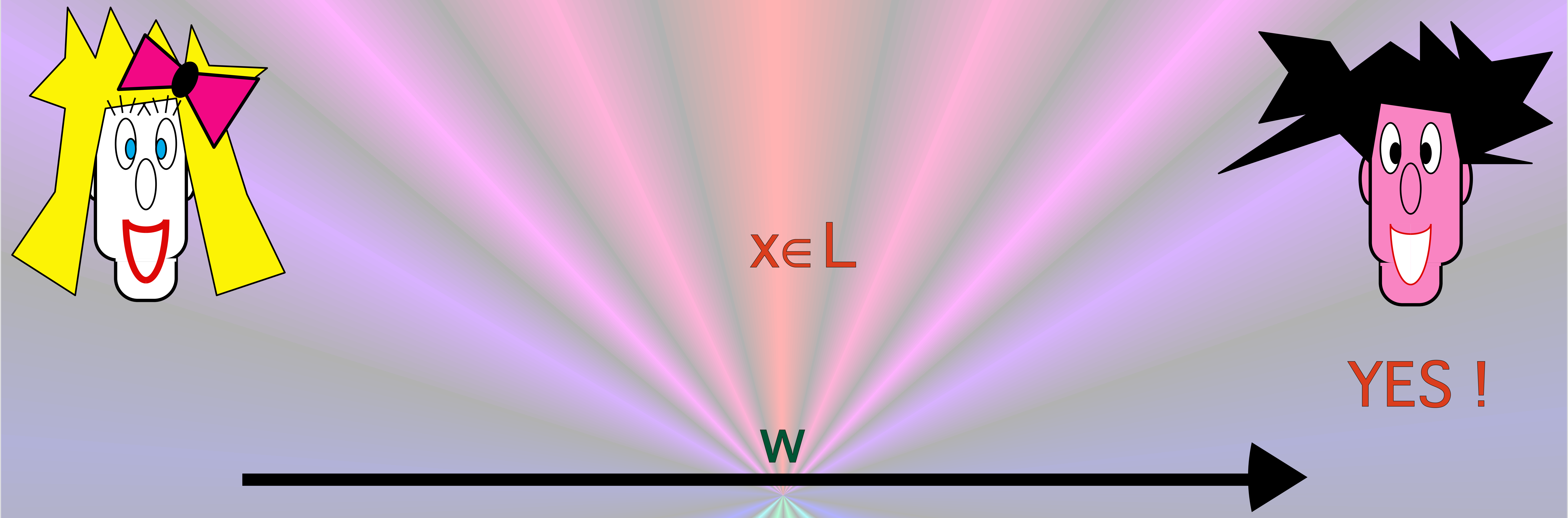
Interactive Zero-Knowledge Proofs and other Two-Party Cryptographic Protocols

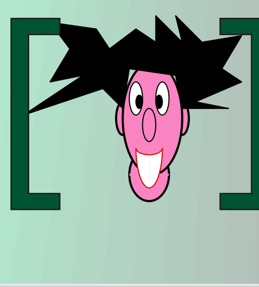
Claude Crépeau

School of Computer Science
McGill University

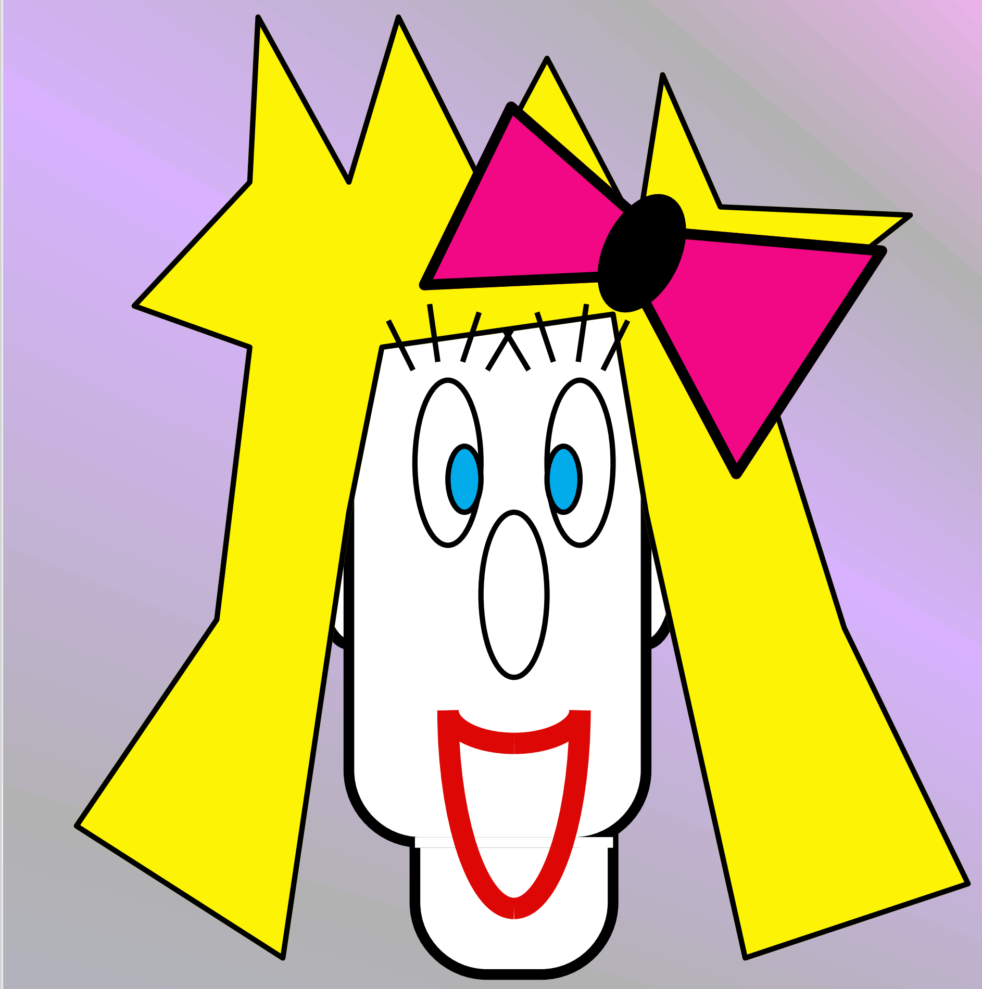
Proofs

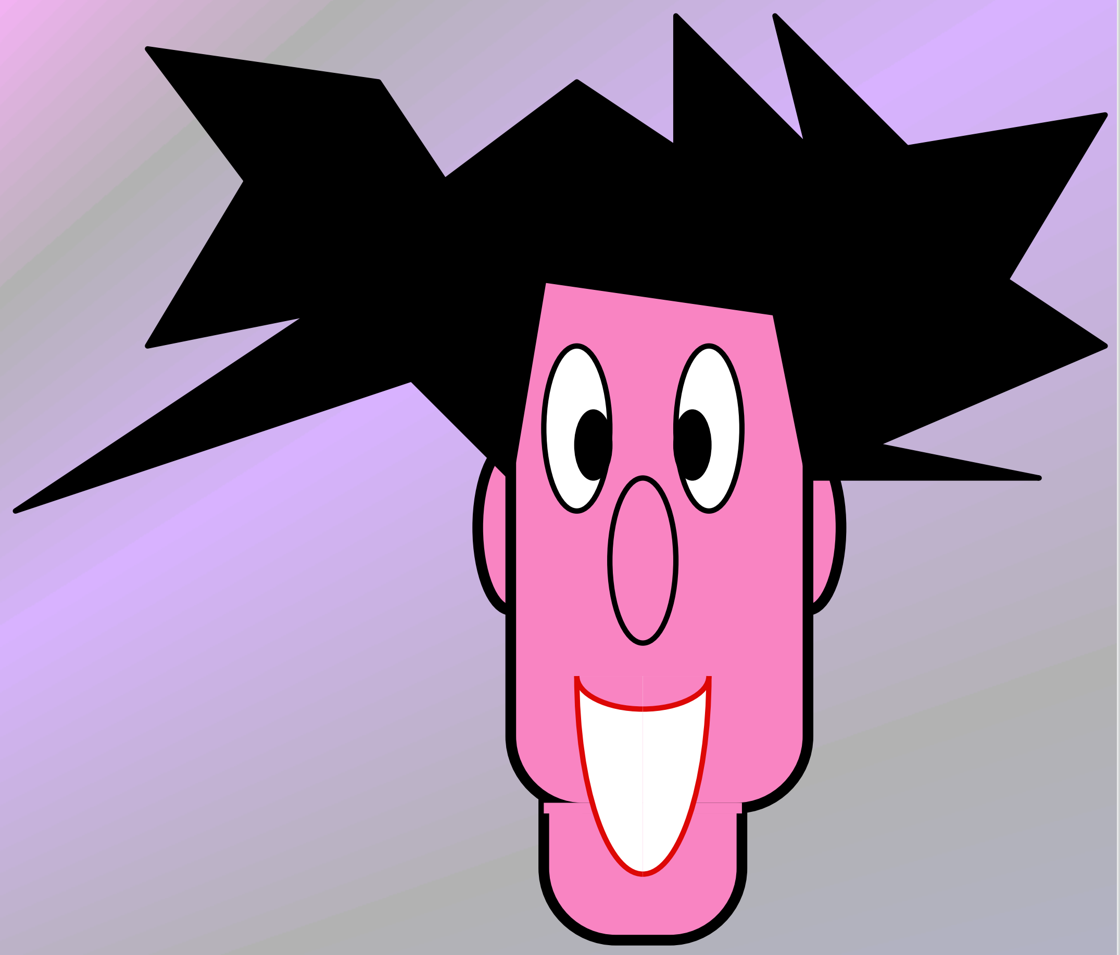
Proofs



∀x∈L∃w Pr([](x,w)=YES) = 1

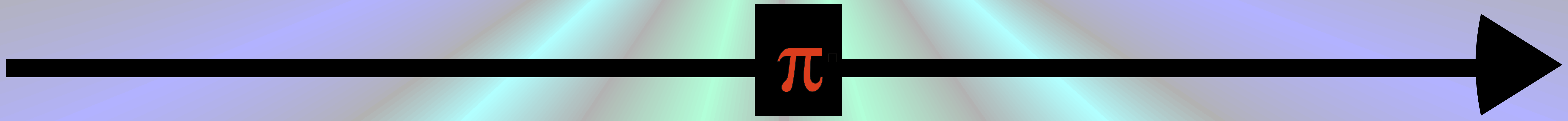
Proofs





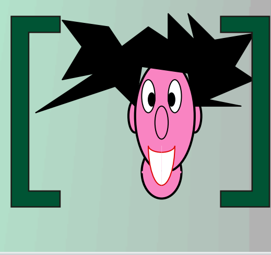
$(G_0,G_1)\in \text{ISO}$

$\left(G_0=\pi(G_1)\right)$

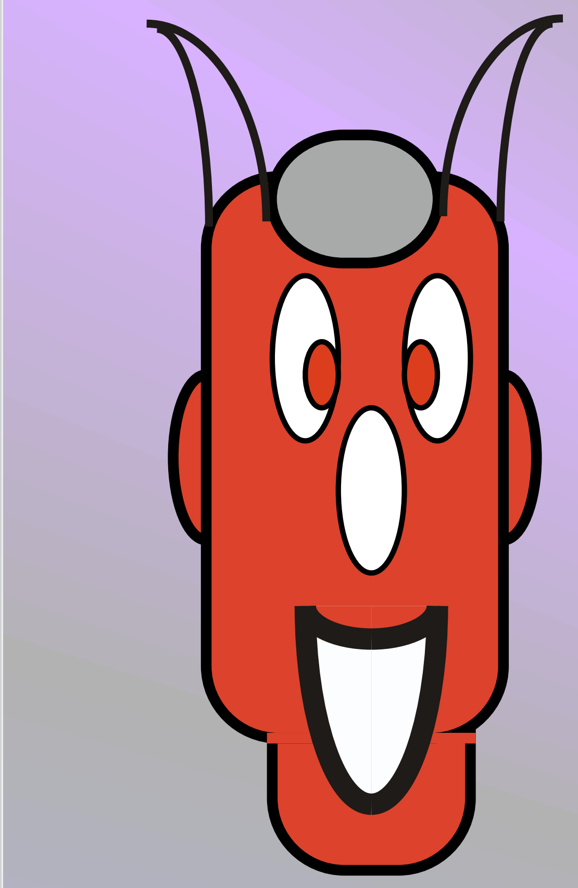


$G_0=\pi(G_1)$

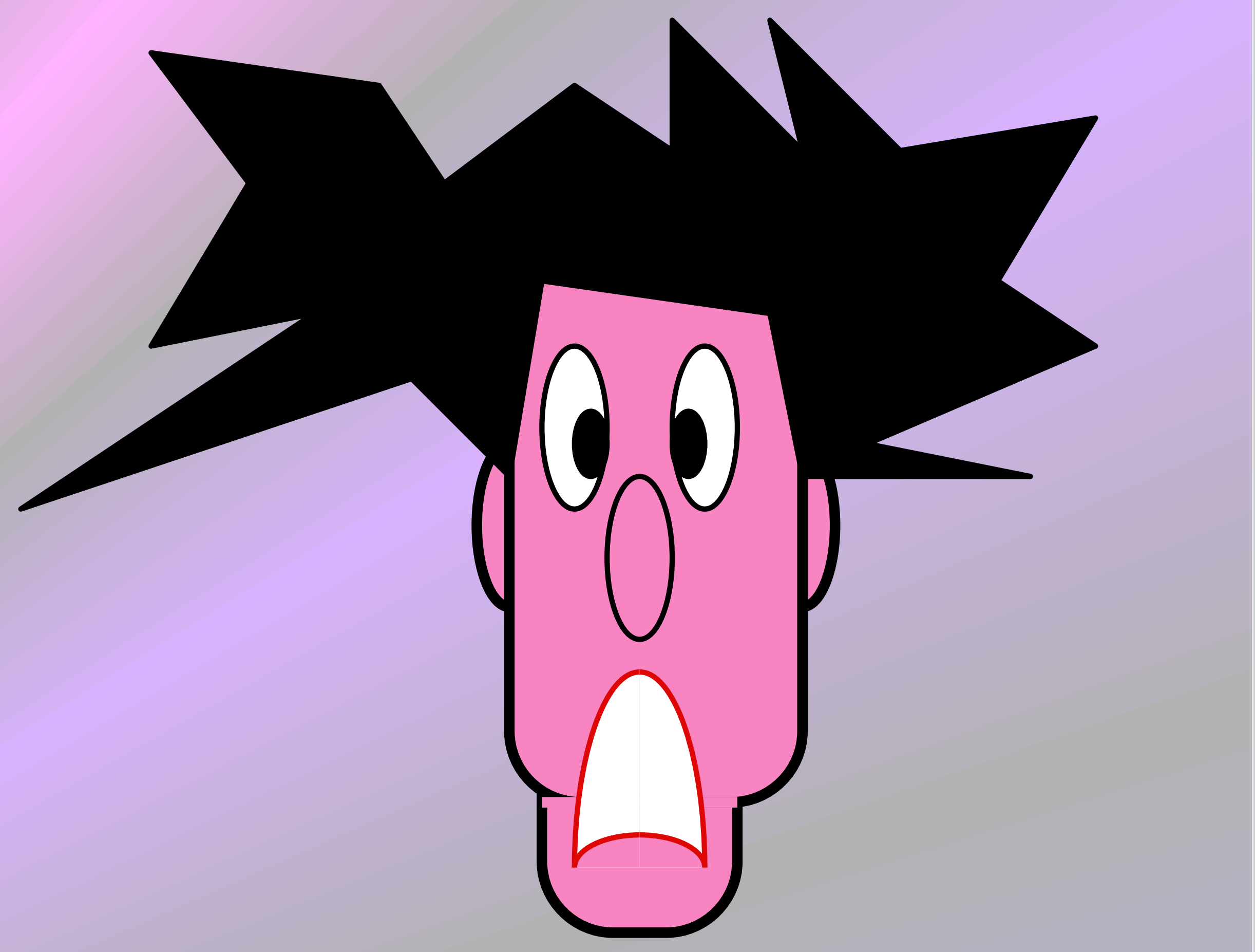
YES !

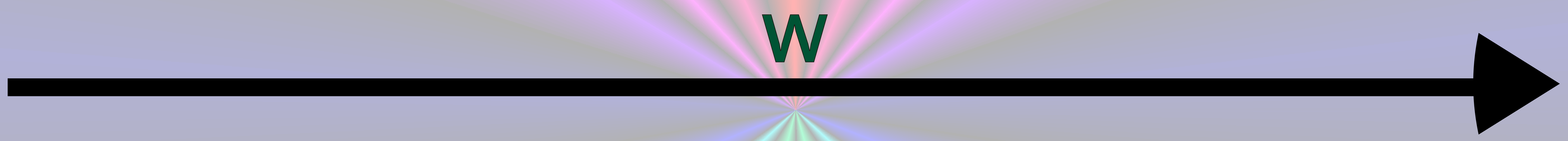
$\forall x\in L\,\exists\pi\ \Pr($ [] $(x,\pi)=\text{YES}\ ) = 1$

Proofs

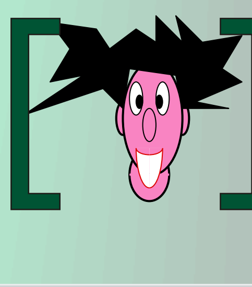


$x \notin L$

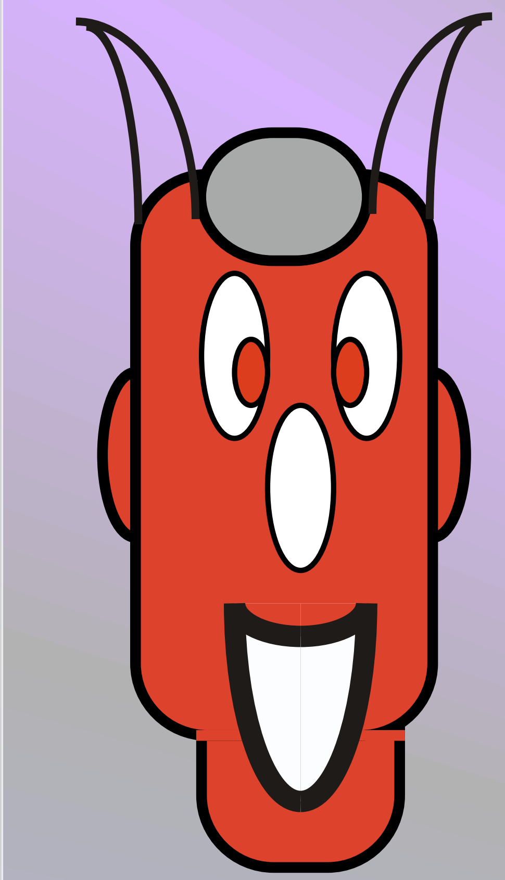


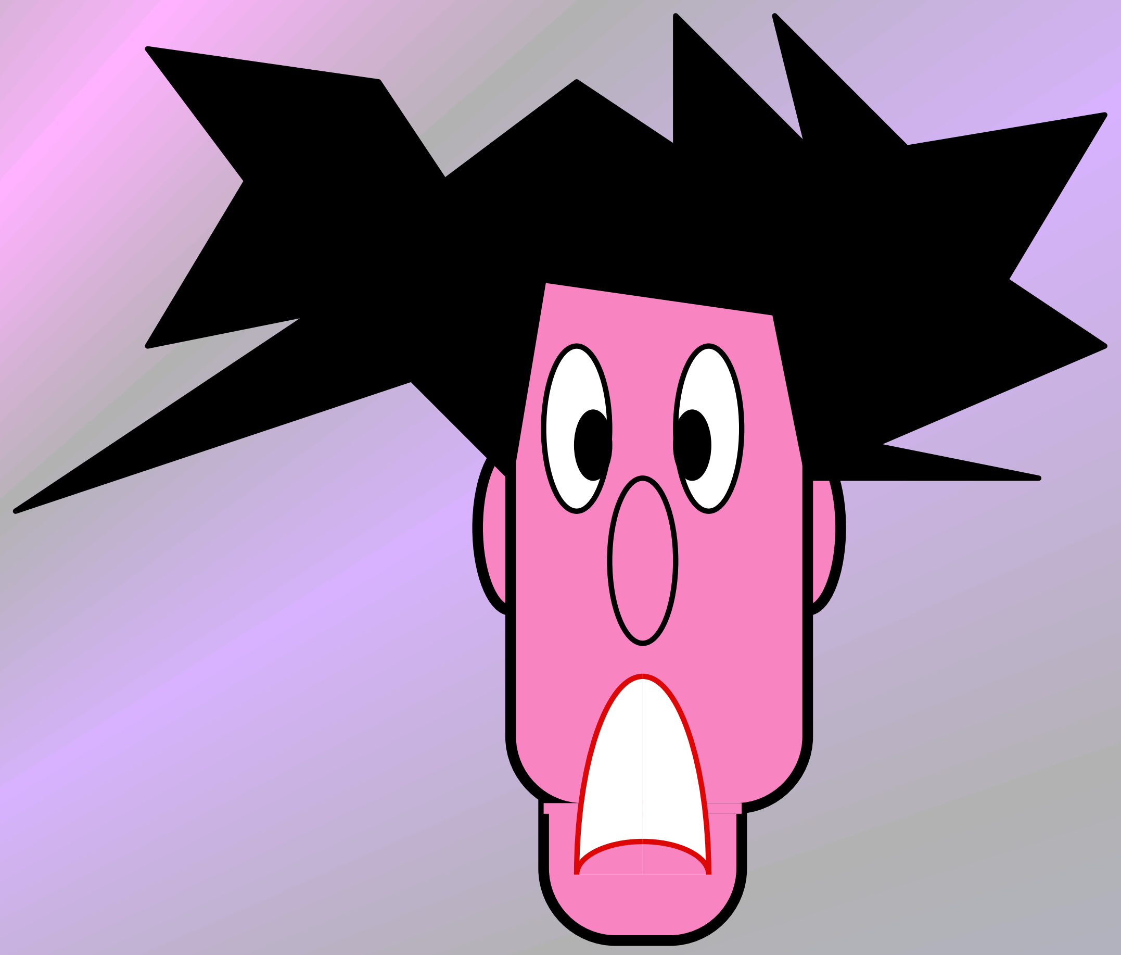


NO !

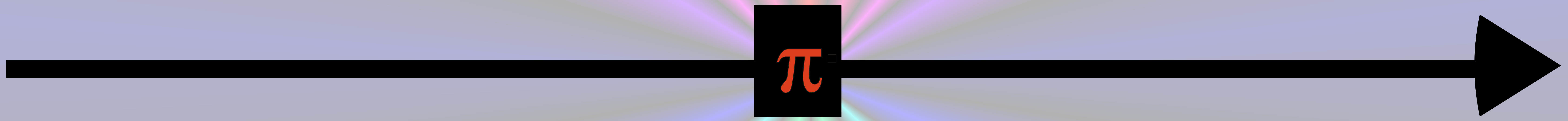
$\forall x \notin L \, \forall w$ Pr([](x,w)=YES) = 0

Proofs





$(G_0,G_1)\notin ISO$



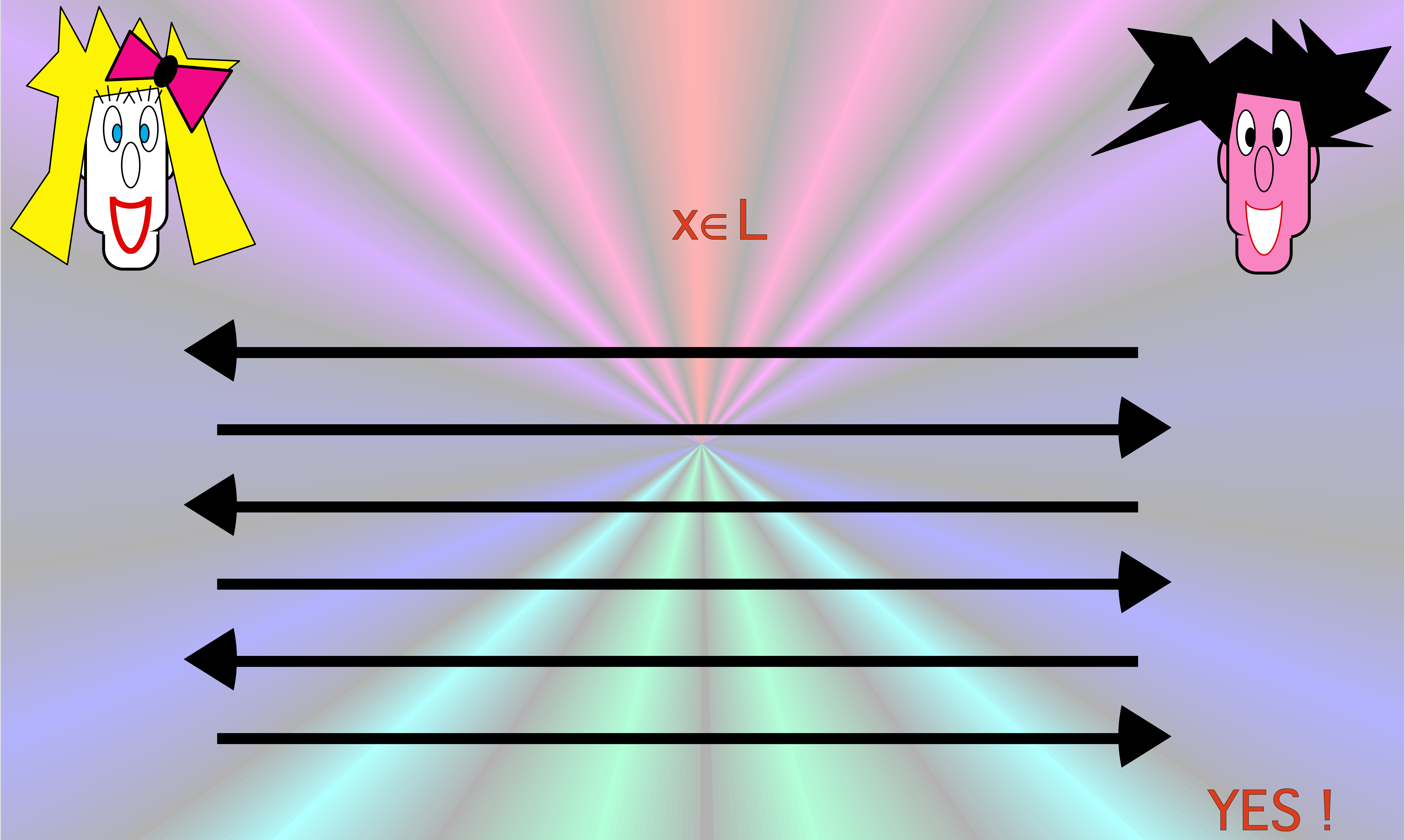
$G_0 \neq \pi(G_1)$

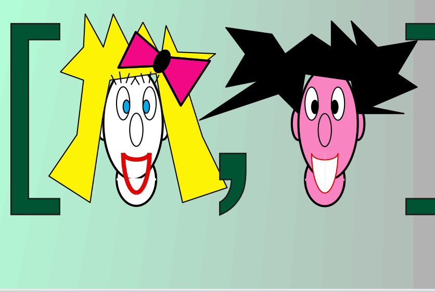
NO !

$\forall x \notin L\ \forall \pi\ \Pr(\ [\ ](x,\pi)=YES\ ) = 0$

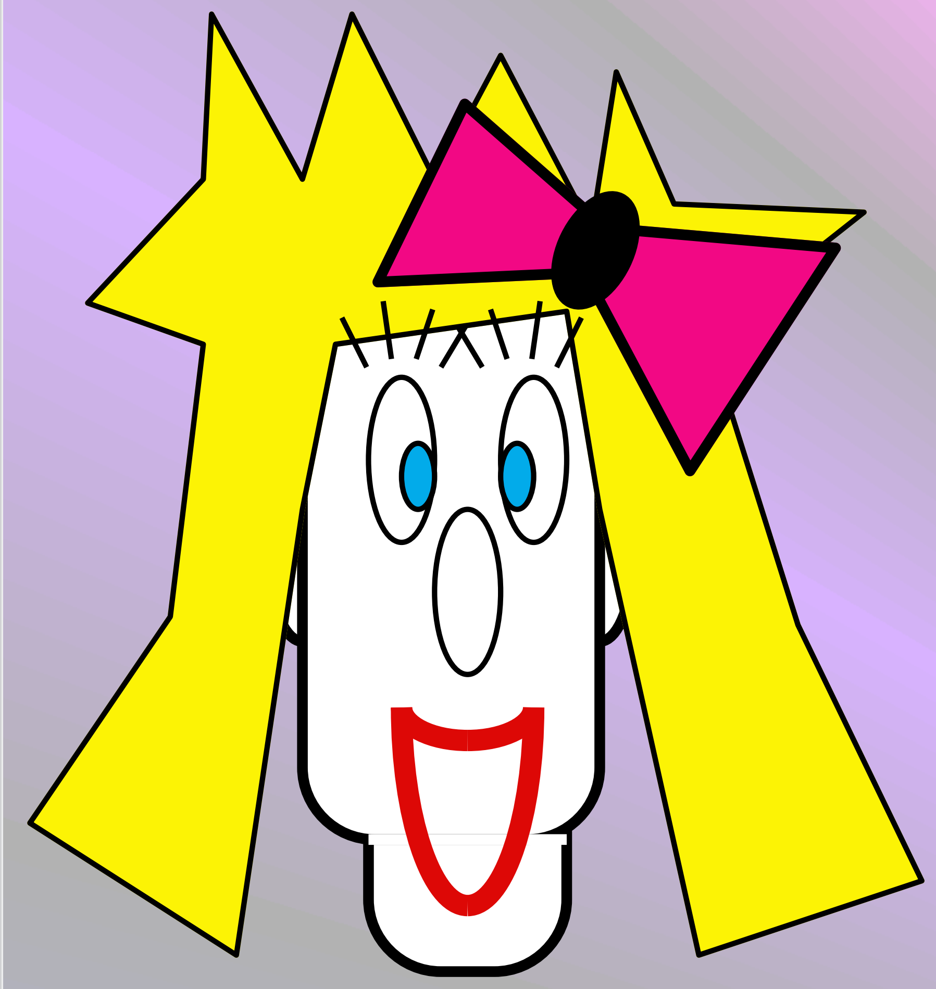
Interactive Proofs

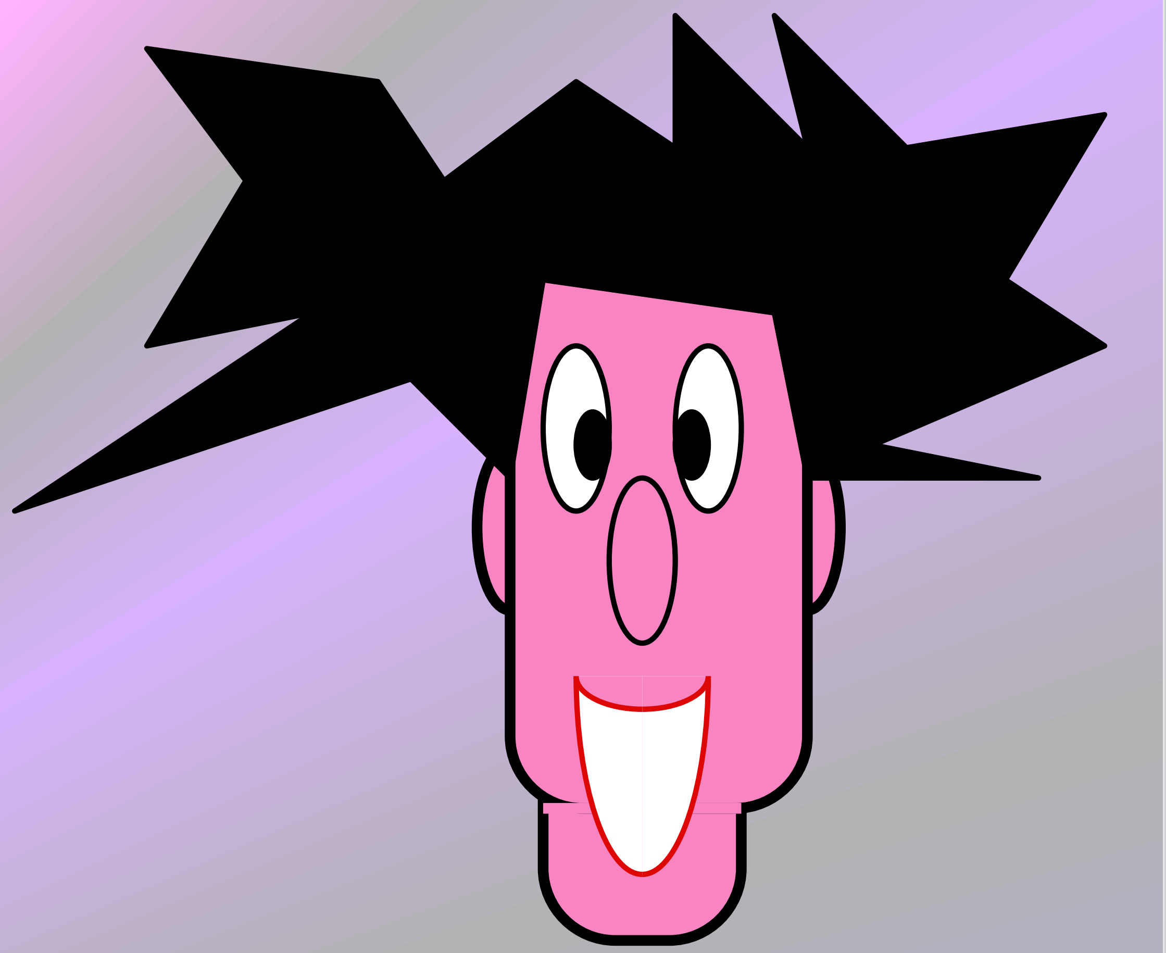
Interactive Proofs and Zero-Knowledge



$\forall x \in L \; \Pr([$  $](x)=\text{YES}) \approx 1$

Interactive Proofs and Zero-Knowledge



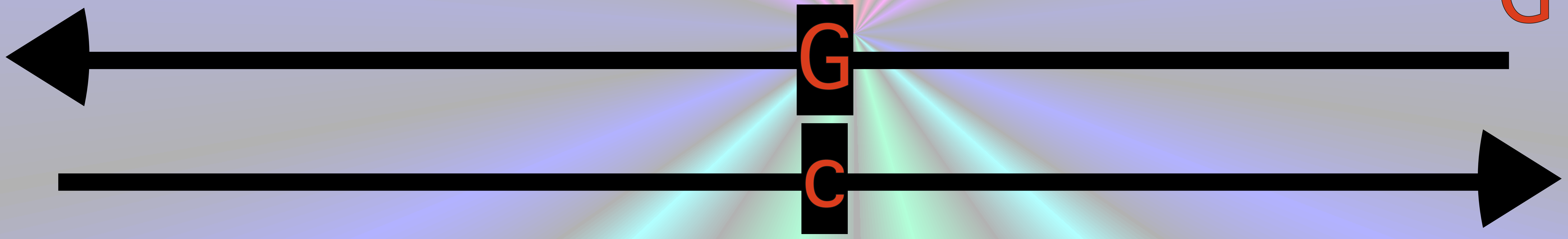


$(G_0,G_1) \notin ISO$

random b,π

$G = \pi(G_b)$

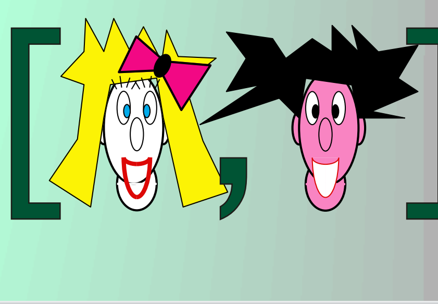
$G \not\approx G_0$ or $G \not\approx G_1$



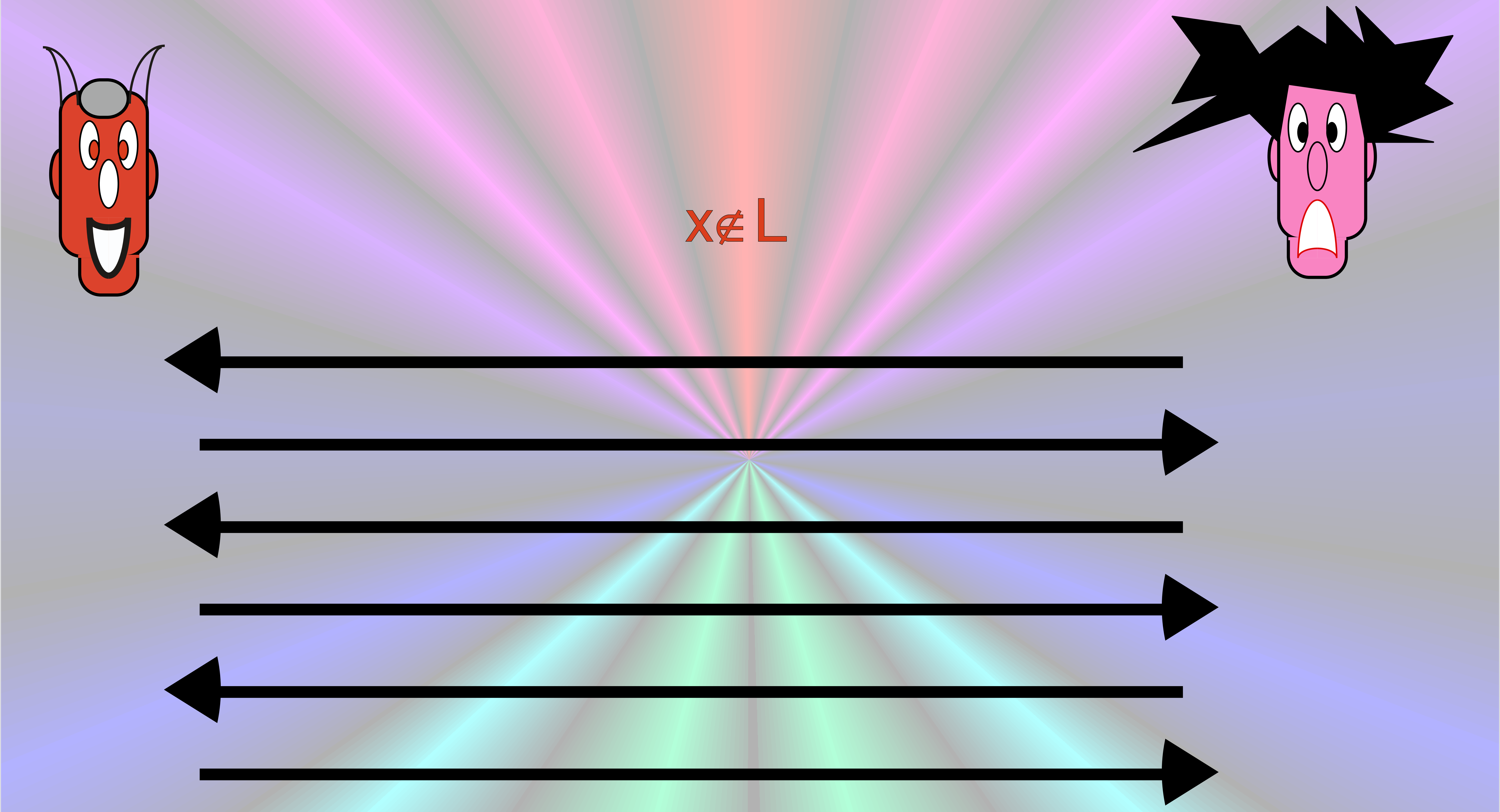
$G \approx G_c$

b = c?

YES !

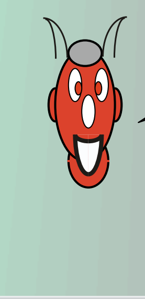
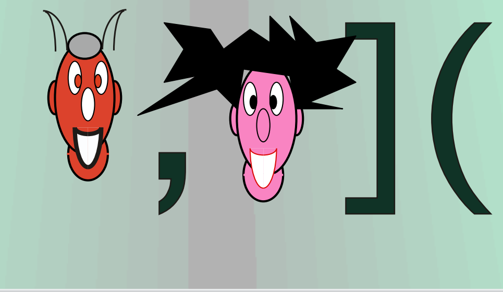
∀x∈L Pr([](x)=YES) = 1

Interactive Proofs and Zero-Knowledge

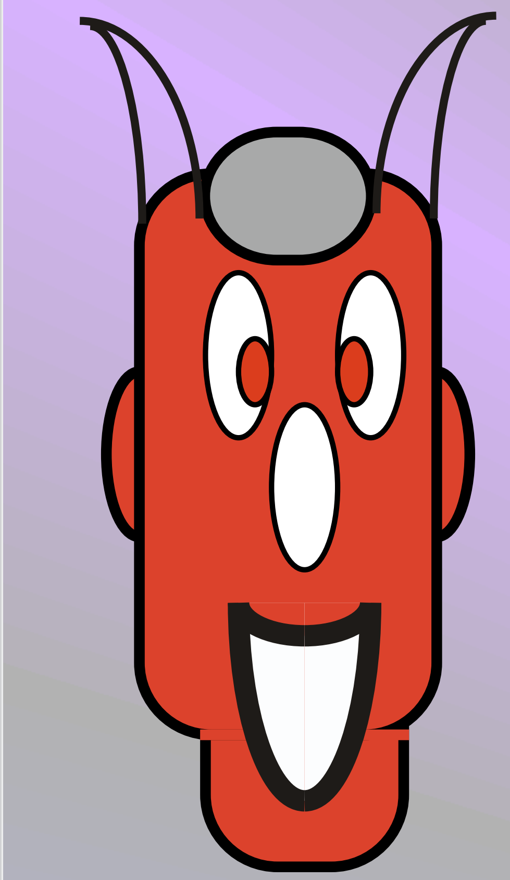


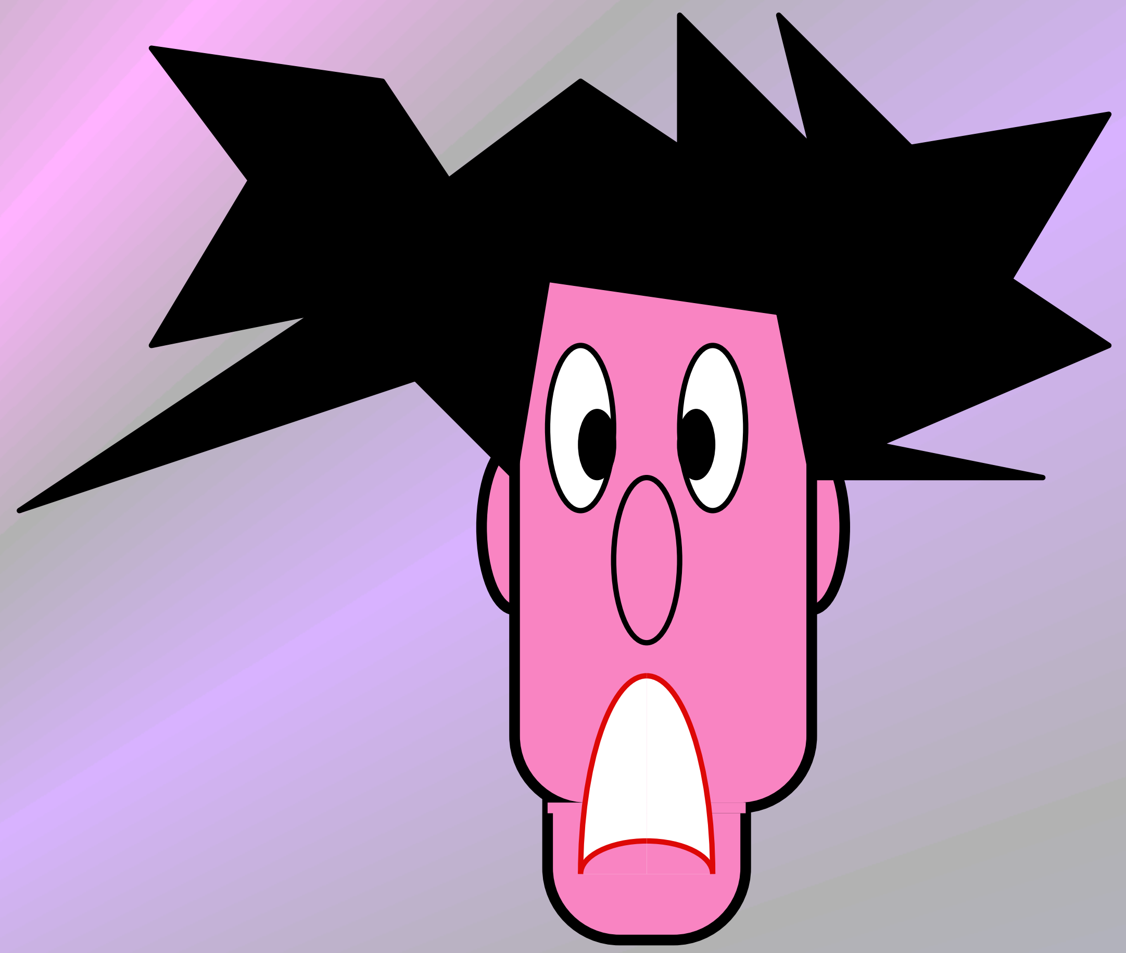
x∉L

NO !

∀x∉L ∀ Pr([,](x)=YES) ≈ 0

Interactive Proofs and Zero-Knowledge



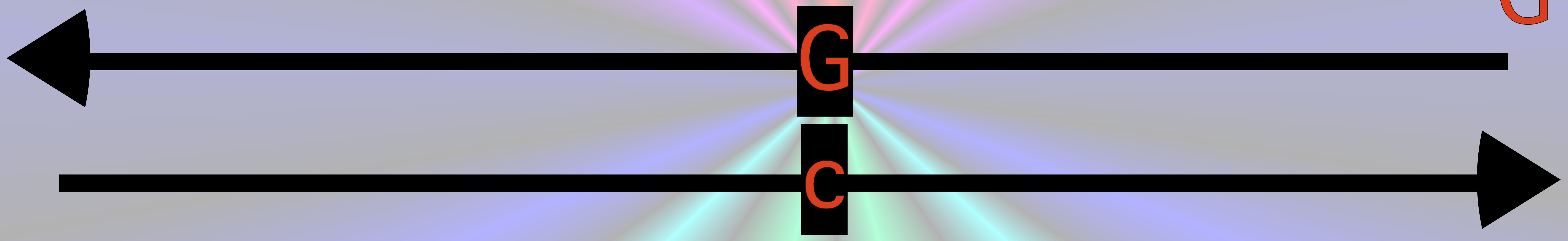


$(G_0,G_1)\in ISO$

random b,π

$G = \pi(G_b)$

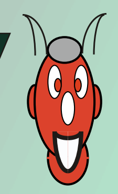
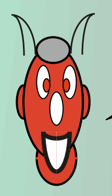
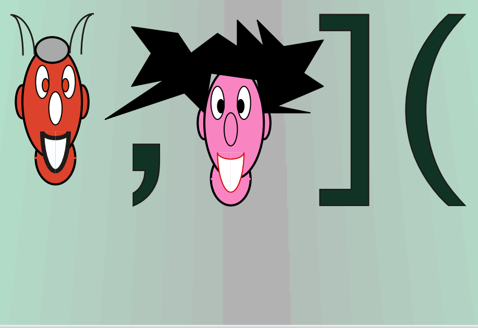
$G\approx G_0$ and $G\approx G_1$



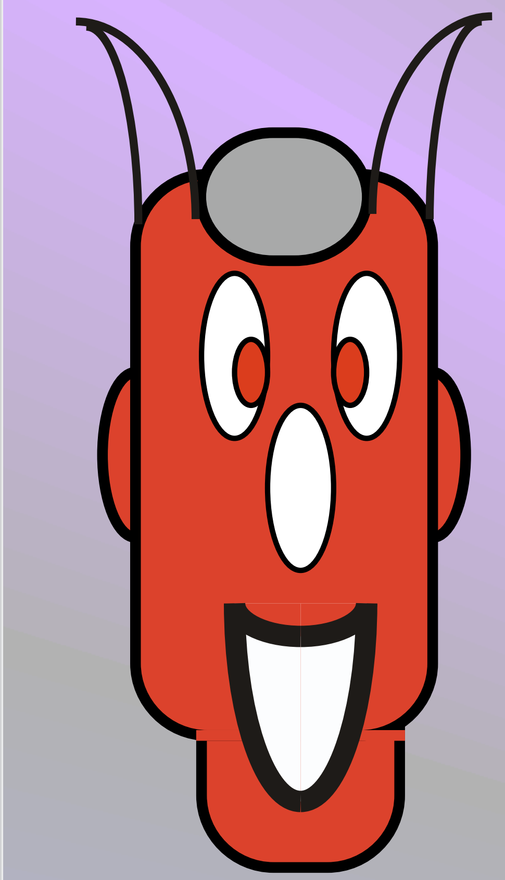
$G\approx G_c$

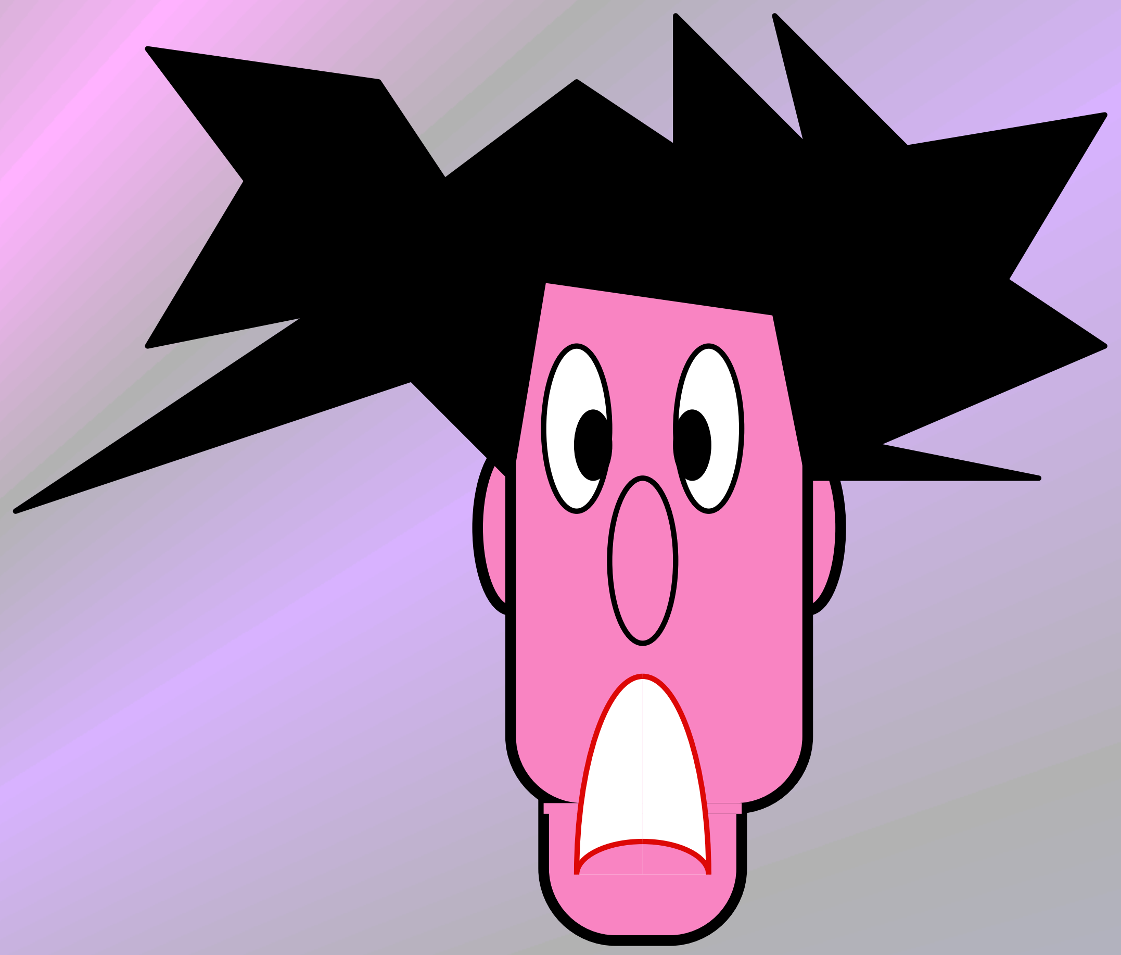
$b = c?$

NO !

$\forall x\notin L\ \forall$  $\Pr(\ [$  $,$  $](x)=YES\ )\ \le {}^{1}/_{2}$

Interactive Proofs and Zero-Knowledge

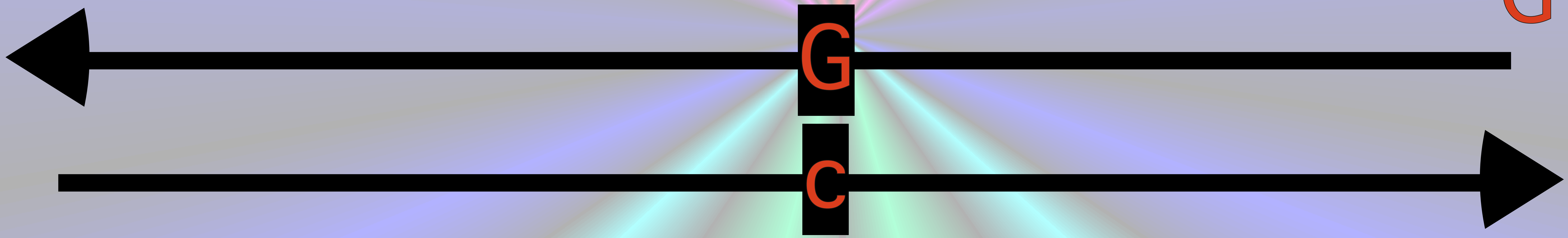




$(G_0,G_1)\in ISO$

random b,π
$G = \pi(G_b)$

$G\approx G_0$ and $G\approx G_1$



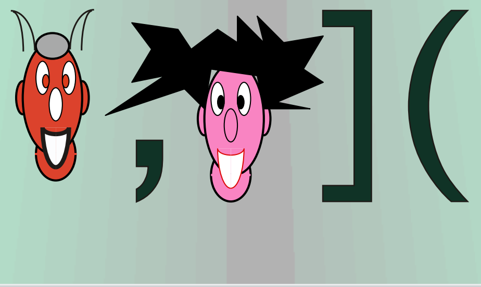
$G\approx G_c$

$b = c?$

REPEAT k TIMES

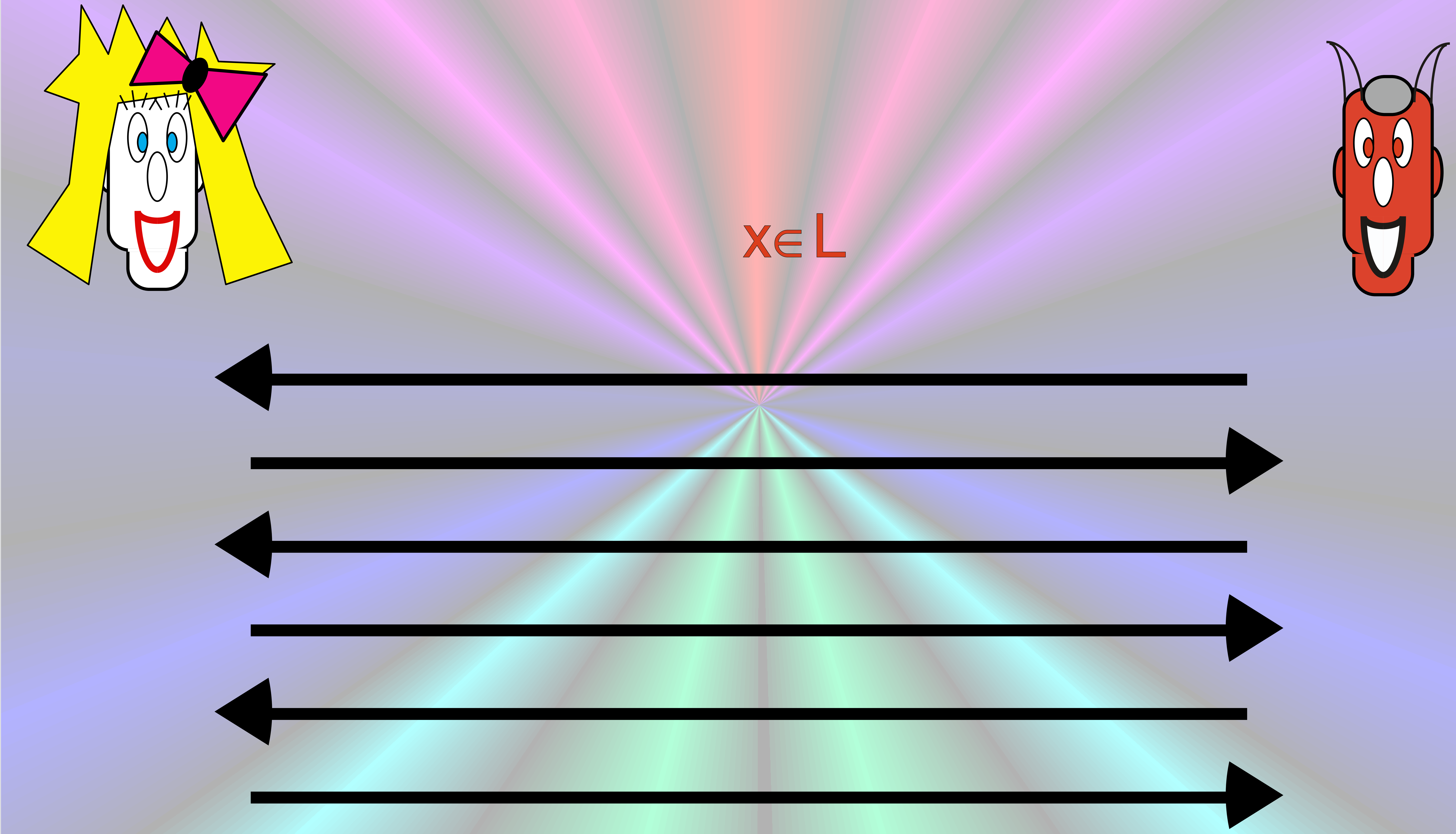
and say "YES" only if all "YES"

NO !

$\forall x\notin L$ $\forall$ Pr([, ](x)=YES) $\leq {}^{1}/_{2^k}$

Zero-Knowledge

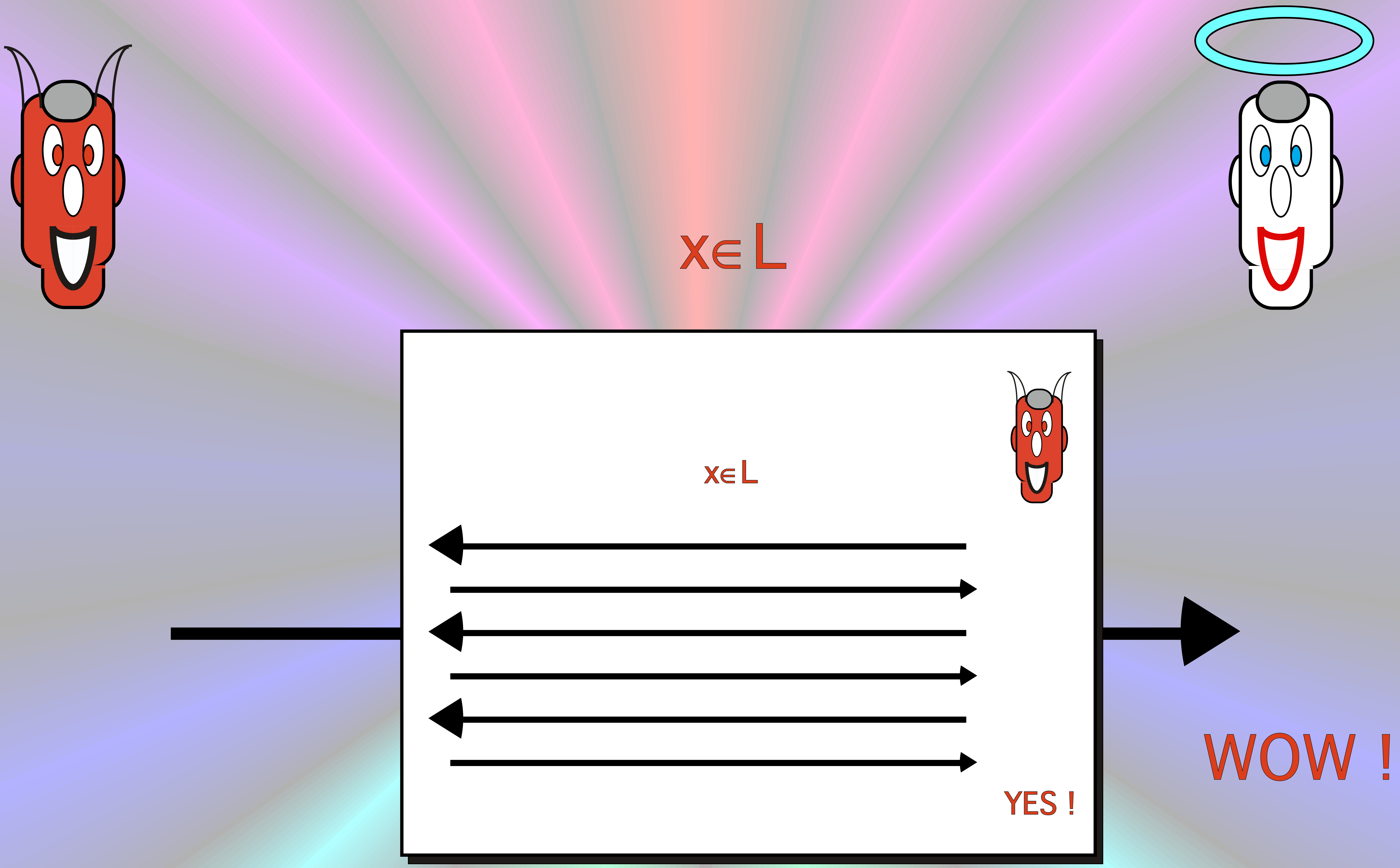
Interactive Proofs and Zero-Knowledge



$x \in L$

YES !

Interactive Proofs and Zero-Knowledge



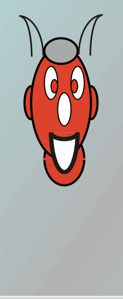
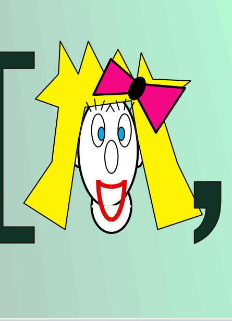
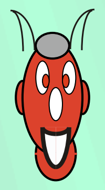
x∈L

x∈L

YES !

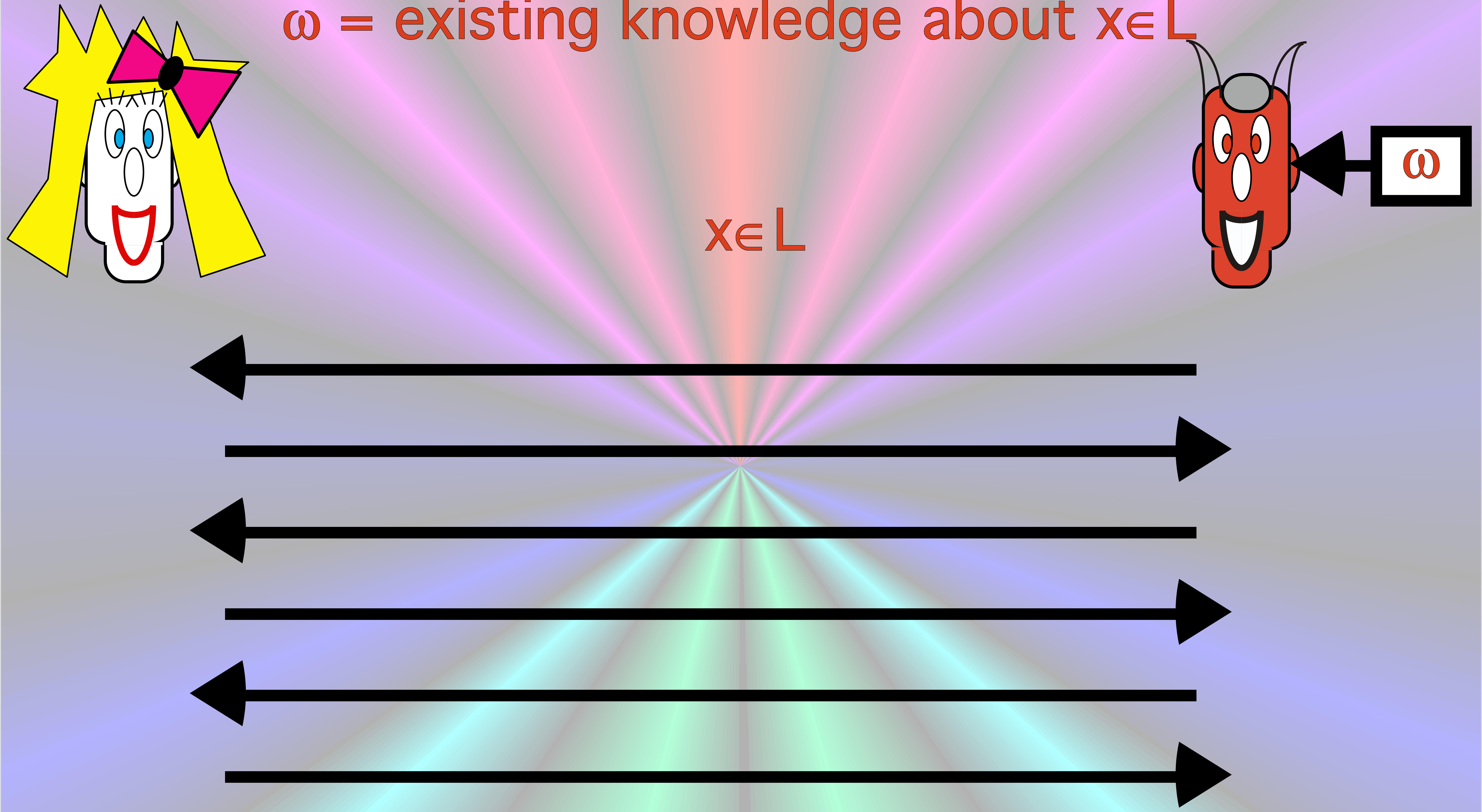
WOW !

Zero-Knowledge and Simulator

∀  ∃ ∀x∈L view[, ](x) = (x)

Auxiliary Input Zero-Knowledge

ω = existing knowledge about $x \in L$

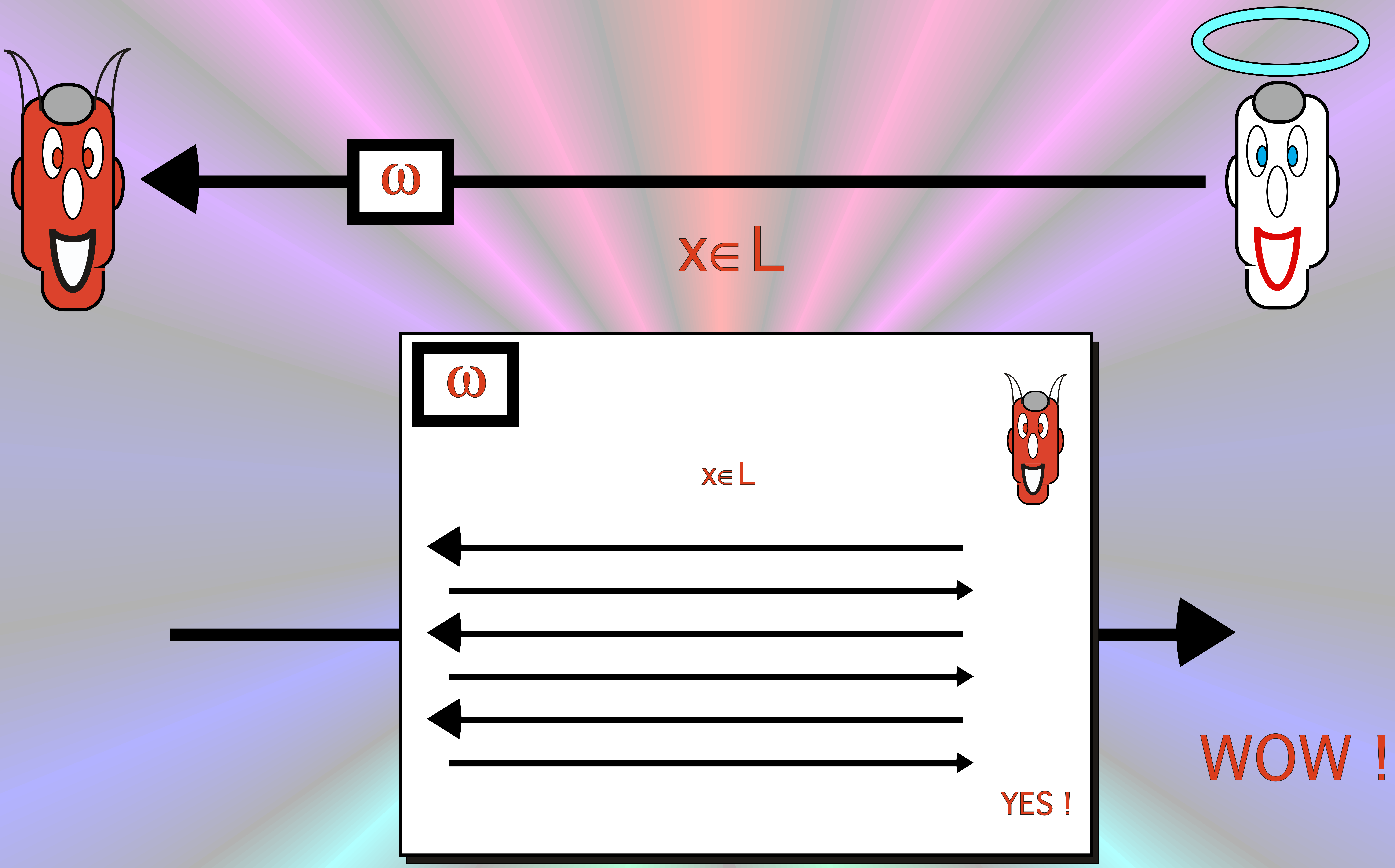


$x \in L$

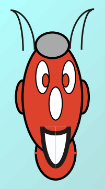
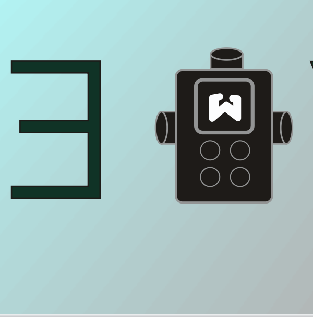
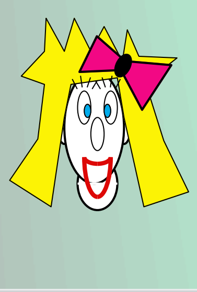
ω

YES !

Auxiliary Input Zero-Knowledge

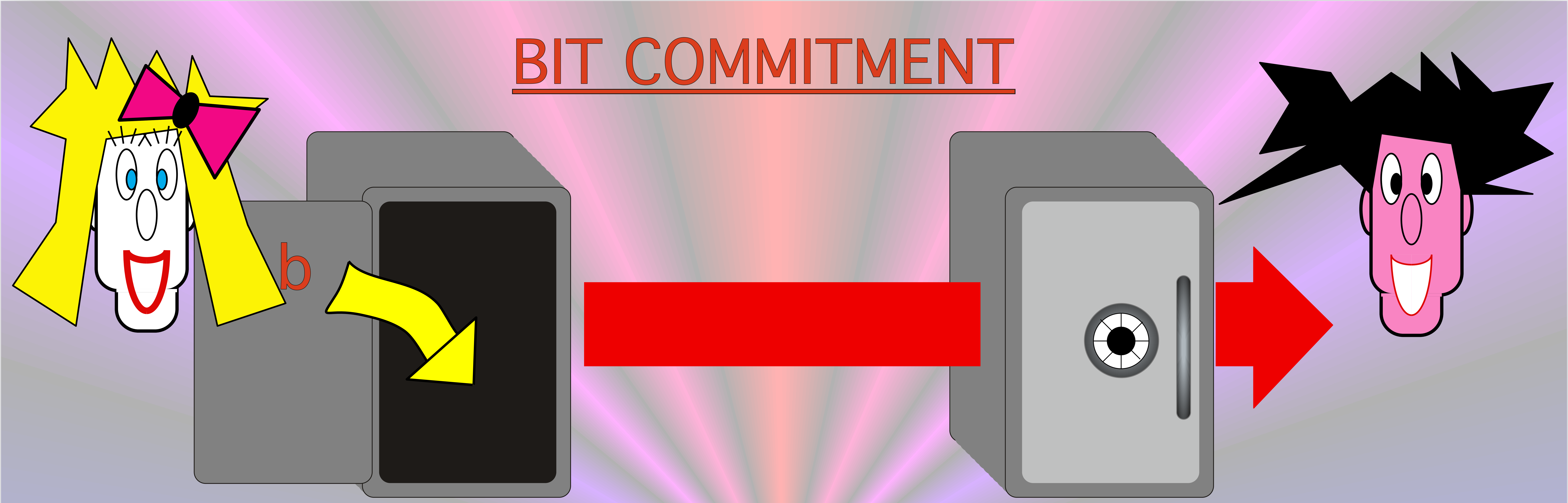


Auxiliary Input Zero-Knowledge

∀  ∃  ∀ω ∀x∈L view[, (ω)](x) = (ω,x)

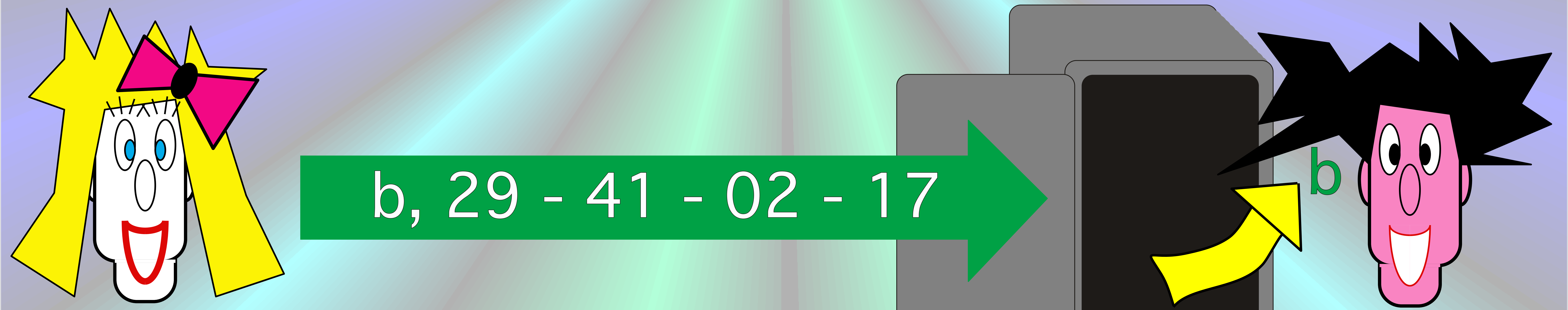
Bit Commitment

BIT COMMITMENT



COMMIT

UNVEIL



BIT COMMITMENT

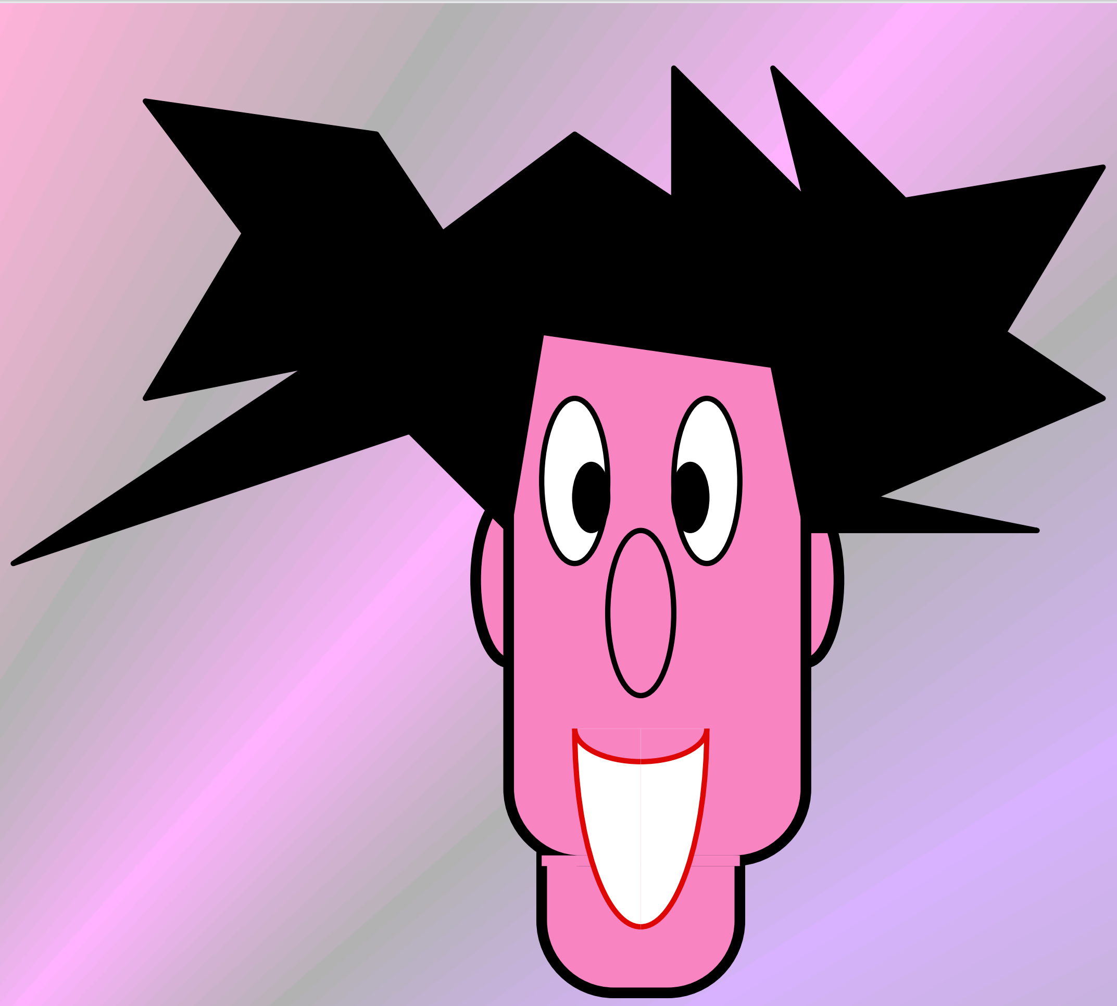
CONCEALING

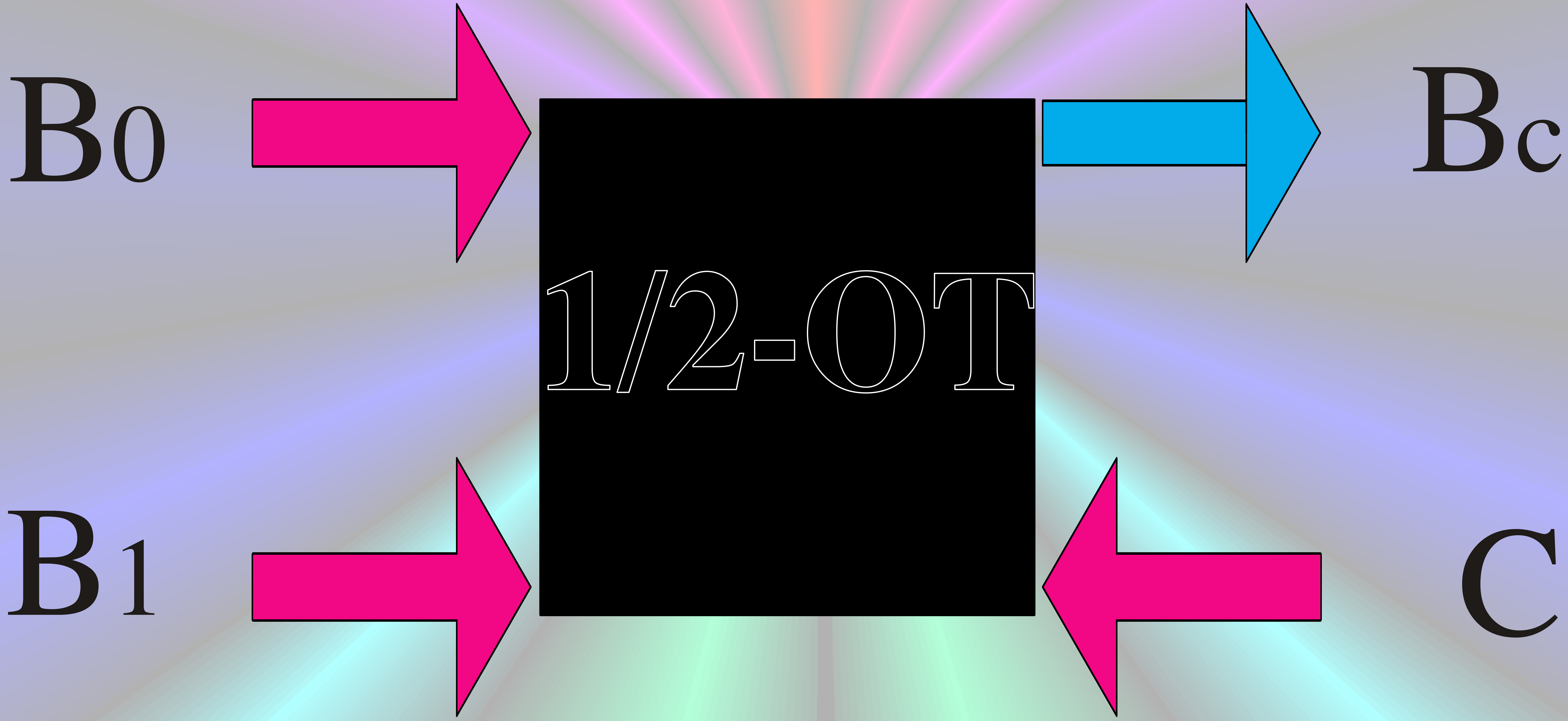
BINDING

¬b, 39 - 21 - 12 - 27
¬b

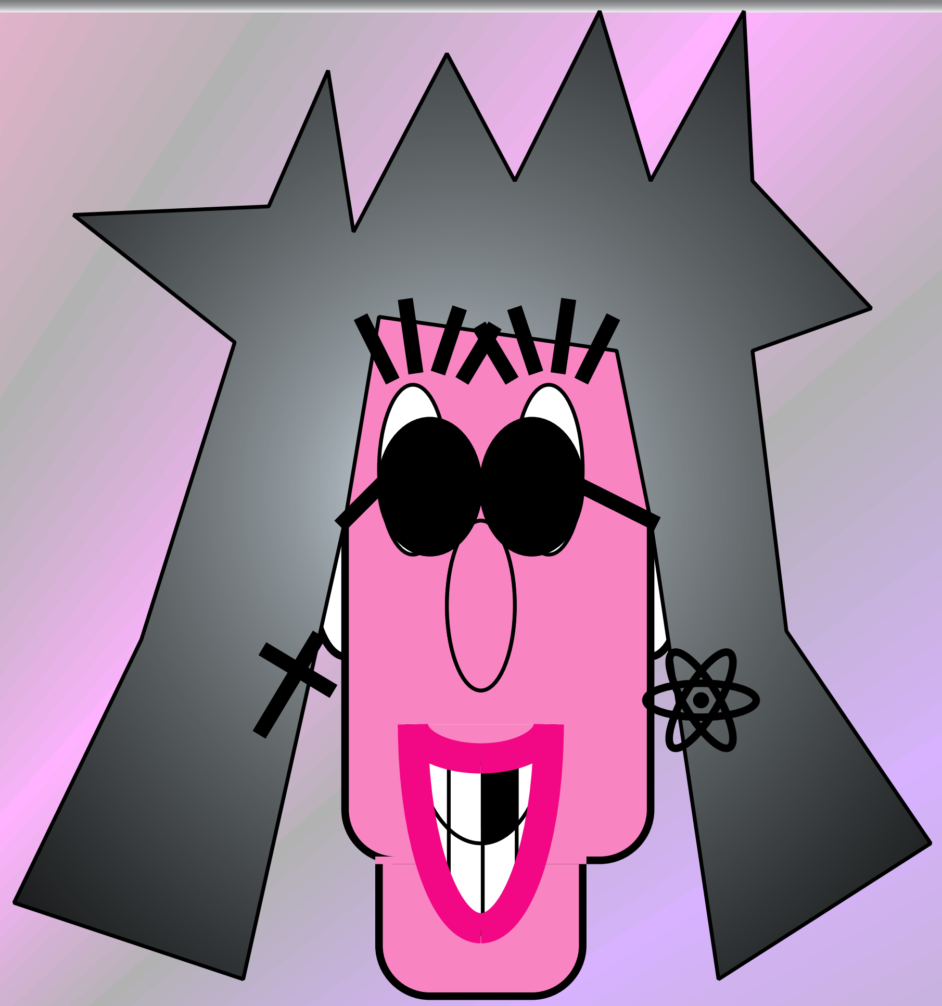
Oblivious Transfer

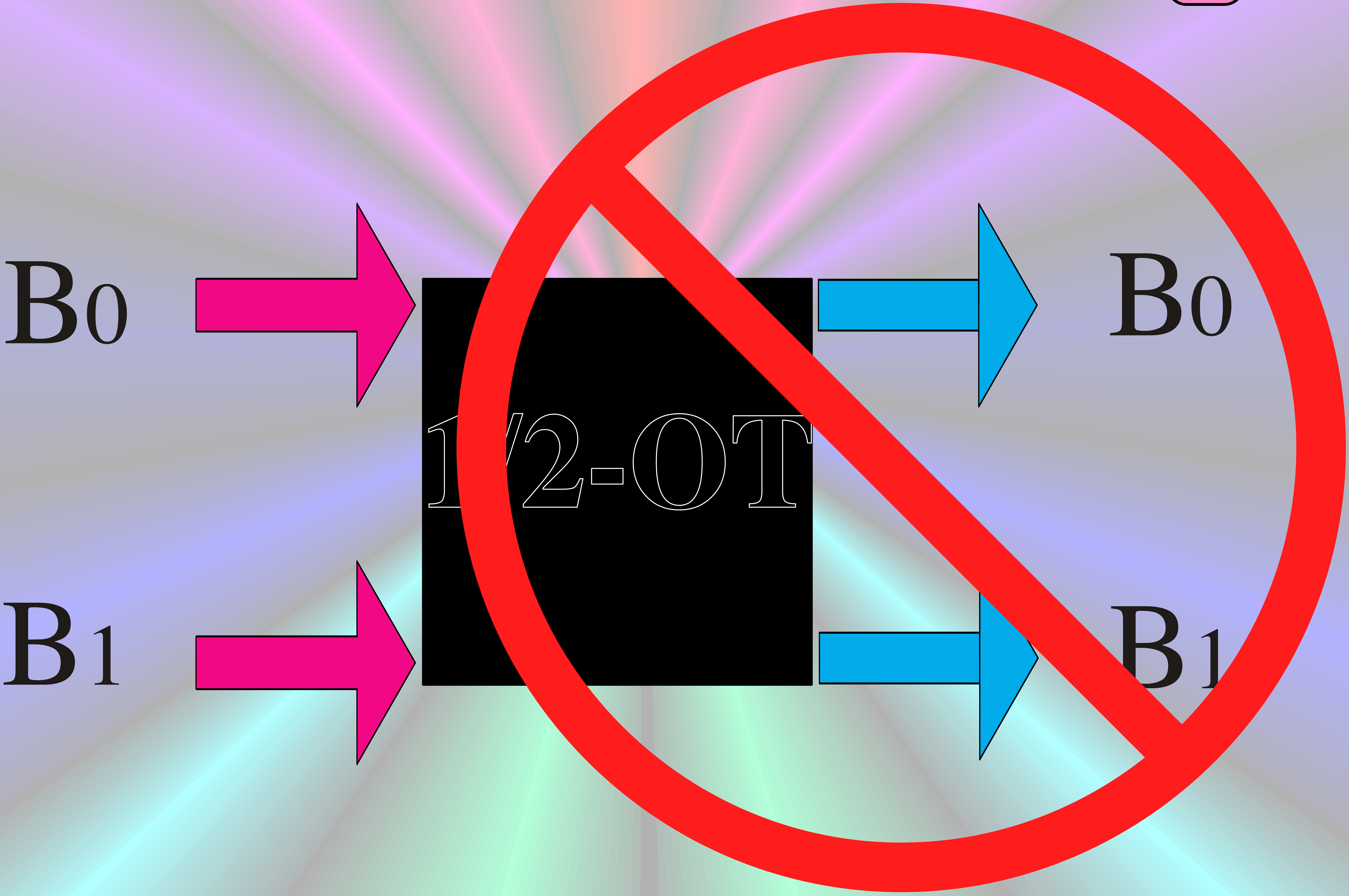
Oblivious Transfer



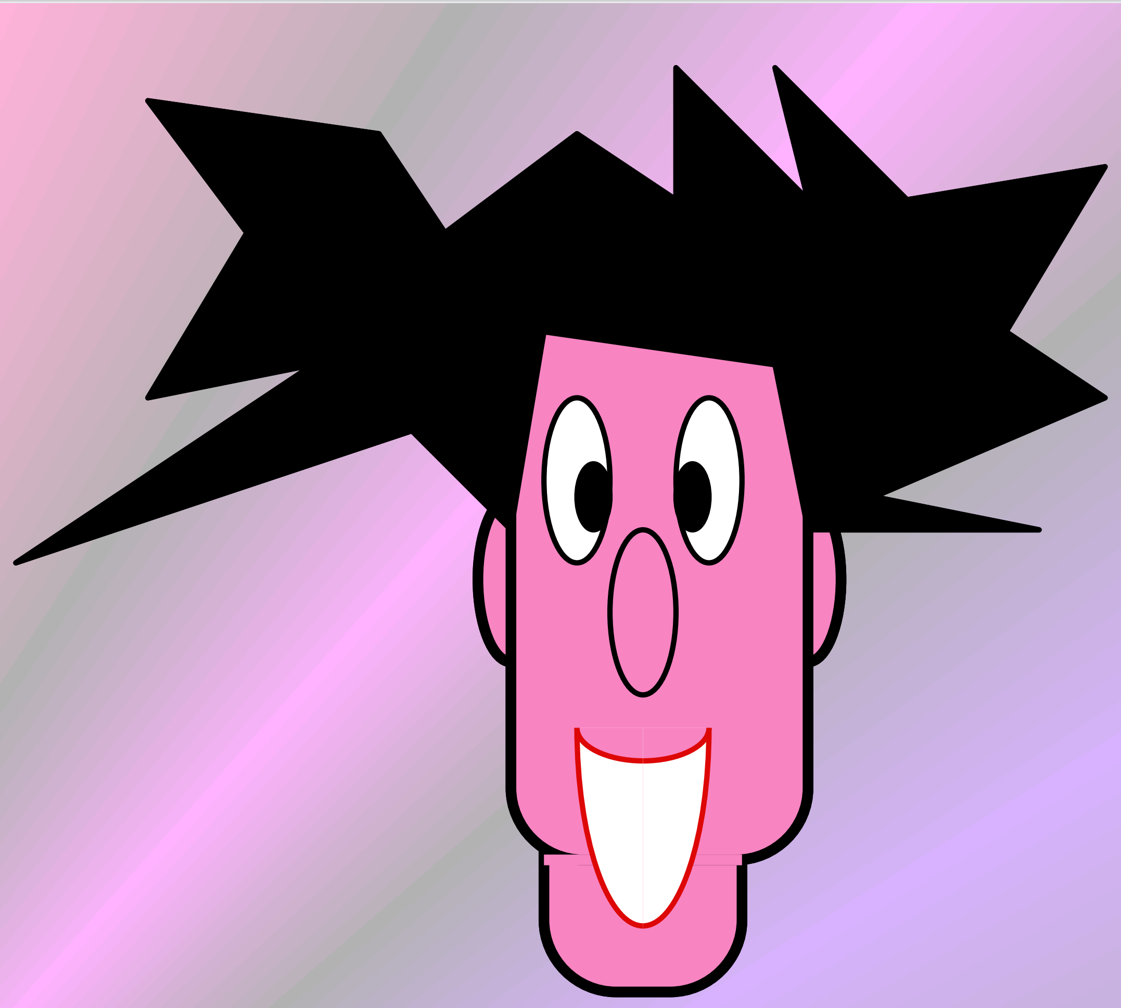


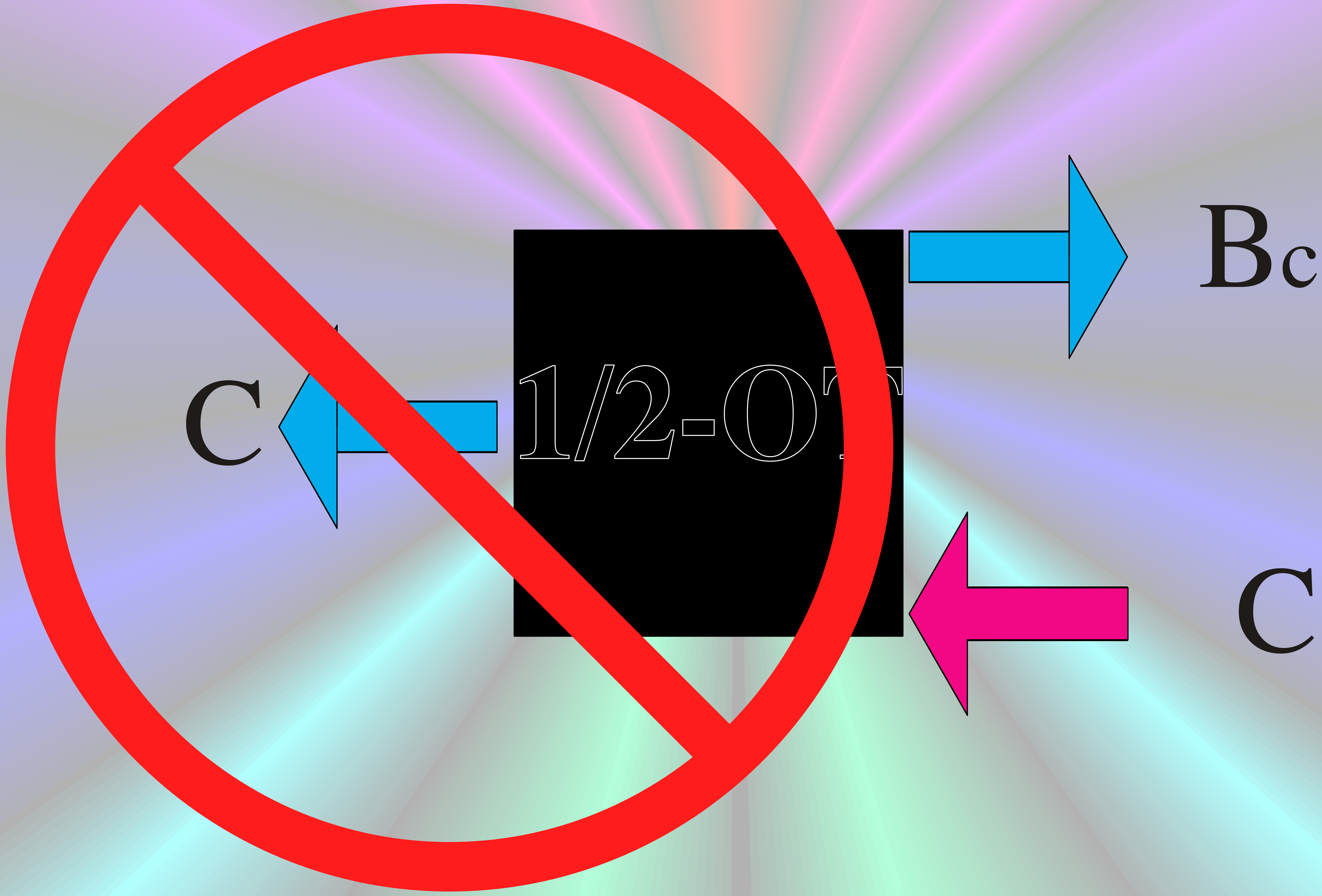
Oblivious Transfer





Oblivious Transfer



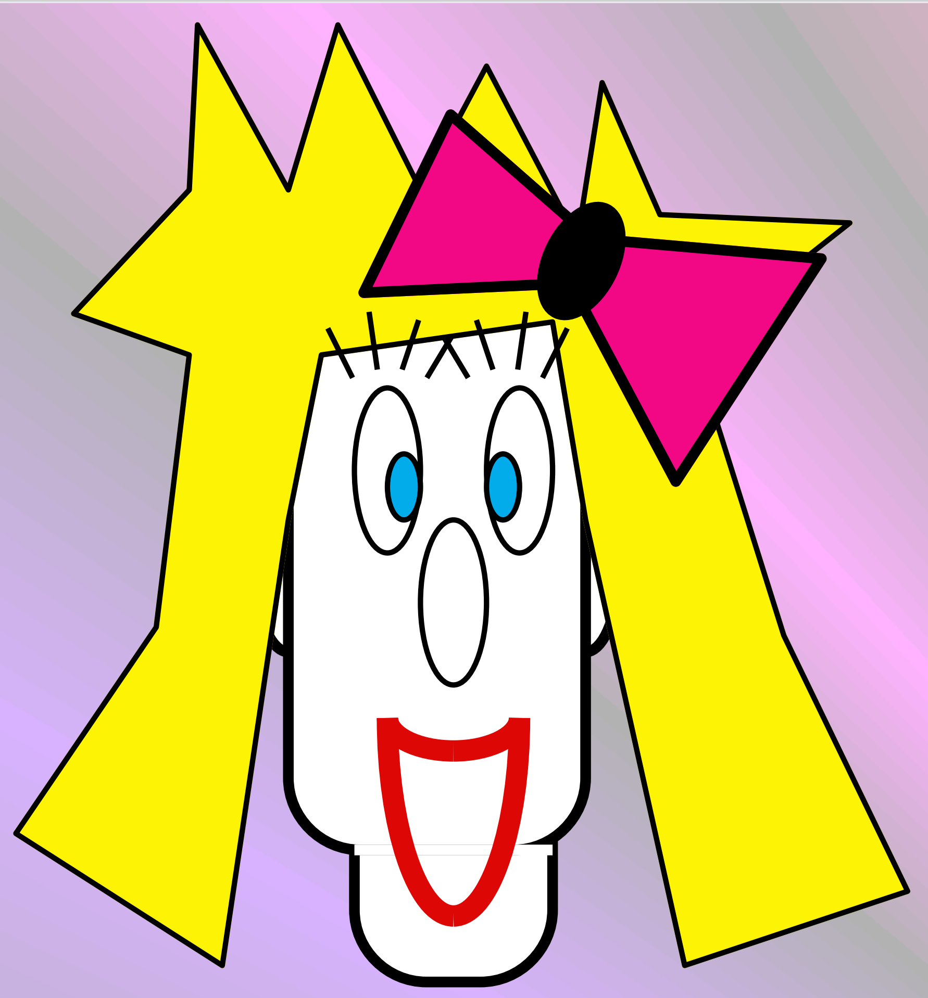


1/2-OT

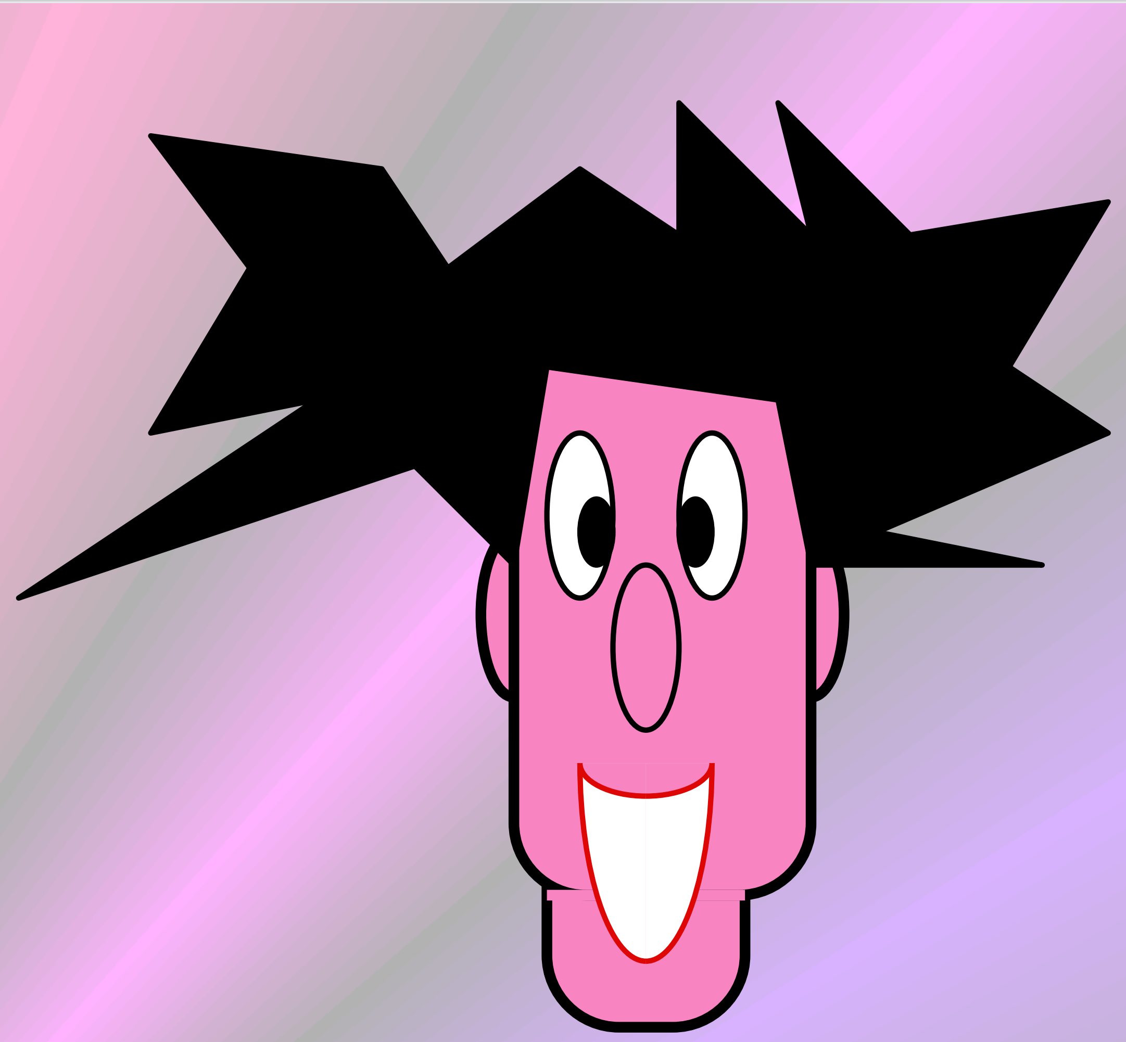
C

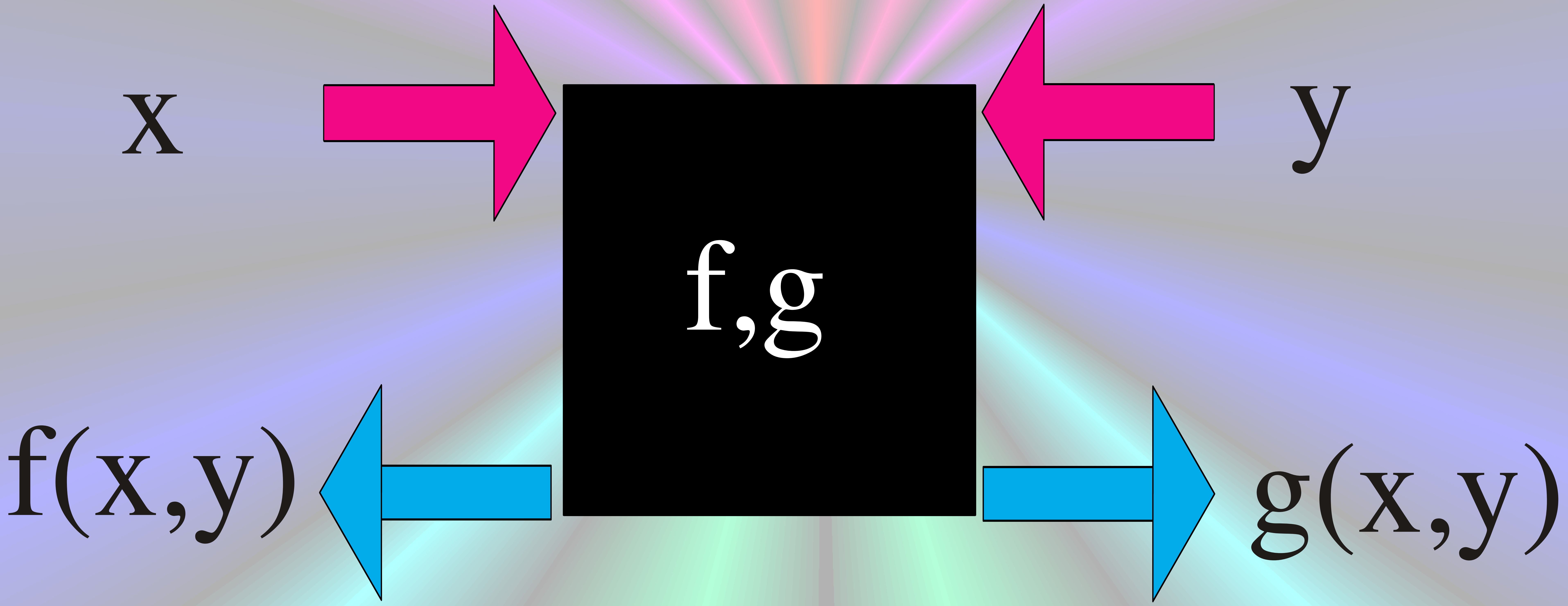
B_c

C

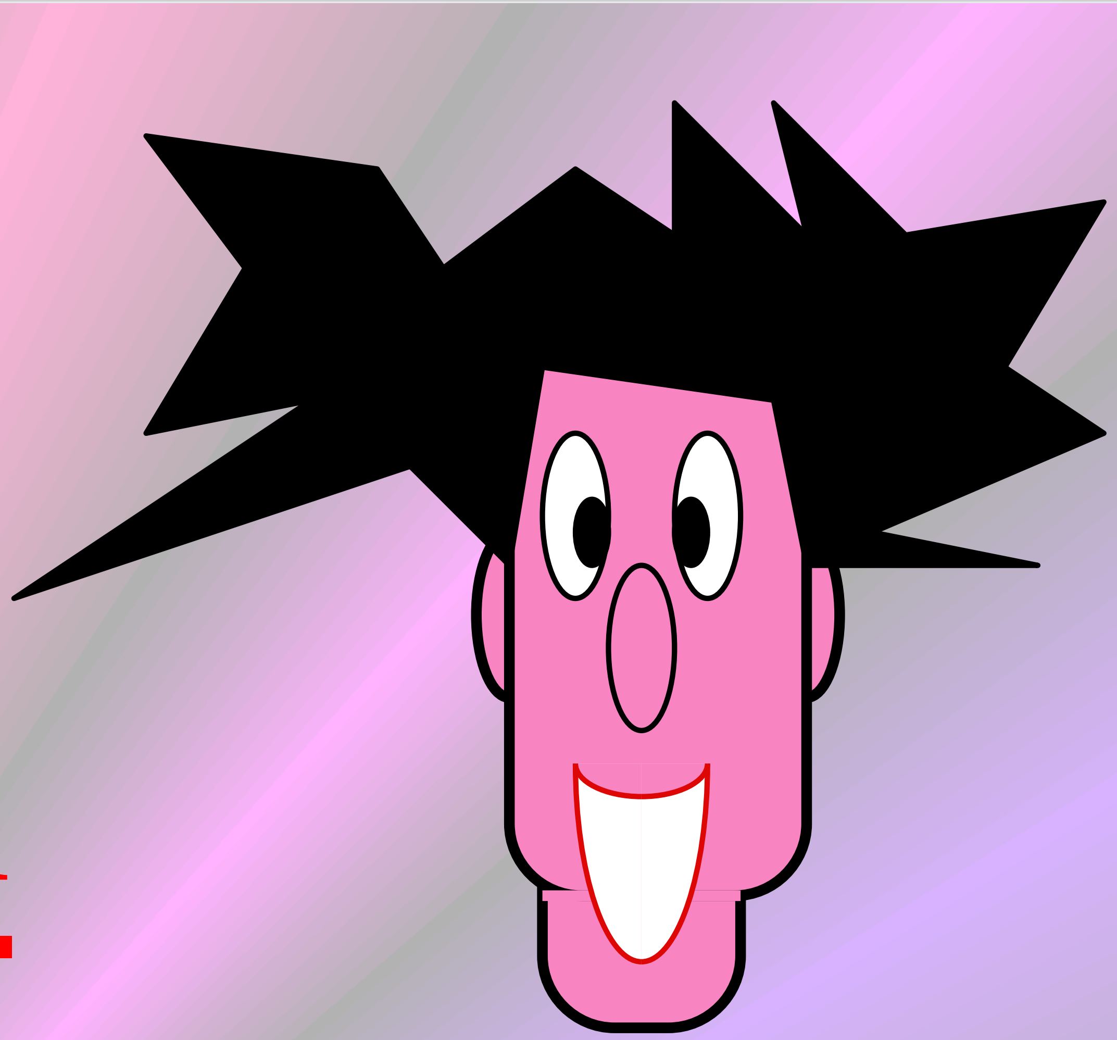


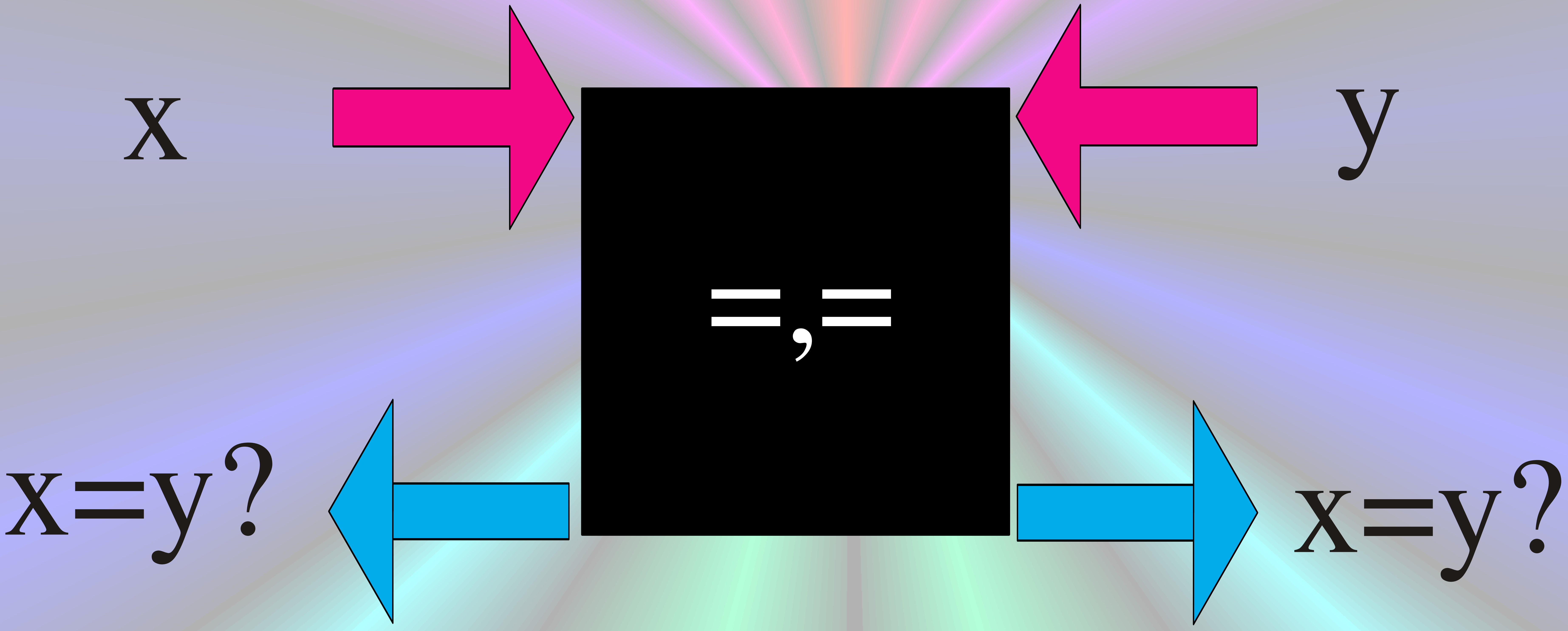
Oblivious Function Evaluation





Mutual Identification





x

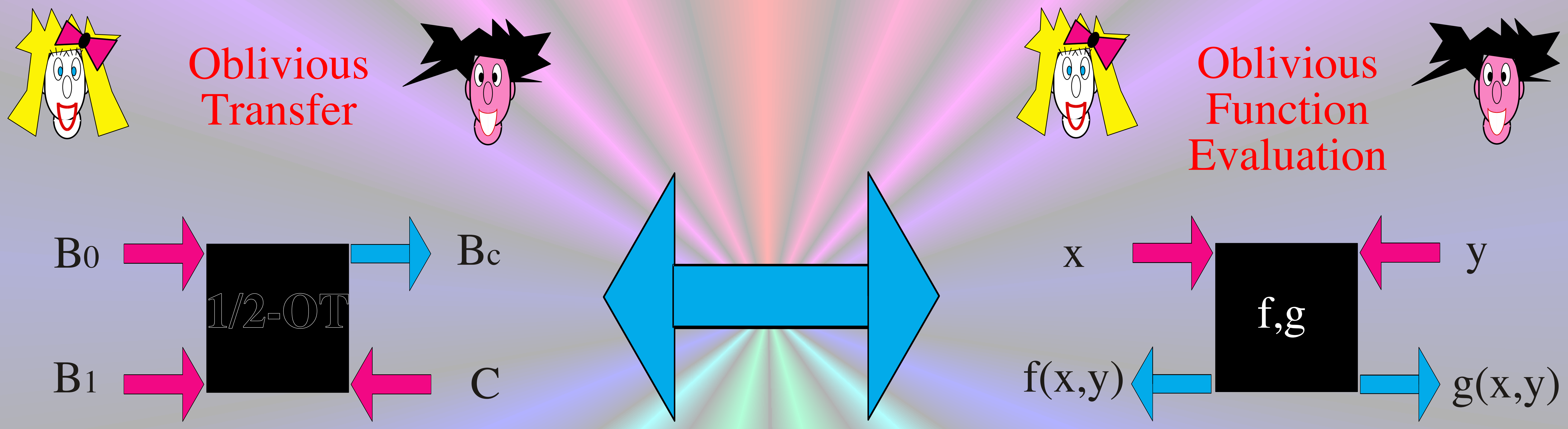
y

=,=

x=y?

x=y?

Cryptographic Reduction



Oblivious Transfer

B_0

B_1

1/2-OT

B_c

C

Oblivious Function Evaluation

x

y

f,g

f(x,y)

g(x,y)

Interactive Zero-Knowledge Proofs and other Two-Party Cryptographic Protocols

Claude Crépeau

School of Computer Science
McGill University