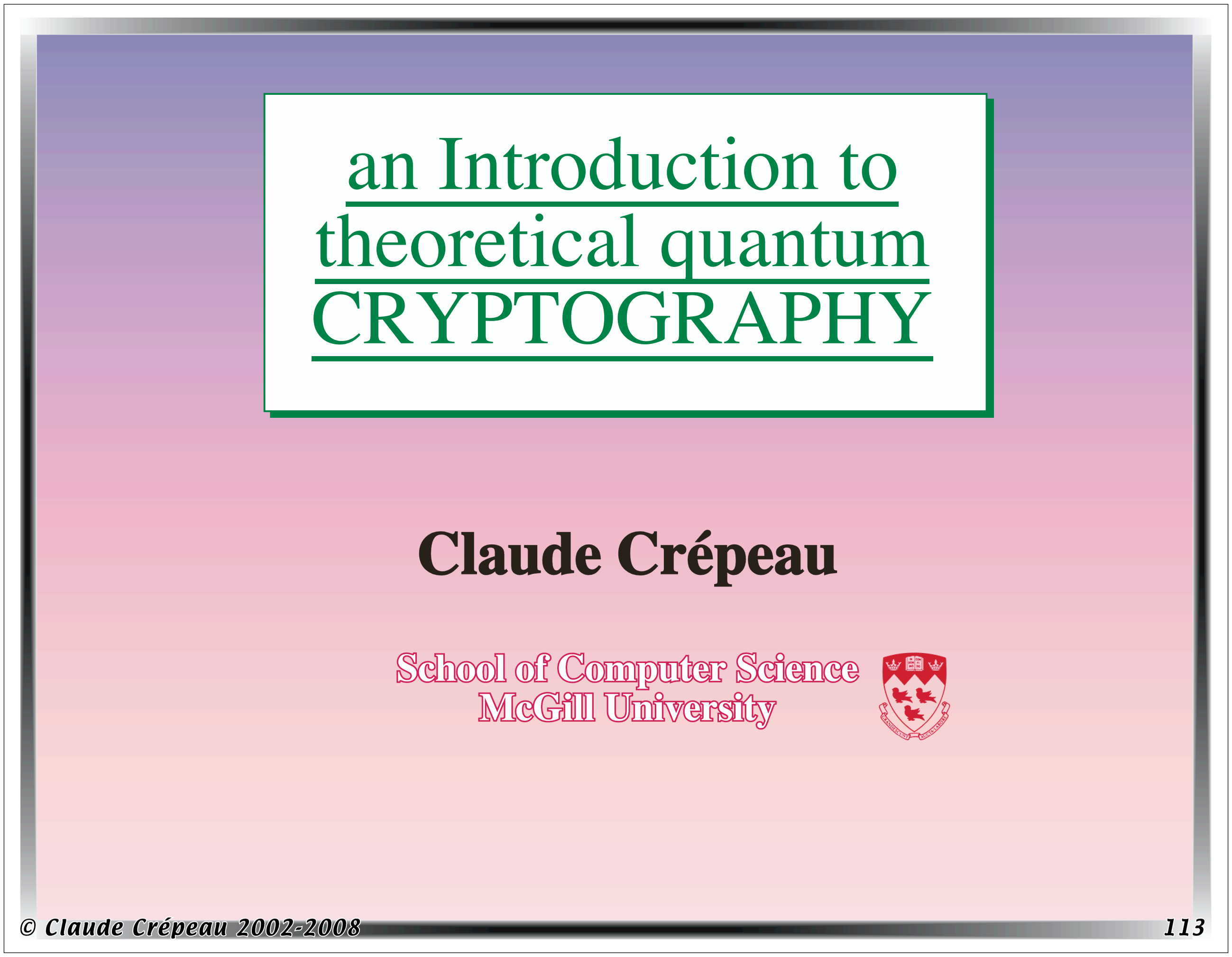


SUCCESS!

Mutual Identification



FAILURE!



an Introduction to theoretical quantum CRYPTOGRAPHY

Claude Crépeau

School of Computer Science
McGill University