Rational Proofs with Multiple Provers

Jing Chen, **Samuel McCauley**, **Shikha Singh**
Department of Computer Science
Stony Brook University

Outline of the Talk

RATIONAL

INTERACTIVE PROOFS

with

MULTI-PROVERs

Interactive Proofs
[GMR, BM 85]

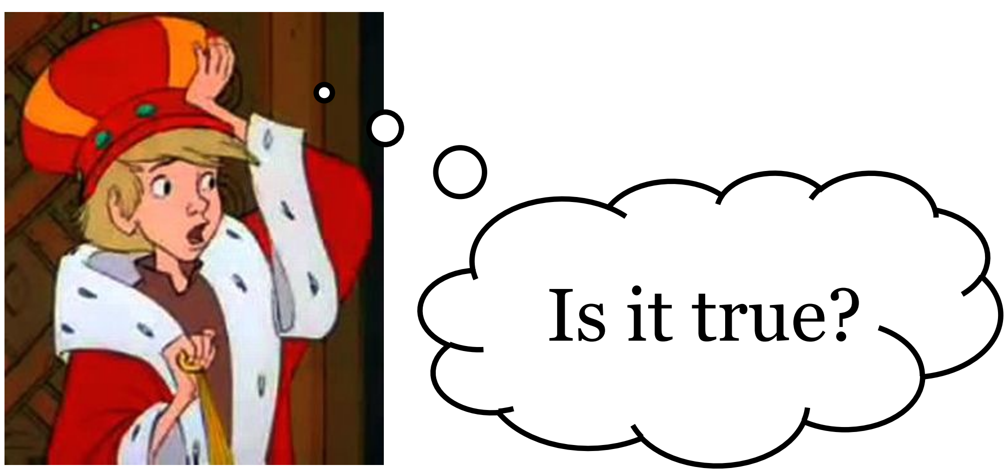
- All-powerful Merlin (Prover) interacts with a polynomial-time, probabilistic Arthur (Verifier)
- IP = PSPACE [Shamir 92]

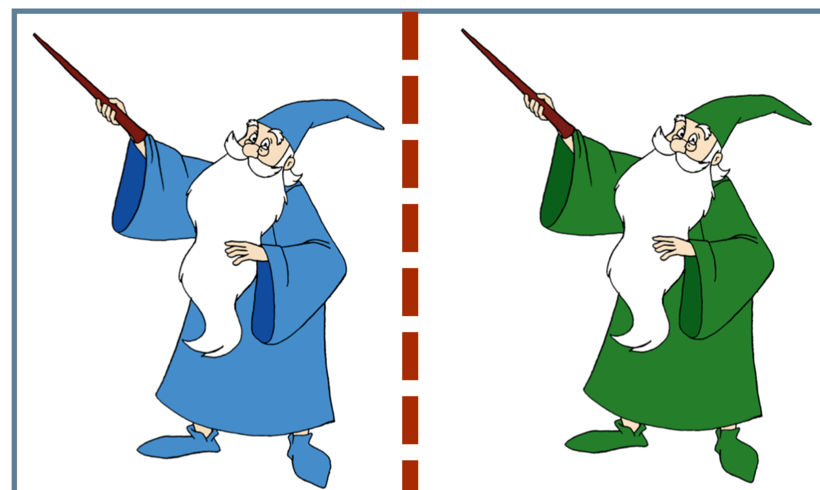
Is it true?

Proof that $x \in L$

Multi-Prover Interactive Proofs
[BGKW 88]

- Provers work together to convince the verifier
- Once protocol begins, provers cannot communicate
- MIP = NEXP [BFL 90]





Proof that $x \in L$

Classical Interactive Proofs

- Merlin can be arbitrary: dishonest or malicious

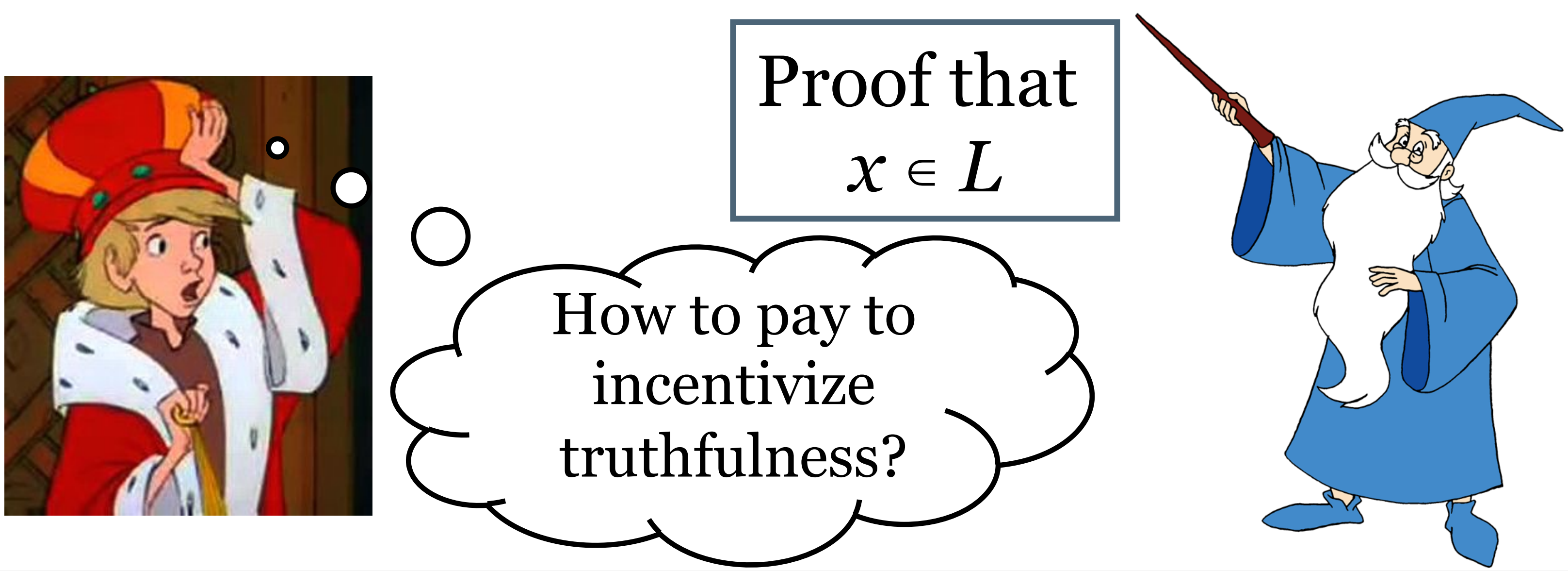
Rational Interactive Proofs
[AM 12]

- Arthur promises Merlin a reward for proving the theorem correctly
- Merlin is rational: he wants to *maximize* this reward

Rational Interactive Proofs

[AM 12]

- Arthur computes the reward based on the transcript and his randomness
- *Correctness* is ensured by Merlin's rationality!



Rational Interactive Proofs
[AM 12]

- Lead to simple and efficient protocols
- Constant rounds: RIP is more powerful
- Polynomial rounds: RIP = IP

Delegation of Computation

- Computation is becoming a commodity
- Should be able to *verify* correctness
- Pay *money* in exchange for services

Google Cloud Platform

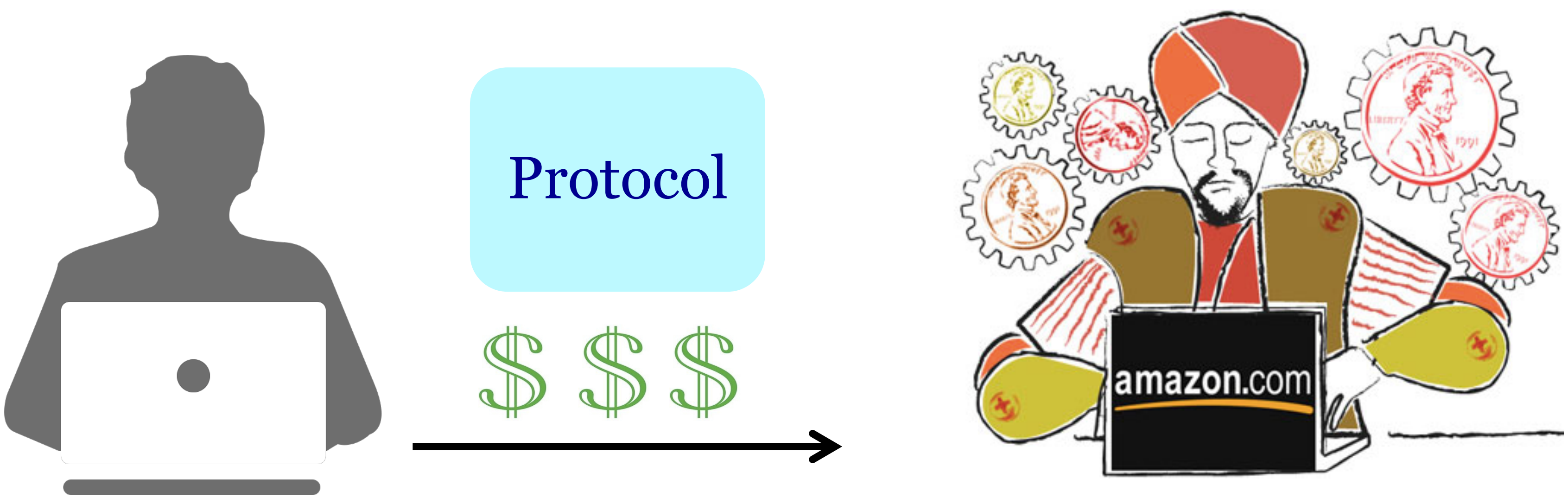
IBM WATSON

Microsoft Azure

amazon web services™ | EC2

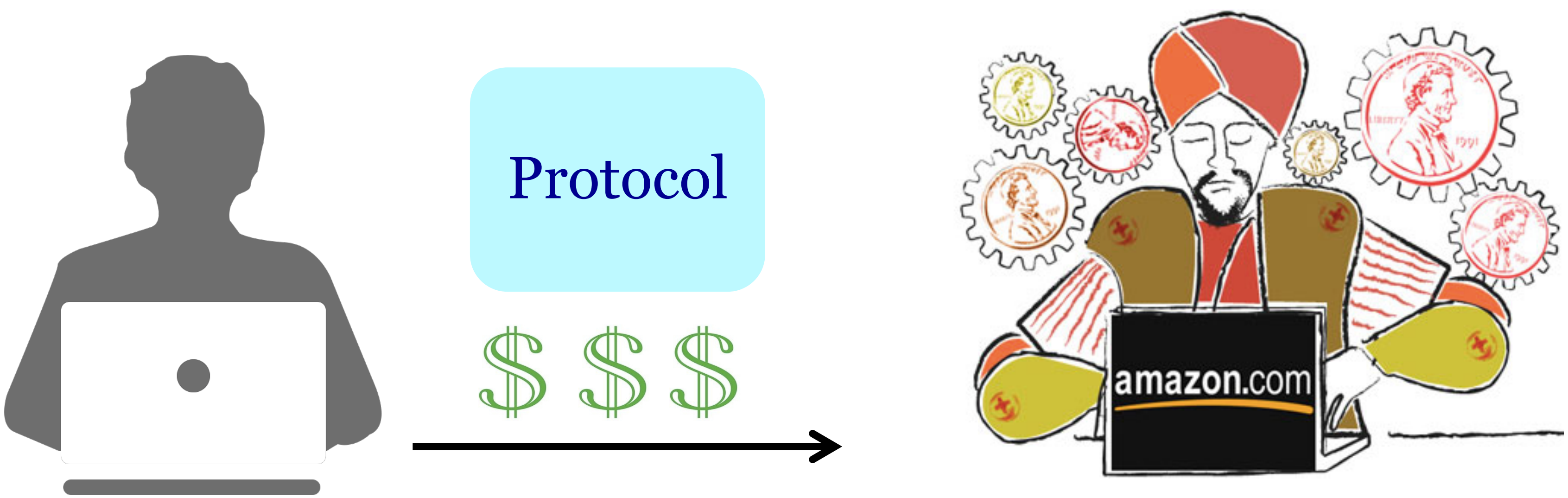
Delegation of Computation

- *Super-efficient* rational proofs [AM 13, GHRV 14, ZB 14, GHRV 16], IP for Muggles [GKR 08]



Delegation of Computation

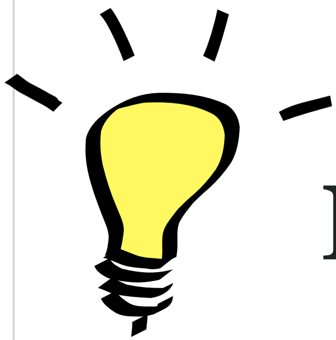
- *Super-efficient* rational proofs [AM 13, GHRV 14, ZB 14, GHRV 16], IP for Muggles [GKR 08]
- All existing work involves a single rational prover



what if?

Arthur has two Merlins

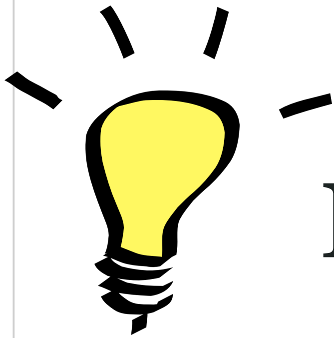
what if?



Arthur has two Merlins

He can crosscheck their answers!

what if?



Arthur has two Merlins

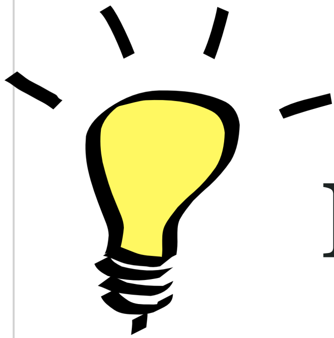
He can crosscheck their answers!

In classical interactive proofs, two provers *increase the power* of the system

Multi-prover IP = NEXP BFL 91

IP = PSPACE Shamir 90

what if?



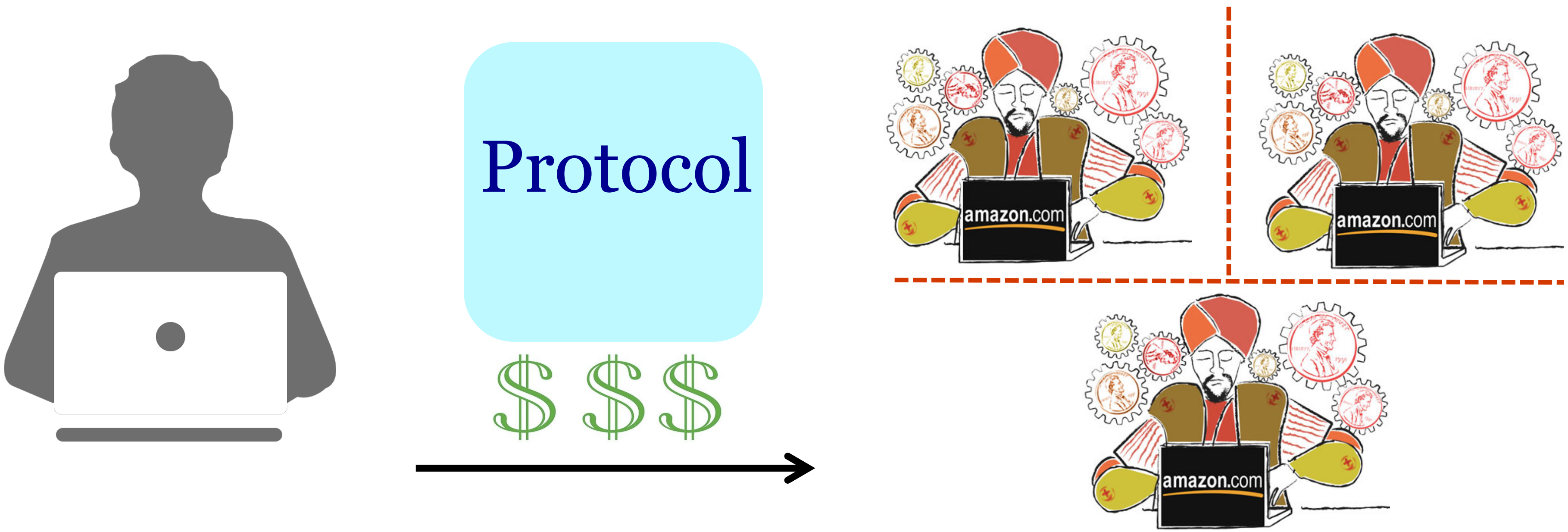
Arthur has two Merlins

He can crosscheck their answers!

"Are multiple Merlins more powerful than one in rational proofs?" - AM 12

We introduce: MRIP

Multi-Prover Rational Interactive Proofs



Multi-Prover Rational Interactive Proofs

- A way to outsource computation to multiple service providers
- A natural extension of RIP and MIP

MRIP: The Model

- Provers can pre-agree on a joint strategy
- They cannot communicate once the protocol begins
- At the end, the verifier computes a total reward
- [Correctness] Any strategy of the provers that maximizes the total reward leads the the verifier to the right answer

Warm Up: MRIP for NEXP

$x \in L$ or $x \notin L$

Warm Up: MRIP for NEXP

$x \in L$ or $x \notin L$

If claim $x \in L$

Warm Up: MRIP for NEXP

$x \in L$ or $x \notin L$ ←

If claim $x \in L$ —Y→ Accept

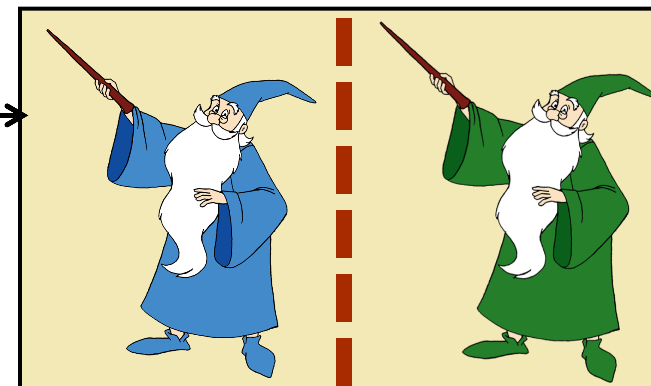
Warm Up: MRIP for NEXP

$x \in L$ or $x \notin L$

If claim $x \in L$

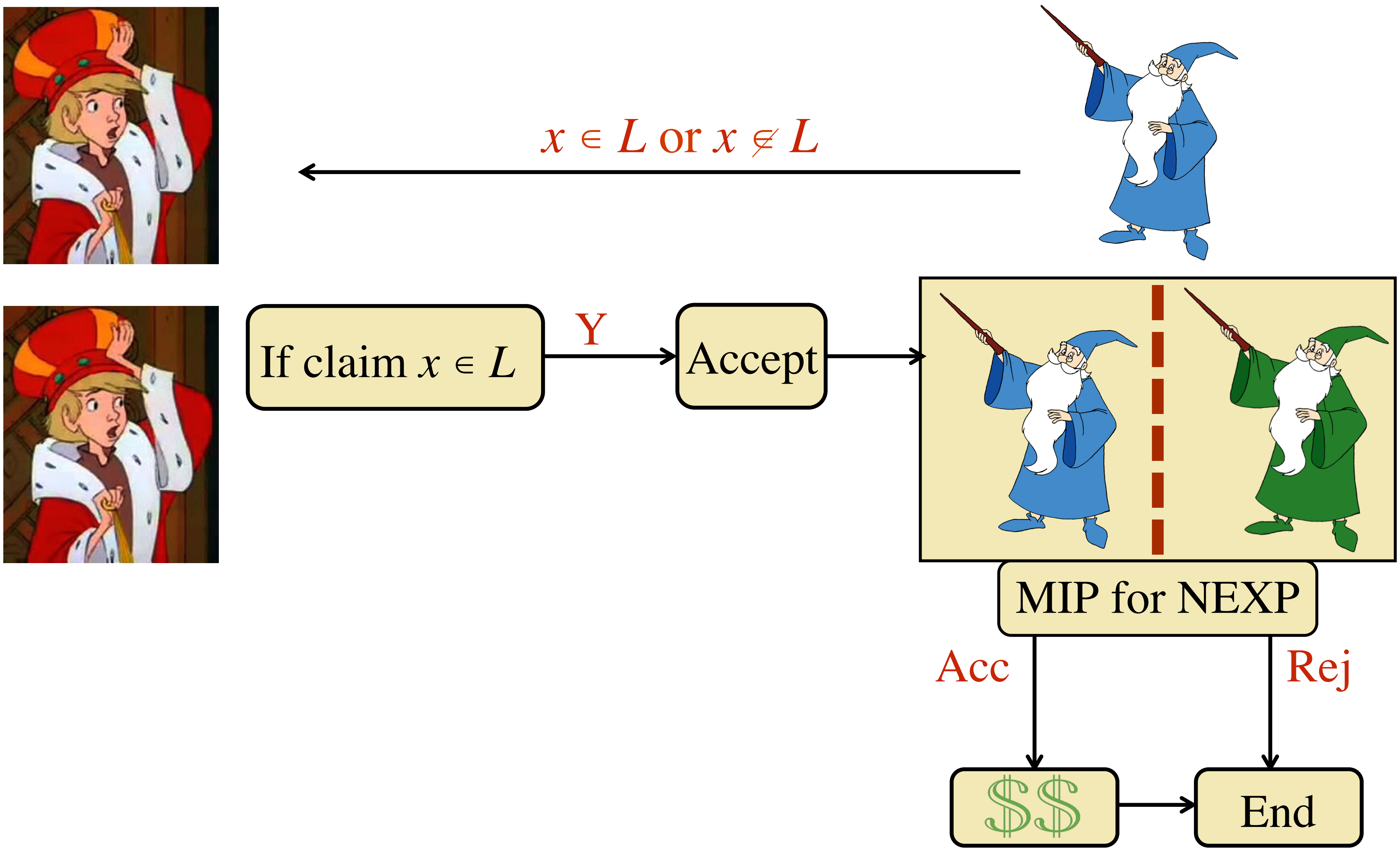
Y

Accept

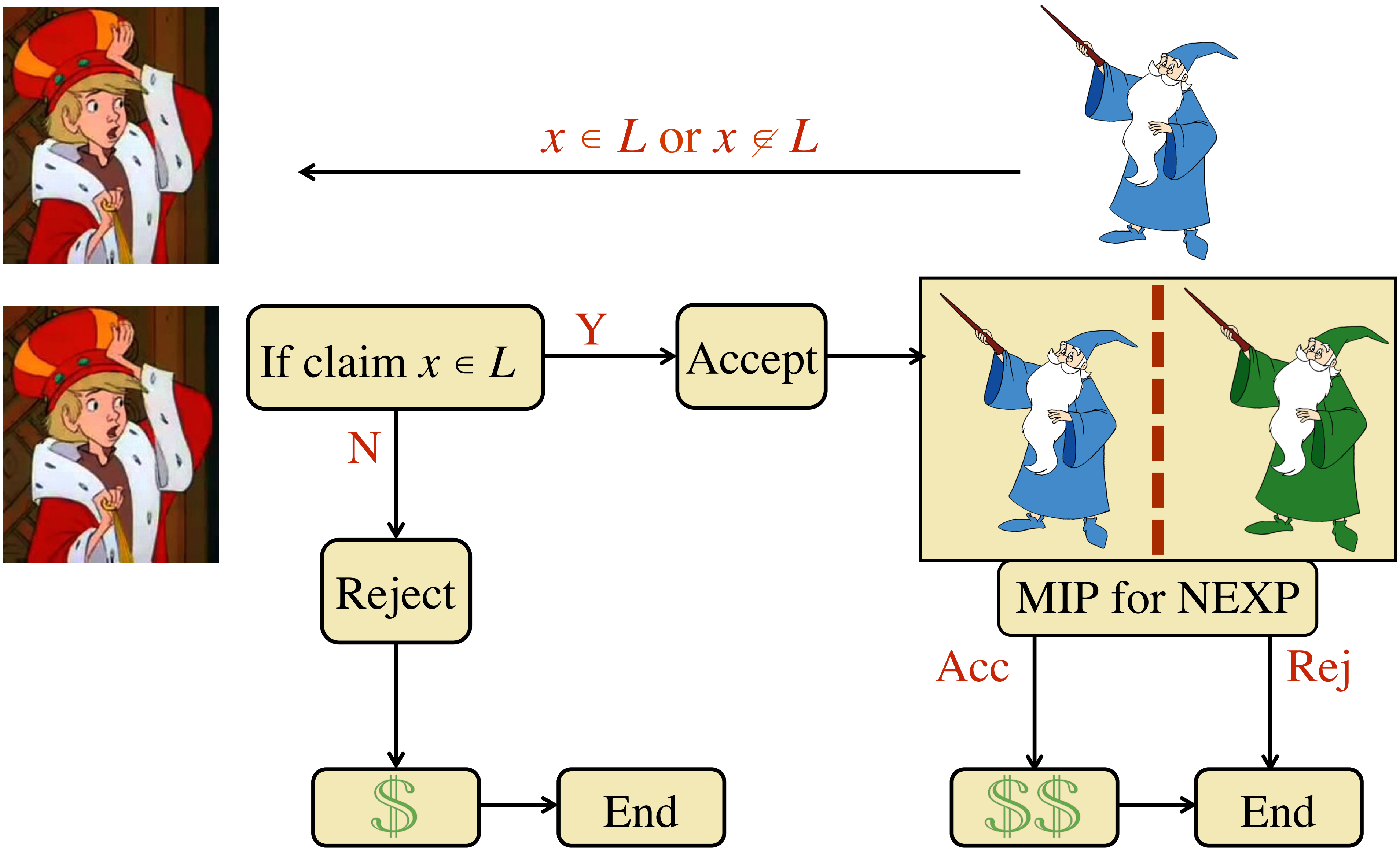


MIP for NEXP

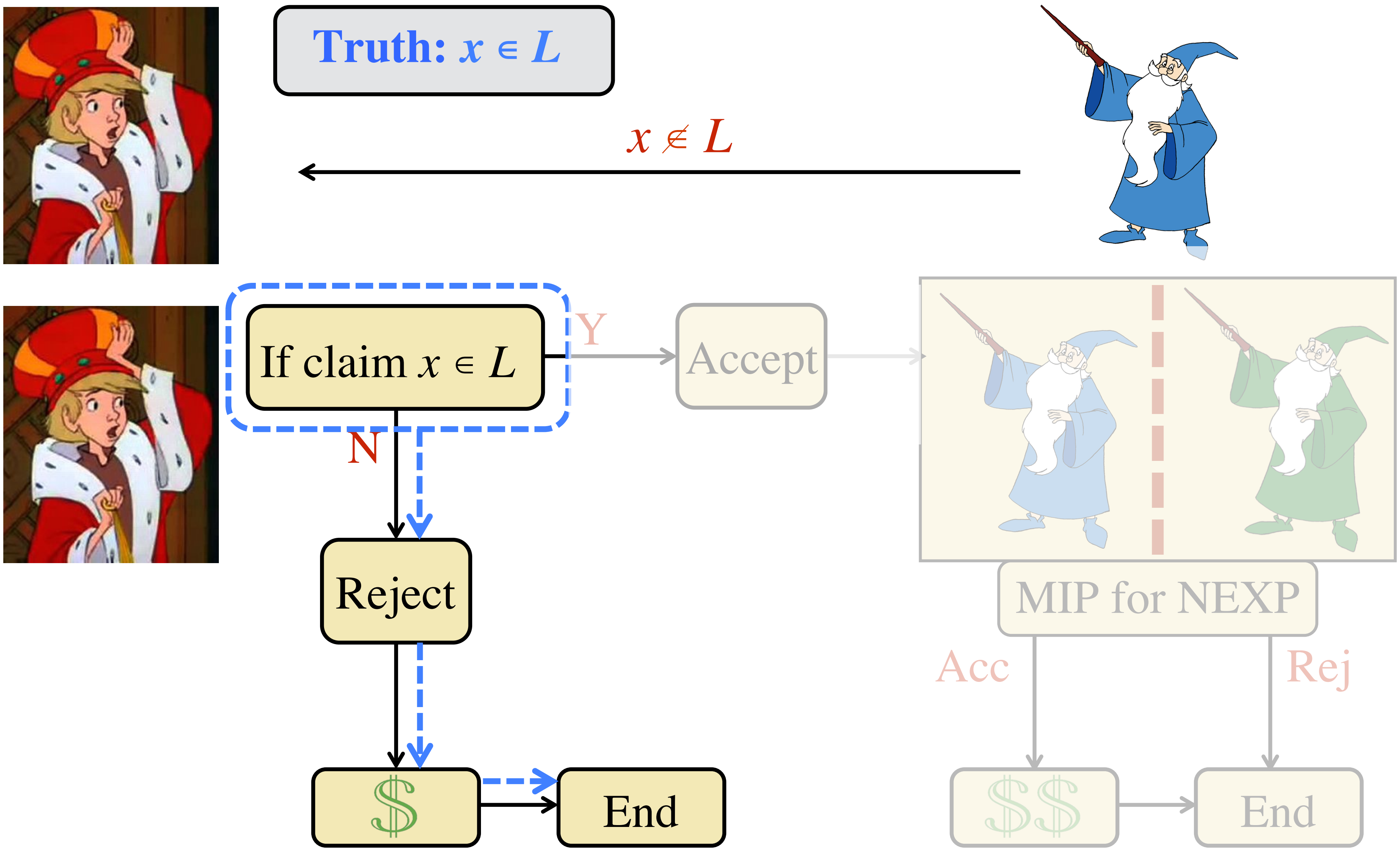
Warm Up: MRIP for NEXP



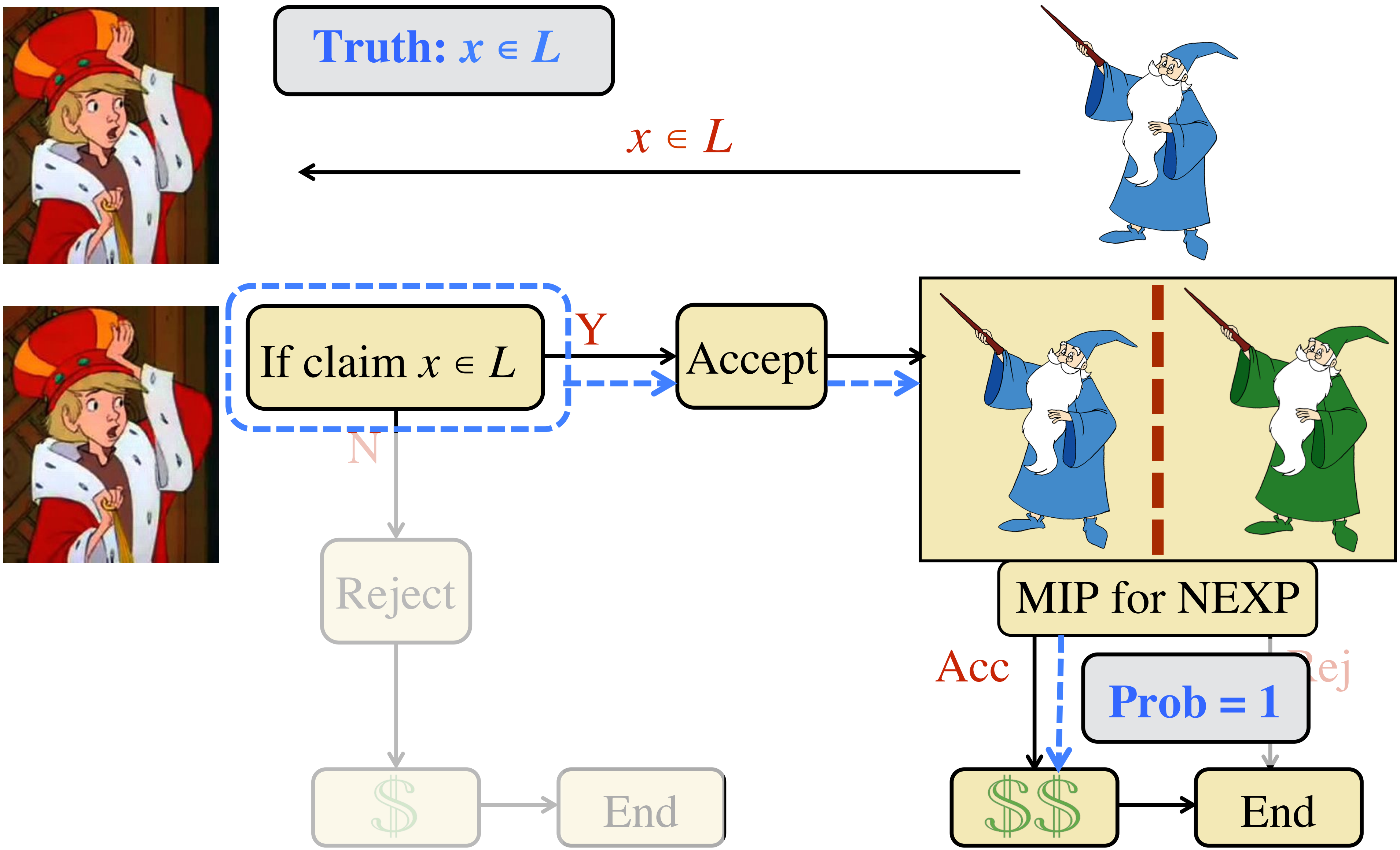
Warm Up: MRIP for NEXP



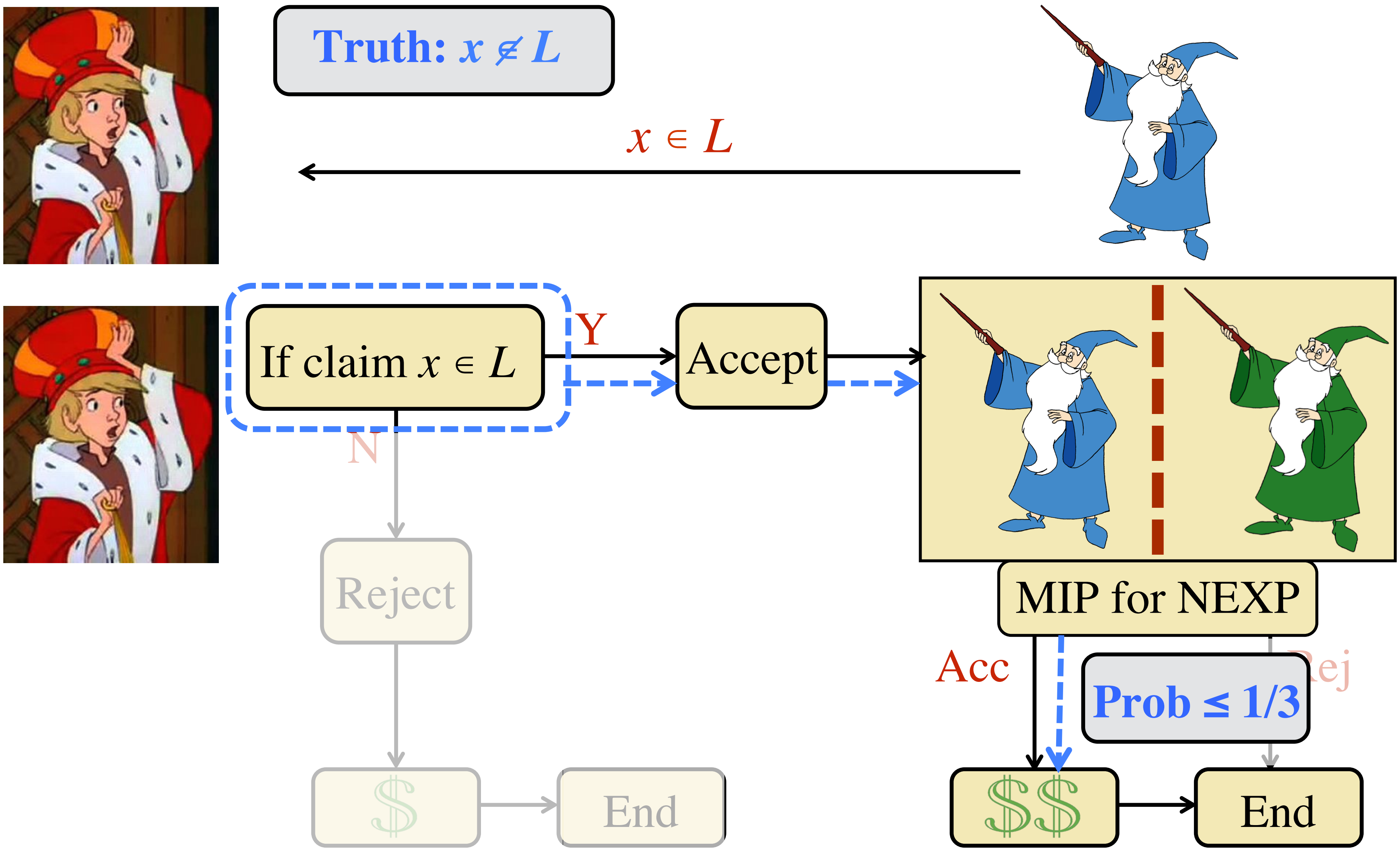
Warm Up: MRIP for NEXP



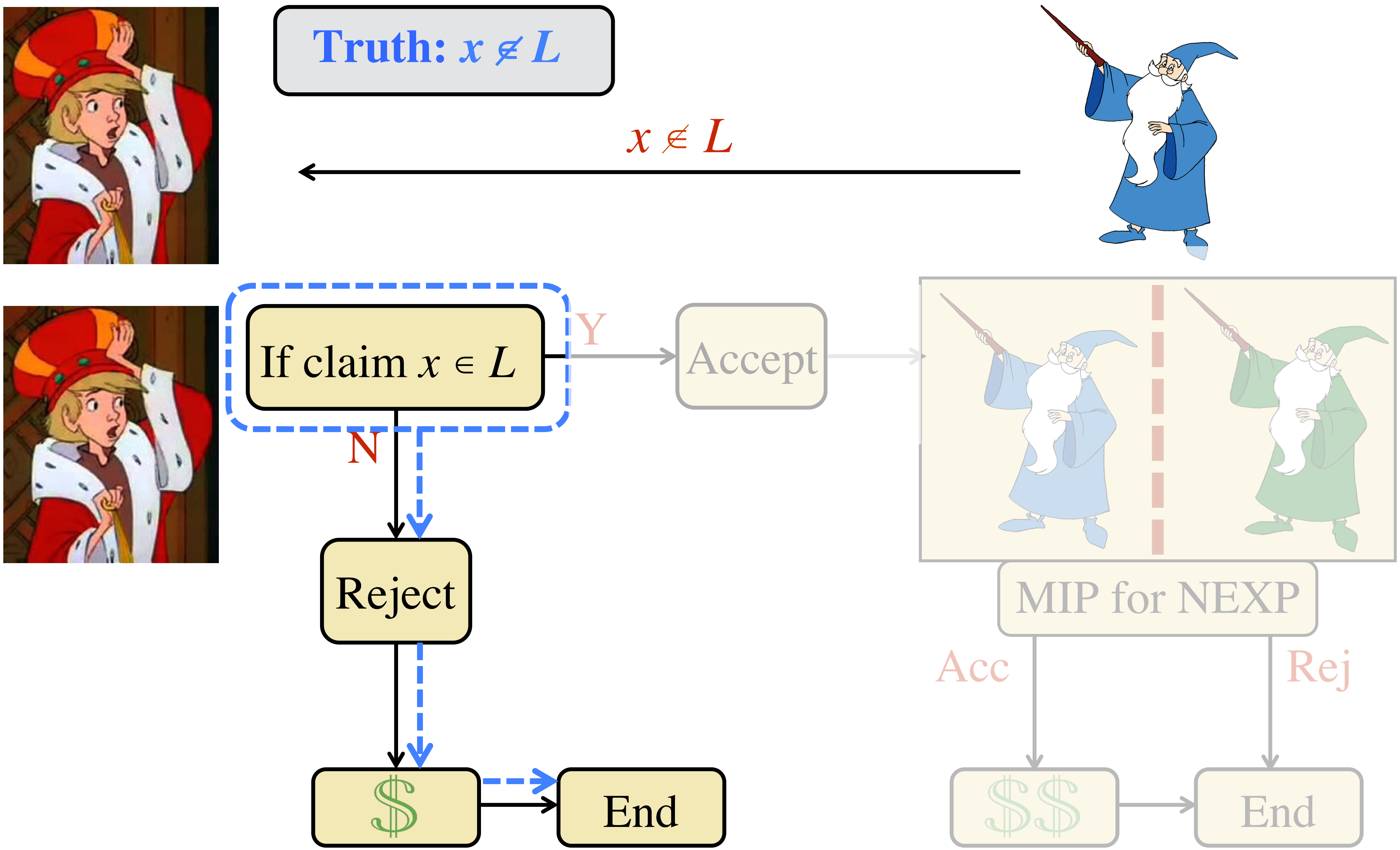
Warm Up: MRIP for NEXP



Warm Up: MRIP for NEXP



Warm Up: MRIP for NEXP

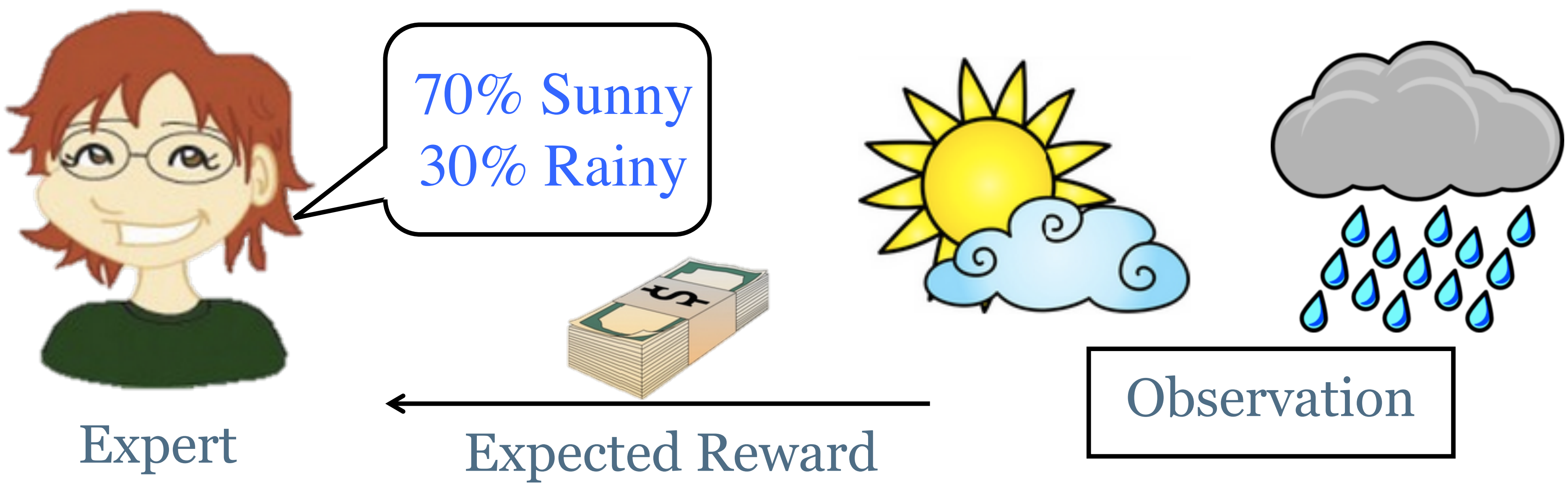


More Efficient MRIP for NEXP

- MIP protocols are often complicated, or computation and communication intensive
- We construct a simple, linear time MRIP protocol for NEXP

More Efficient MRIP for NEXP

- Construct MRIP for an NEXP-complete language
- *Use Brier's Scoring Rule:* $\mathsf{BSR}(D,\omega) = 2D(\omega) - \sum_{\omega \in \Sigma} D(\omega)^2 - 1$



MRIP for NEXP-Complete Language

Oracle 3SAT [BFL 91] : *Given a Boolean 3-CNF B, does there exist a function A such that for all w, B (w, A (b_1), A(b_2), A(b_3)) is satisfied, where $b_1b_2b_3$ is a suffix of w?*

MRIP for NEXP-Complete Language

Oracle 3SAT [BFL 91] : *Given a Boolean 3-CNF B, does there exist a* ***function A*** *such that for all w B (w, A (b*$_1$*), A(b*$_2$*), A(b*$_3$*)) is satisfied, where b*$_1$*b*$_2$*b*$_3$ *is a suffix of w?*

- A has $2^{|w|}$ solutions = B satisfied with probability 1
- Verifier cannot obtain true sample for the scoring rule
  - Use second prover to help sample
- What if prover is honest about a bad choice of A?
  - BSR maximized when all or none satisfied

Is MRIP strictly more powerful?

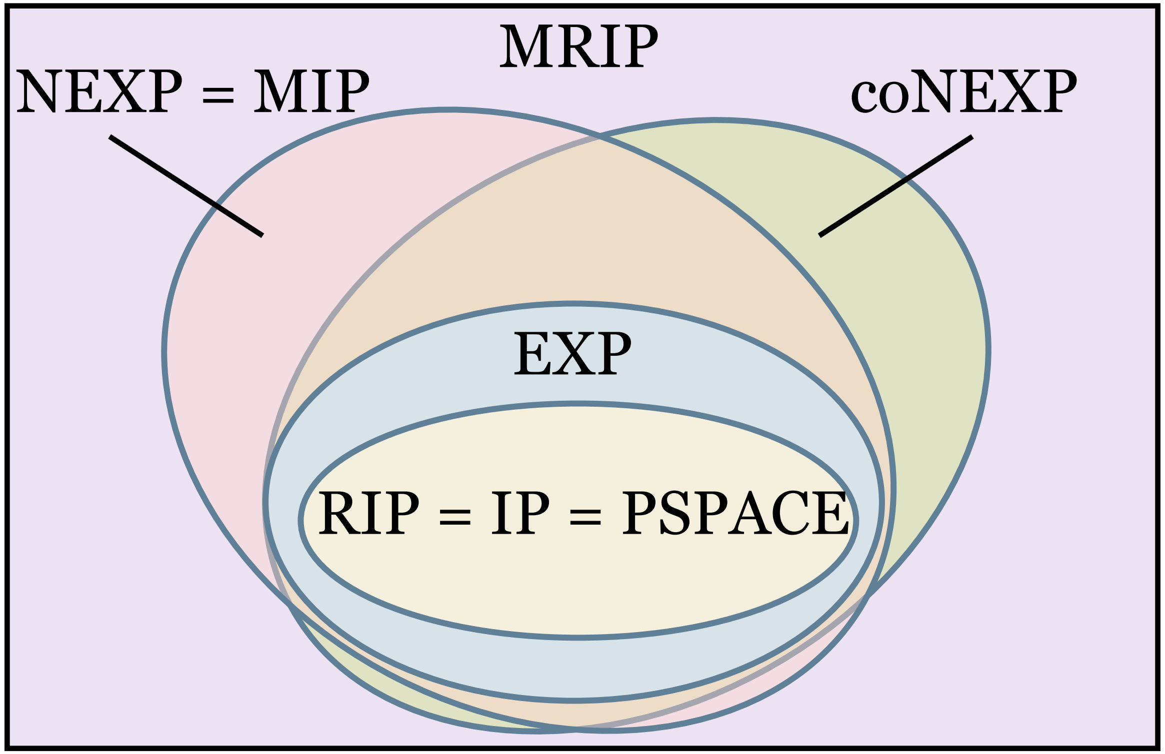
- Recall:
  - MRIP contains MIP
  - However, with a single prover: RIP = IP [AM 12]

MRIP is Closed under Complement

- A rational Merlin correctly reports $x \in L$ or $x \notin L$
- MRIP contains NEXP, so MRIP also contains coNEXP

MRIP vs RIP and MIP

- Assuming NEXP ≠ coNEXP:
  - MRIP is more powerful than both RIP and MIP



Exactly How Powerful is MRIP?

Theorem: $MRIP = EXP^{||NP}$

Exponential-time Turing Machine with non-adaptive access to an NP oracle

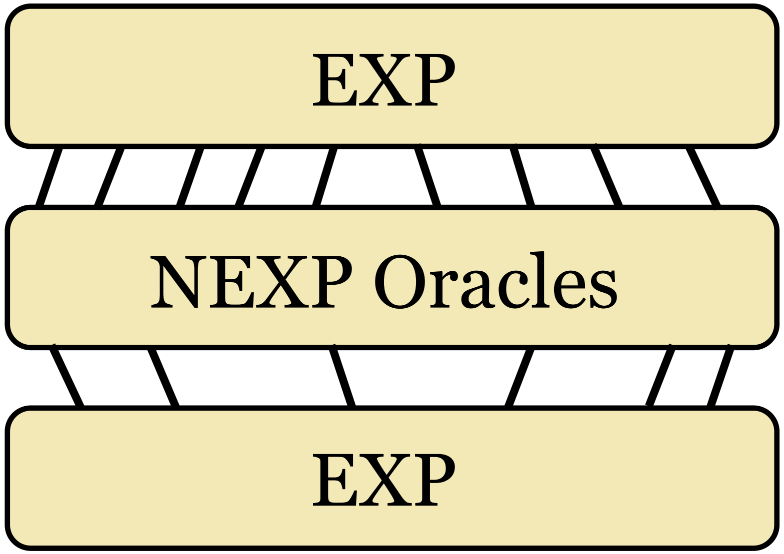
MRIP = $\mathrm{EXP}^{||\mathrm{NP}}$ (proof sketch)

Lemma: $EXP^{||NP} = EXP^{||poly\text{-}NEXP}$

To show: $MRIP = EXP^{||poly\text{-}NEXP}$

$\text{MRIP} = \text{EXP}^{||\text{NP}}$ (proof sketch)

- Divide computation into 3 parts
- EXP protocol uses DC circuit characterization
- Challenge: compose rewards together as a final reward which incentivizes truth in *each* protocol



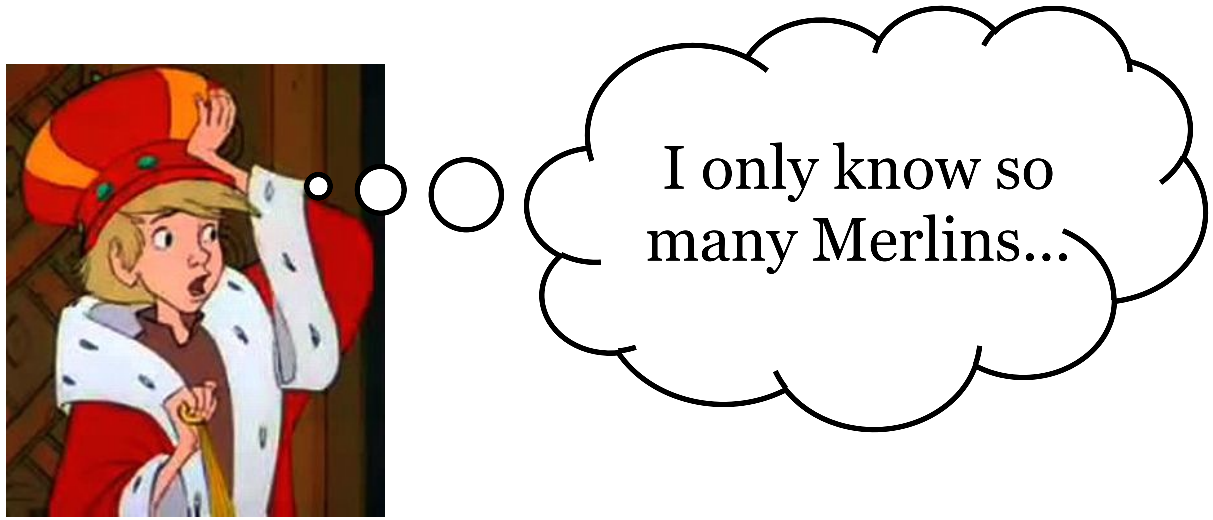
When paying for (verifiable) computation, we can solve more difficult problems by employing multiple provers and cross-checking their answers!

TAKE AWAY

Ask us questions separately and cross-check the results to get better answers

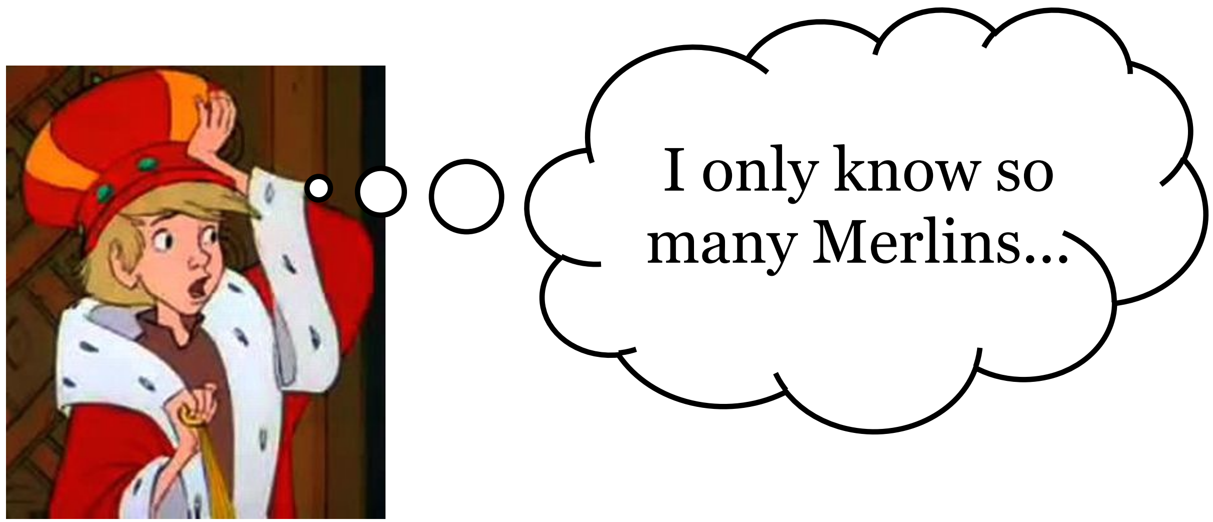
Fewer provers and rounds

- For MIP 2 provers, 1 round suffice [FL92]



Fewer provers and rounds

- For MIP 2 provers, 1 round suffice [FL92]

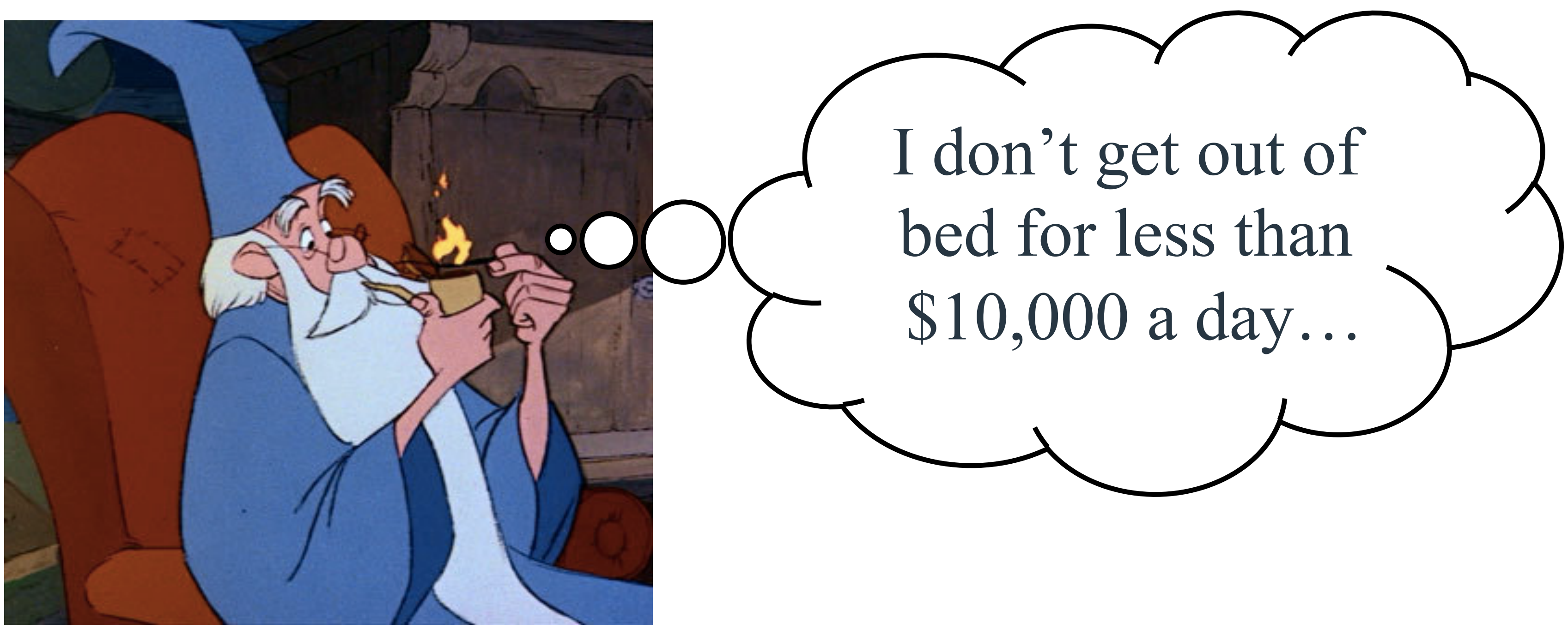


Theorem: *Two provers and five* rounds achieve the full power of MRIP.*

This slide is intentionally left blank.

Utility Gap

- So far, truthfulness guarantees *maximum* reward
- But how much do the provers lose by lying?
- We call this loss the *utility gap*



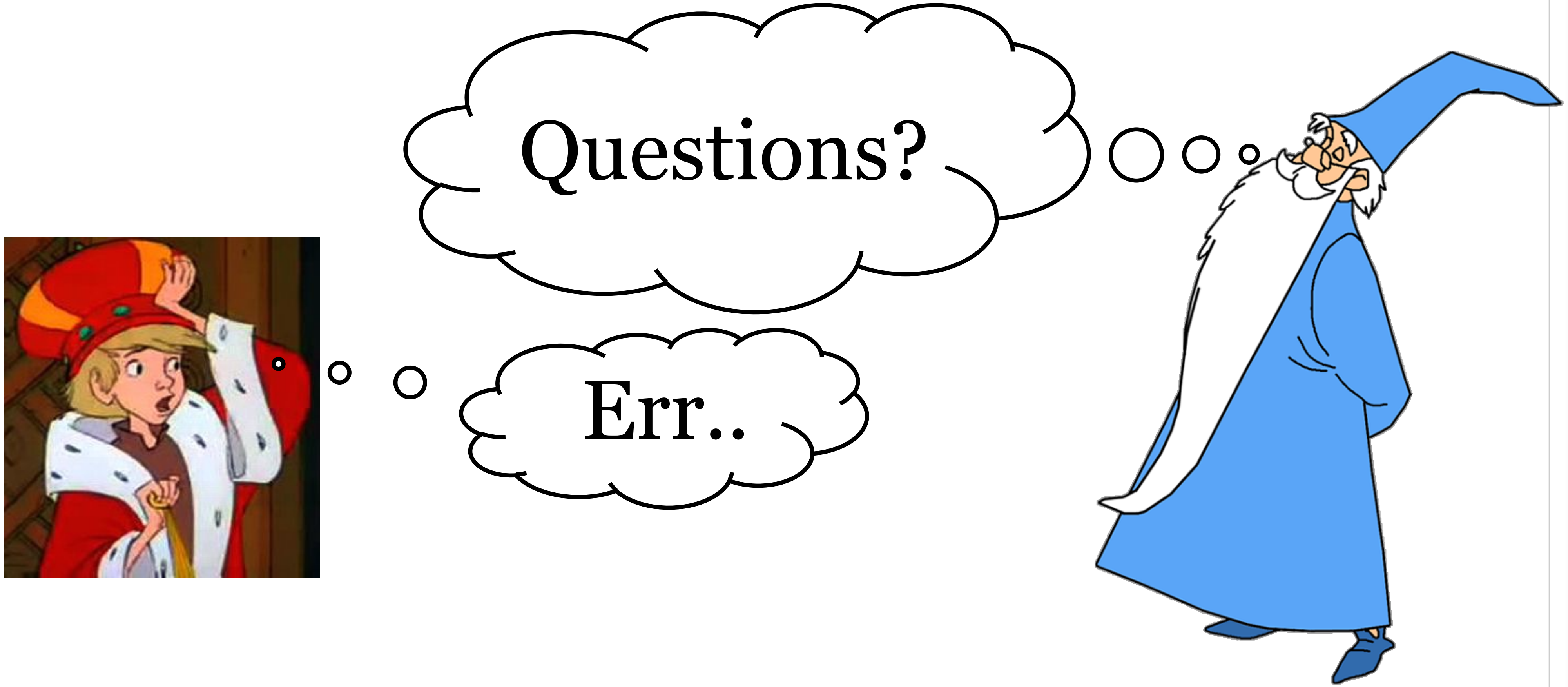
MRIP with Utility Gap

- Polynomial gap: $P^{||NEXP}$
- Constant gap: Contains both NEXP and coNEXP

Compare to $EXP^{||NP}$
for MRIP with arbitrary gap

Conclusion and Future Directions

- How to exploit the rationality of two provers
- What does this mean in terms of delegation of computation?
  - Scale down our protocols
- Interesting connections to existing models
  - Streaming Interactive Proofs [CTY 11, etc.]



Thank You!

2 Provers and 5 Rounds are Sufficient