Quantum Zero-Knowledge

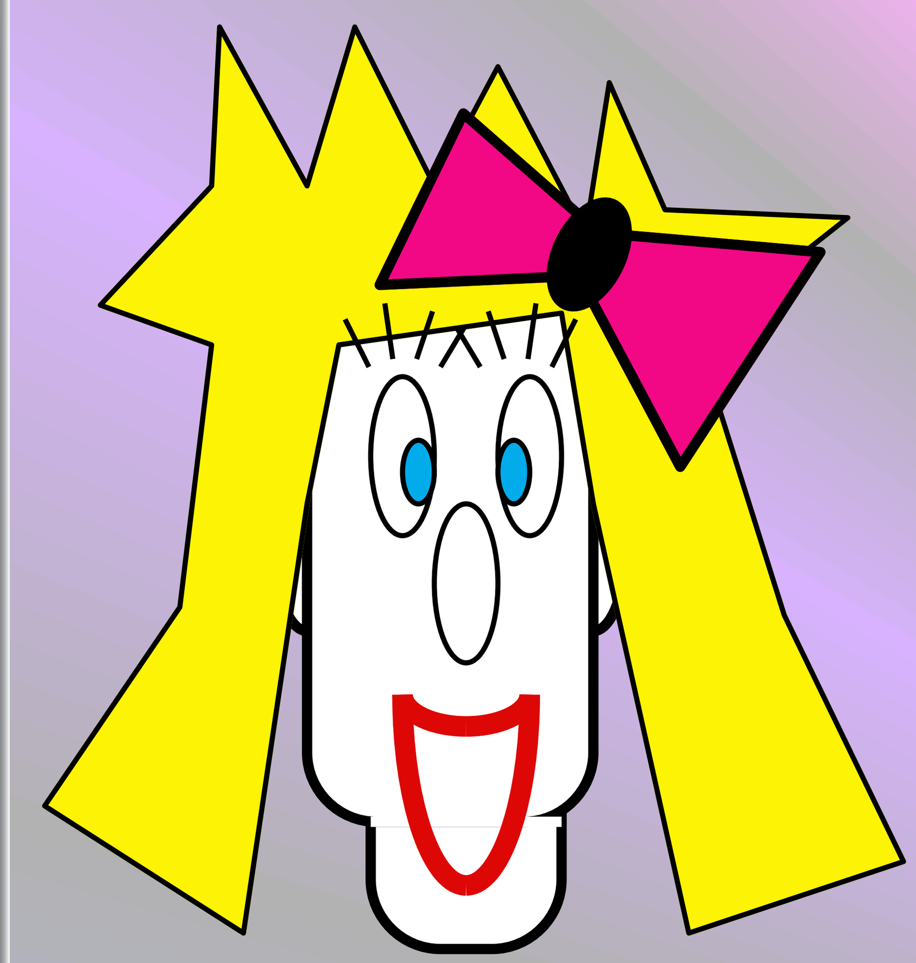
Claude Crépeau

School of Computer Science
McGill University

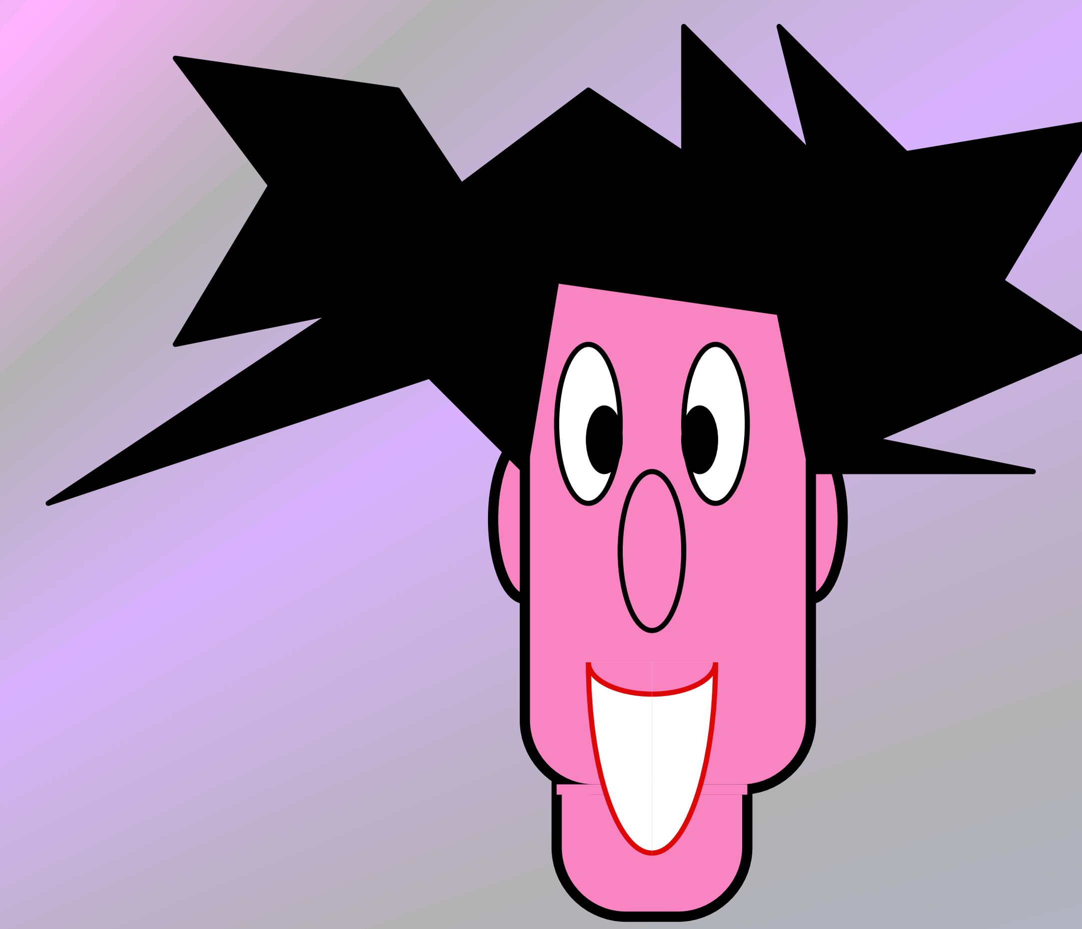
joint work with
J. van de Graaf and A. Smith

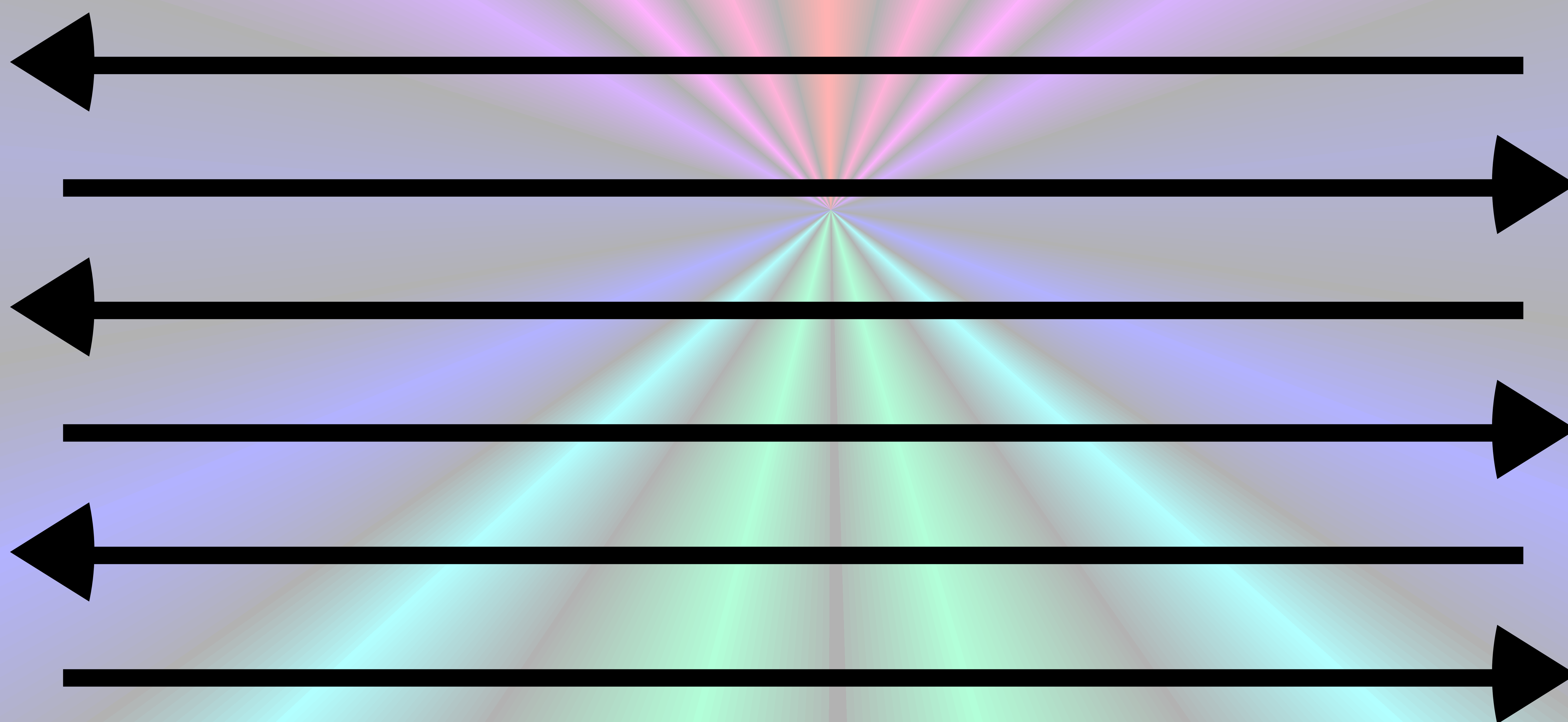
Interactive Proofs

Interactive Proofs and Zero-Knowledge

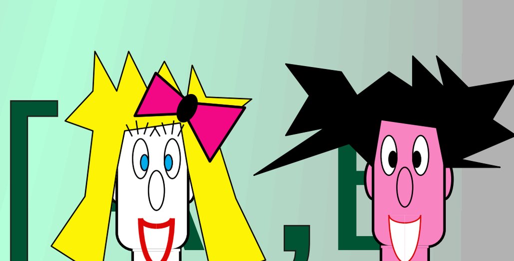


$x \in L$





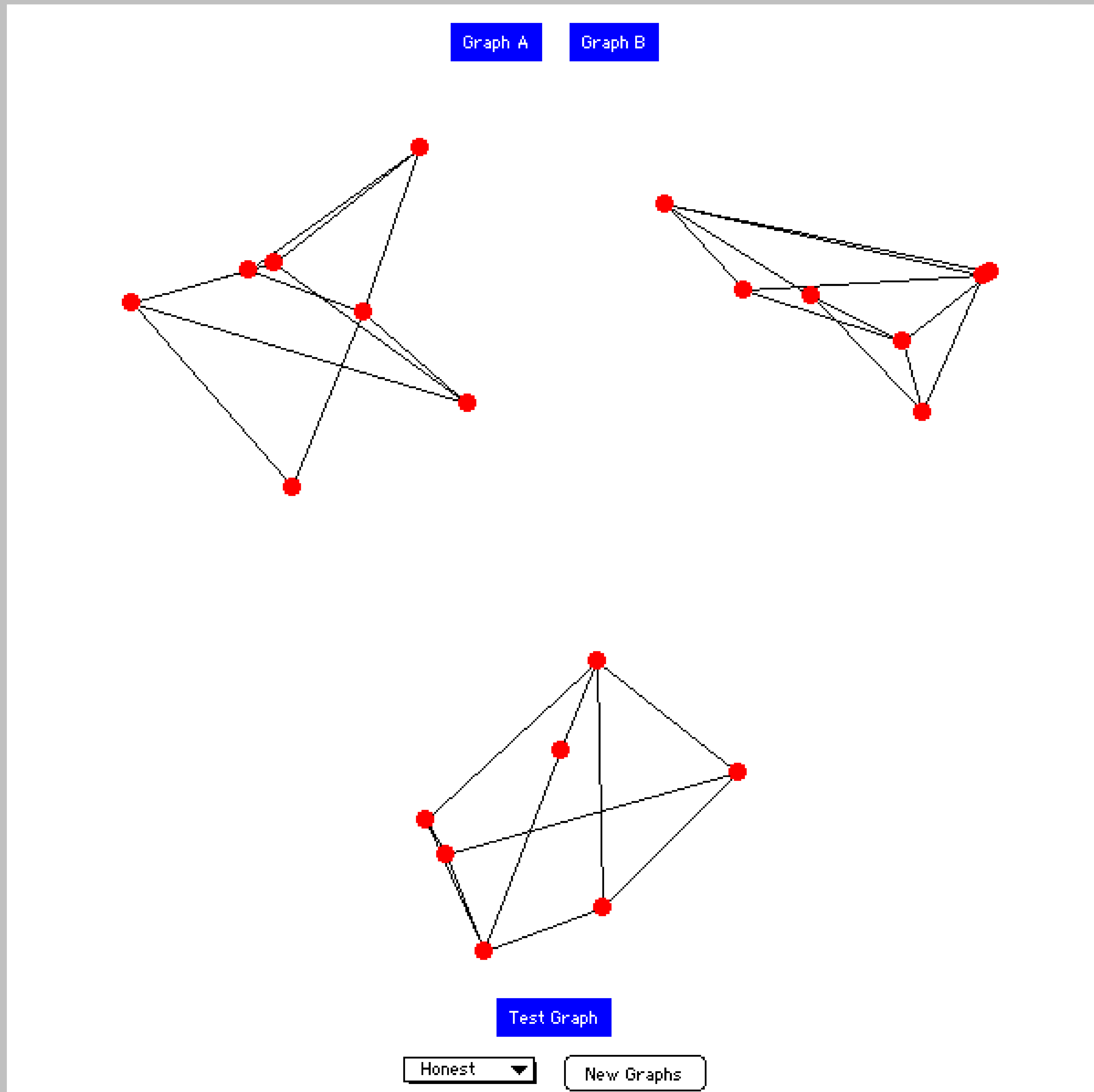
YES !

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

Location: http://www.IRO.UMontreal.ca/~marcilj/InteractiveProof/ What's Related

- You will accept that the two graphs are isomorphic if the Test Graph was always isomorphic to the chosen graph.

Let's try it!



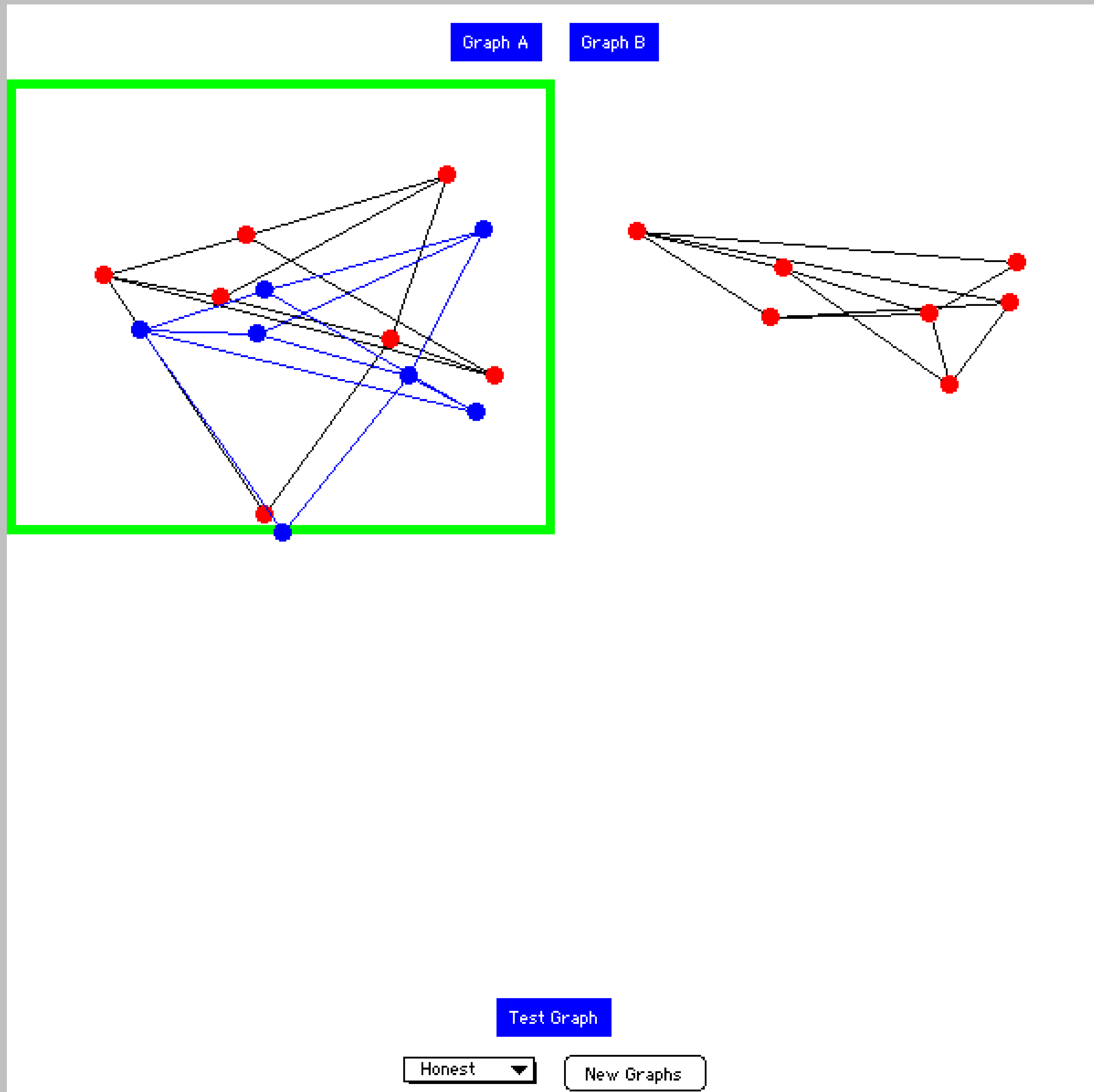
Note : you can redraw a graph by Ctrl-clicking on it

Text taken from Cryptography, Theory and practice.

Location: http://www.IRO.UMontreal.ca/~marcilj/InteractiveProof/ What's Related

- You will accept that the two graphs are isomorphic if the Test Graph was always isomorphic to the chosen graph.

Let's try it!



Note : you can redraw a graph by Ctrl-clicking on it

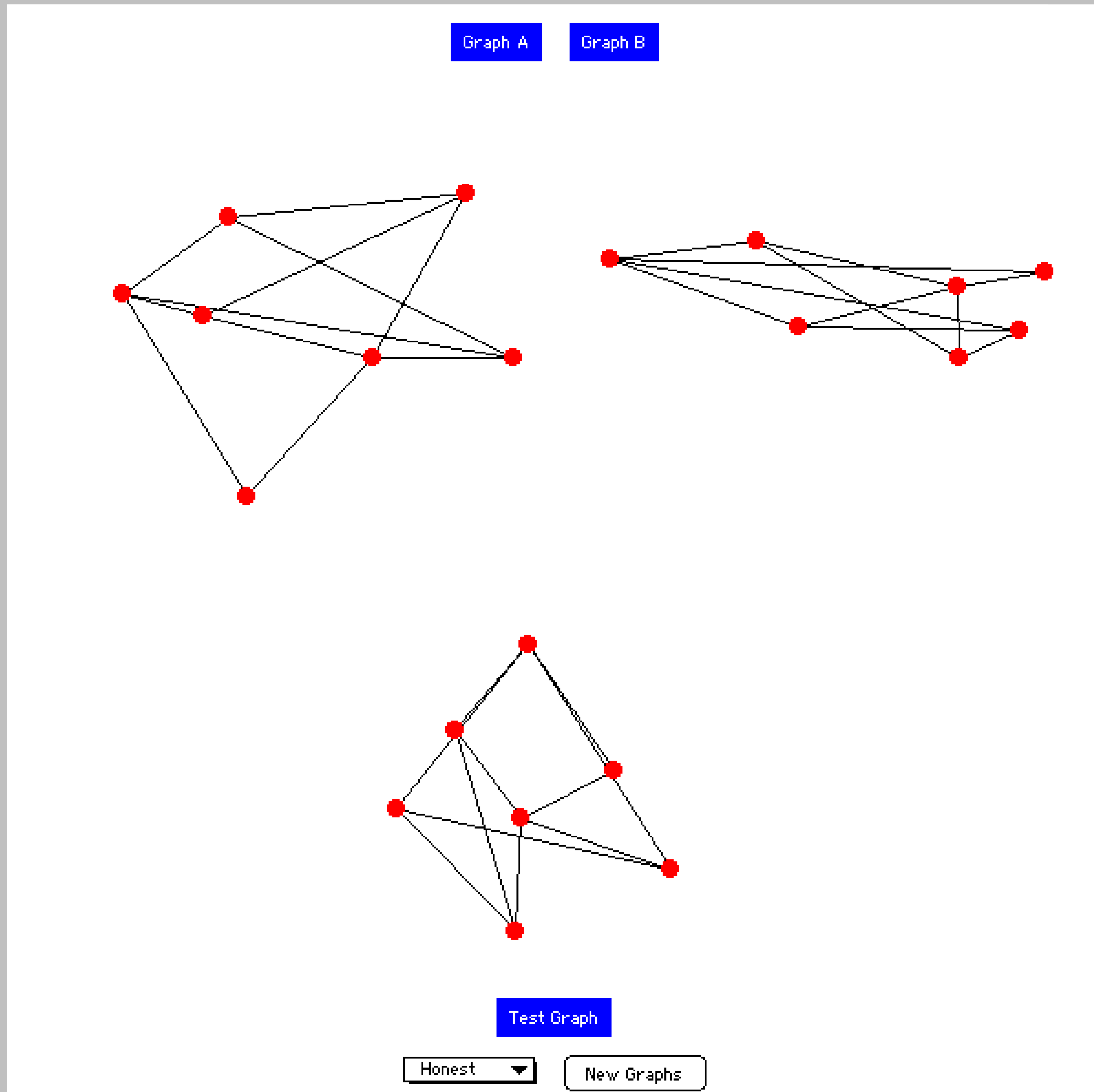
Text taken from Cryptography, Theory and practice.

Applet InteractiveProof running

Location : http://www.IRO.UMontreal.ca/~marcilj/InteractiveProof/ What's Related

- You will accept that the two graphs are isomorphic if the Test Graph was always isomorphic to the chosen graph.

Let's try it!



Note : you can redraw a graph by Ctrl-clicking on it

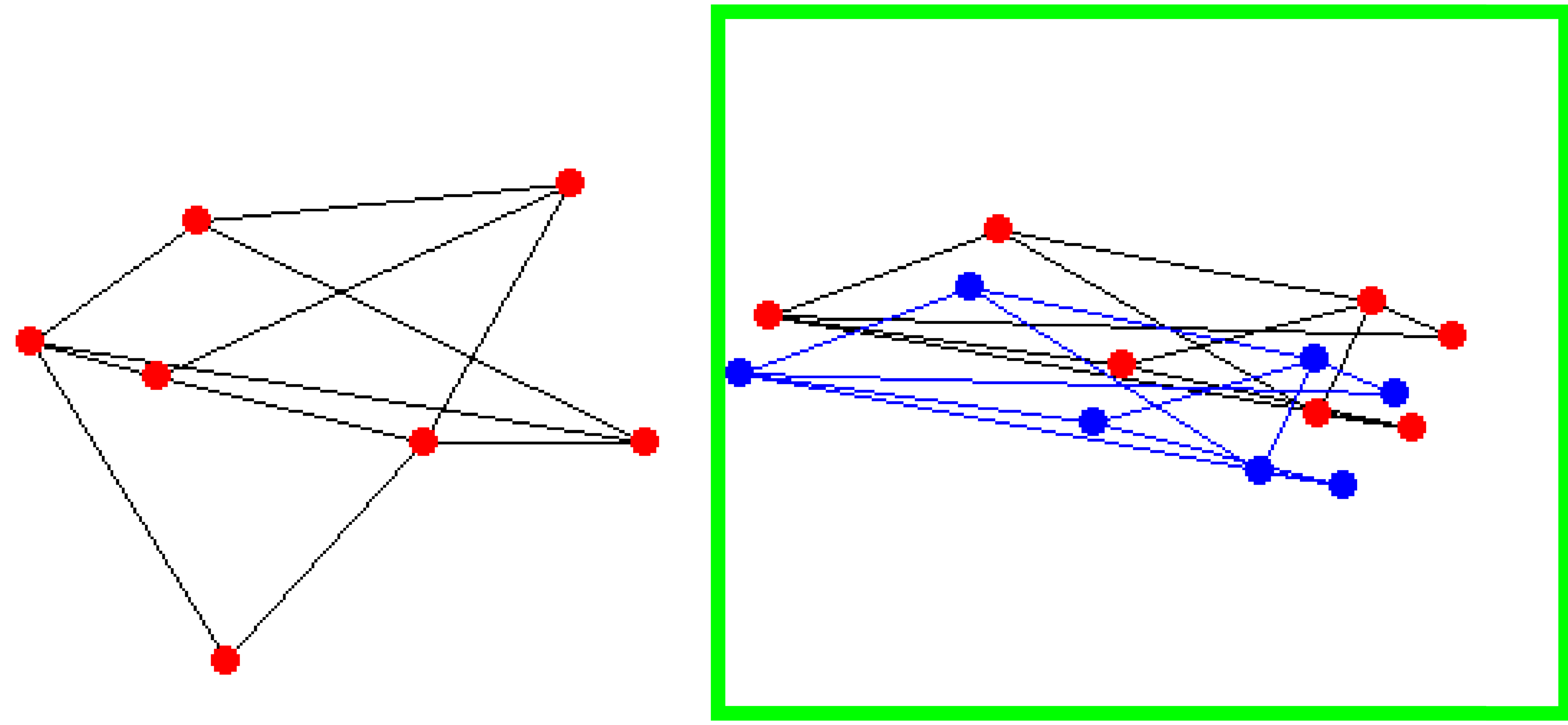
Text taken from Cryptography, Theory and practice.

Location: http://www.IRO.UMontreal.ca/~marcilj/InteractiveProof/ What's Related

- You will accept that the two graphs are isomorphic if the Test Graph was always isomorphic to the chosen graph.

Let's try it!

Graph A Graph B



Test Graph

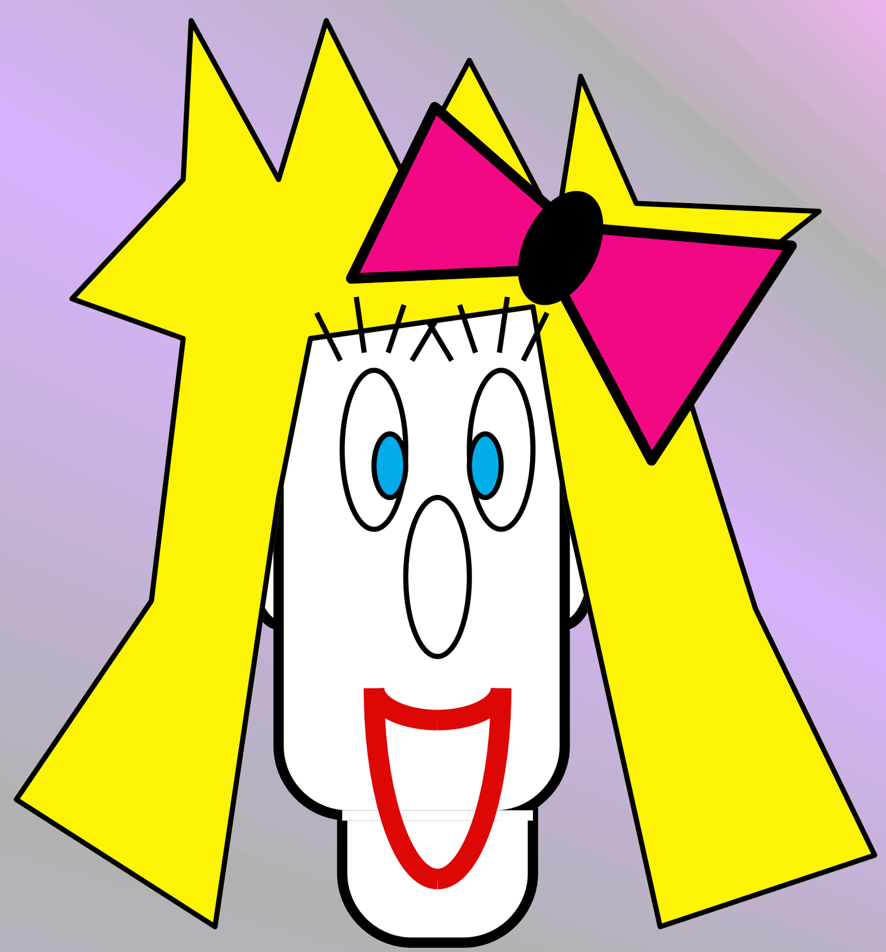
Honest New Graphs

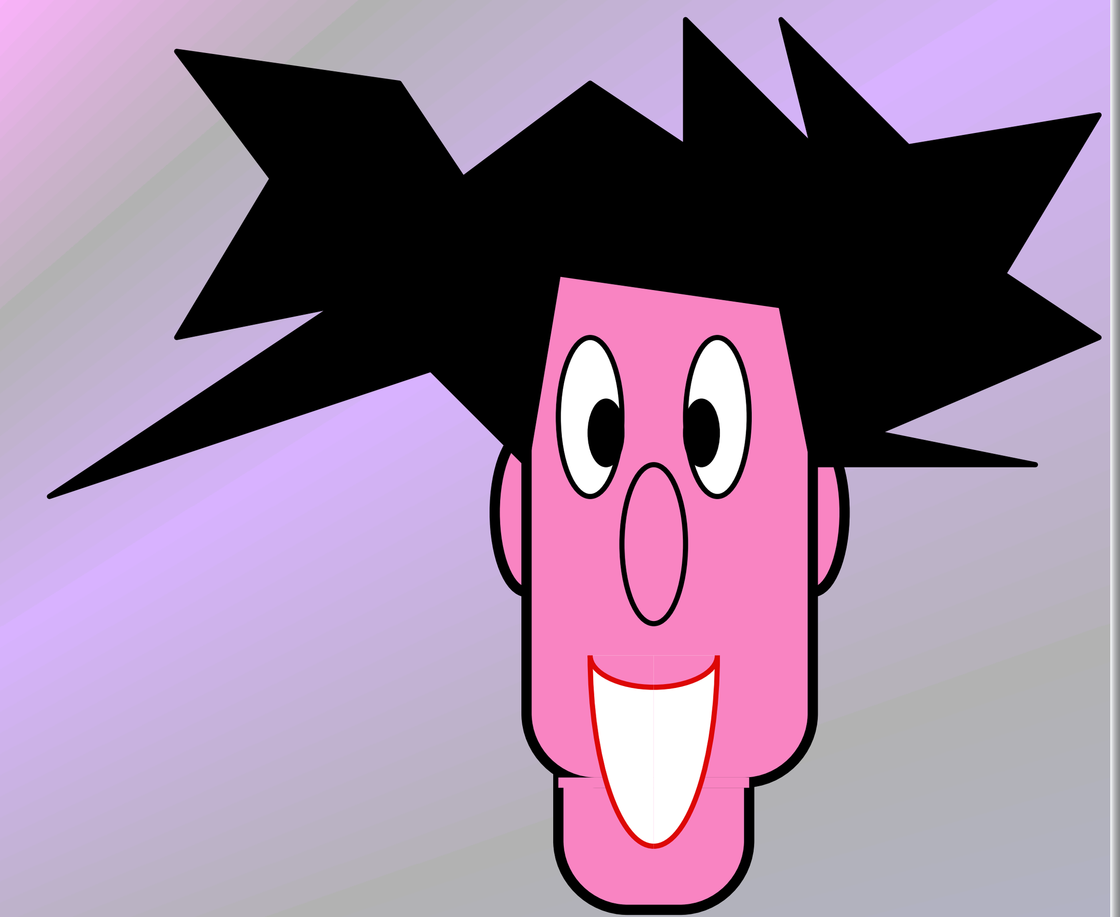
Note : you can redraw a graph by Ctrl-clicking on it

Text taken from Cryptography, Theory and practice.

Applet InteractiveProof running

Interactive Proofs and Zero-Knowledge





$(G_0, G_1) \in ISO$

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

$G := \pi_0(G_0)$

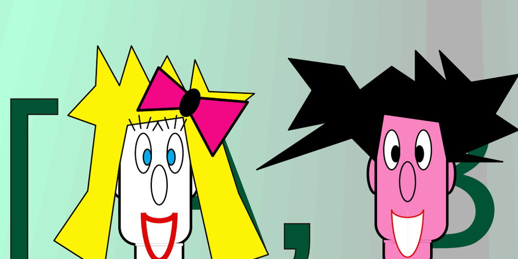
$\xrightarrow{\;G\;}$

$\xleftarrow{\;c\;}$

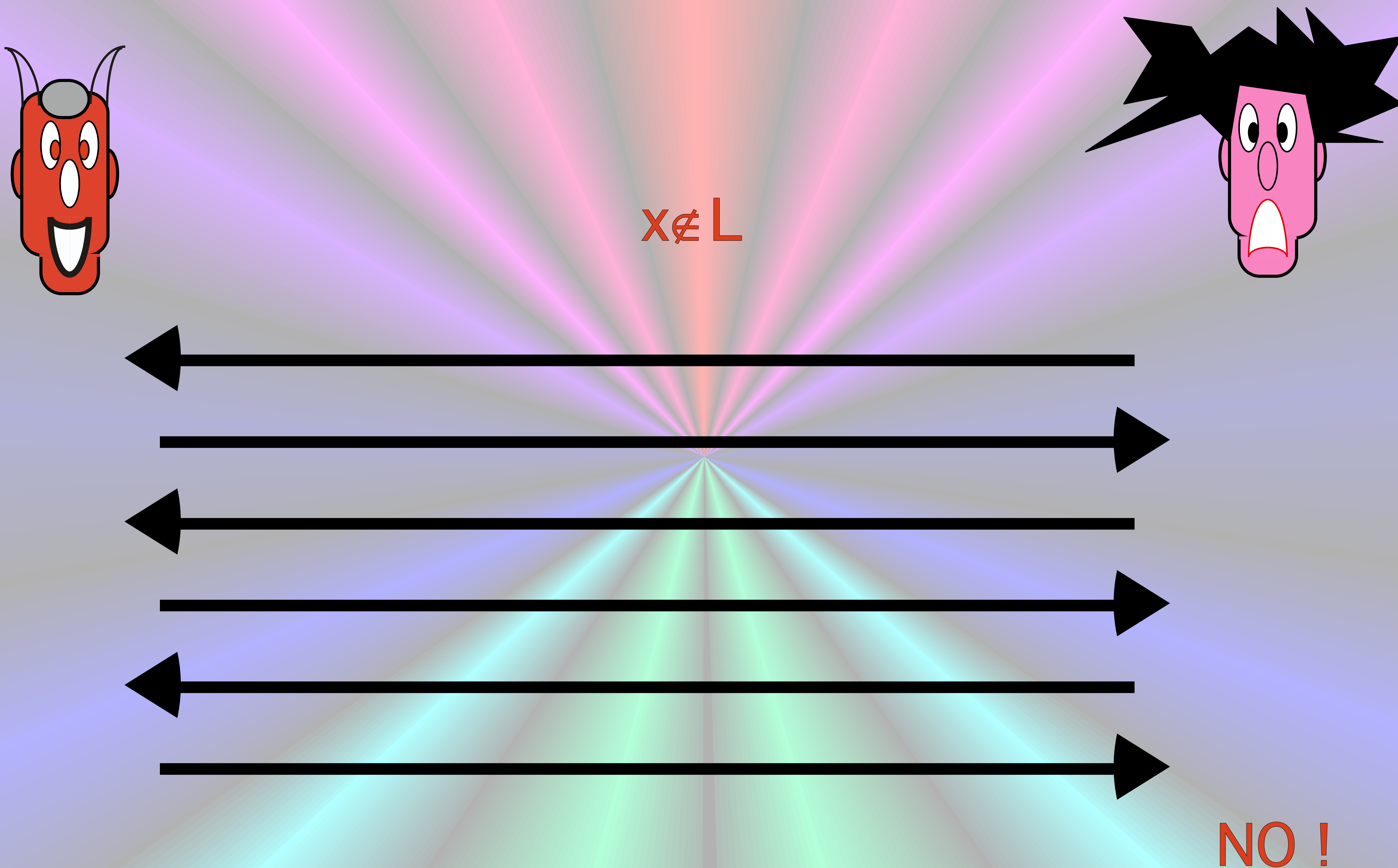
$\xrightarrow{\;\rho = \pi_0 \circ \pi^c\;}$

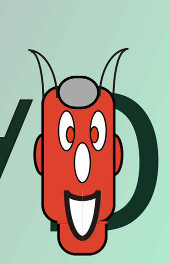
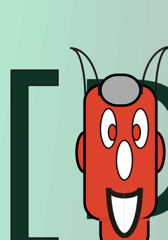
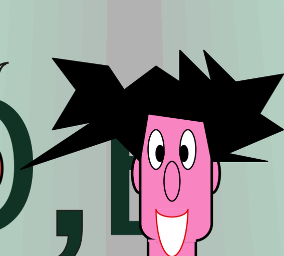
$G = \rho(G_c)$?

YES !

$\forall x \in L \ \Pr($ [](x)=YES $) = 1$

Interactive Proofs and Zero-Knowledge

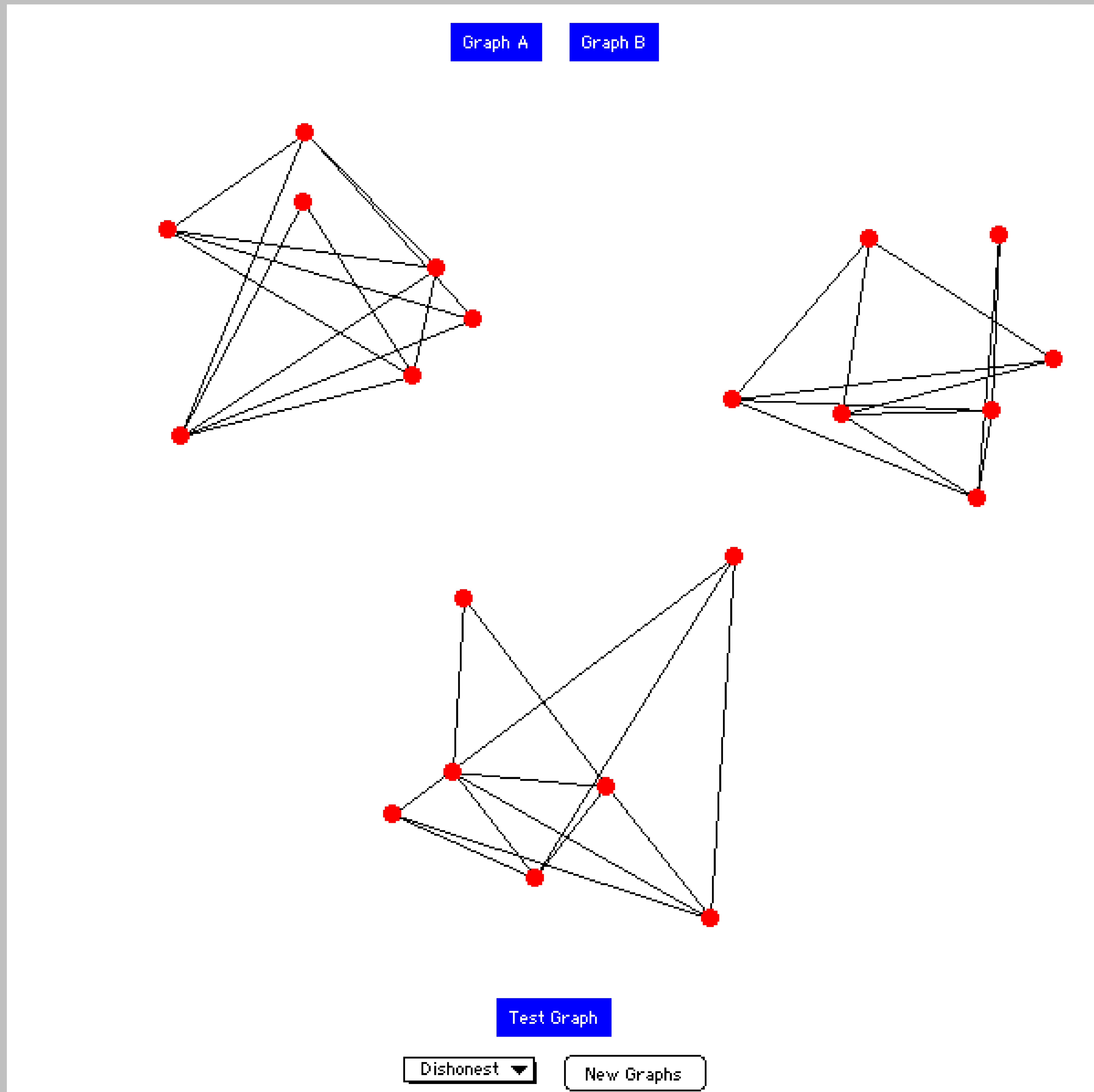


∀x∉L ∀ Pr([,](x)=YES) ≈ 0

Location: http://www.IRO.UMontreal.ca/~marcilj/InteractiveProof/ What's Related

- You will accept that the two graphs are isomorphic if the Test Graph was always isomorphic to the chosen graph.

Let's try it!



Note : you can redraw a graph by Ctrl-clicking on it

Text taken from Cryptography, Theory and practice.

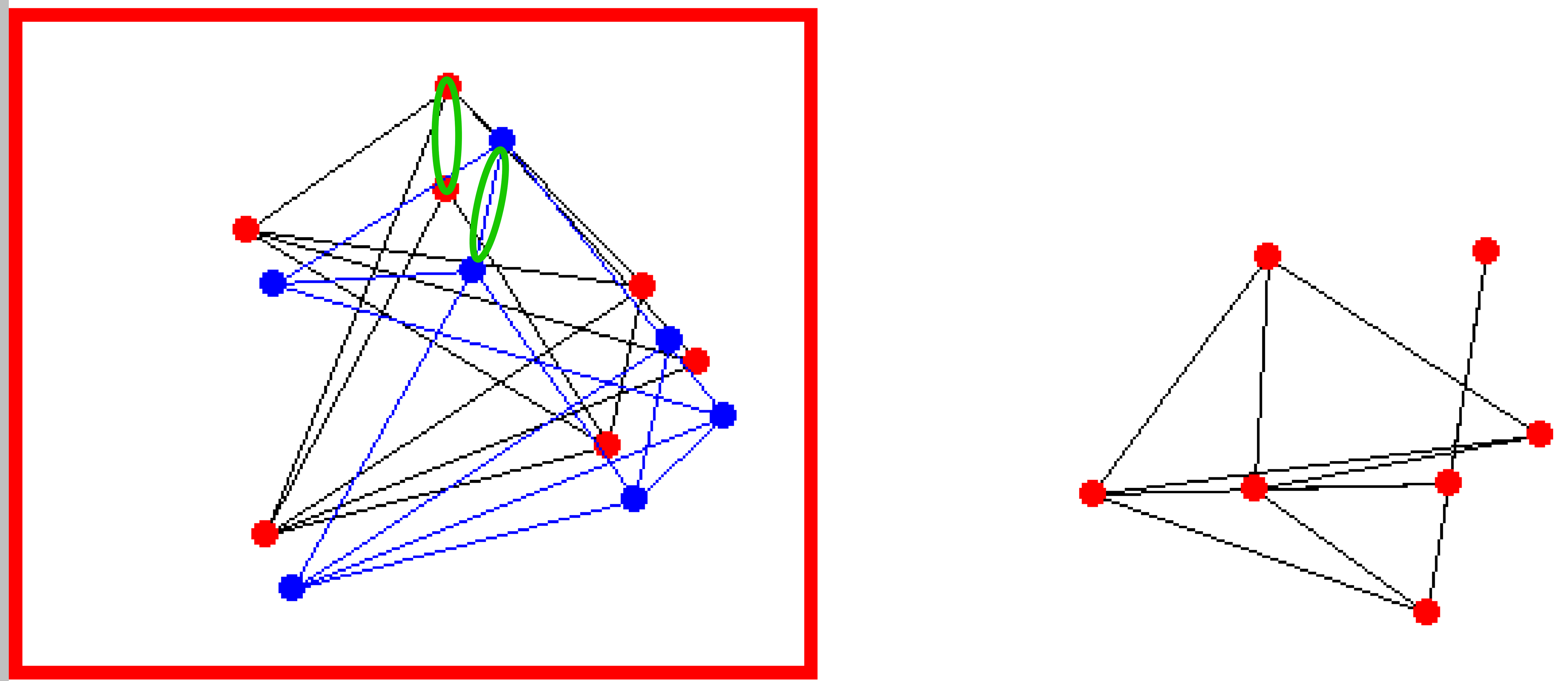
Applet InteractiveProof running

Location: http://www.IRO.UMontreal.ca/~marcilj/InteractiveProof/ What's Related

- You will accept that the two graphs are isomorphic if the Test Graph was always isomorphic to the chosen graph.

Let's try it!

Graph A Graph B



Test Graph

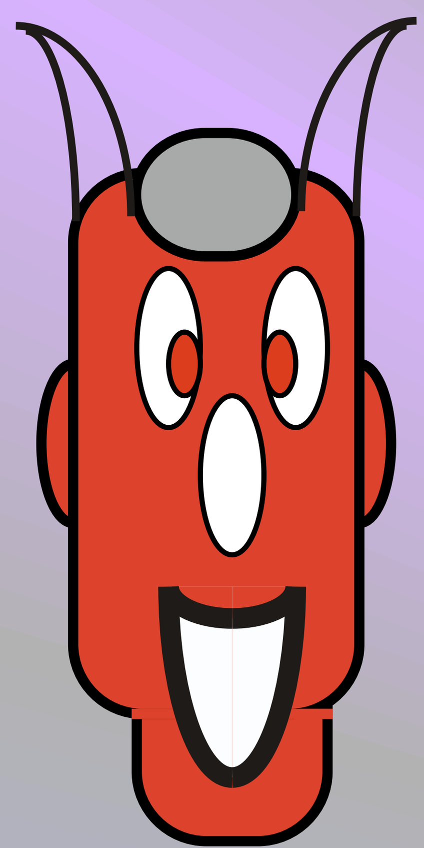
Dishonest New Graphs

Note : you can redraw a graph by Ctrl-clicking on it

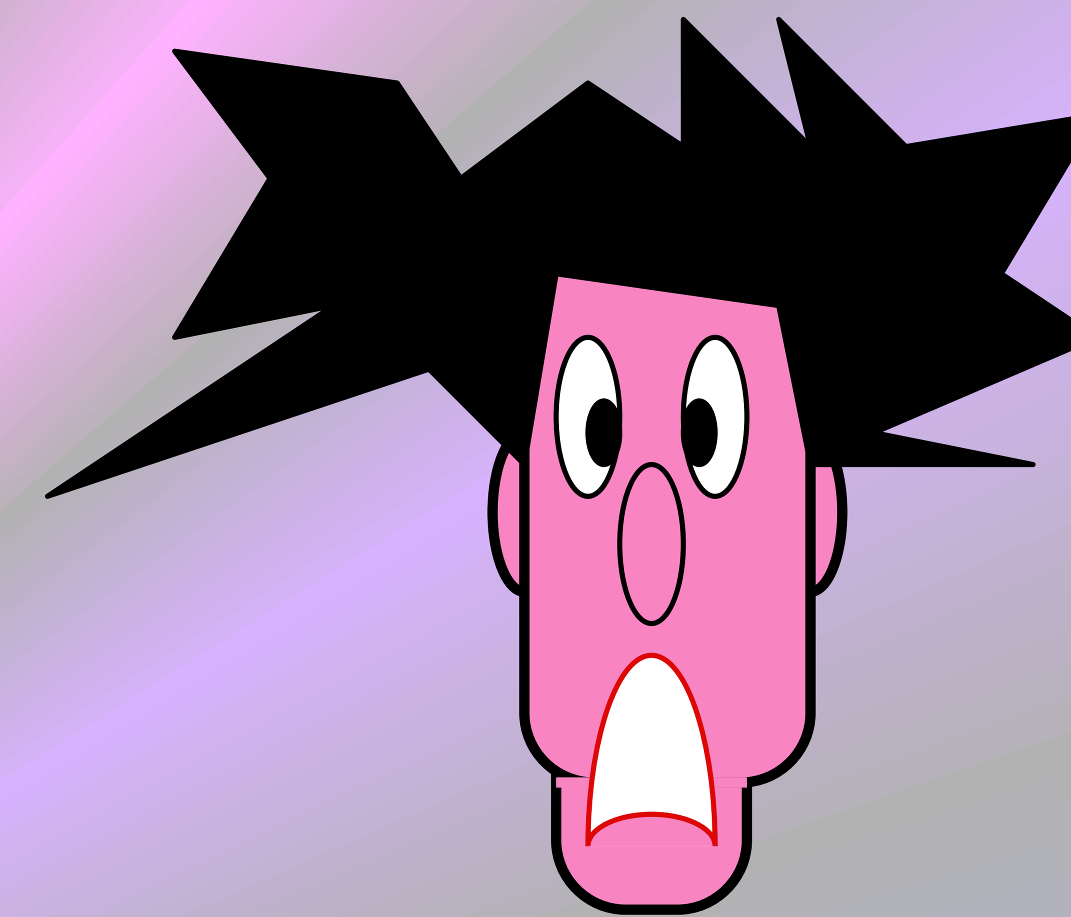
Text taken from Cryptography, Theory and practice.

Applet InteractiveProof running

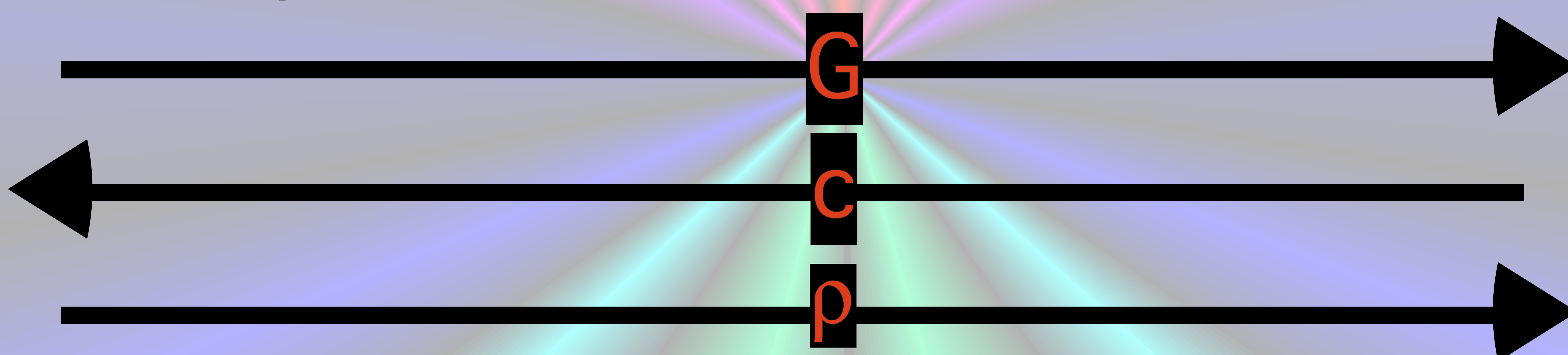
Interactive Proofs and Zero-Knowledge



$(G_0,G_1)\notin ISO$



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

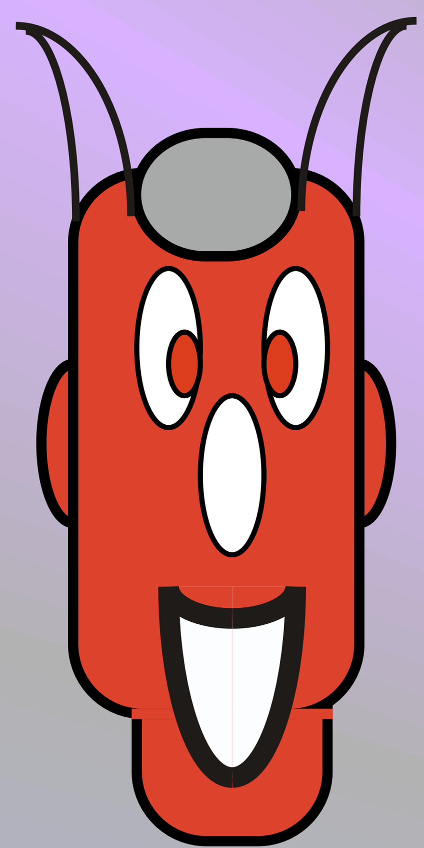


$G = \rho(G_c)$?

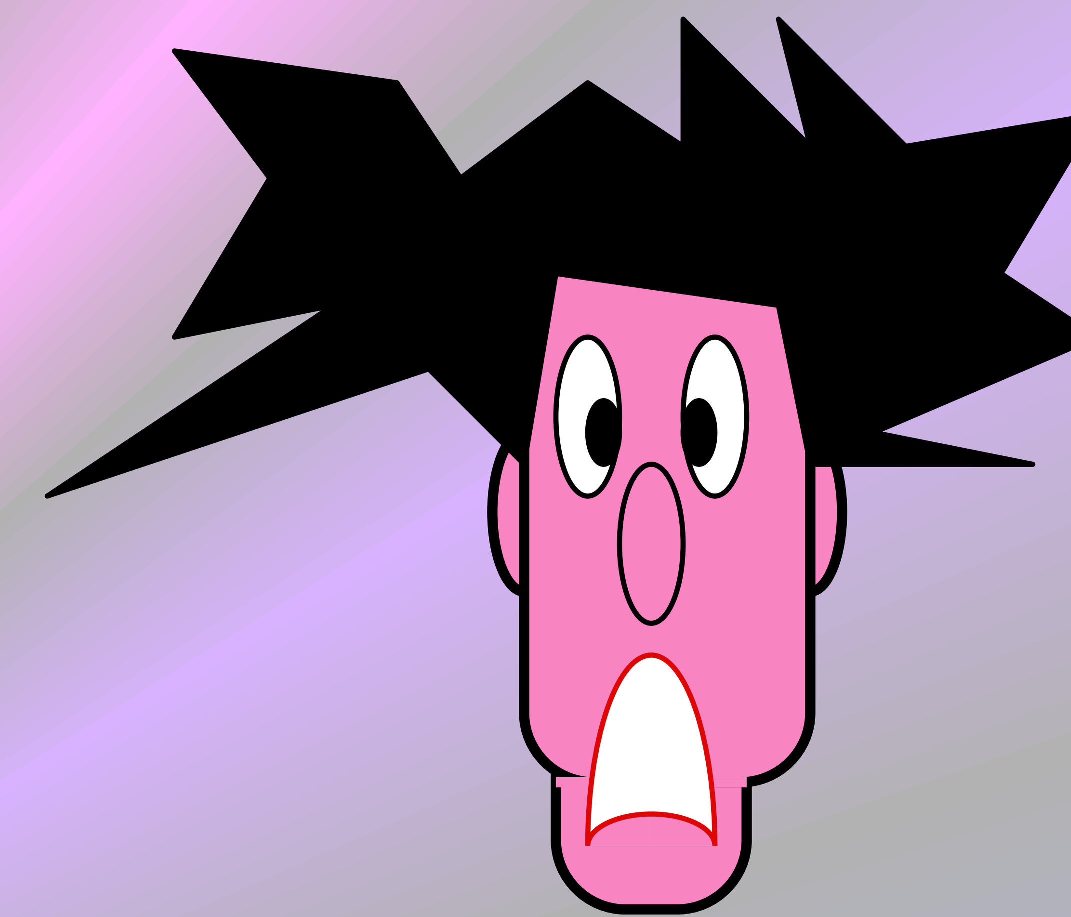
NO !

$\forall x\notin L\ \forall\ \Pr(\ [\ ,\ ](x)=YES\ ) \le {}^1/_2$

Interactive Proofs and Zero-Knowledge



$(G_0,G_1)\notin ISO$



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

$\xrightarrow{\quad G \quad}$

$\xleftarrow{\quad c \quad}$

$\xrightarrow{\quad \rho \quad}$

$G = \rho(G_c)$?

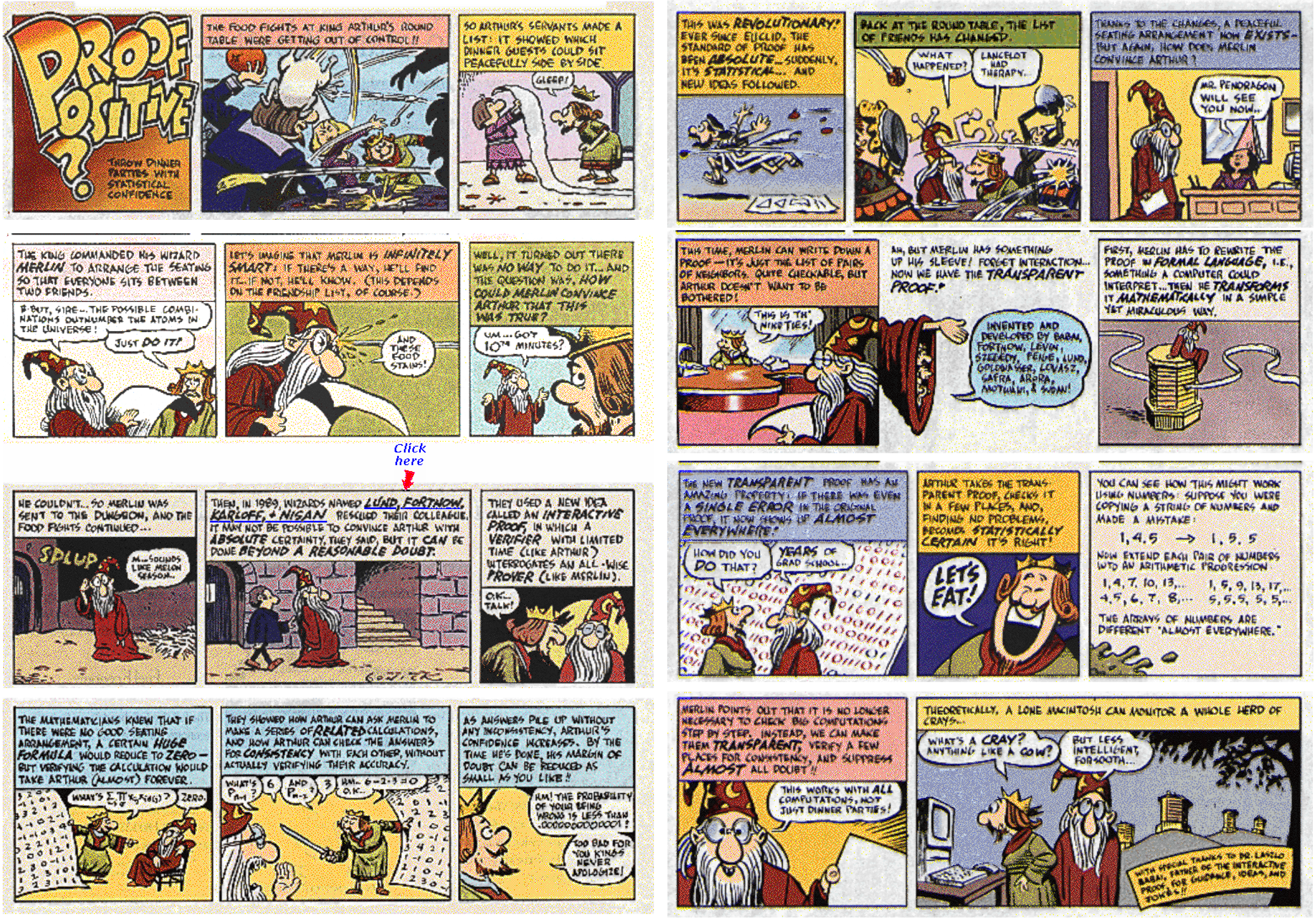
REPEAT k TIMES

and say "YES" only if all "YES"

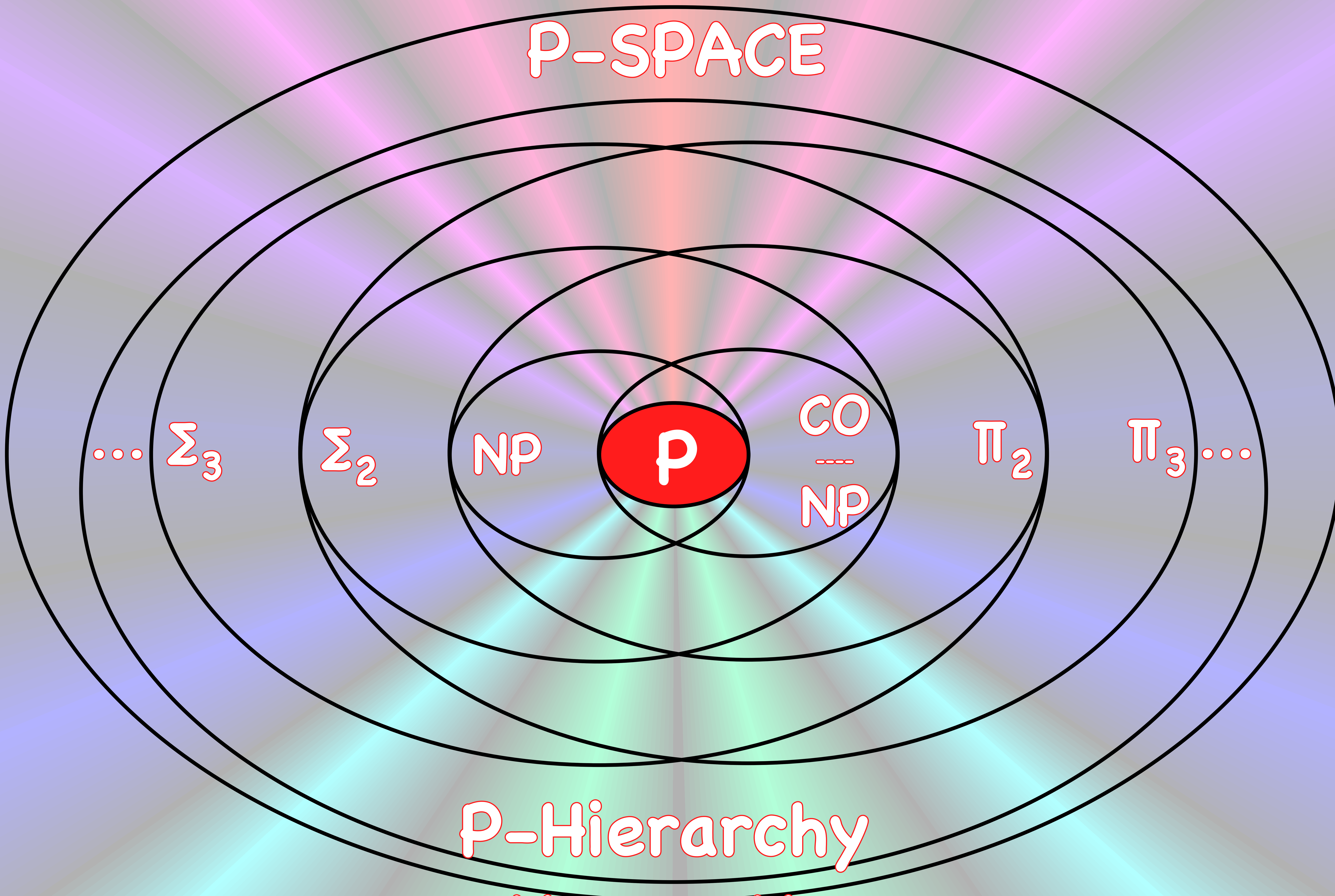
NO !

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

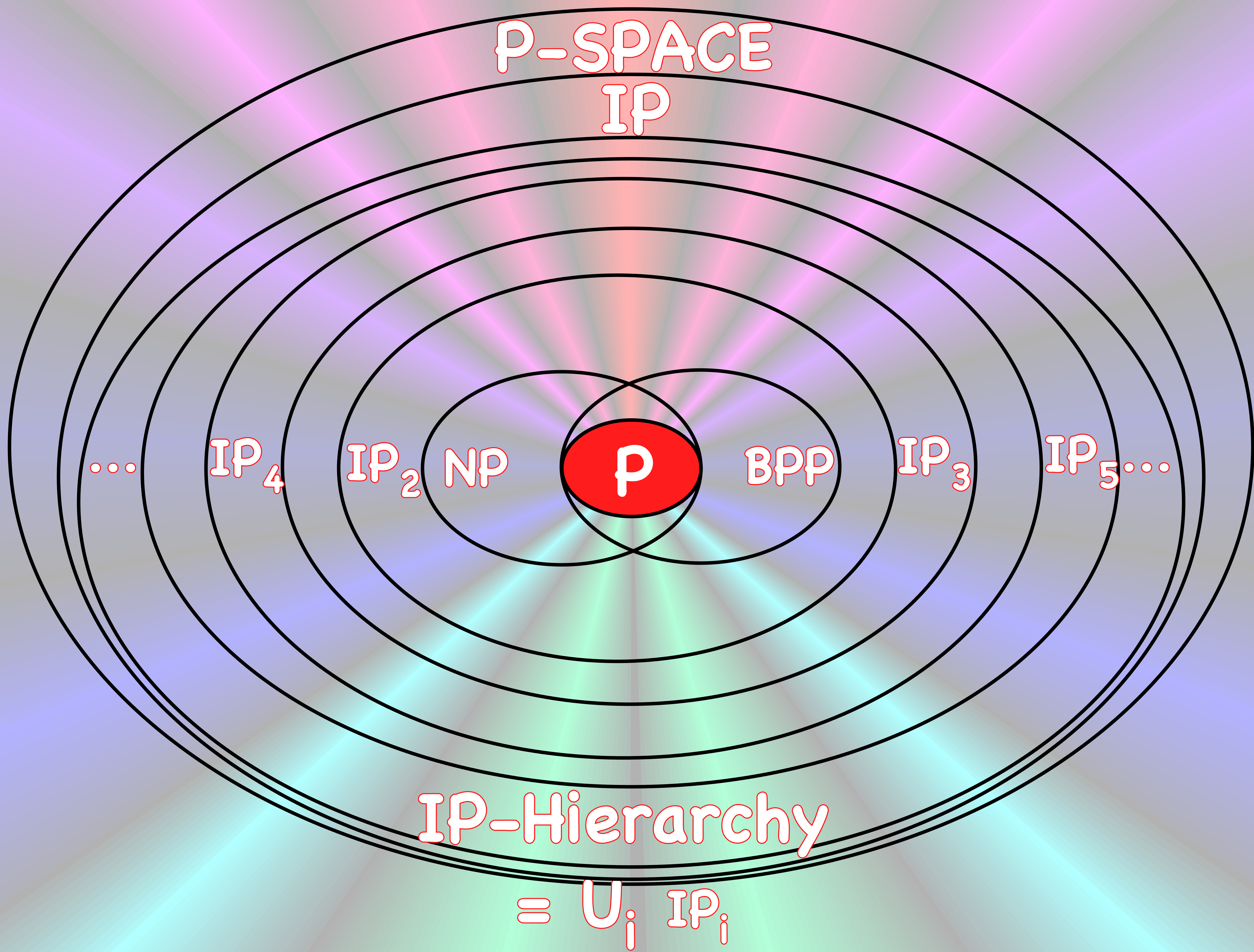
Complexity and Arthur-Merlin Games


PROOF POSITIVE?
THROW DINNER PARTIES WITH STATISTICAL CONFIDENCE
THE FOOD FIGHTS AT KING ARTHUR'S ROUND TABLE WERE GETTING OUT OF CONTROL!!
SO ARTHUR'S SERVANTS MADE A LIST: IT SHOWED WHICH DINNER GUESTS COULD SIT PEACEFULLY SIDE BY SIDE.
GLEEP!
THE KING COMMANDED HIS WIZARD MERLIN TO ARRANGE THE SEATING SO THAT EVERYONE SITS BETWEEN TWO FRIENDS.
B-BUT, SIRE... THE POSSIBLE COMBINATIONS OUTNUMBER THE ATOMS IN THE UNIVERSE!
JUST DO IT!
LET'S IMAGINE THAT MERLIN IS INFINITELY SMART: IF THERE'S A WAY, HE'LL FIND IT... IF NOT, HE'LL KNOW. (THIS DEPENDS ON THE FRIENDSHIP LIST, OF COURSE.)
AND THESE FOOD STAINS!
WELL, IT TURNED OUT THERE WAS NO WAY TO DO IT... AND THE QUESTION WAS, HOW COULD MERLIN CONVINCE ARTHUR THAT THIS WAS TRUE?
UM... GOT 10^{74} MINUTES?
HE COULDN'T... SO MERLIN WAS SENT TO THE DUNGEON, AND THE FOOD FIGHTS CONTINUED...
SPLUP
M... SOUNDS LIKE MELON SEASON...
THEN, IN 1989, WIZARDS NAMED LUND, FORTNOW, KARLOFF, + NISAN RESCUED THEIR COLLEAGUE. IT MAY NOT BE POSSIBLE TO CONVINCE ARTHUR WITH ABSOLUTE CERTAINTY, THEY SAID, BUT IT CAN BE DONE BEYOND A REASONABLE DOUBT.
THEY USED A NEW IDEA CALLED AN INTERACTIVE PROOF, IN WHICH A VERIFIER WITH LIMITED TIME (LIKE ARTHUR) INTERROGATES AN ALL-WISE PROVER (LIKE MERLIN).
O.K... TALK!
THE MATHEMATICIANS KNEW THAT IF THERE WERE NO GOOD SEATING ARRANGEMENT, A CERTAIN HUGE FORMULA WOULD REDUCE TO ZERO — BUT VERIFYING THE CALCULATION WOULD TAKE ARTHUR (ALMOST) FOREVER.
ZERO.
THEY SHOWED HOW ARTHUR CAN ASK MERLIN TO MAKE A SERIES OF RELATED CALCULATIONS, AND HOW ARTHUR CAN CHECK THE ANSWERS FOR CONSISTENCY WITH EACH OTHER, WITHOUT ACTUALLY VERIFYING THEIR ACCURACY.
WHAT'S P_{n-1}?
6
AND P_{n-2}?
3
HM... 6−2·3=0 O.K...
AS ANSWERS PILE UP WITHOUT ANY INCONSISTENCY, ARTHUR'S CONFIDENCE INCREASES. BY THE TIME HE'S DONE, HIS MARGIN OF DOUBT CAN BE REDUCED AS SMALL AS YOU LIKE!!
HM! THE PROBABILITY OF YOUR BEING WRONG IS LESS THAN .000000000001!
TOO BAD FOR YOU KINGS NEVER APOLOGIZE!
THIS WAS REVOLUTIONARY! EVER SINCE EUCLID, THE STANDARD OF PROOF HAS BEEN ABSOLUTE... SUDDENLY, IT'S STATISTICAL... AND NEW IDEAS FOLLOWED.
BACK AT THE ROUND TABLE, THE LIST OF FRIENDS HAS CHANGED.
WHAT HAPPENED?
LANCELOT HAD THERAPY...
THANKS TO THE CHANGES, A PEACEFUL SEATING ARRANGEMENT NOW EXISTS — BUT AGAIN, HOW DOES MERLIN CONVINCE ARTHUR?
MR. PENDRAGON WILL SEE YOU NOW...
THIS TIME, MERLIN CAN WRITE DOWN A PROOF — IT'S JUST THE LIST OF PAIRS OF NEIGHBORS. QUITE CHECKABLE, BUT ARTHUR DOESN'T WANT TO BE BOTHERED!
THIS IS TH' NINETIES!
AH, BUT MERLIN HAS SOMETHING UP HIS SLEEVE! FORGET INTERACTION... NOW WE HAVE THE TRANSPARENT PROOF.*
INVENTED AND DEVELOPED BY BABAI, FORTNOW, LEVIN, SZEGEDY, FEIGE, LUND, GOLDWASSER, LOVASZ, SAFRA, ARORA, MOTWANI, & SUDAN!
FIRST, MERLIN HAS TO REWRITE THE PROOF IN FORMAL LANGUAGE, I.E., SOMETHING A COMPUTER COULD INTERPRET... THEN HE TRANSFORMS IT MATHEMATICALLY IN A SIMPLE YET MIRACULOUS WAY.
THE NEW TRANSPARENT PROOF HAS AN AMAZING PROPERTY: IF THERE WAS EVEN A SINGLE ERROR IN THE ORIGINAL PROOF, IT NOW SHOWS UP ALMOST EVERYWHERE!
HOW DID YOU DO THAT?
YEARS OF GRAD SCHOOL...
ARTHUR TAKES THE TRANSPARENT PROOF, CHECKS IT IN A FEW PLACES, AND, FINDING NO PROBLEMS, BECOMES STATISTICALLY CERTAIN IT'S RIGHT!
LET'S EAT!
YOU CAN SEE HOW THIS MIGHT WORK USING NUMBERS: SUPPOSE YOU WERE COPYING A STRING OF NUMBERS AND MADE A MISTAKE:
1, 4, 5 → 1, 5, 5
NOW EXTEND EACH PAIR OF NUMBERS INTO AN ARITHMETIC PROGRESSION
1, 4, 7, 10, 13,... 1, 5, 9, 13, 17,...
4, 5, 6, 7, 8,... 5, 5, 5, 5, 5,...
THE ARRAYS OF NUMBERS ARE DIFFERENT "ALMOST EVERYWHERE."
MERLIN POINTS OUT THAT IT IS NO LONGER NECESSARY TO CHECK BIG COMPUTATIONS STEP BY STEP. INSTEAD, WE CAN MAKE THEM TRANSPARENT, VERIFY A FEW PLACES FOR CONSISTENCY, AND SUPPRESS ALMOST ALL DOUBT!!
THIS WORKS WITH ALL COMPUTATIONS, NOT JUST DINNER PARTIES!
THEORETICALLY, A LONE MACINTOSH CAN MONITOR A WHOLE HERD OF CRAYS...
WHAT'S A CRAY? ANYTHING LIKE A COW?
BUT LESS INTELLIGENT, FORSOOTH...
WITH SPECIAL THANKS TO DR. LASZLO BABAI, FATHER OF THE INTERACTIVE PROOF, FOR GUIDANCE, IDEAS, AND JOKES!!

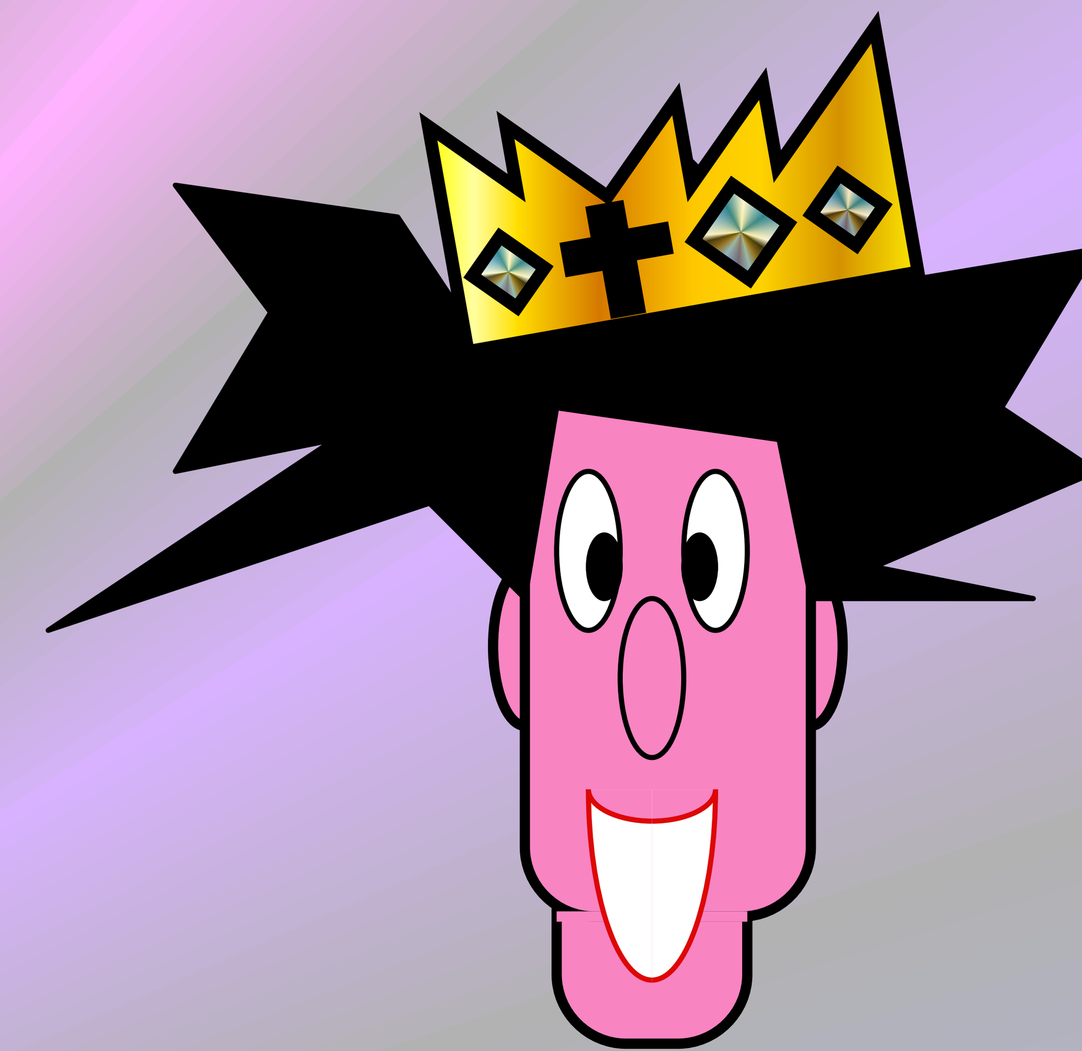
Click here



$= \cup_i \Sigma_i = \cup_i \Pi_i$


P-SPACE
IP
... IP$_4$ IP$_2$ NP P BPP IP$_3$ IP$_5$...
IP-Hierarchy
$= \bigcup_i$ IP$_i$

Arthur-Merlin GAMES
(Arthur-Morgane GAMES)



$x \in L$

01100010101011010101010 ←

→

00010101010111010101010 ←

→

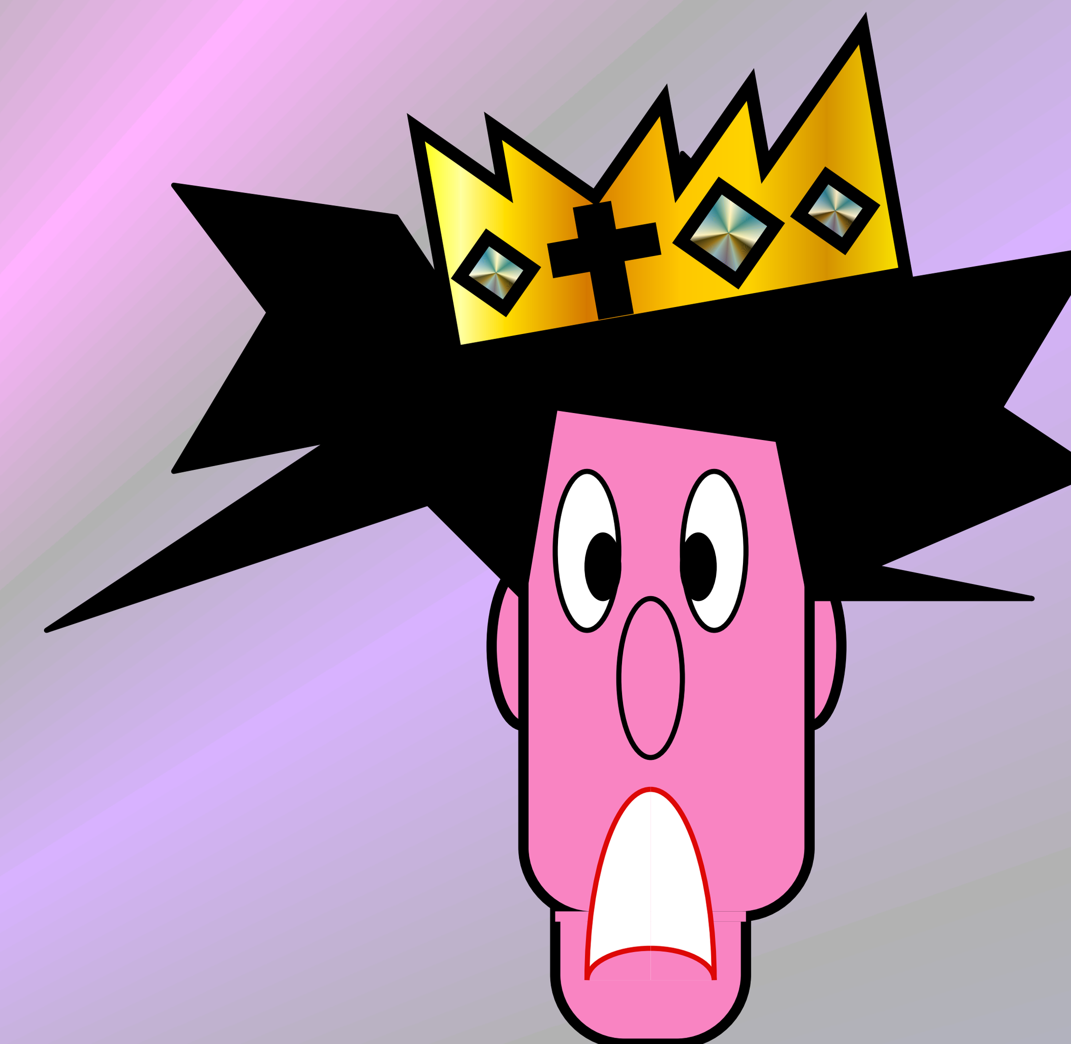
01011011010000101010101 ←

→

YES !

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

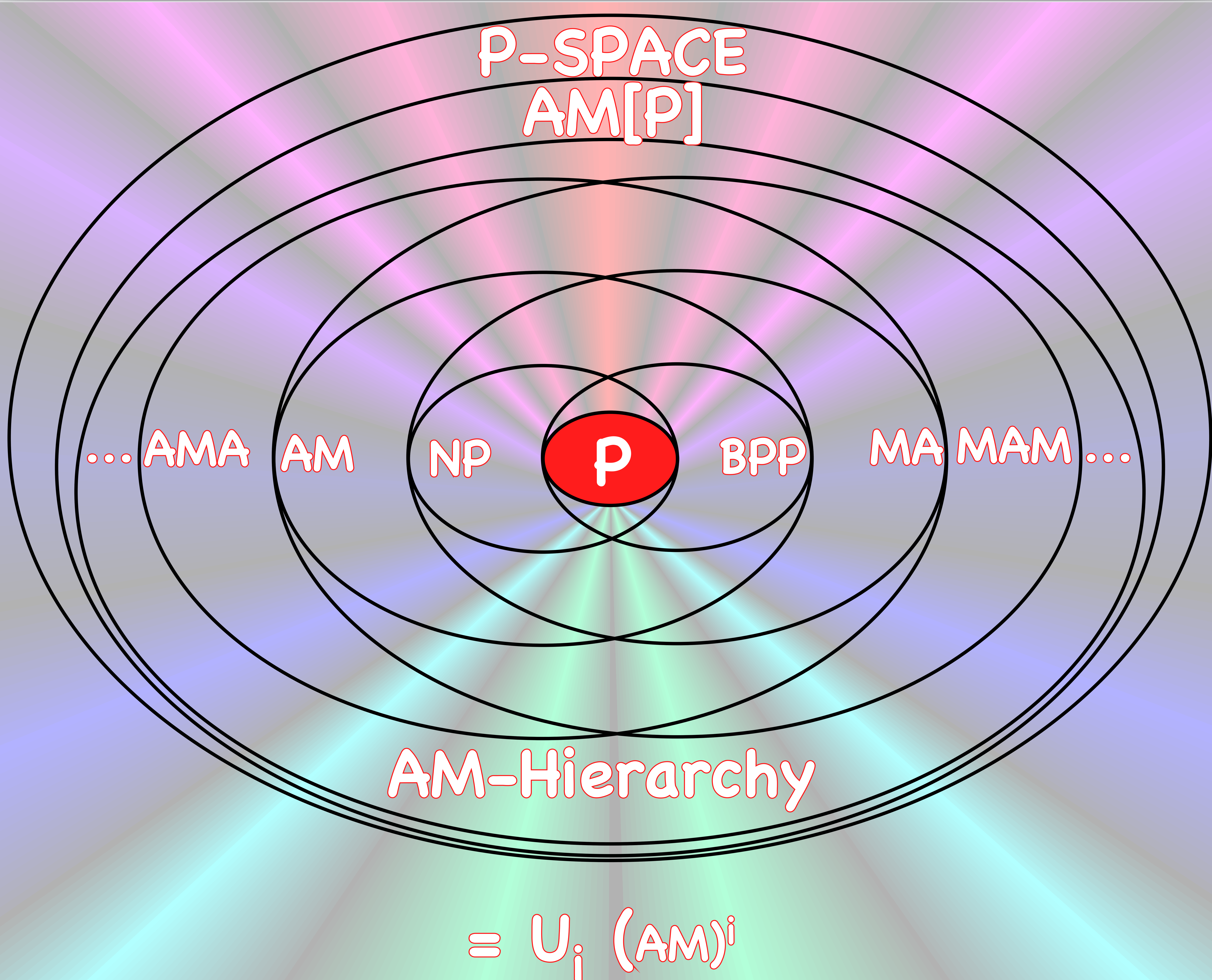
Arthur-Merlin GAMES

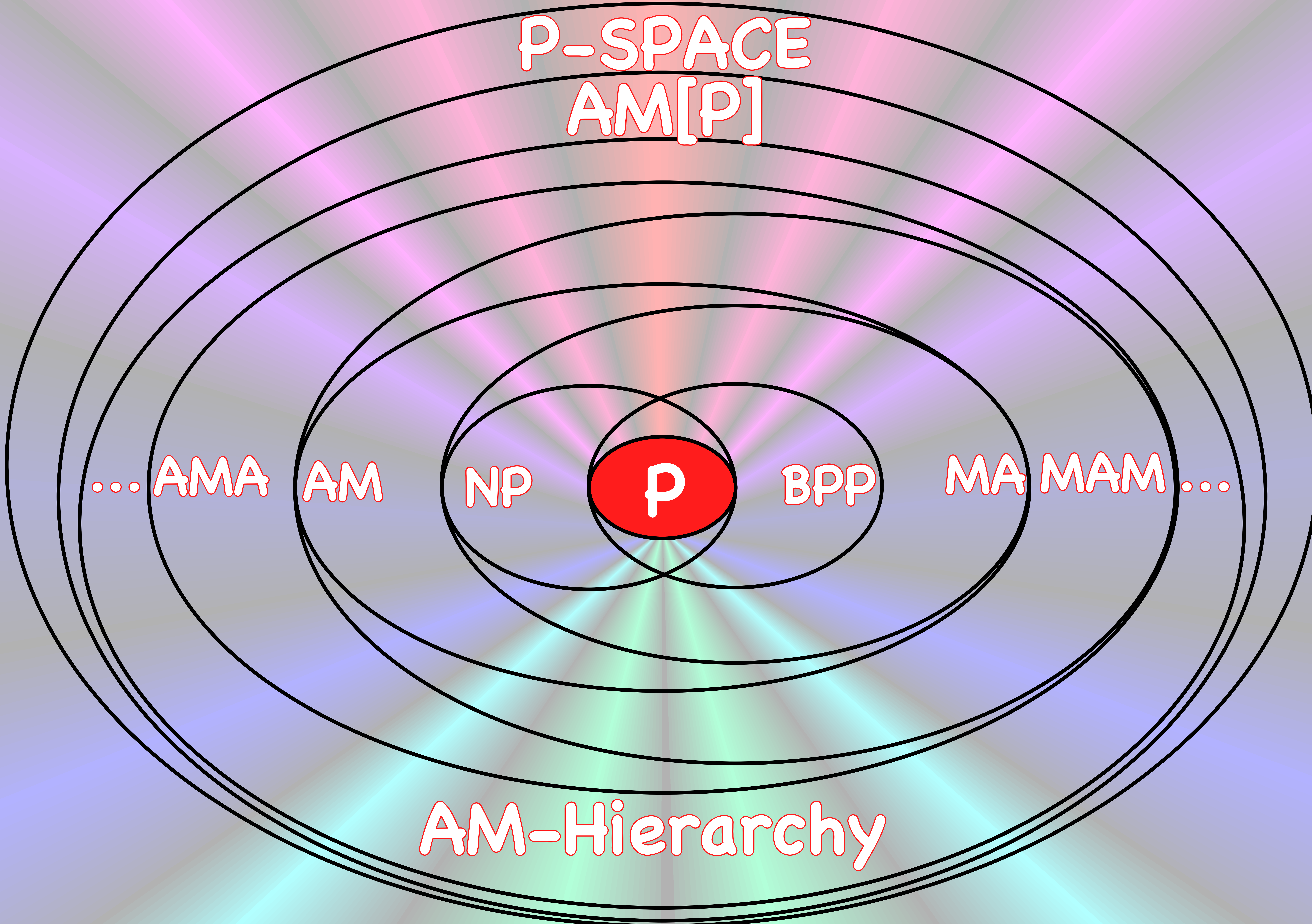


$x \notin L$

NO !

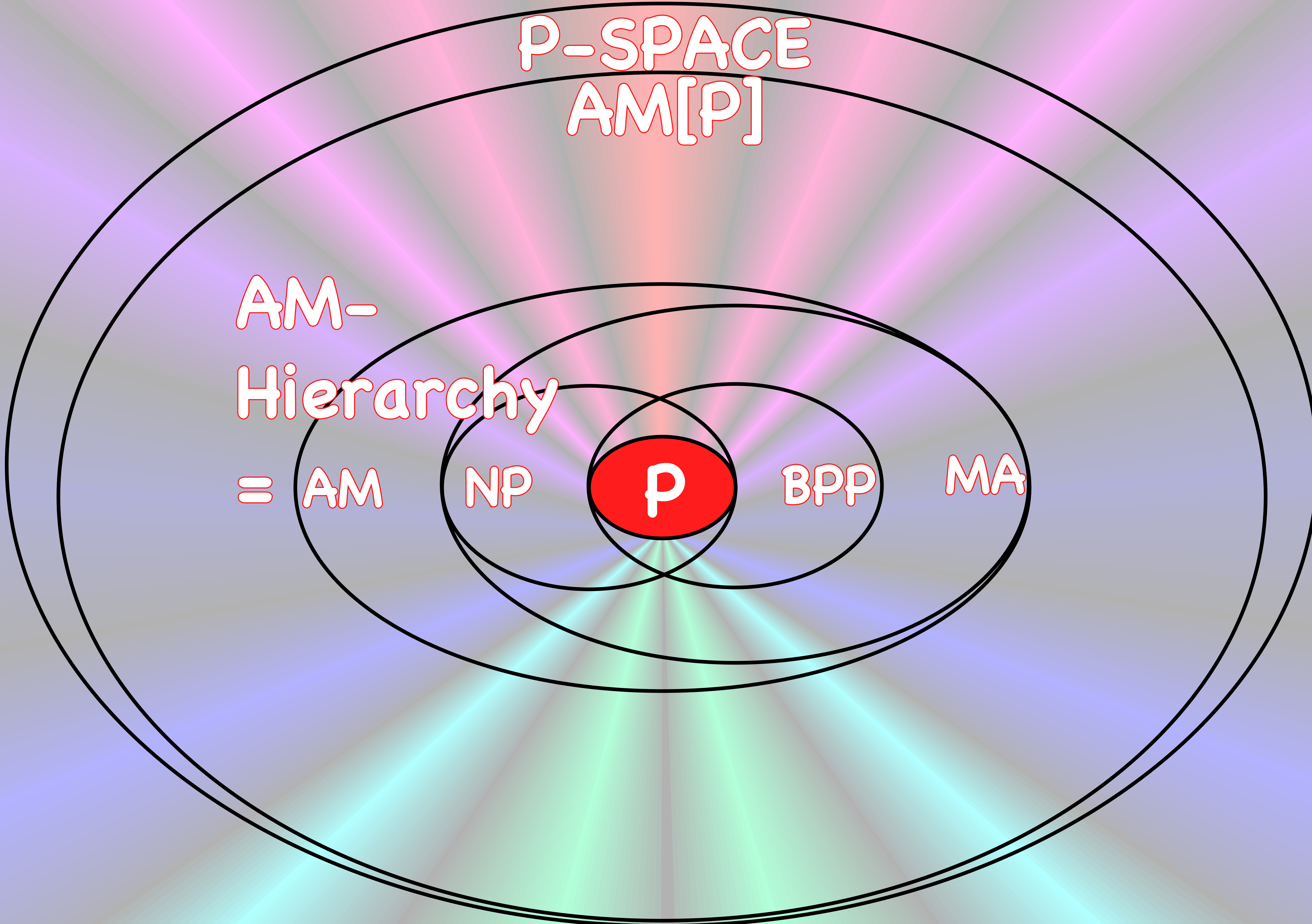
$\forall x \notin L\ \forall D\ \Pr(\ [D,B](x)=YES\ ) \approx 0$


P-SPACE
AM[P]
...AMA
AM
NP
P
BPP
MA
MAM...
AM-Hierarchy
= U_i (AM)^i



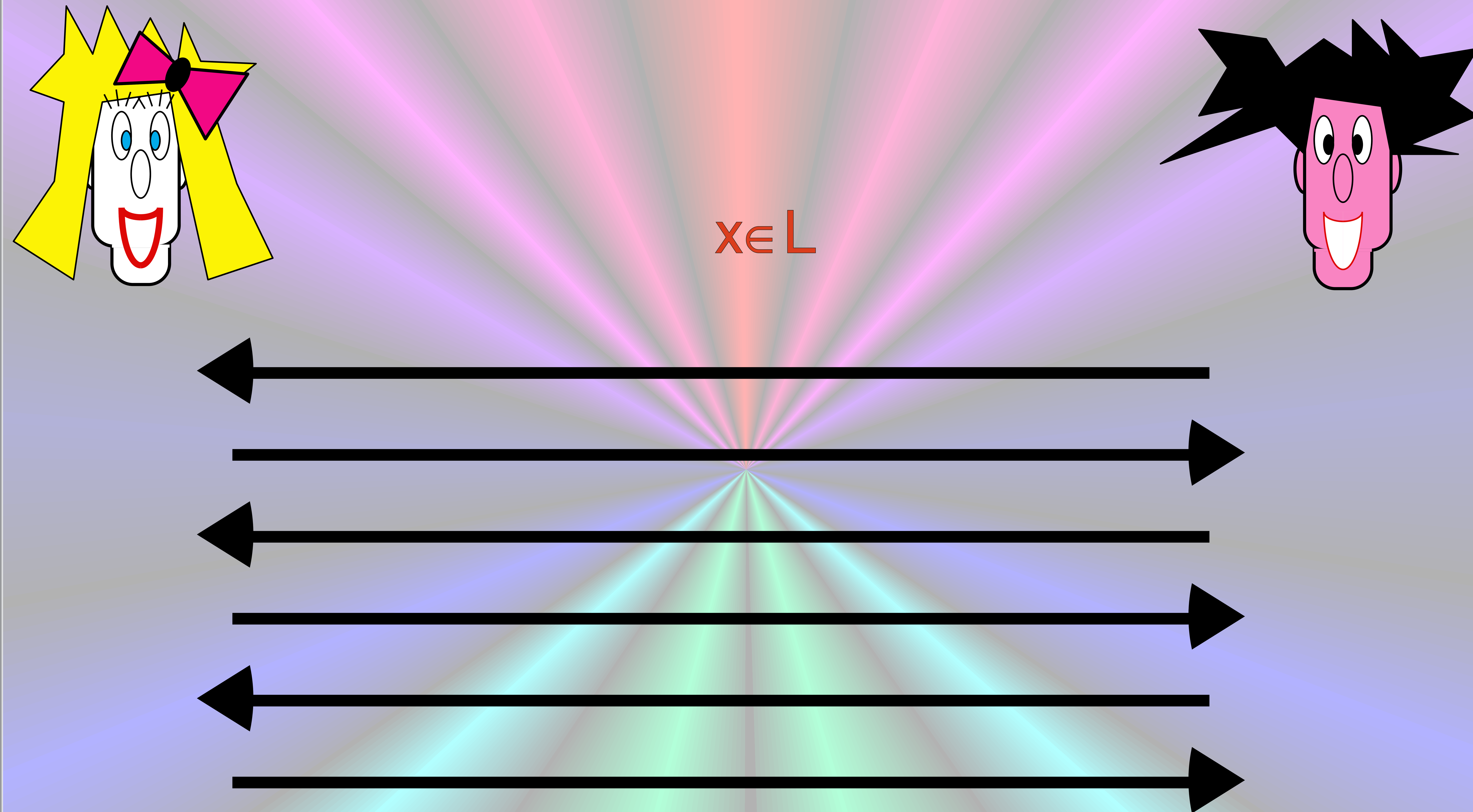
$= \bigcup_i (\mathrm{AM})^i$

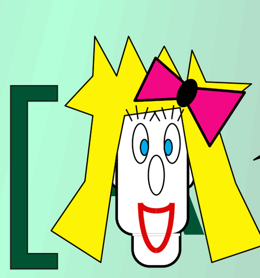
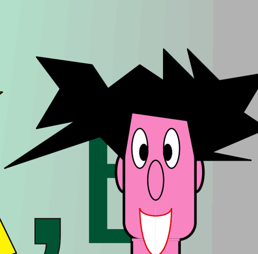
[BABAI]

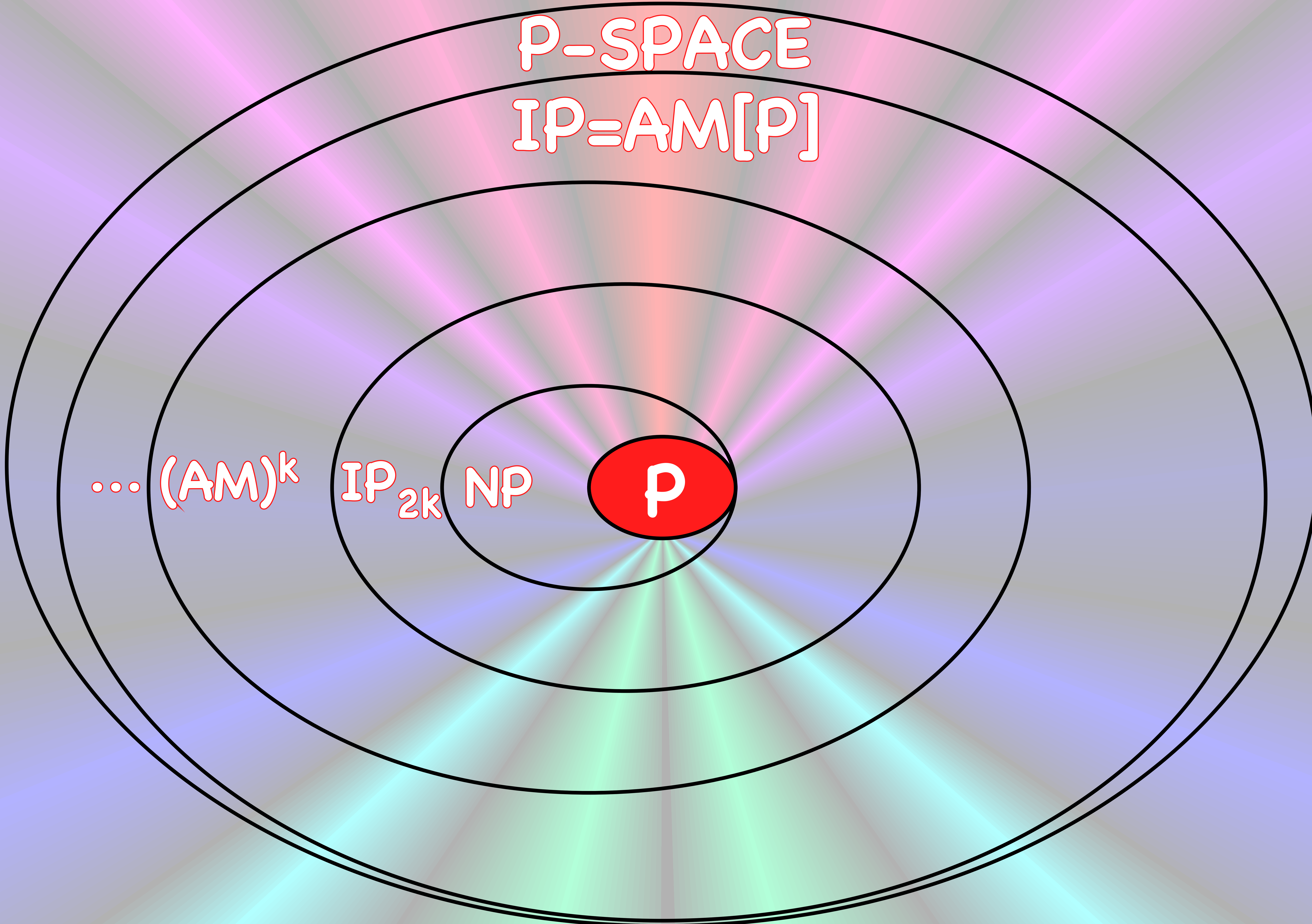


[BABAI]

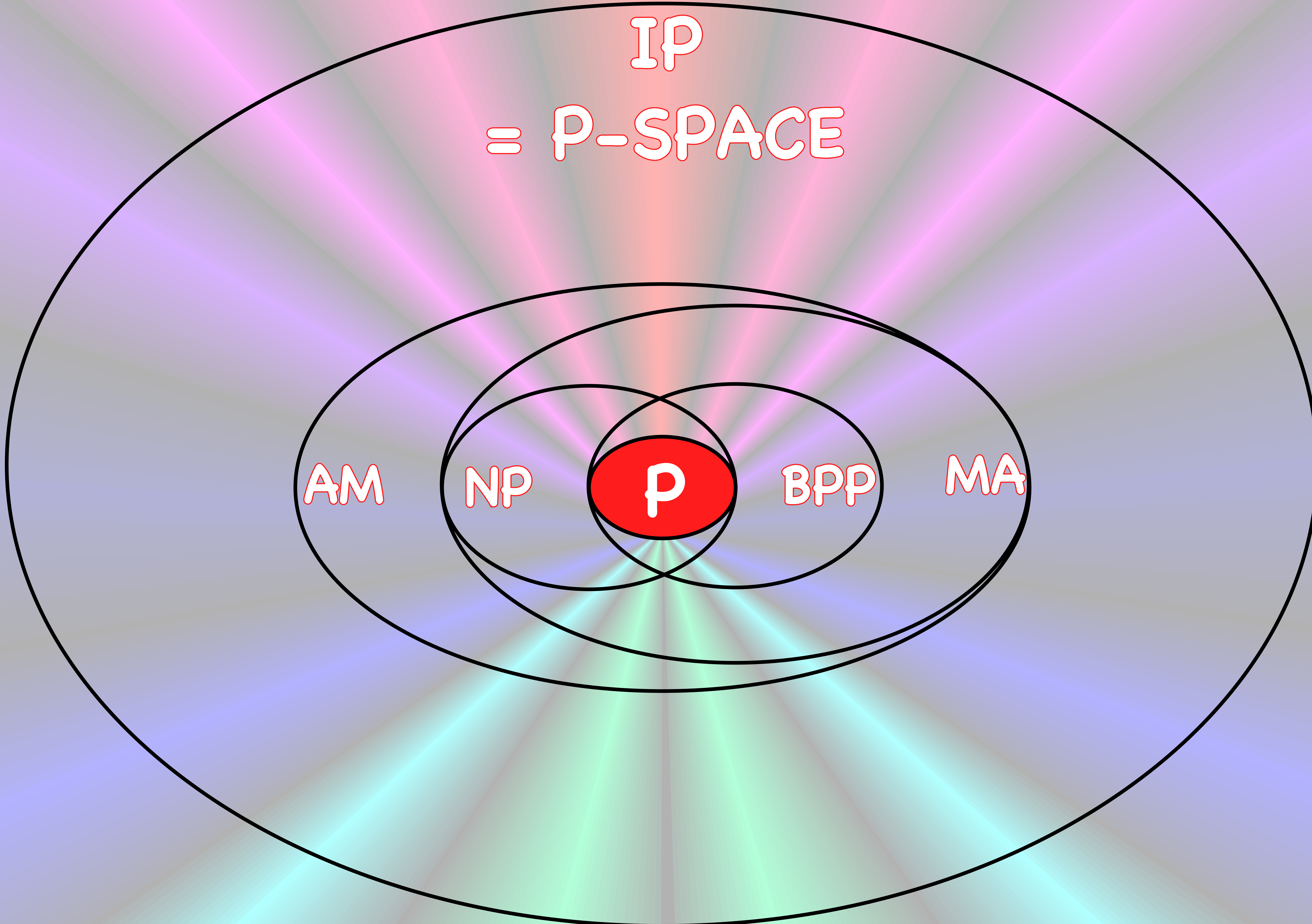
Interactive Proofs



$\forall x \in L$ Pr([,](x)=YES) ≈ 1



[Goldwasser-Sipser]



The entire IP hieracrhy

[Shamir]

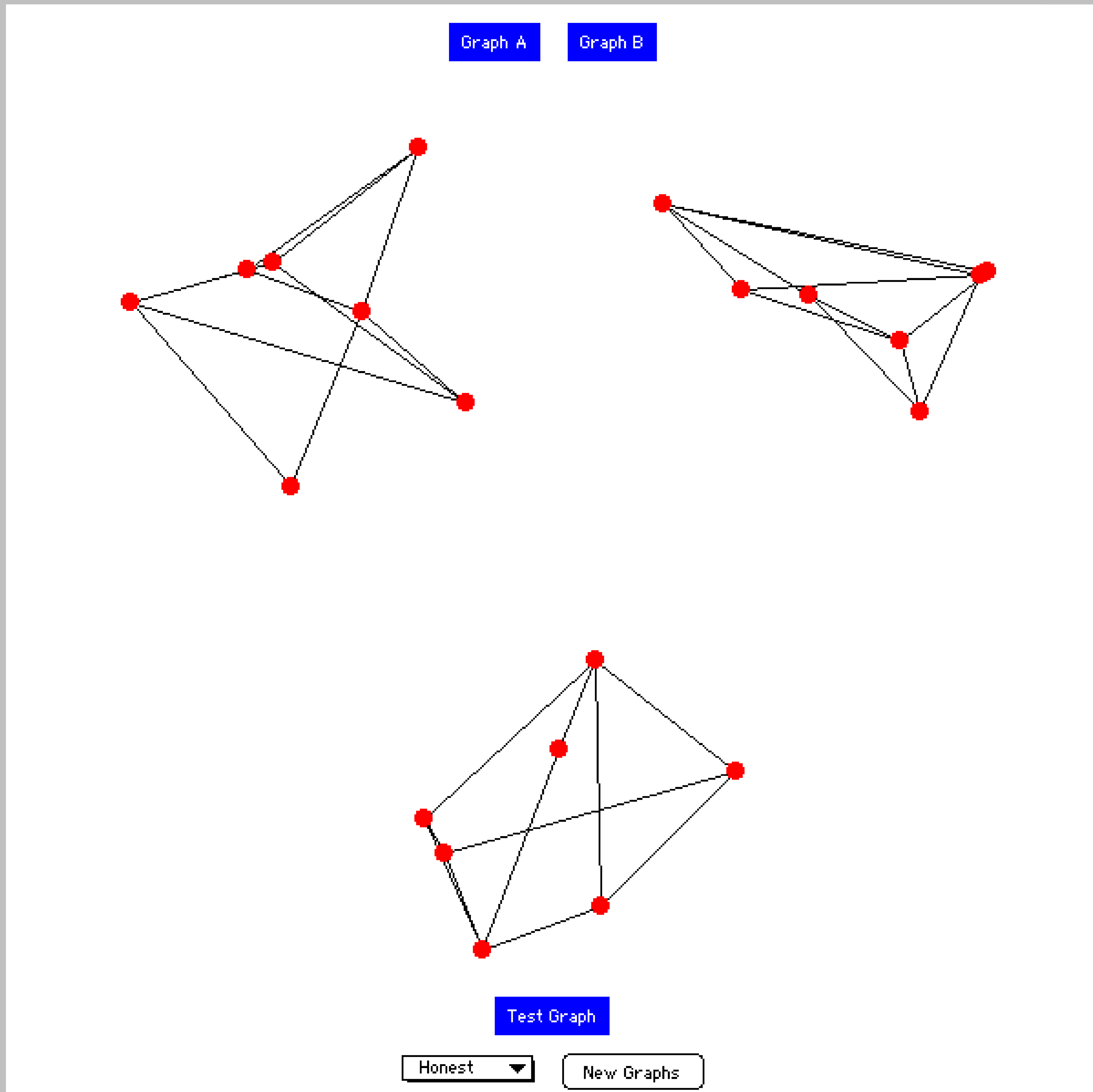
Non-ISO	SAT	Sorting	square root extraction mod p=4k+1
Non-EQ	3-COL	Linear Programming	finding a generator mod p
...	ISO	Primality	finding an irreducible poly
	EQ	Shortest Path	...
	...	...	

Non-ISO$\in$IP$_2$=AM

Location: http://www.IRO.UMontreal.ca/~marcilj/InteractiveProof/ What's Related

- You will accept that the two graphs are isomorphic if the Test Graph was always isomorphic to the chosen graph.

Let's try it!



Note : you can redraw a graph by Ctrl-clicking on it

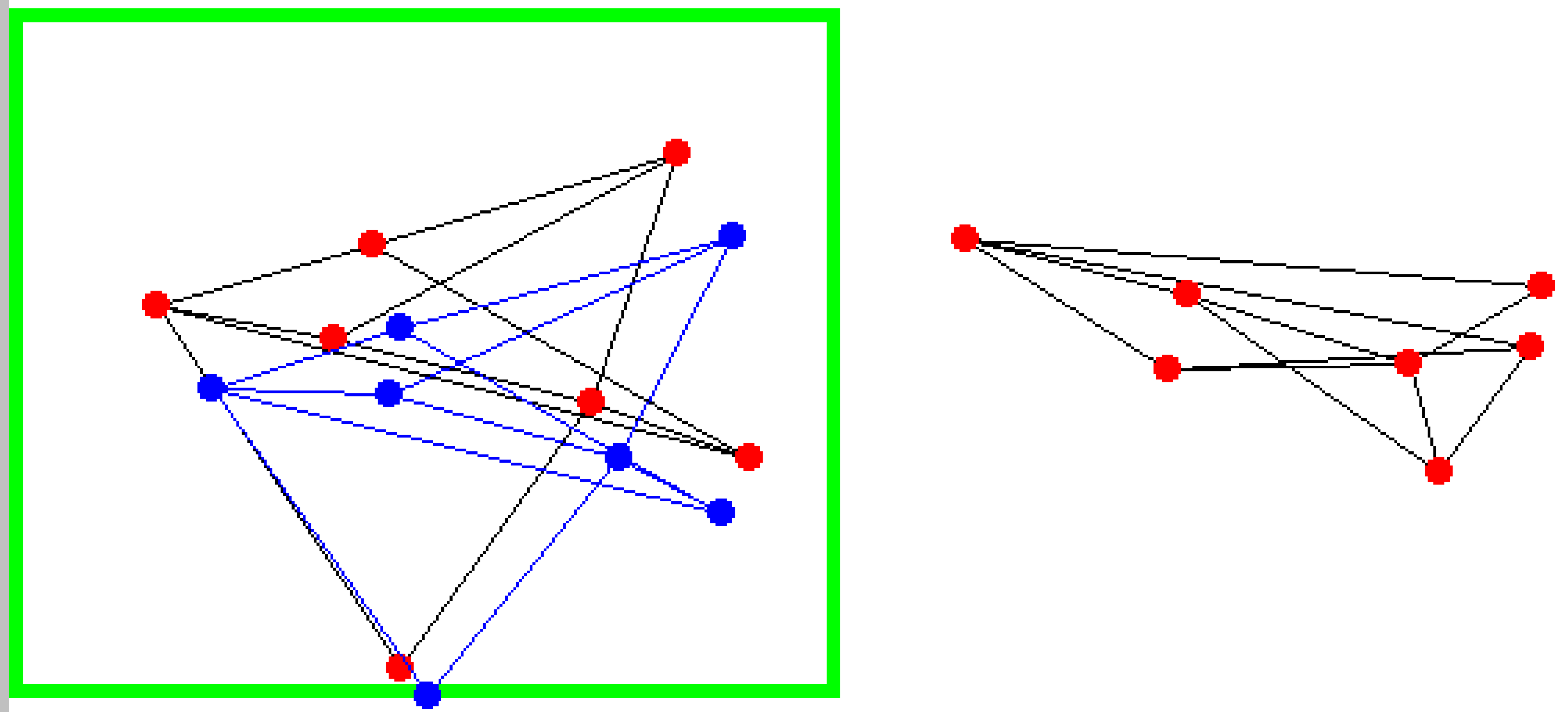
Text taken from Cryptography, Theory and practice.

Location: http://www.IRO.UMontreal.ca/~marcilj/InteractiveProof/ What's Related

- You will accept that the two graphs are isomorphic if the Test Graph was always isomorphic to the chosen graph.

Let's try it!

Graph A Graph B



Test Graph

Honest New Graphs

Note : you can redraw a graph by Ctrl-clicking on it

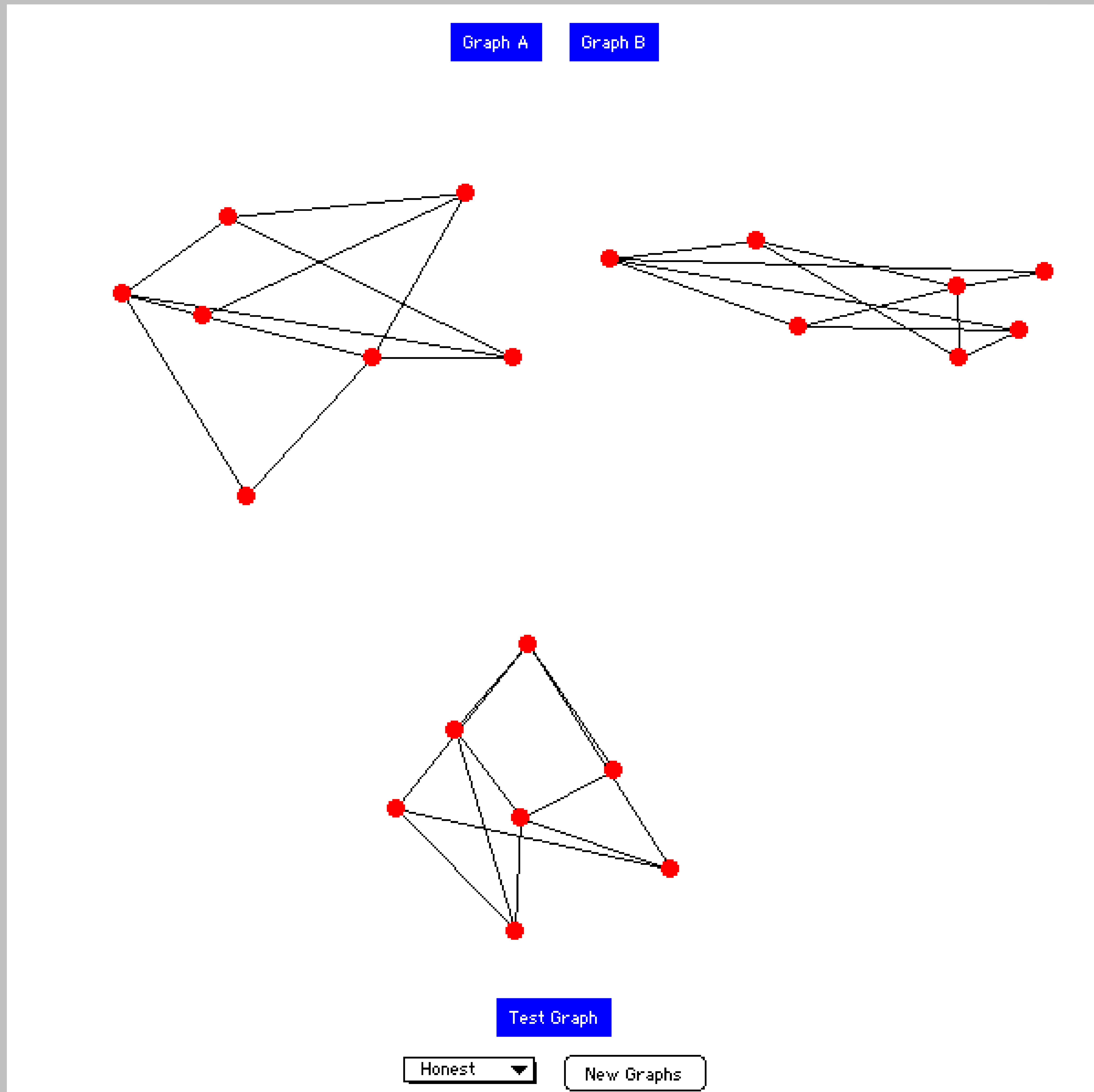
Text taken from Cryptography, Theory and practice.

Applet InteractiveProof running

Location: http://www.IRO.UMontreal.ca/~marcilj/InteractiveProof/ What's Related

- You will accept that the two graphs are isomorphic if the Test Graph was always isomorphic to the chosen graph.

Let's try it!



Note : you can redraw a graph by Ctrl-clicking on it

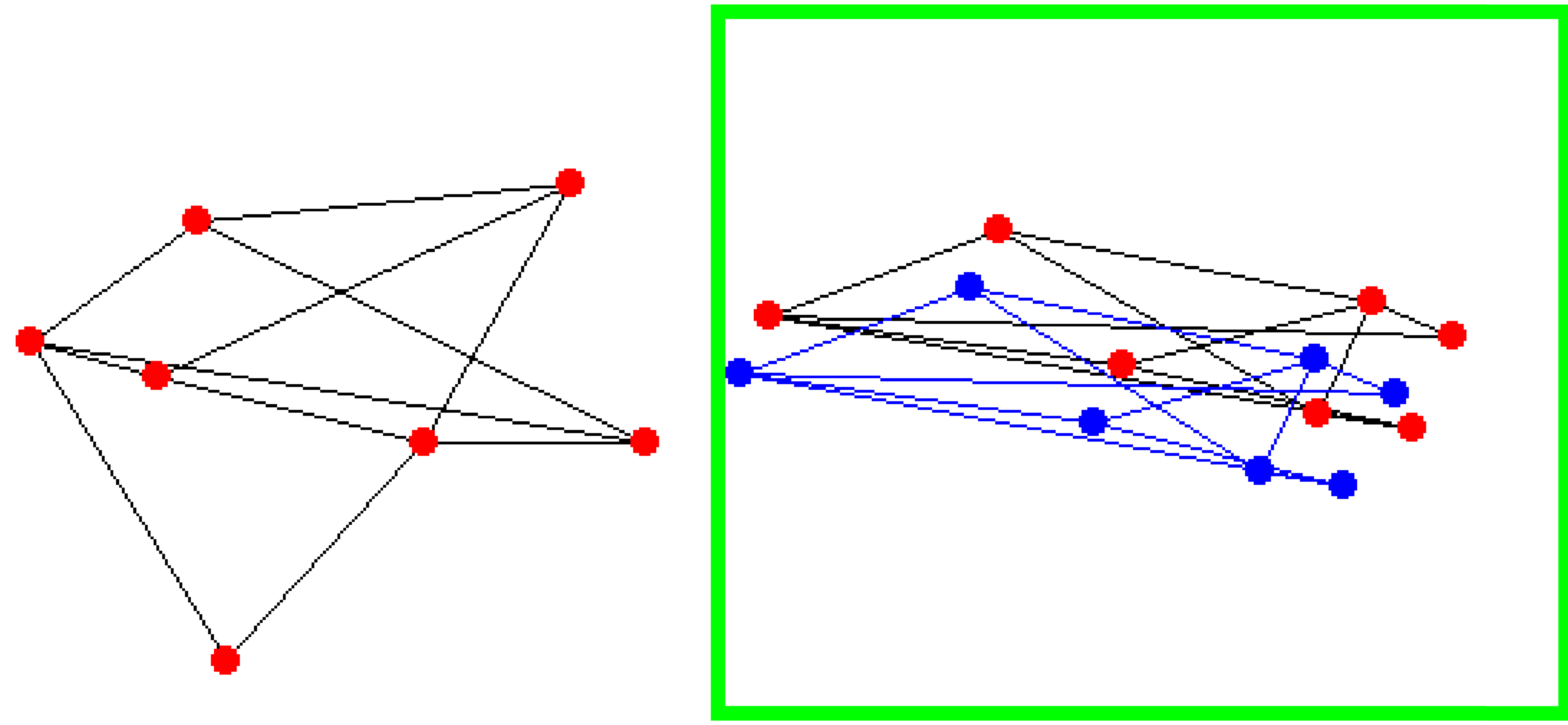
Text taken from Cryptography, Theory and practice.

Location: http://www.IRO.UMontreal.ca/~marcilj/InteractiveProof/ What's Related

- You will accept that the two graphs are isomorphic if the Test Graph was always isomorphic to the chosen graph.

Let's try it!

Graph A Graph B



Test Graph

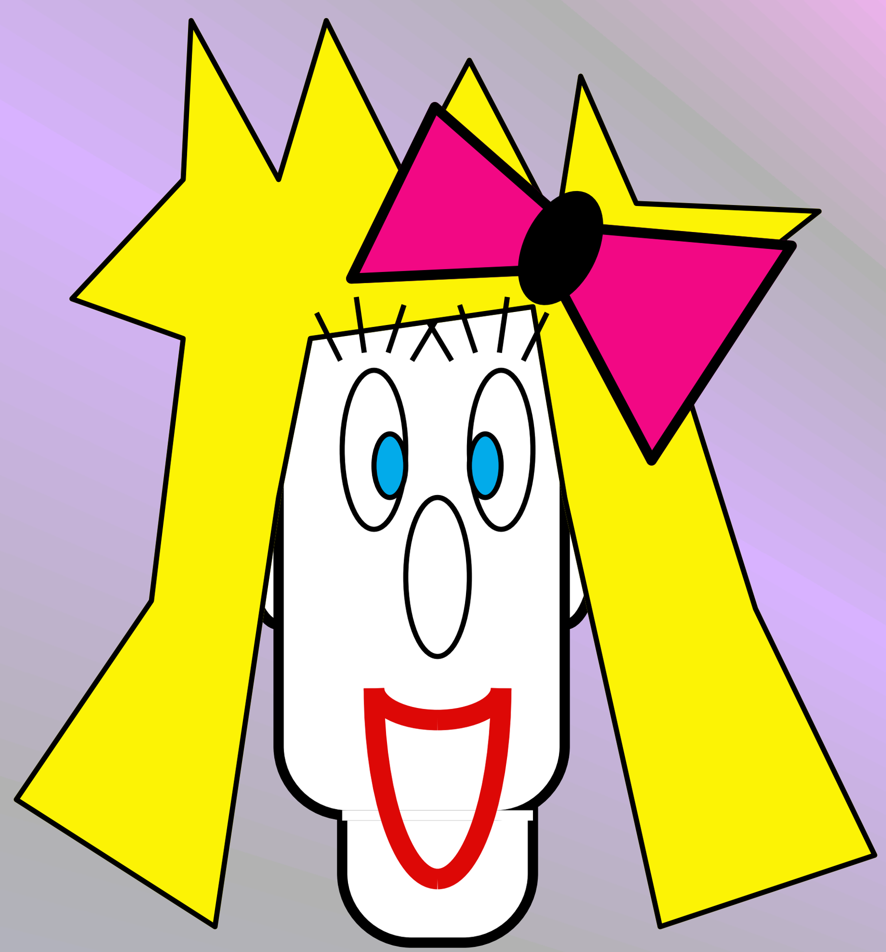
Honest New Graphs

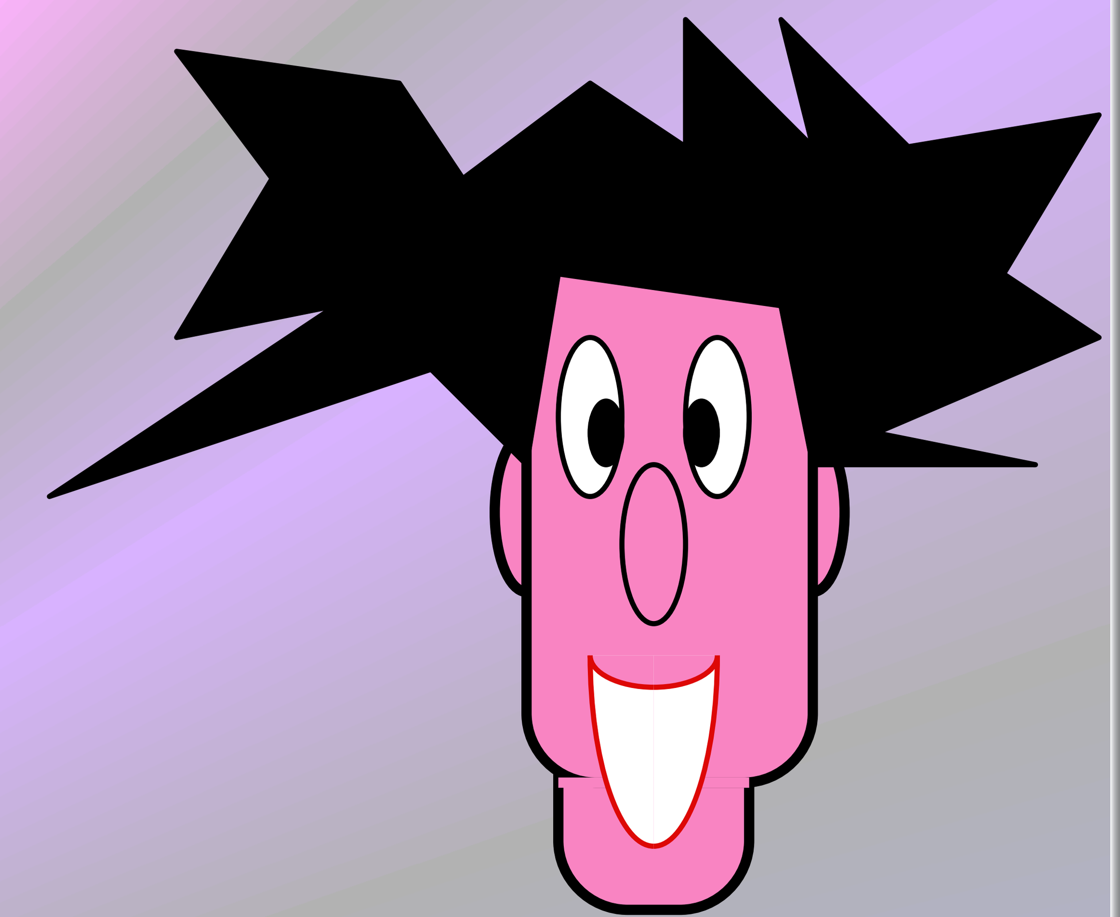
Note : you can redraw a graph by Ctrl-clicking on it

Text taken from Cryptography, Theory and practice.

Applet InteractiveProof running

Interactive Proofs

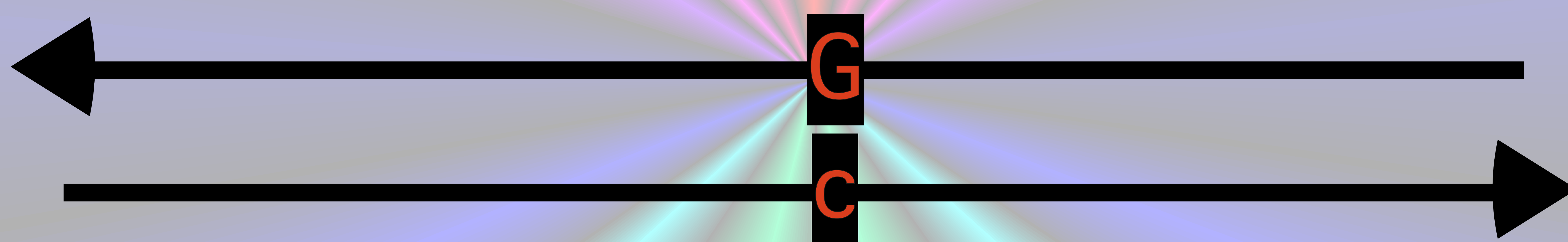




$(G_0, G_1) \in$ Non-ISO

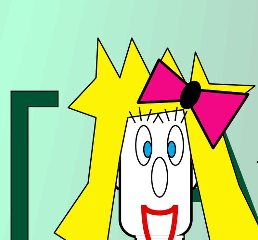
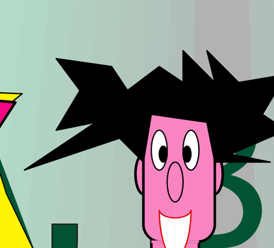
$\left(G_0 \neq \pi(G_1)\right)$

$G := \sigma(G_b)$

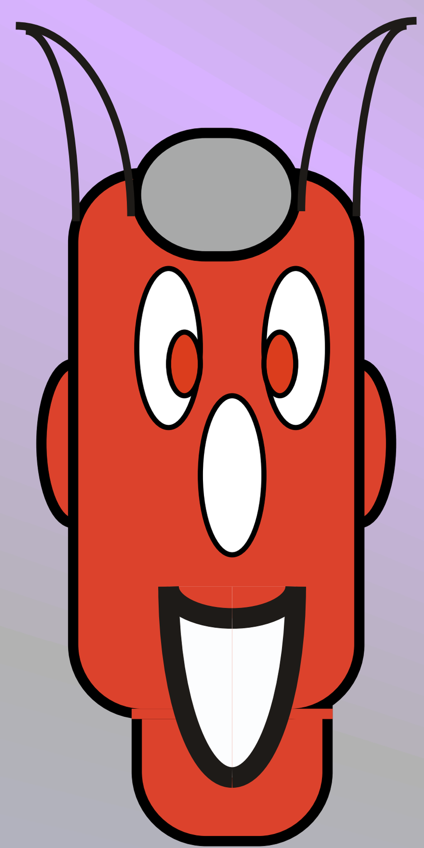


$c = b?$

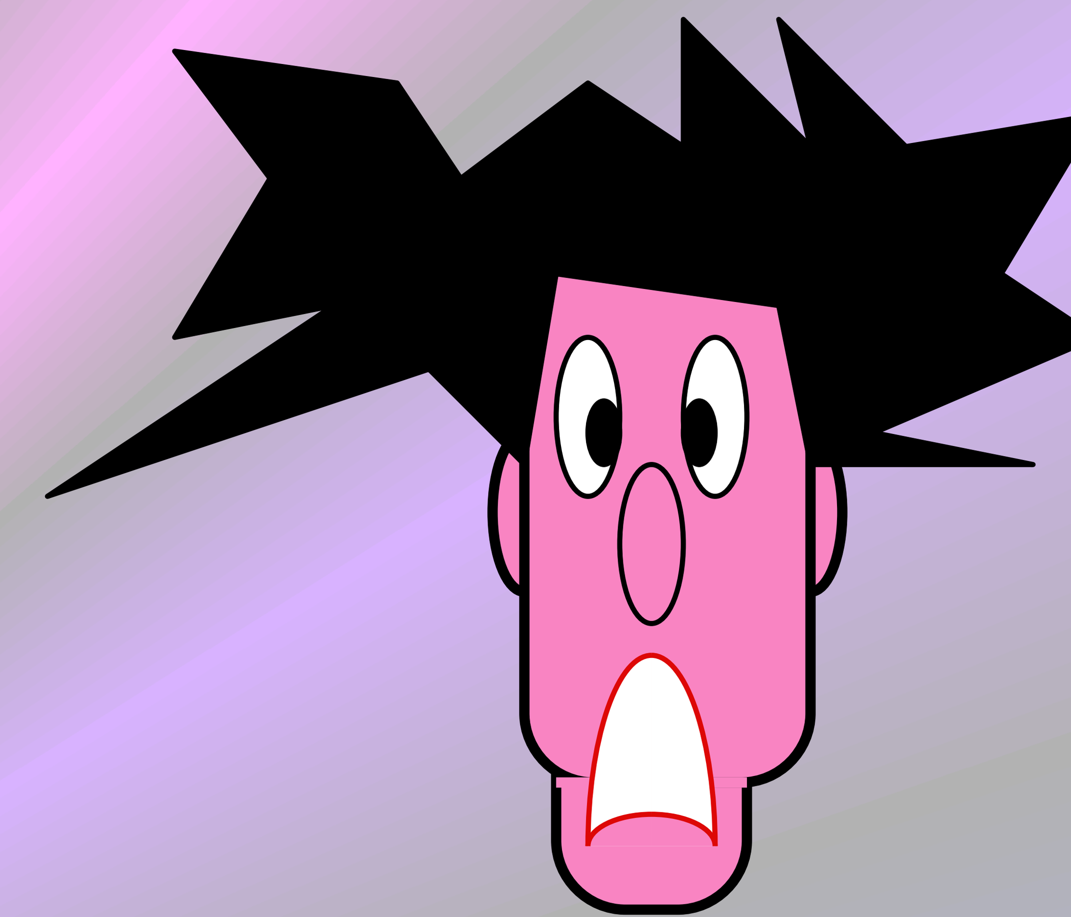
YES !

$\forall x \in L$ Pr([, ](x)=YES) = 1

Interactive Proofs

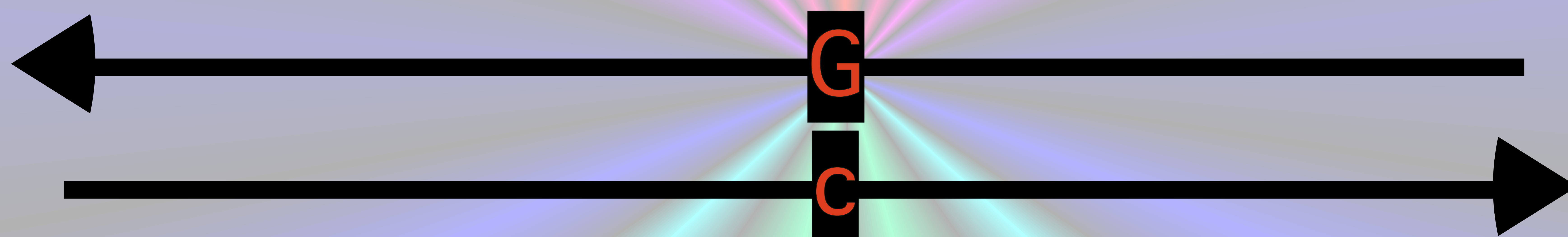


$(G_0, G_1) \notin$ Non-ISO



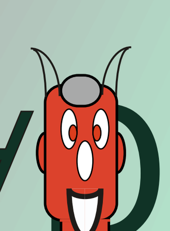
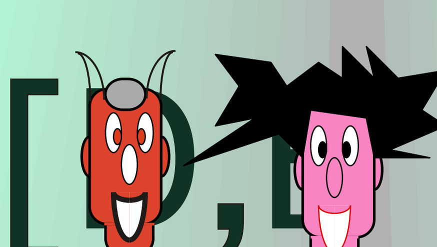
$G \approx G_0$ and $G \approx G_1$

$G := \sigma(G_b)$

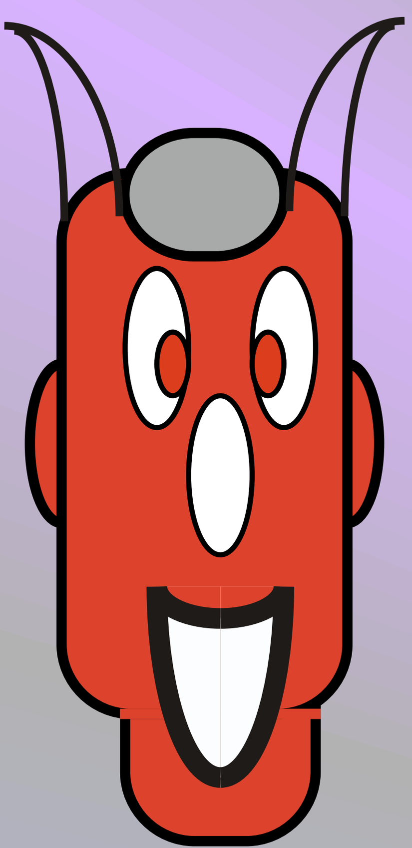


$c = b$?

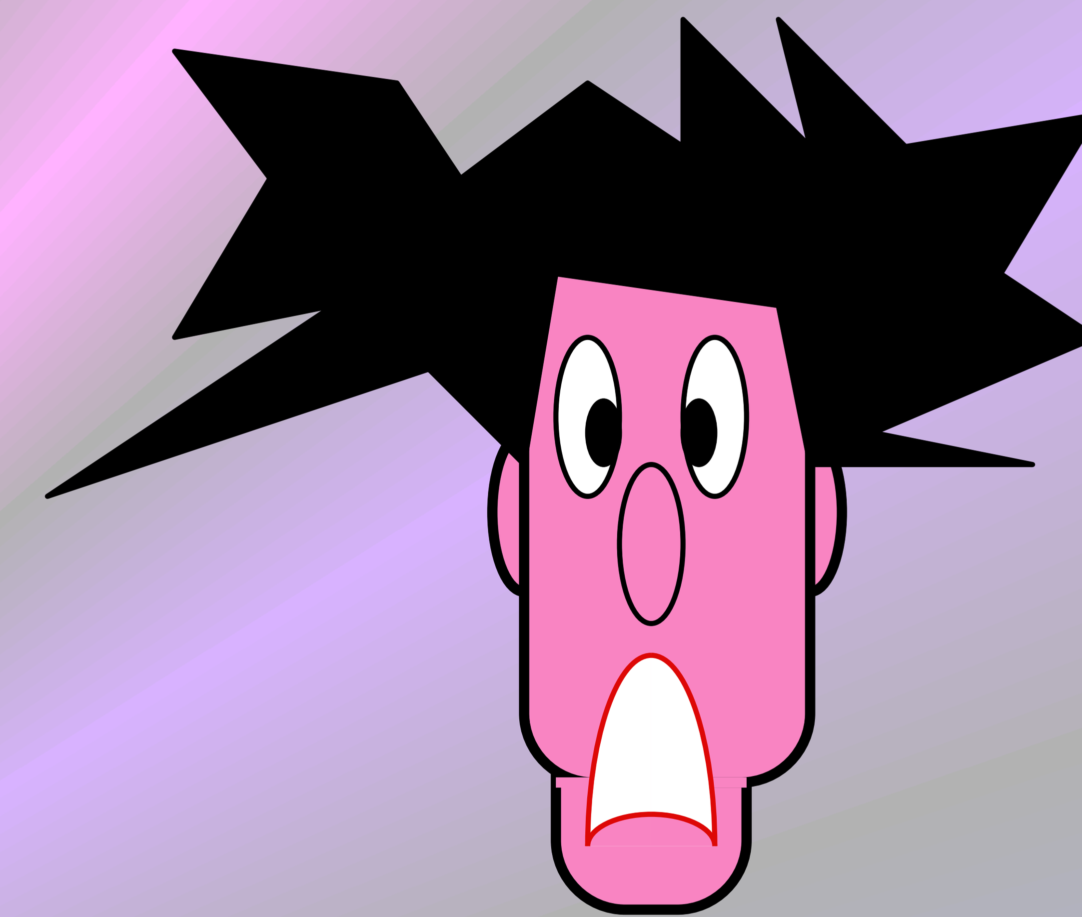
NO !

$\forall x \notin L\ \forall$  Pr([](x)=YES) $\le {}^1/_2$

Interactive Proofs



$(G_0,G_1) \notin$ Non-ISO



$\Gamma_i \approx G_0$ and $\Gamma_i \approx G_1$

$\Gamma_i := \sigma_i(G_{b_i})$

$\Gamma_1, \Gamma_2, \ldots, \Gamma_k$

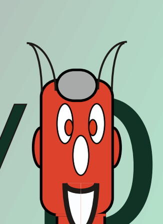
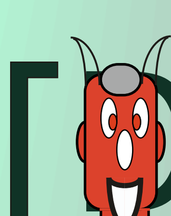
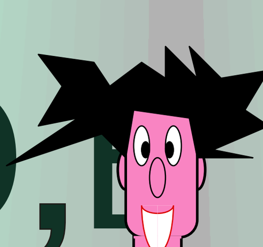
$c_1, c_2, \ldots, c_k$

$c_i = b_i$?

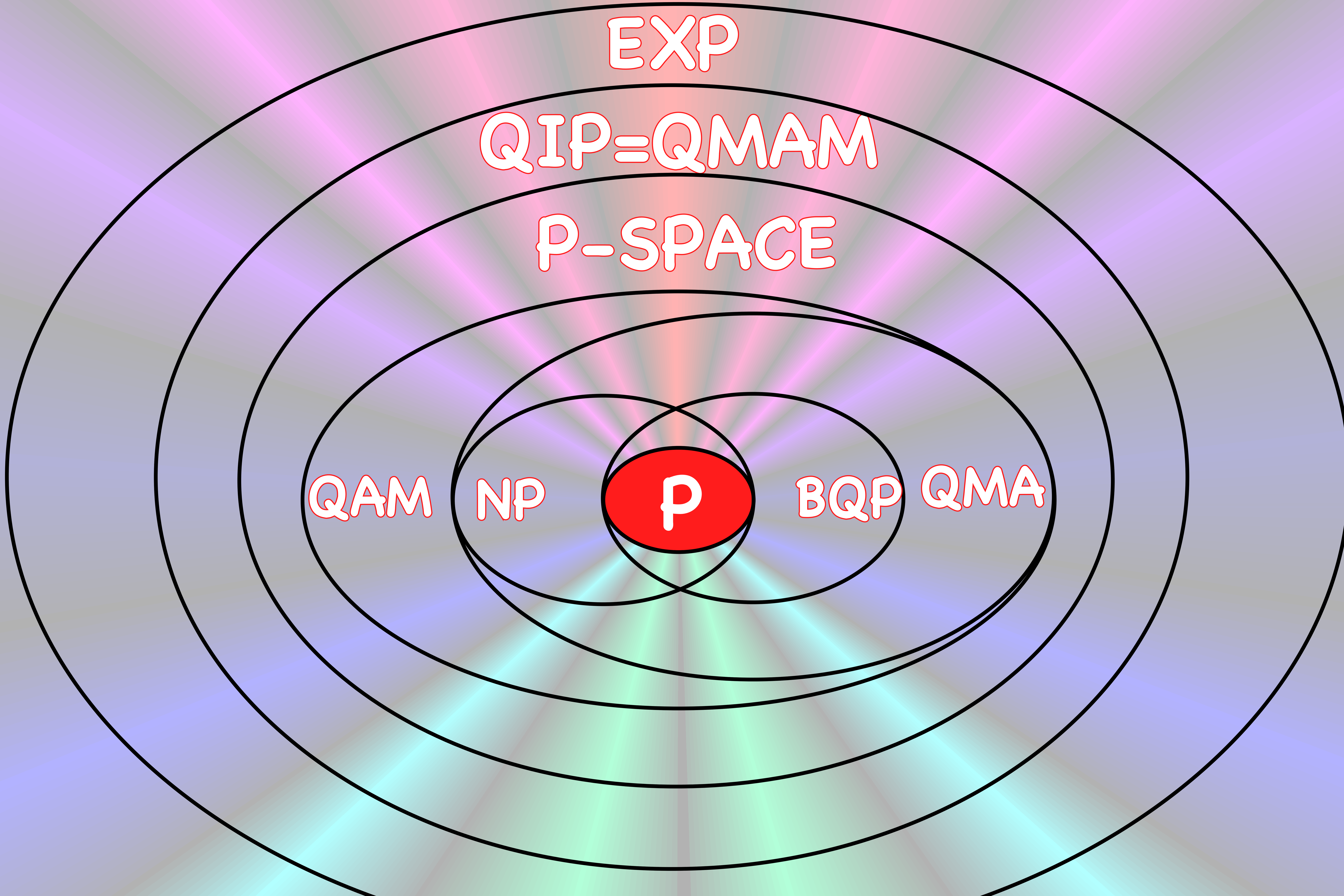
REPEAT k TIMES

and say "YES" only if all "YES"

NO !

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

Quantum Interactive Proofs

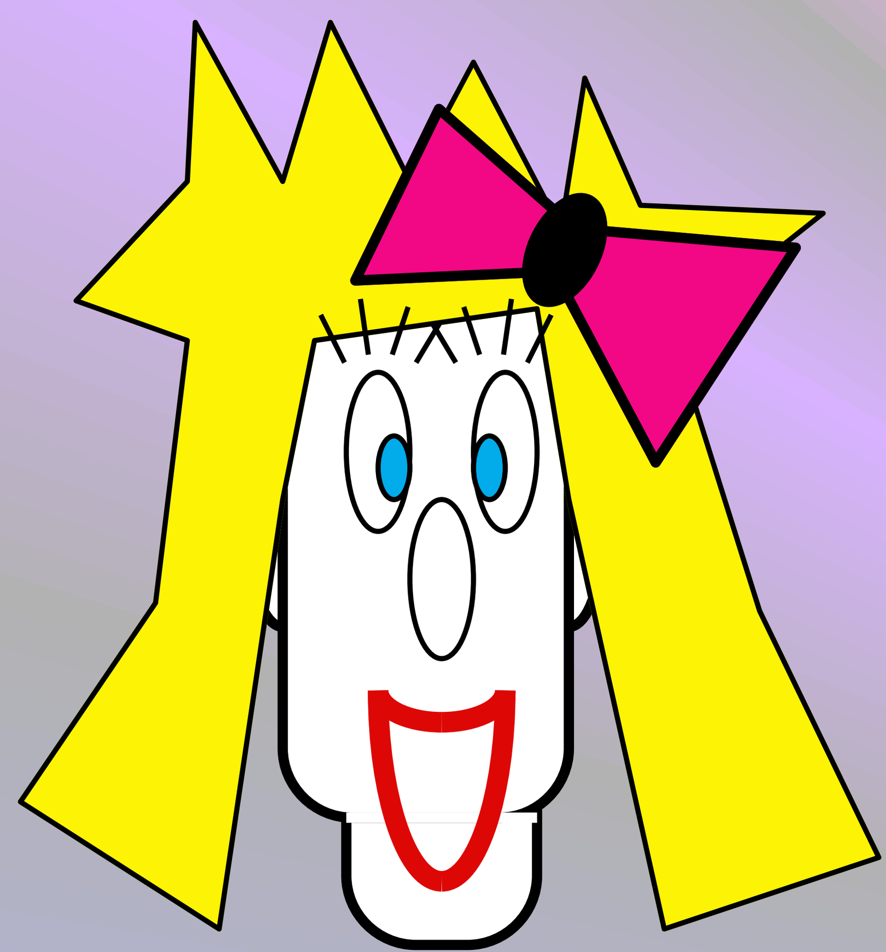


The entire QIP hieracrhy

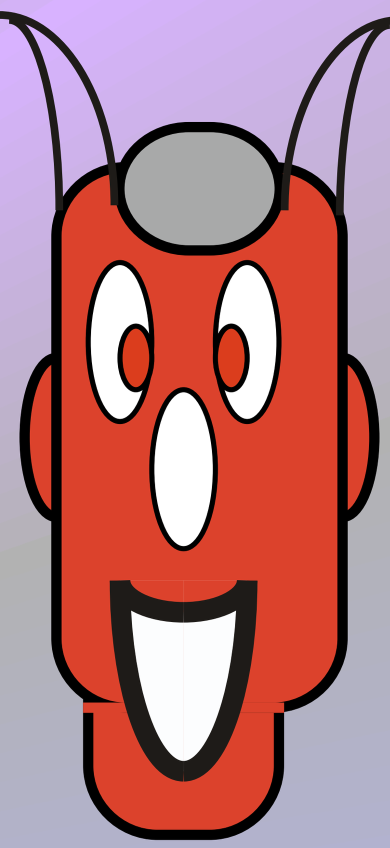
[Watrous et al]

Zero-Knowledge

Zero-Knowledge

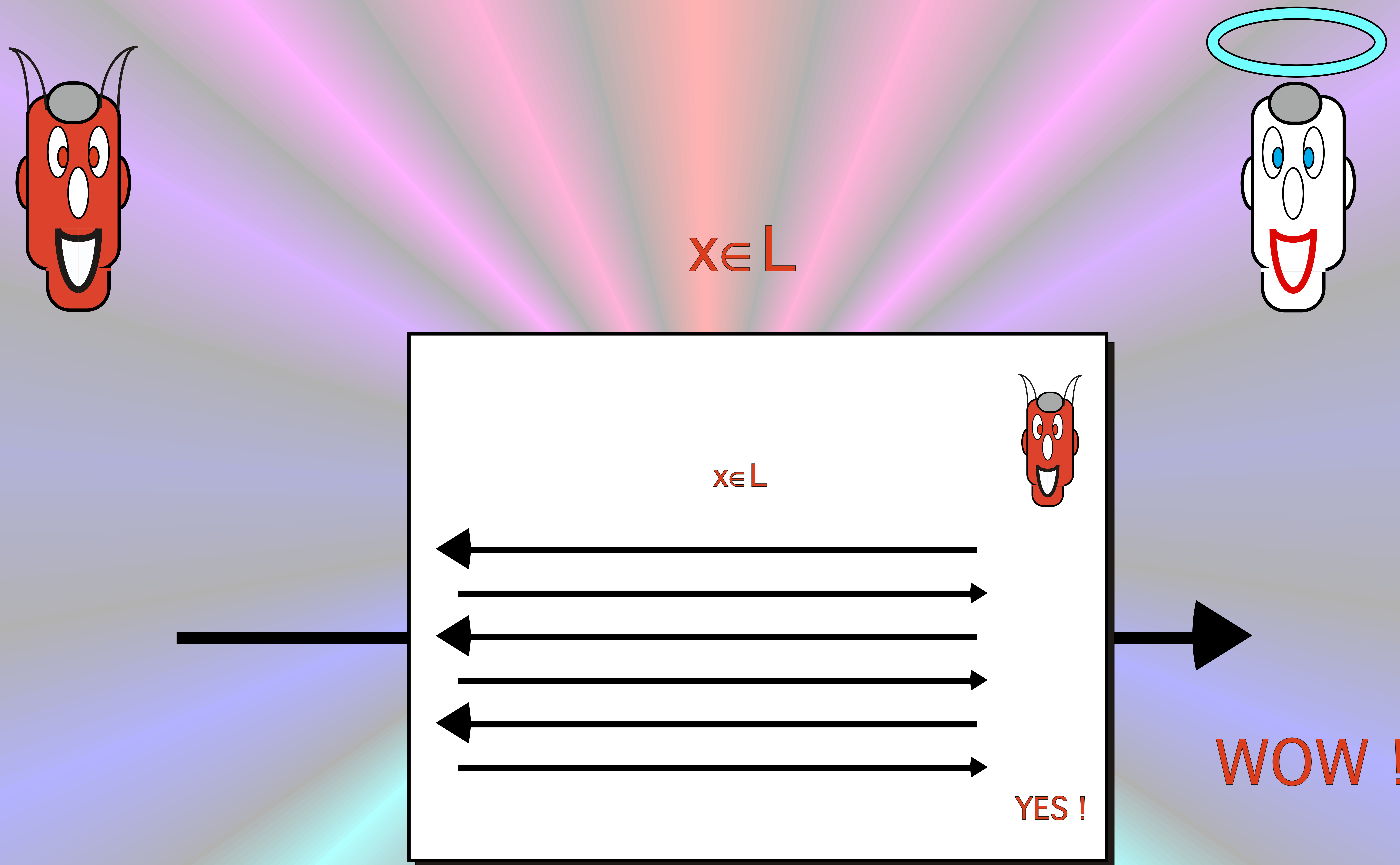


$x \in L$



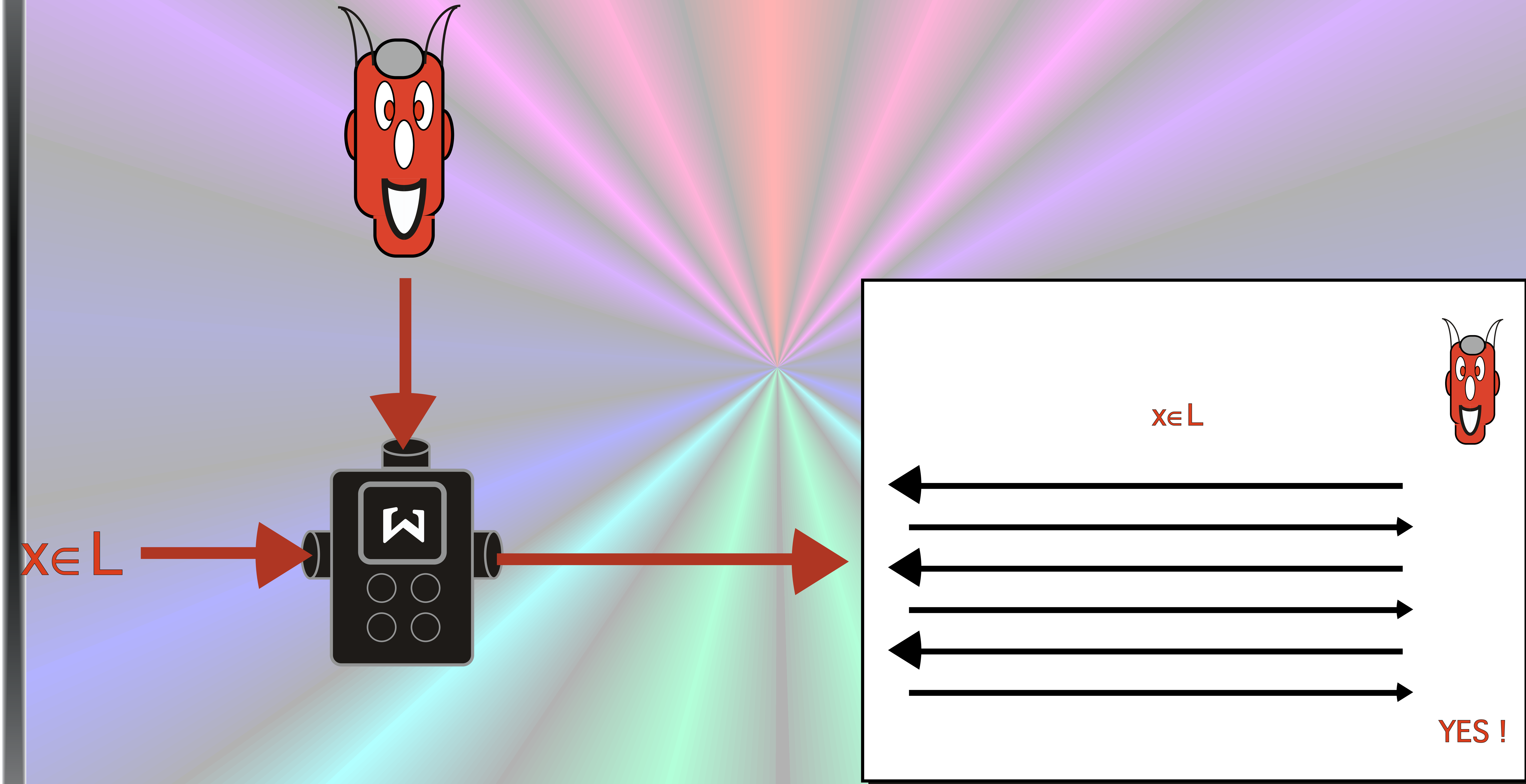
YES !

Zero-Knowledge

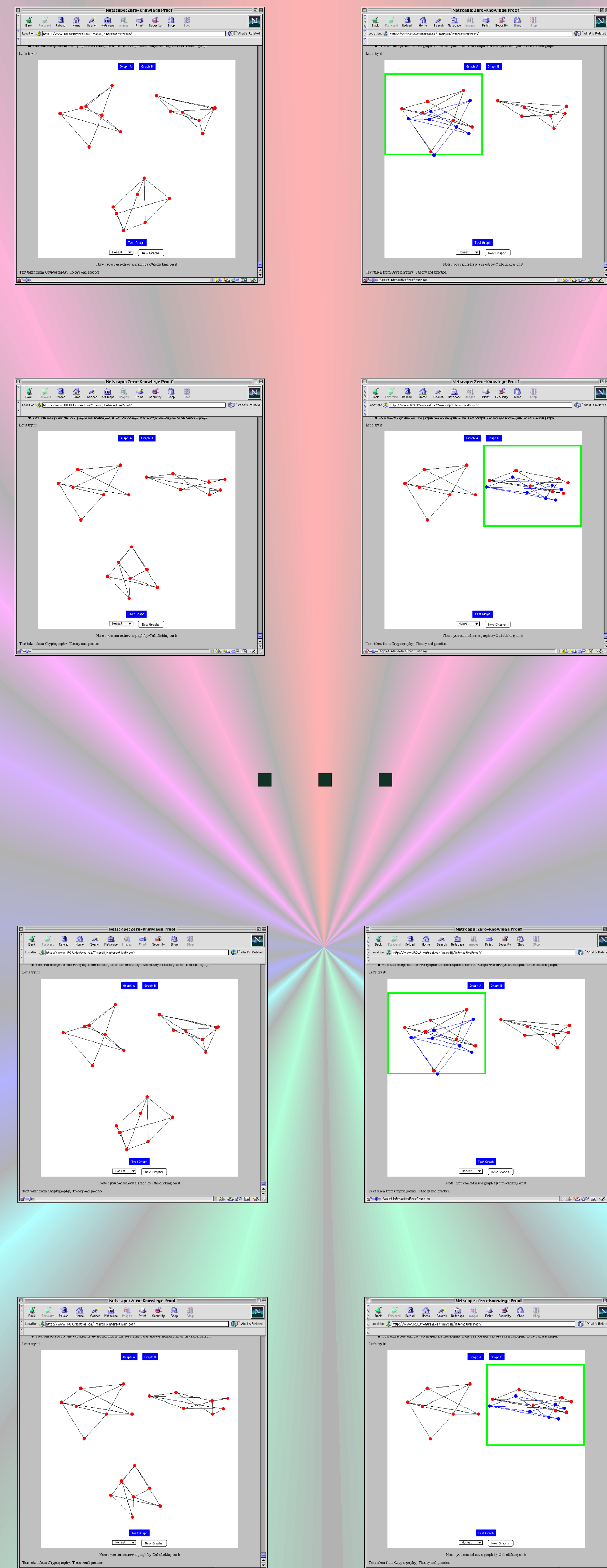


Transferability of a proof.

Zero-Knowledge and Simulator

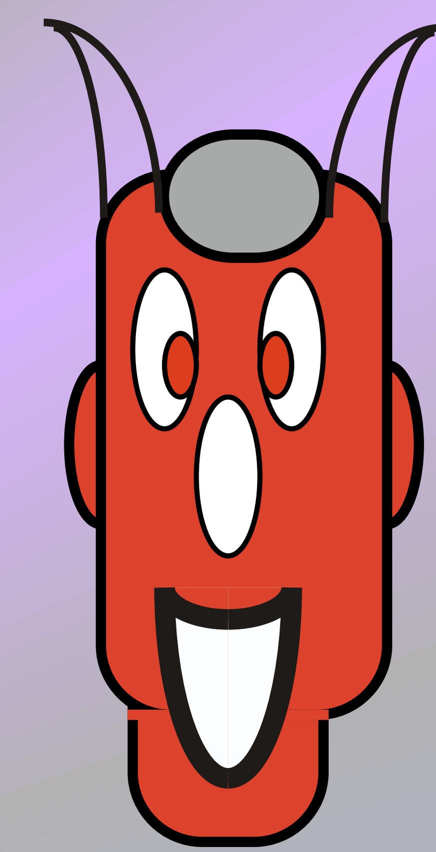


$$\forall D\ \exists S\ \forall x\in L \quad \text{view}[A,D](x) = S(x)$$



$$\forall D\ \exists S\ \forall x \in L\quad \text{view}[A, D](x) = S(x)$$

Zero-Knowledge and Simulator



$(G_0,G_1) \in ISO$

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

b

$G := \pi_0(G_b)$

G

c

if b = c

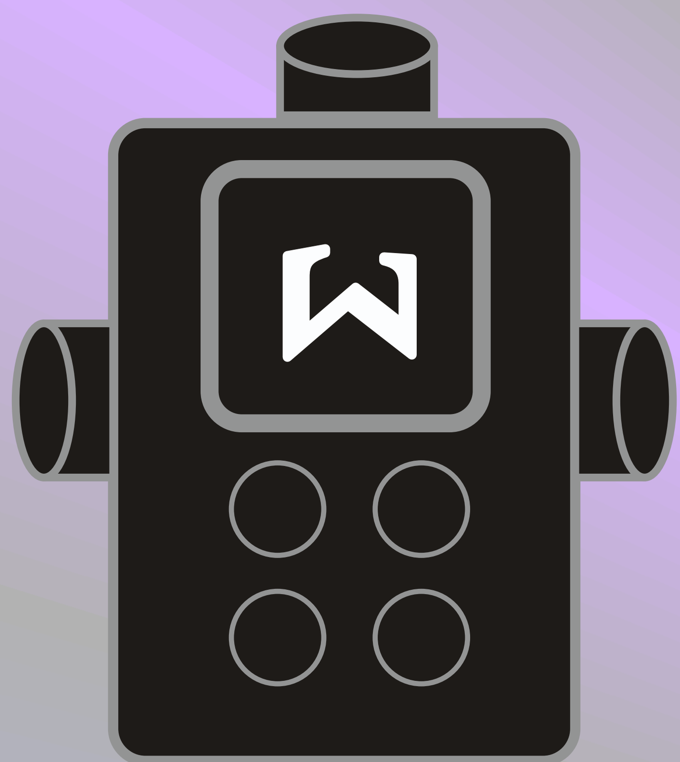
$\rho = \pi_0$

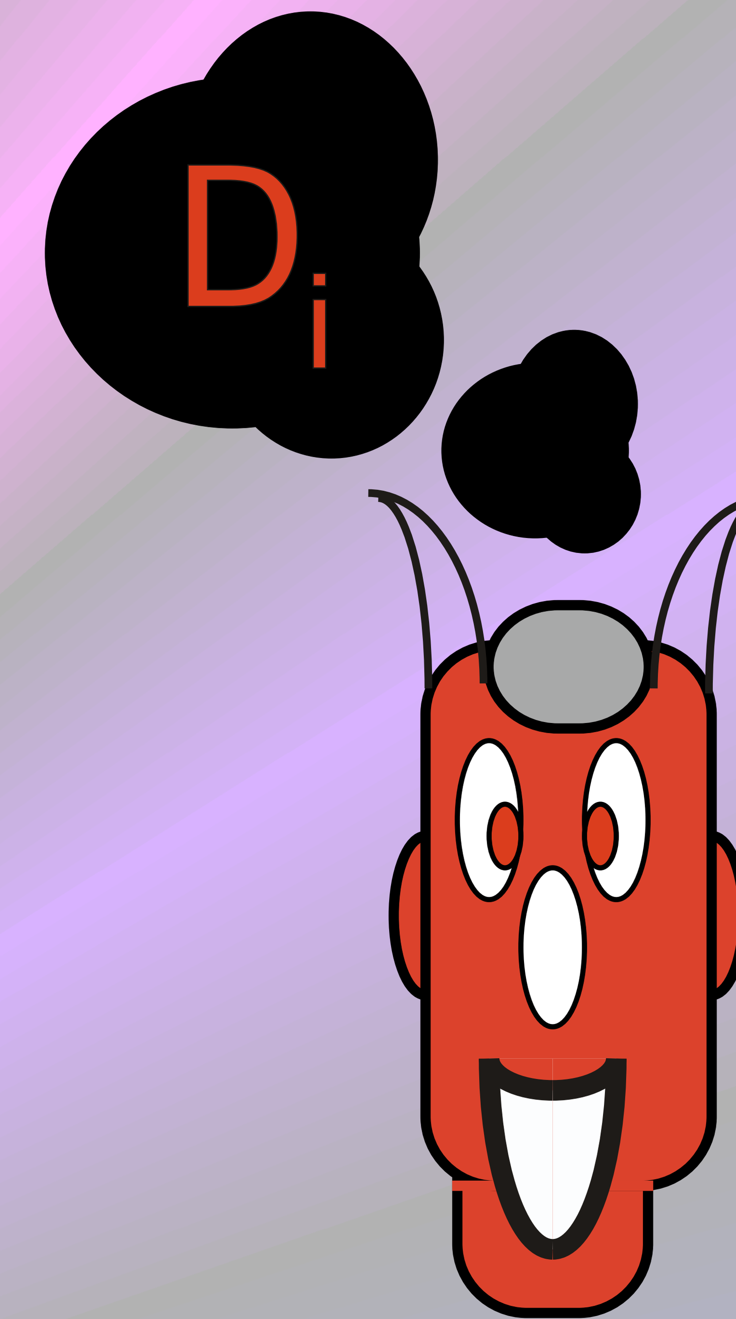
then proceed

else restart

$\forall D\ \exists S\ \forall x \in L\ \ \text{view}[A, D](x) = S(x)$

the rewinding paradigm





REPEAT k TIMES

$(G_0,G_1) \in ISO$

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

D_i: b_i

$G_i := \pi_i(G_{bi})$

G_i →

← c_i

$\rho=\pi_i$ →

if $b_i = c_i$

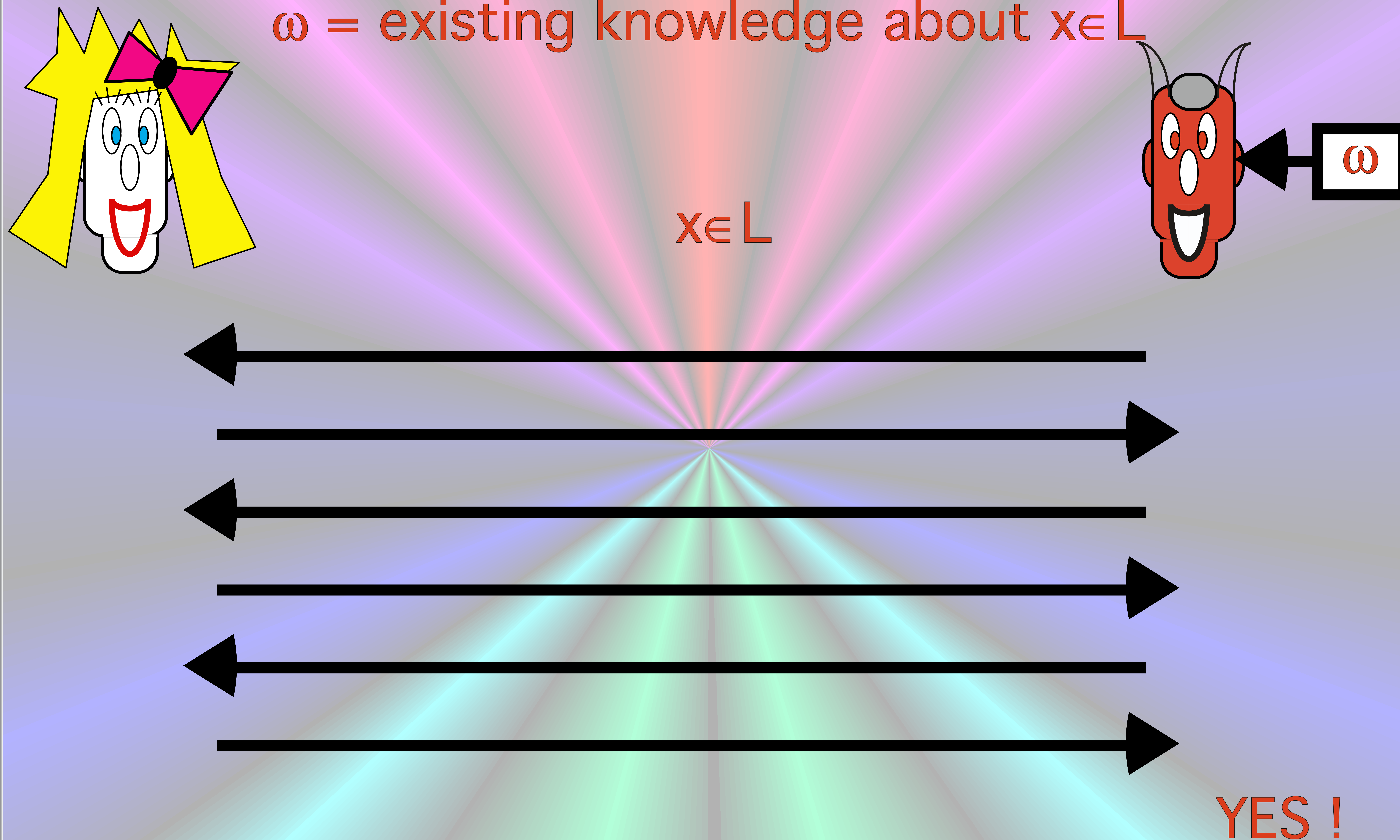
then proceed

else rewind to D_i

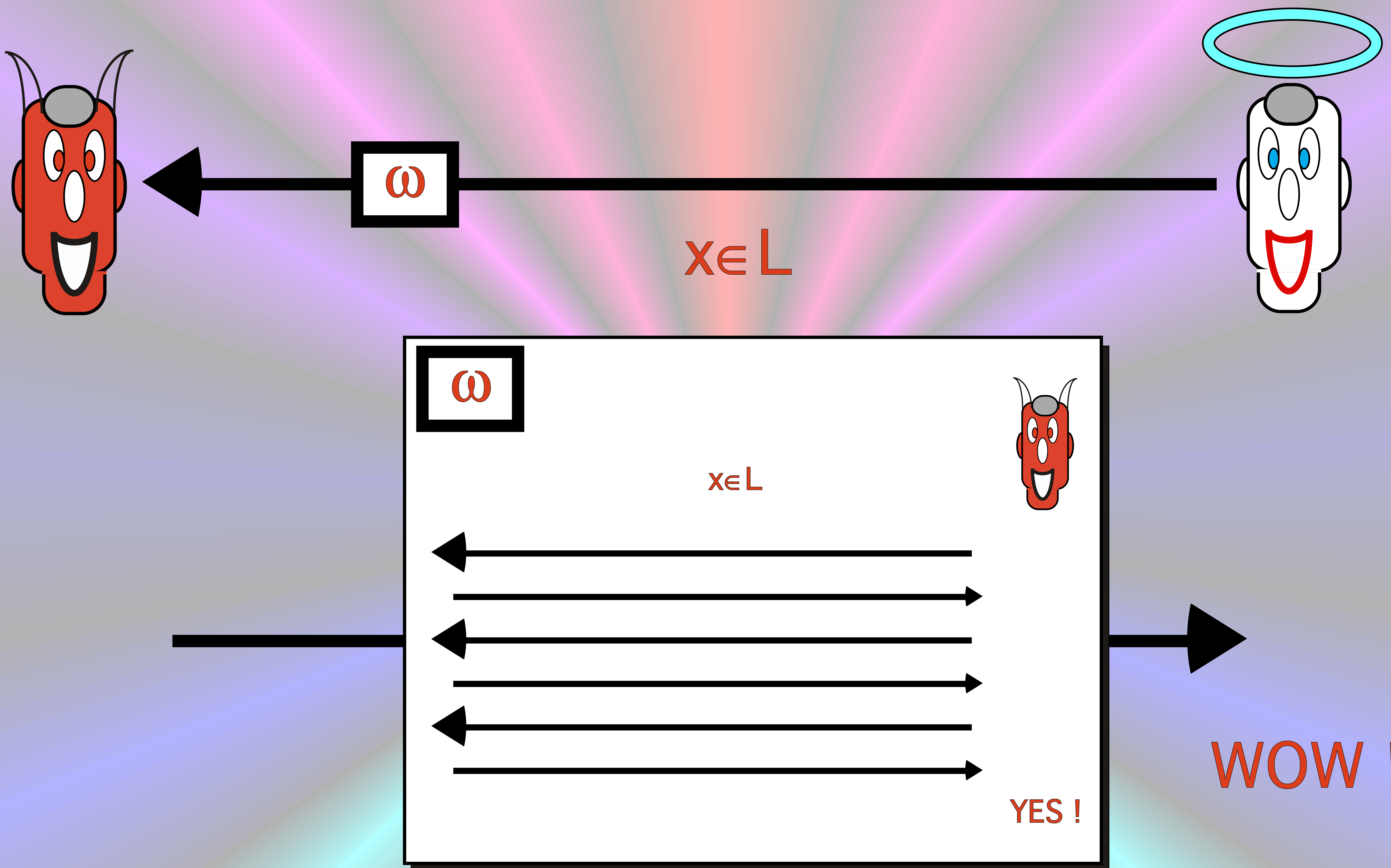
$\forall D\ \exists S\ \forall x\in L\ \ \text{view}[A,D](x) = S(x)$

Auxiliary Input Zero-Knowledge

ω = existing knowledge about $x \in L$

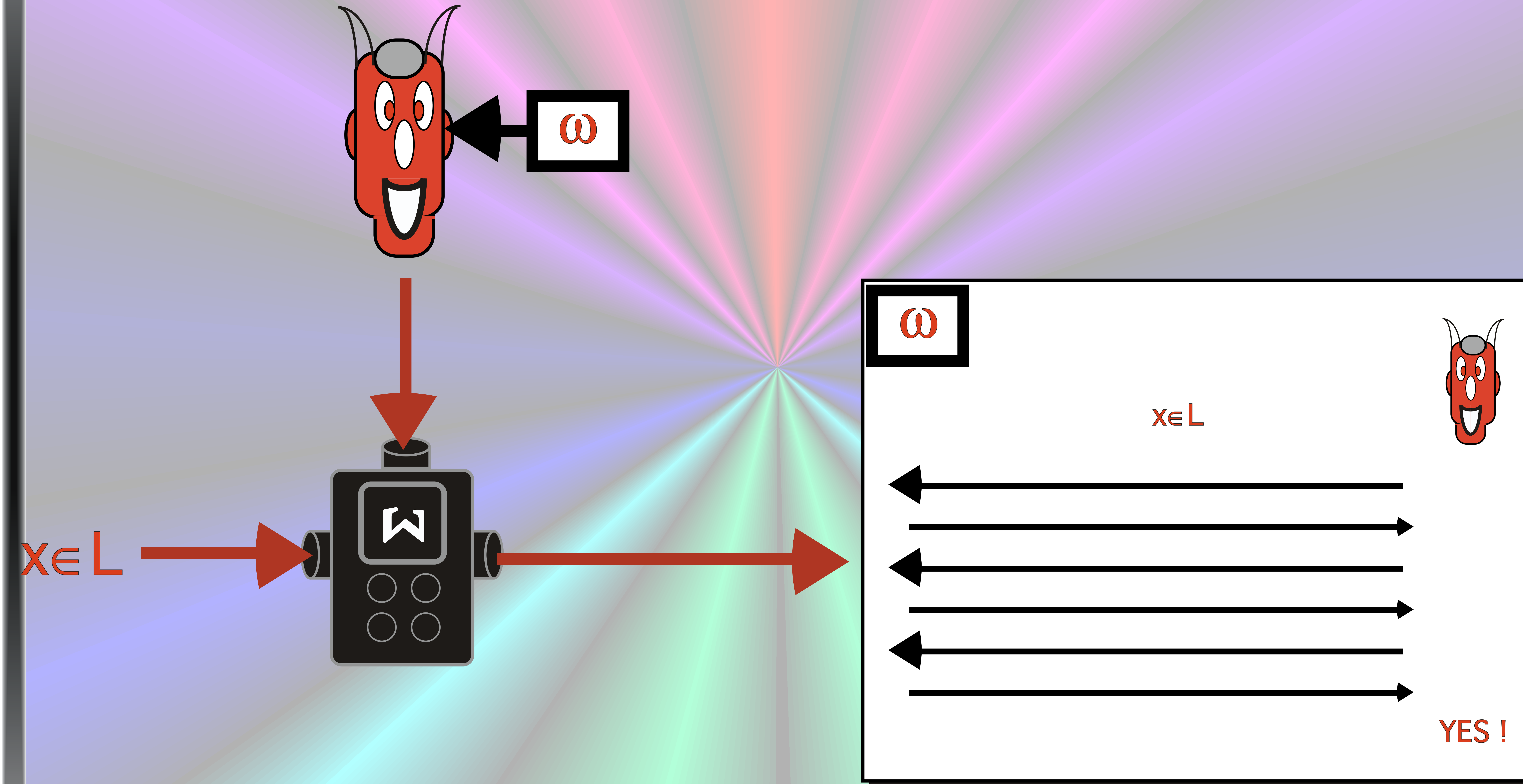


Auxiliary Input Zero-Knowledge



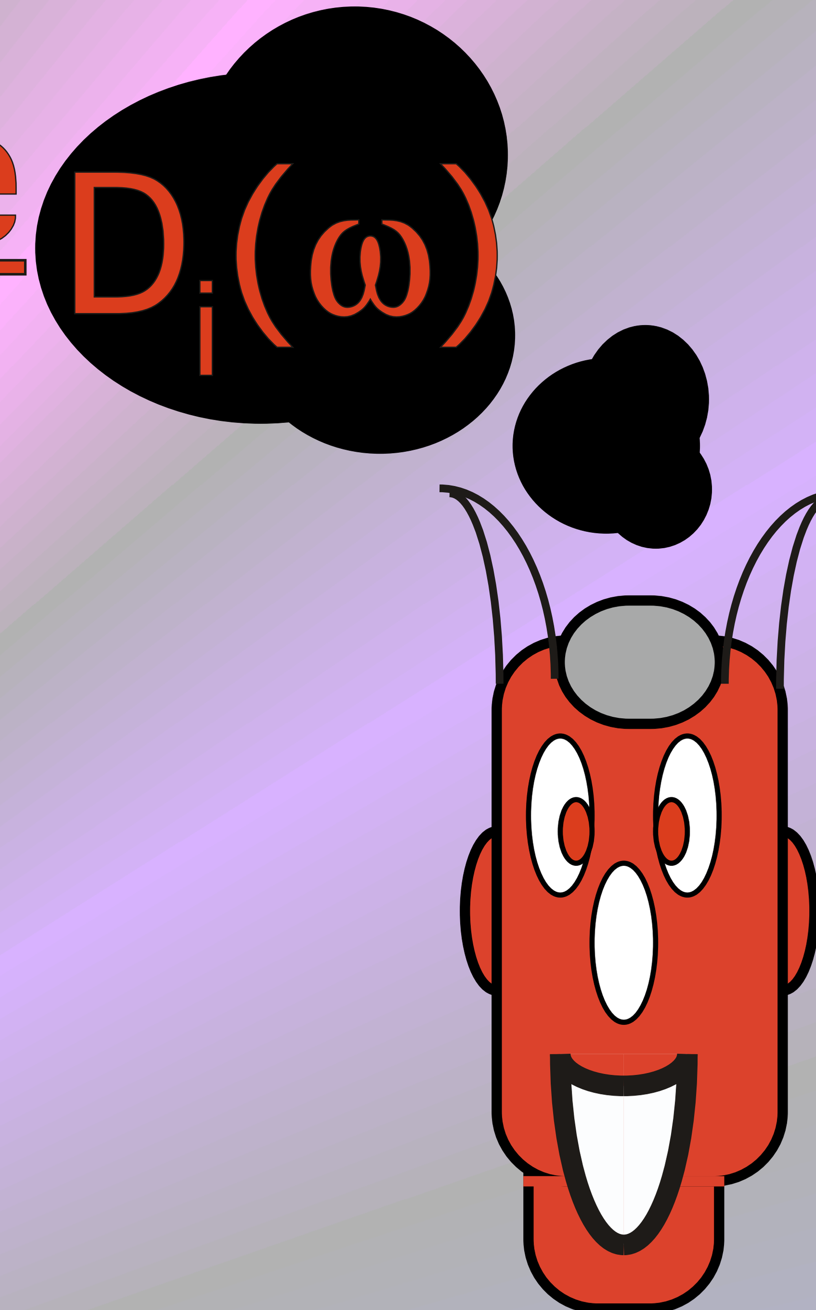
Contextual transferability of a proof.

Auxiliary Input Zero-Knowledge



$$\forall D\ \exists S\ \forall x\in L,\omega \quad \mathrm{view}[A,D(\omega)](x) = S(x,\omega)$$

Auxiliary Input Zero-Knowledge



REPEAT k TIMES

$(G_0,G_1)\in ISO$

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

$D_i(\omega)$: b_i

$G_i := \pi_i(G_{b_i})$

G_i →

← c_i

$\rho=\pi_i$ →

if $b_i = c_i$

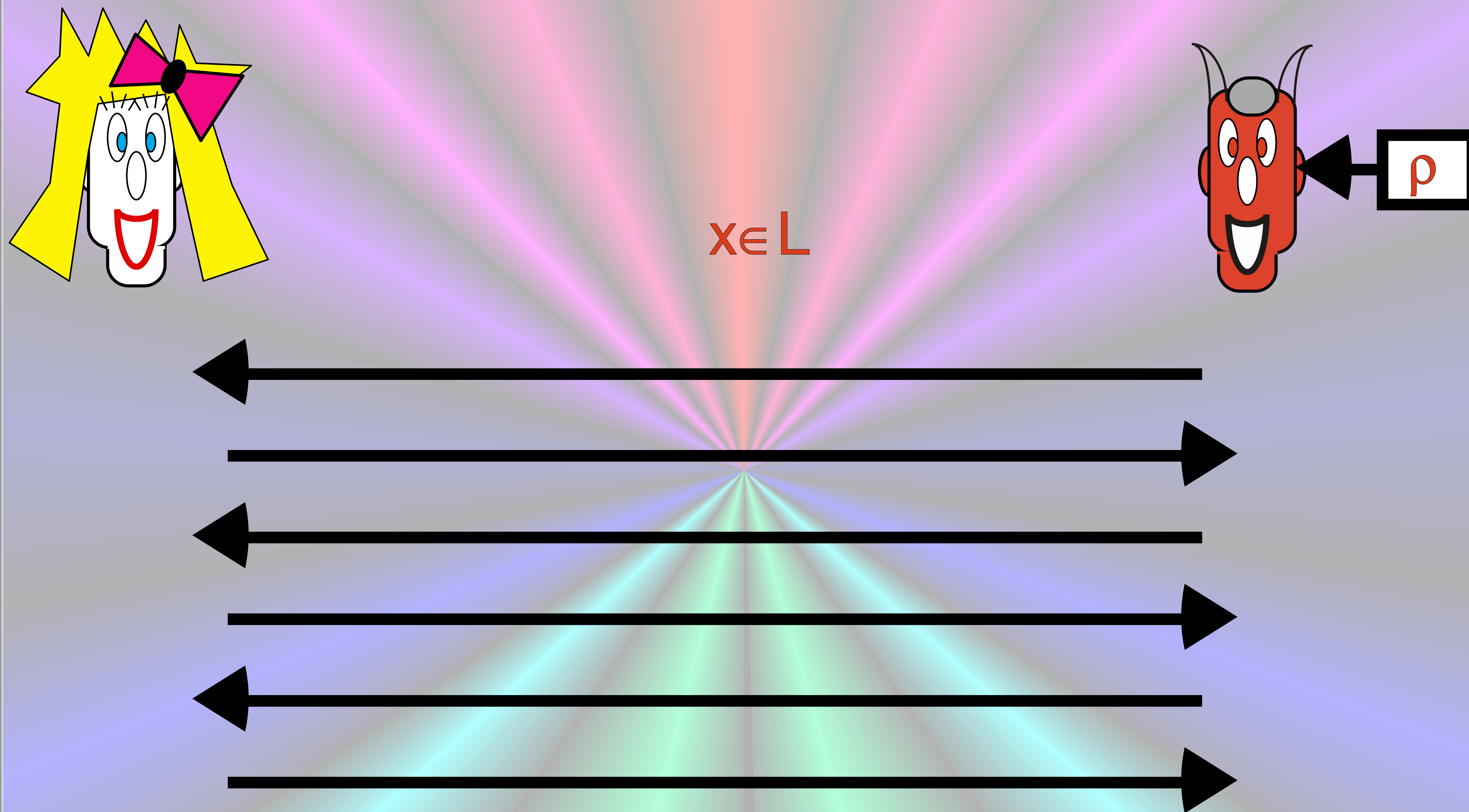
then proceed

else rewind to $D_i(\omega)$

$\forall D\ \exists S\ \forall x\in L,\omega\quad \text{view}[A,D(\omega)](x) = S(x,\omega)$

Quantum Zero-Knowledge

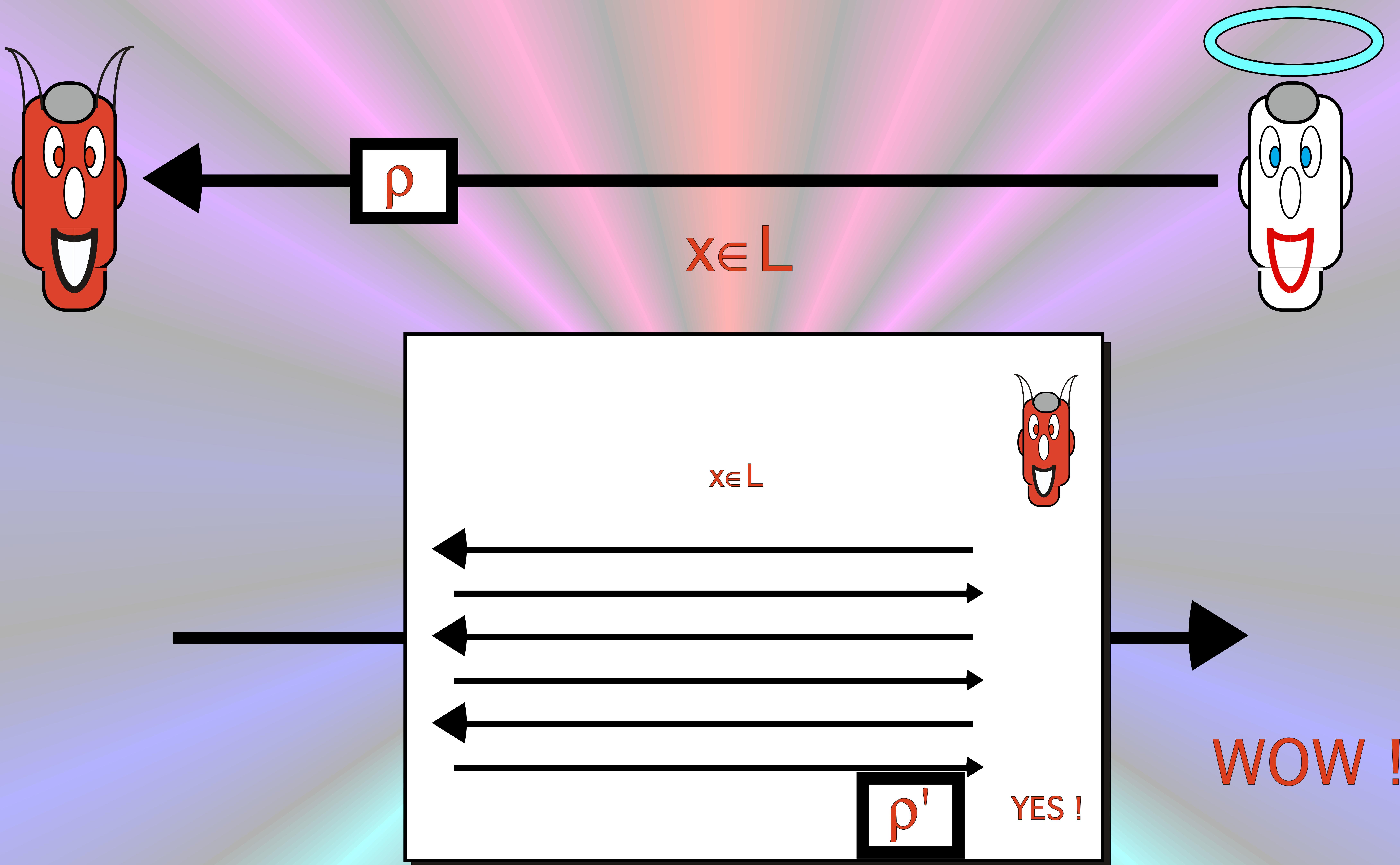
Auxiliary Q-Input Zero-Knowledge



YES !

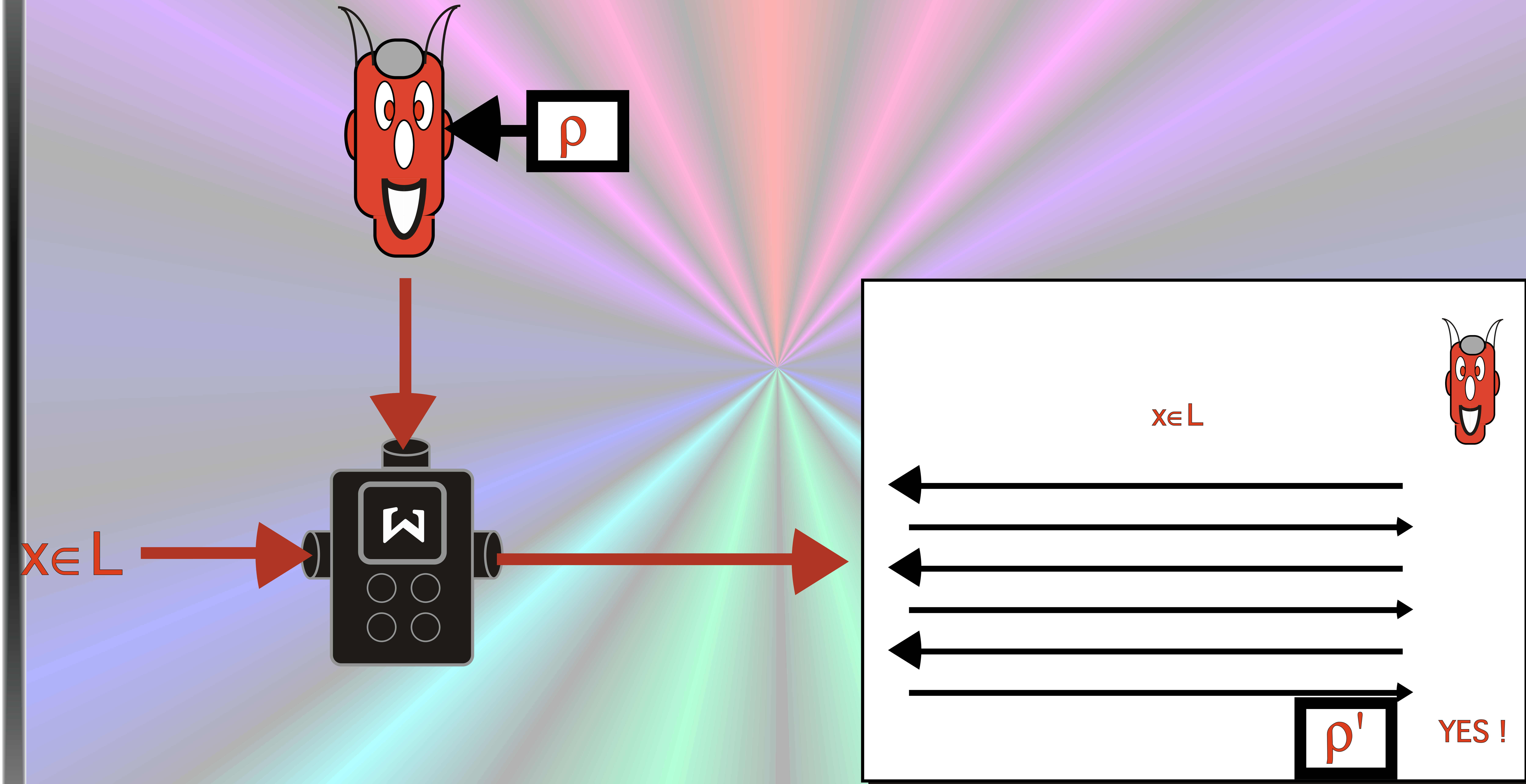
Leftover Q-input: $\boxed{\rho'}$

Auxiliary Q-Input Zero-Knowledge



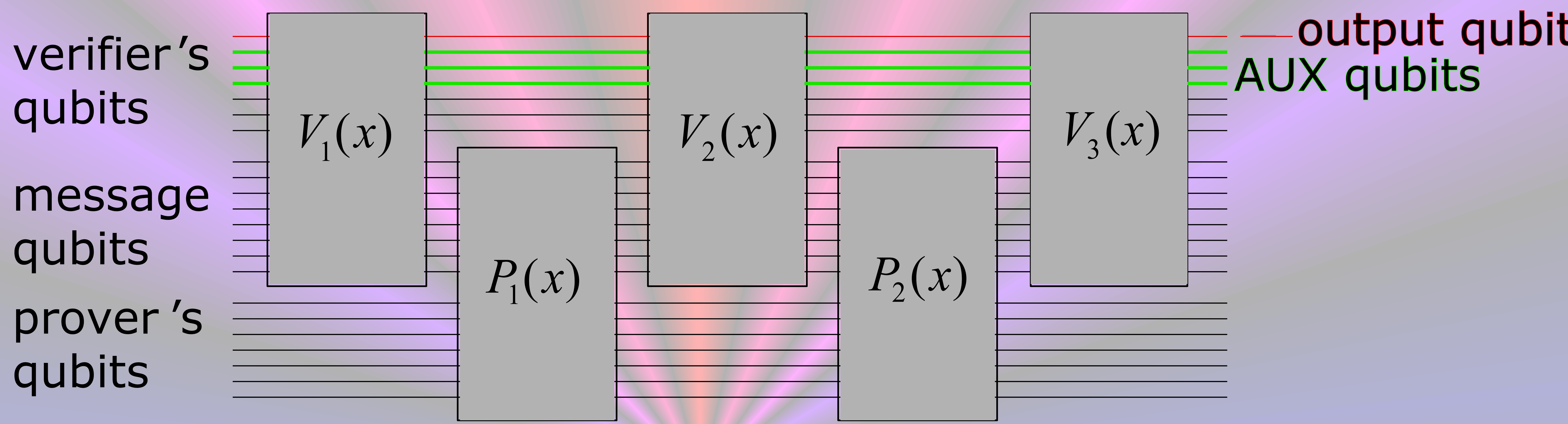
Quantum-Contextual transferability of a proof.

Auxiliary Q-Input Zero-Knowledge

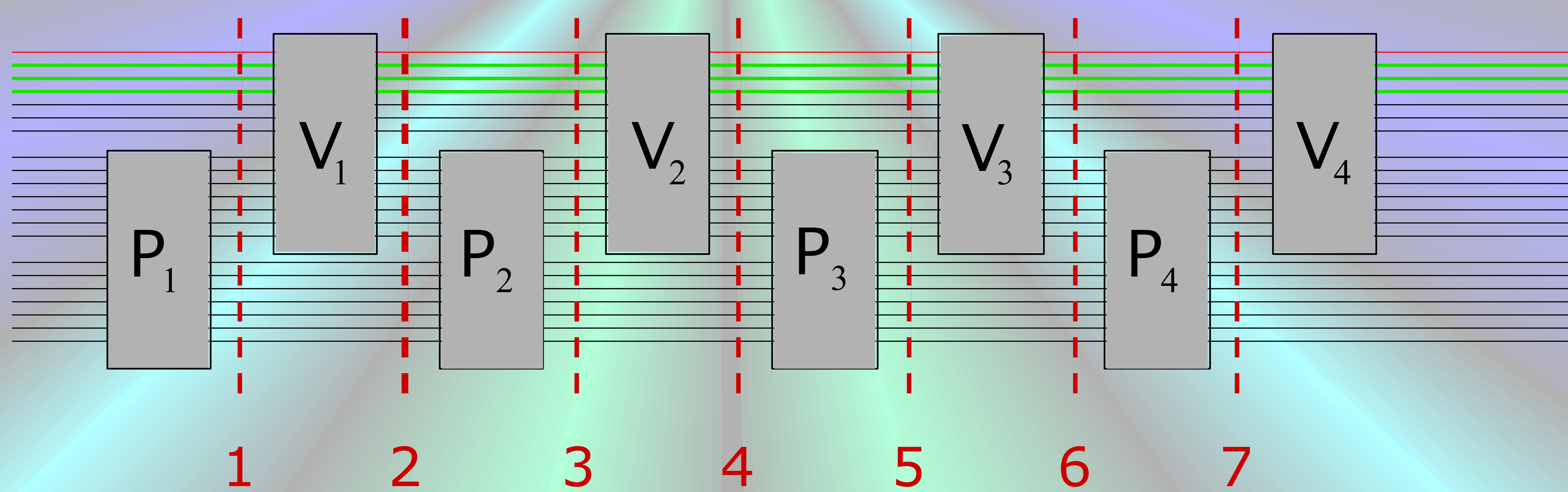


$$\forall D\ \exists S\ \forall x \in L, \rho \quad view[A, D(\rho)](x) = S(x, \rho)$$

Quantum Zero-Knowledge: Formalizing the Model



messages:



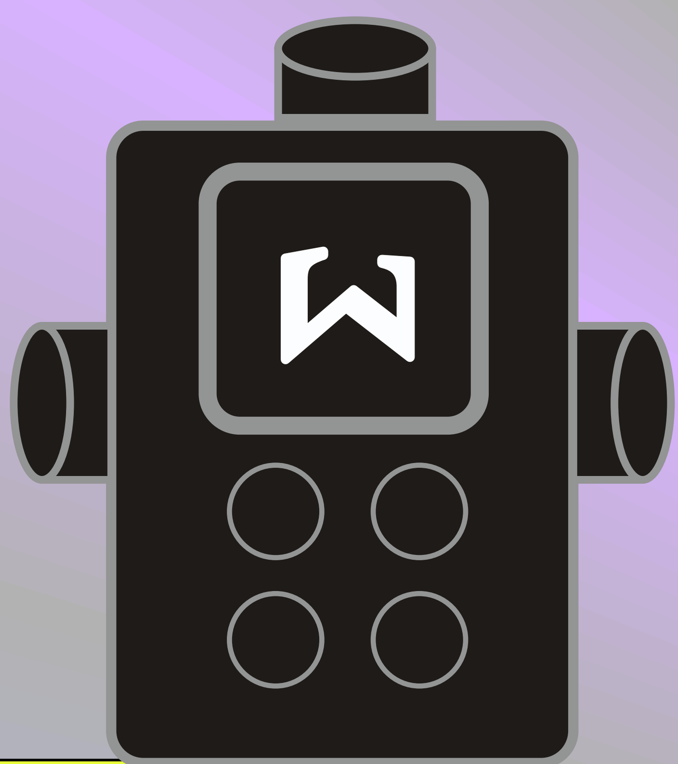
Auxiliary Q-Input Zero-Knowledge

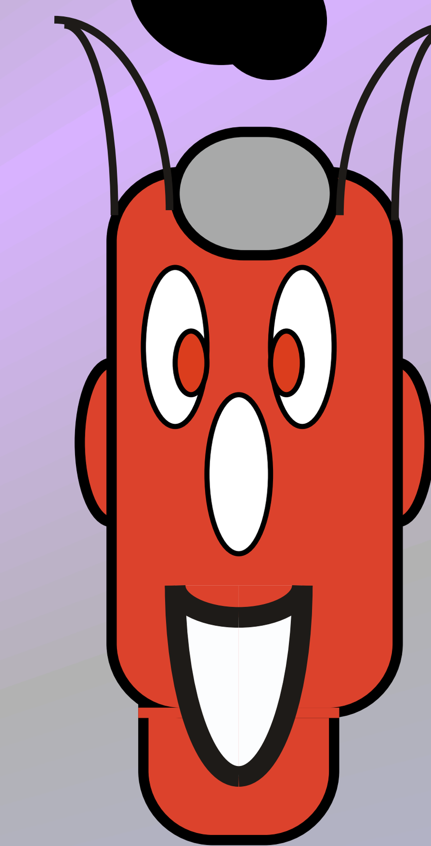
$\forall D\ \exists S\ \forall x \in L\ \forall \rho\ \forall i \in poly(|x|)\ view[P, D(\rho)](x,i) = S(\rho, x, i)$

Auxiliary Q-Input Zero-Knowledge

$D_i(\rho)$

REPEAT k TIMES





$(G_0,G_1)\in ISO$

$(G_0=\pi(G_1))$

$D_i(\rho)$: b_i

$G_i := \pi_i(G_{bi})$

G_i

c_i

$\rho=\pi_i$

if $b_i = c_i$

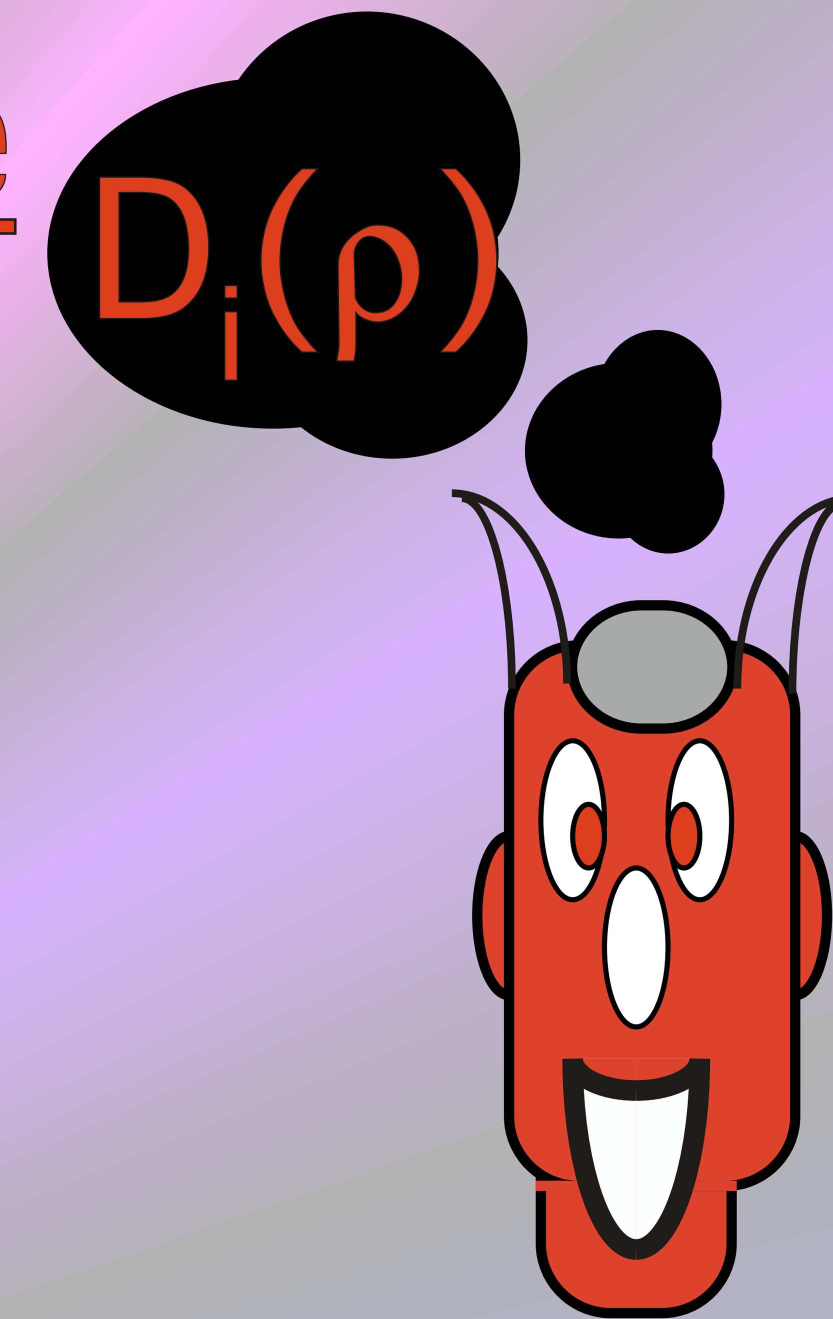
then proceed

else rewind to $D_i(\rho)$

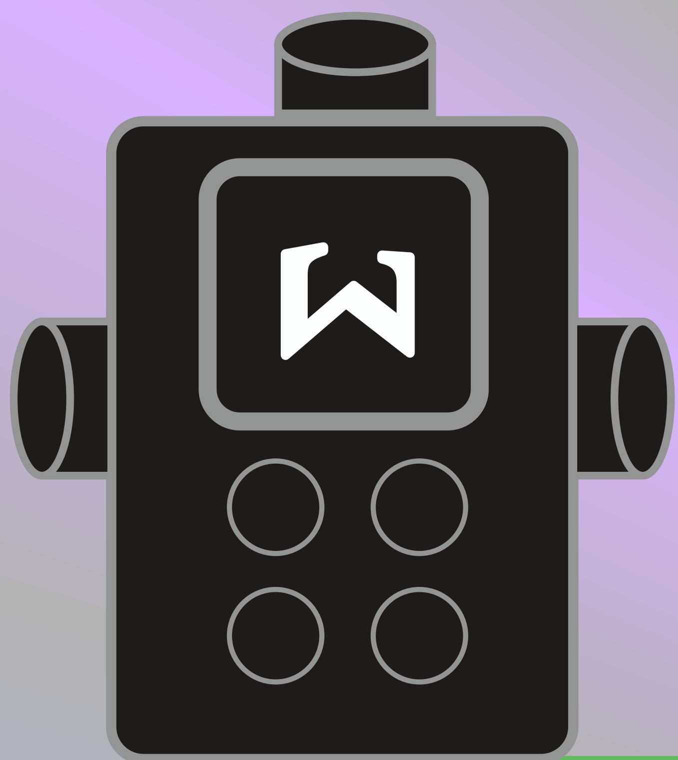
$\forall D\ \exists S\ \forall x\in L\ \forall \rho\ \forall i\in poly(|x|)\ view[A,D(\rho)](x,i) = S(\rho,x,i)$

[Watrous]

Auxiliary Q-Input Zero-Knowledge



REPEAT k TIMES



$(G_0,G_1)\in ISO$

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

$b_i = |0\rangle+|1\rangle$

$G_i := \pi_i(G_{bi})$

G_i →

← $c_i = |0\rangle+|1\rangle$

if $b_i = c_i$ → $\rho=\pi_i$

without measuring b_i nor c_i...

then proceed you may now measure b_i and c_i...

else Apply transformation so that $b_i=c_i$!!!

$\forall D\ \exists S\ \forall x\in L\ \forall\rho\ \forall i\in poly(|x|)\ view[A,D(\rho)](x,i) = S(\rho,x,i)$

ISO∈QZK

etc

Conclusions

- Auxiliary Q-Input Zero-Knowledge is possible
- Natural ZK languages: Non-ISO & Cie ?

Quantum Zero-Knowledge

Claude Crépeau

School of Computer Science
McGill University

joint work with
J. van de Graaf and A. Smith

Quantum Zero-Knowledge

Claude Crépeau

School of Computer Science
McGill University

joint work with
J. van de Graaf and A. Smith