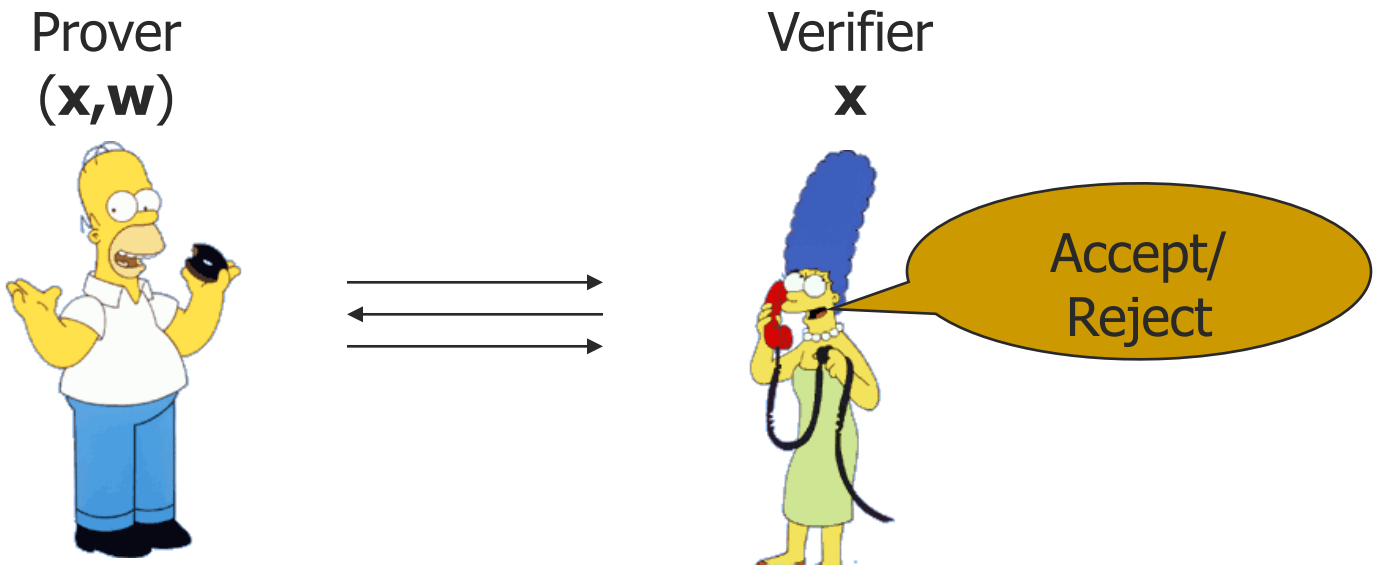
Isolated PoK and Isolated ZK

Ivan Damgård, Jesper Buus Nielsen and Daniel Wichs

Proofs of Knowledge (Review)

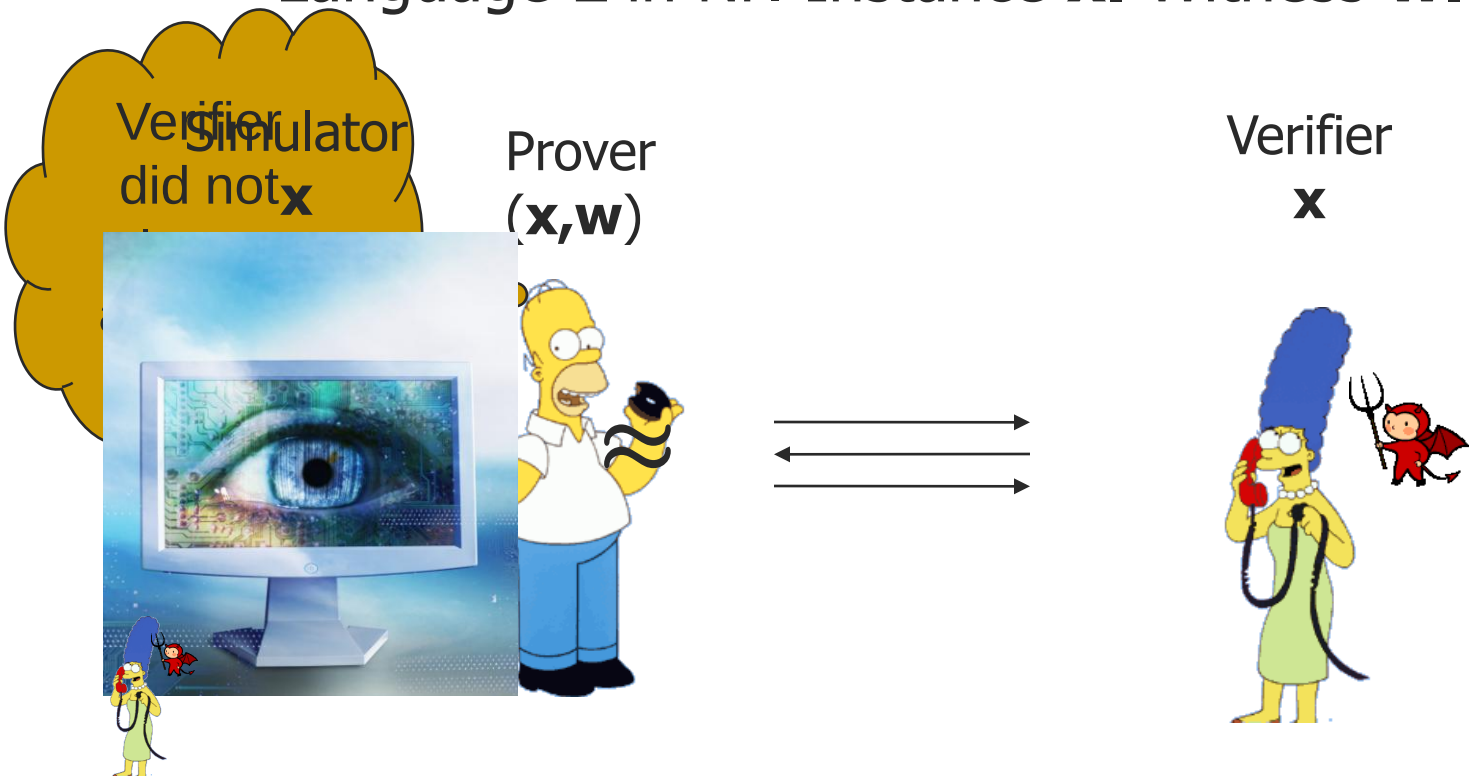
Language **L** in NP. Instance **x.** Witness **w.**



- **Completeness:** If the Prover, Verifier are both honest then the Verifier outputs “Accept” W.O.P

Zero Knowledge (Review)

Language **L** in NP. Instance **x.** Witness **w.**

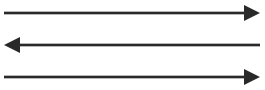


Simulator ensures that verifier could have produced entire conversation on its own.

Knowledge Soundnes (Review)

Language **L** in NP. Instance **x.** Witness **w.**

Extractor recovers **w** from the prover.



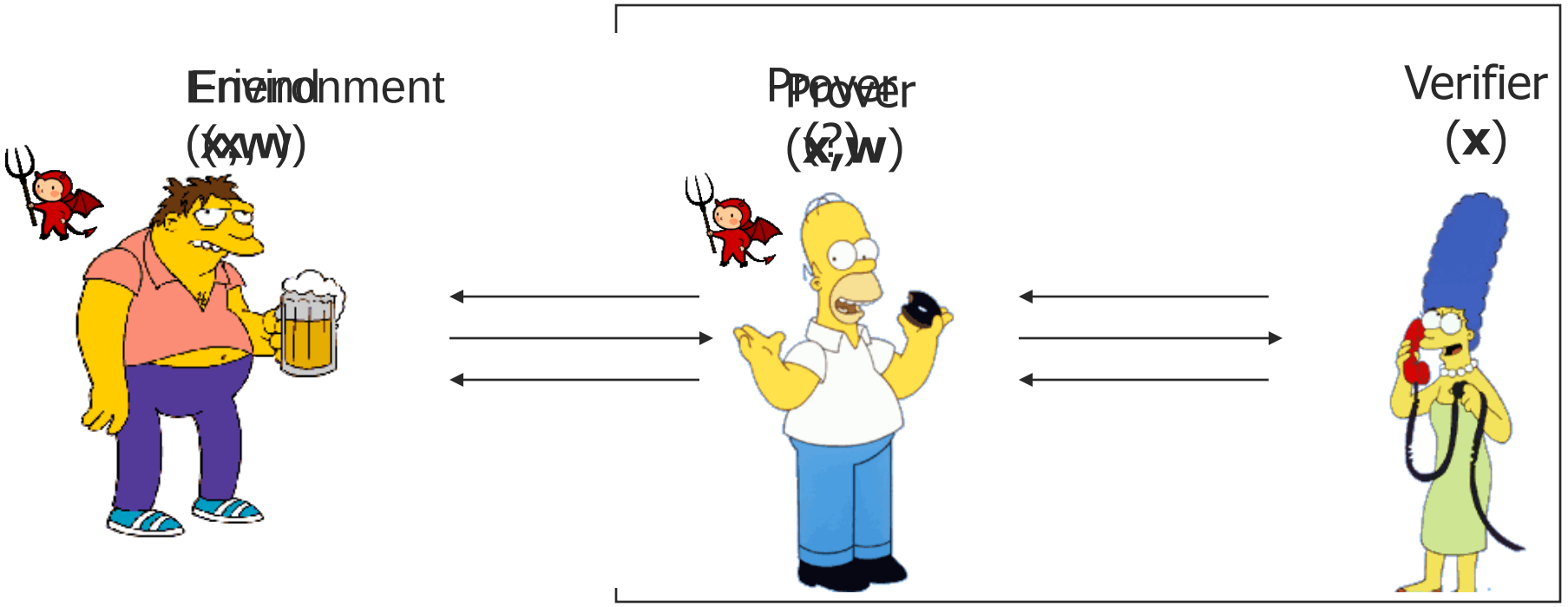
Verifier
x

If "Accept", prover knows **w.**

Extractor

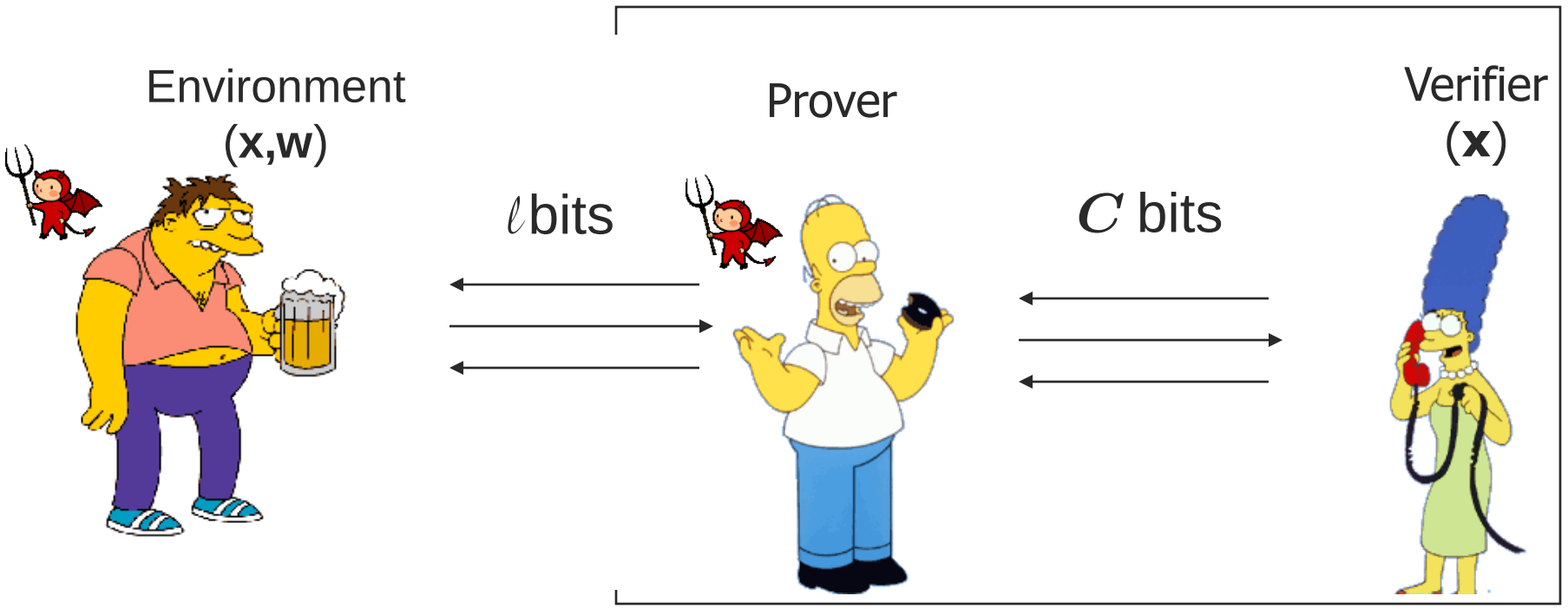
Isolation?

- Standard definitions/constructions assume isolation.
- Prover can run a *man-in-the-middle attack* between the *"friend"* and the verifier.
- No non-trivial protocol can guarantee that the prover knows **w**.
- Similar setting considered by Universal Composability.



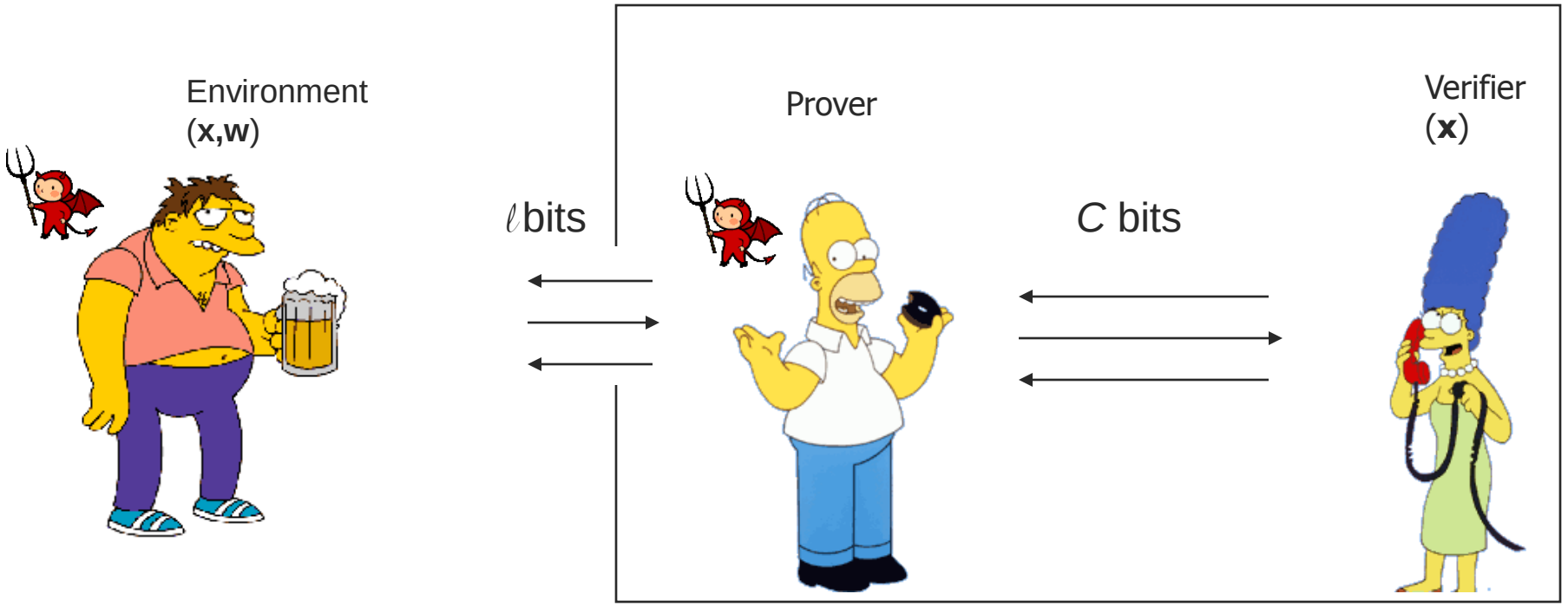
What can be done without full isolation?

- Setup assumptions (CRS, KRK,…) can be used to get UC security.
- This Talk: Assume prover is ℓ-isolated during the proof.
- Necessary condition: $C > \ell$.



Definitions and goals:

- An ℓ-Isolated PoK (ℓ-IPoK) is a protocol where no ℓ-isolated cheating prover can produce successful proof without knowing the witness.
- Goal: Construct an IPoK compiler. For any ℓ, compile an ℓ-IPoK.
- For now, assume that the verifier is fully isolated.



Why Study Partial Isolation?

- In certain settings it is reasonable to assume that Prover has more bandwidth with Verifier than with other parties.
  - Prover and Verifier are in same room with a high bandwidth channel between them but the prover has only low-bandwidth channels to the outside world.
  - Prover is implemented on a tamper-proof hardware token. Proposed by [Katz07] to solve general UC-MPC, but token needed to be completely isolated.

Presentation Road-Map

- Background, Motivation, Definition

- A simple construction of an ℓ-IPoK protocol with a large communication/round complexity.

- Lower bound on # of rounds in Black Box extractable ℓ-IPoK.

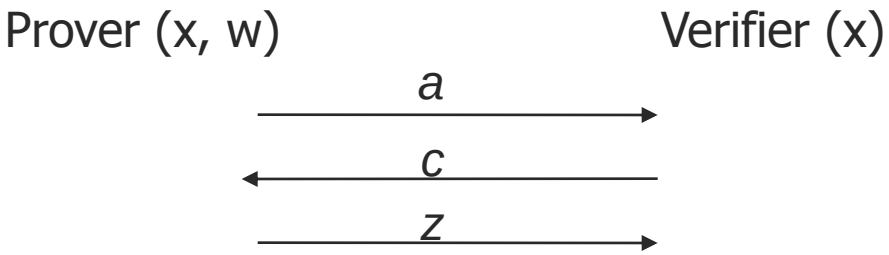
- A construction of an ℓ-IPoK protocol with optimal communication complexity.

- A non-black-box construction in the RO model with optimal communication/round complexity.

- Zero Knowledge when the Verifier is only partially Isolated

Review: Σ-Protocols

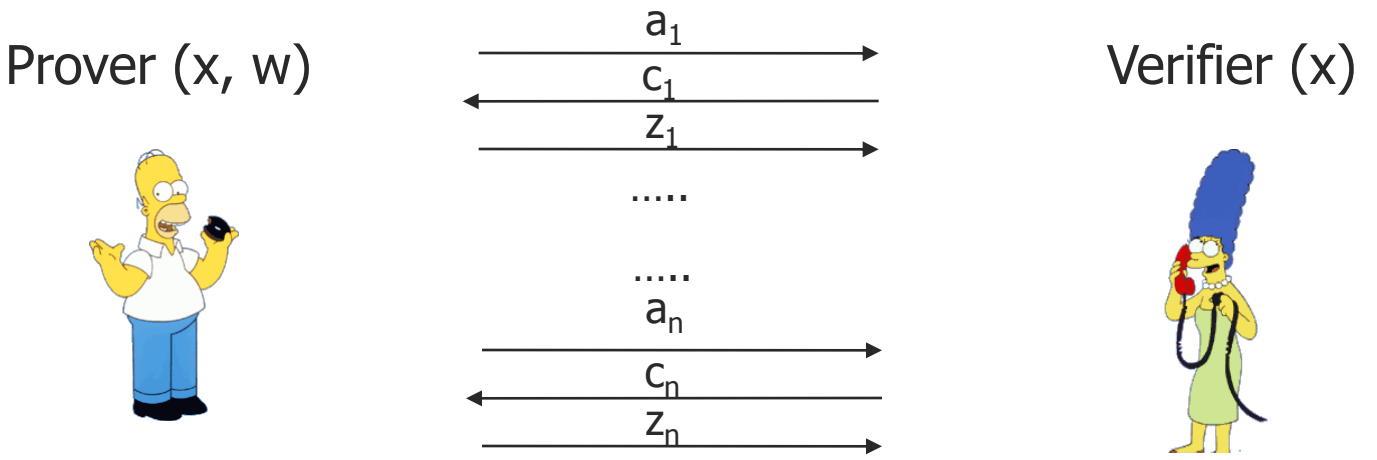
- Assume L $\in$ NP and Σ is a Σ-protocol for L.



- Special Knowledge Soundness
  - Can recover **w** from any two accepting conversations (a,c,z) and (a,c',z') with c $\neq$ c'.
- Honest Verifier Zero Knowledge
  - Implies Zero Knowledge when challenges are only 1 bit.

Compiling an ℓ-IPoK from a Σ-Protocol

- **Theorem:** Repeating Σ with 1 bit challenges (ℓ+κ) times sequentially results in an ℓ-IPoK with security parameter κ.
- Intuition: The prover cannot communicate even 1 bit on at least κ rounds and hence must know the witness!



Parameters

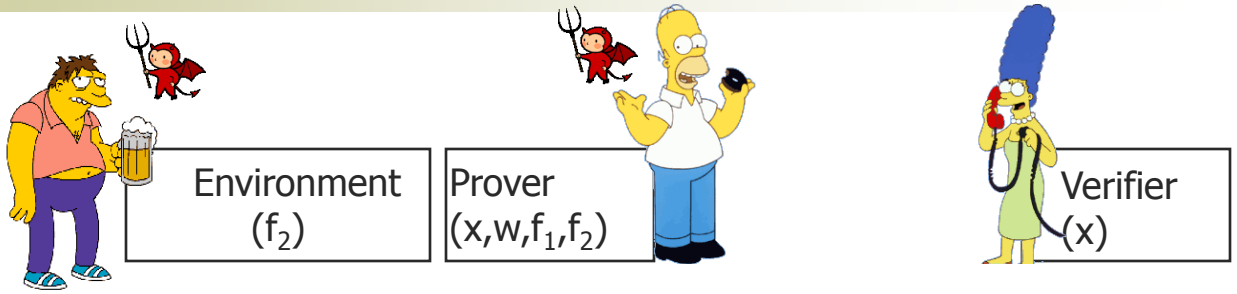
$O(\ell + \kappa)$	Round Complexity
$O((\ell + \kappa)\lvert\Sigma\rvert)$	Communication Complexity C
$O(\lvert\Sigma\rvert)$	Overhead = C/ℓ. Assume ℓ is large.

Presentation Road-Map

- Background, Motivation, Definition
- A simple construction of an ℓ-IPoK protocol with a large communication/round complexity.
- Lower bound on # of rounds in Black Box extractable ℓ-IPoK.
- A construction of an ℓ-IPoK protocol with optimal communication complexity.
- A non-black-box construction in the RO model with optimal communication/round complexity.
- Zero Knowledge when the Verifier is only partially Isolated

Round Complexity of BB extractable ℓ-IPoK

- Let f_1, f_2 be PRFs.
- The prover follows the protocol honestly.
- "Checks in" with the Environment before producing any output.
- Rewinding requires finding a collission on f_1 or guessing f_2 at a new input!



If there are ρ rounds of communication then

$\ell/\rho = O(\log(\kappa))$

$\Rightarrow$ The number of rounds grows linearly with ℓ.

Presentation Road-Map

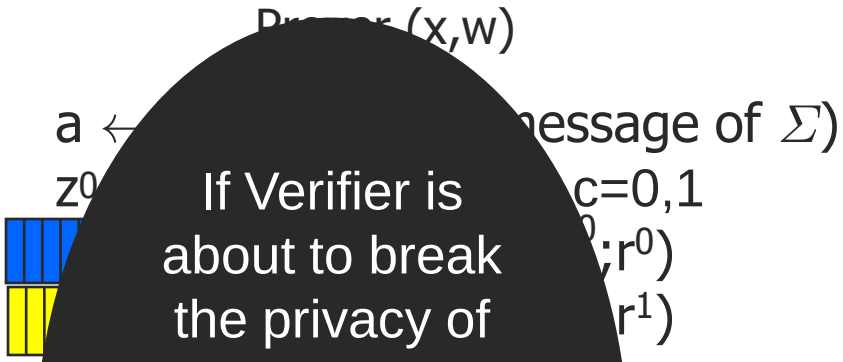
- Background, Motivation, Definition
- A simple construction of an ℓ-IPoK protocol with a large communication/round complexity.
- Number of rounds in BB extractable ℓ-IPoK is linear in ℓ.
- A construction of an ℓ-IPoK protocol with optimal communication complexity.
- A non-black-box construction in the RO model with optimal communication/round complexity.
- Zero Knowledge when the Verifier is only partially Isolated

Reducing the Communication

- Task: Design an ℓ-IPoK where the communication complexity and round complexity are both $O(\ell)$.
- We need lots of short rounds.
- Idea: Use a *ramp secret sharing scheme* to split **w** into small parts. Have lots of rounds where verifier get a small share of **w**.
  - Make sure honest verifier does not break privacy of **w**.
  - Extractor can recover enough shares to recover **w**.

This is a single *epoch* with **N** =O(ℓ/κ) *rounds*.

Protocol consists of **M**=O(κ) epochs.



If Verifier is about to break the privacy of the yellow/blue sharing – prover quits. Happens w/ negligible probability when verifier is honest.

Choose $\perp$ so that the probability of getting too many yellow/blue shares to break privacy is negligible.

Verify: (a,b,z^b) is accepting for Σ
Collected shares $S^b[i]$ match the decommitment.

This is a single *epoch* with **N** =O(ℓ/κ) *rounds*.

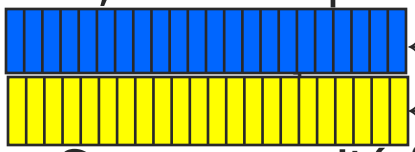
Protocol consists of **M**=O(κ) epochs.

Prover (x,w)

Verifier (x)

a $\leftarrow$ (random first message of Σ)

z^0, $z^1 \leftarrow$ responses to c=0,1



$\leftarrow SS(z^0;r^0)$

$\leftarrow SS(z^1;r^1)$

$C_0 \leftarrow commit(z^0||r^0)$

$C_1 \leftarrow commit(z^1||r^1)$

a, C_0,C_1

e $\in$ {0,1,$\perp$}

0/1/$\perp$

b $\in$ {0,1}

Extractor rewinds to each round in each epoch and tries the "other" challenge.

- If Prover communicates, that share is *lost.*
- Share might also be incorrect.
- Thrm: On at least one epoch, extractor can recover other *correct* response and hence **w**.

is accepting for Σ

Collected shares $S^b[i]$ match the decommitment.

Parameters

Assume $\ell = \Omega(\kappa|\Sigma|)$

O(ℓ)	Round Complexity
O(ℓ)	Communication Complexity C
O(1)	Overhead = C/ℓ

Presentation Road-Map

- Background, Motivation, Definition
- A simple construction of an ℓ-IPoK protocol with a large communication/round complexity.
- Number of rounds in BB extractable ℓ-IPoK is linear in ℓ.
- A construction of an ℓ-IPoK protocol with optimal communication complexity.
- A non-black-box construction in the RO model with optimal communication/round complexity.
- Zero Knowledge when the Verifier is only partially Isolated

Random Oracle Protocol

Use RO as commitment scheme

- Valid commitments can only be computed by the prover alone.
- Extractable by looking at RO queries (non-BB).

- Prover only wins if he queries the RO only for the challenge asked by verifier.

$\Rightarrow 1/2^{\kappa}$

Random Oracle
H: $\{0,1\}^* \rightarrow \{0,1\}^{\kappa}$

Prover (**x**,**w**)

Verifier (**x**)

$r \leftarrow$ random string of length $\ell + \kappa$

For i=1,…,κ:
$a_i \leftarrow$ (first message of Σ)
z_i^0, z_i^1 responses
$\sigma_i^0 = H(z_i^0, r, r_i^0)$
$\sigma_i^1 = H(z_i^1, r, r_i^1)$

$\{a_i, \sigma_i^0, \sigma_i^1\}_{i=1,\ldots,\kappa}$

$c_1, c_2, \ldots, c_{\kappa}$

$c_i \leftarrow \{0,1\}$

$\{r_i(c_i), z_i(c_i)\}_{i=1,\ldots,\kappa}$

Presentation Road-Map

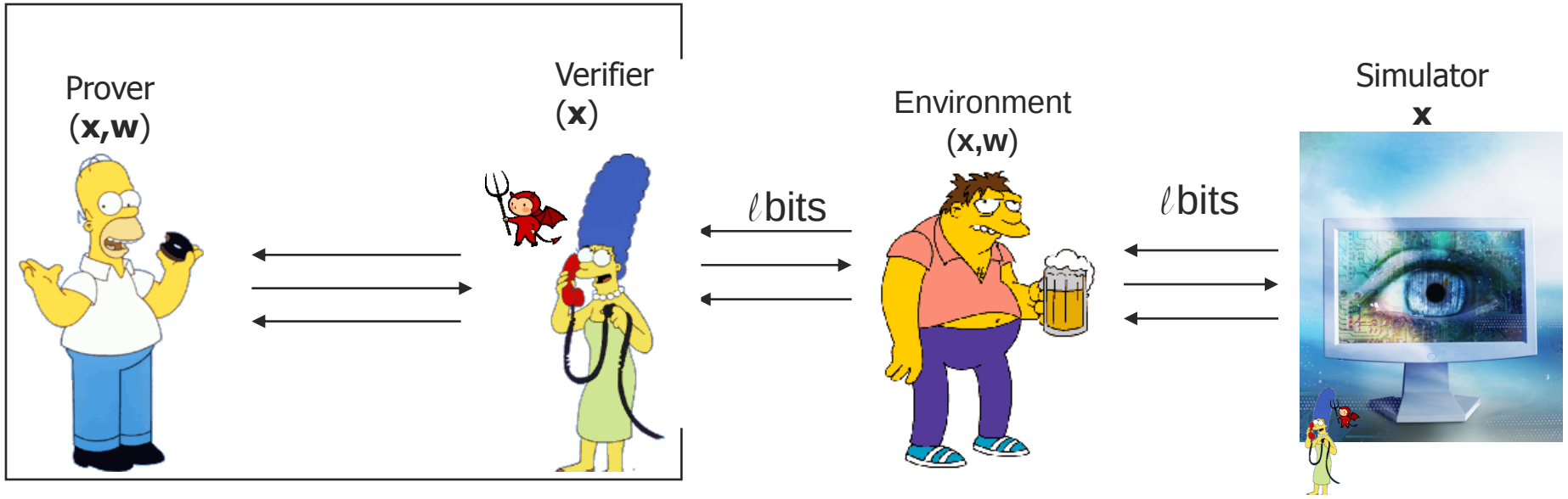
- Background, Motivation, Definition
- A simple construction of an ℓ-IPoK protocol with a large communication/round complexity.
- Number of rounds in BB extractable ℓ-IPoK is linear in ℓ.
- A construction of an ℓ-IPoK protocol with optimal communication complexity.
- A non-black-box construction in the RO model with optimal communication/round complexity.

➡ Zero Knowledge when the Verifier is only partially Isolated

ℓ-Isolated Zero Knowledge (ℓ-IZK)

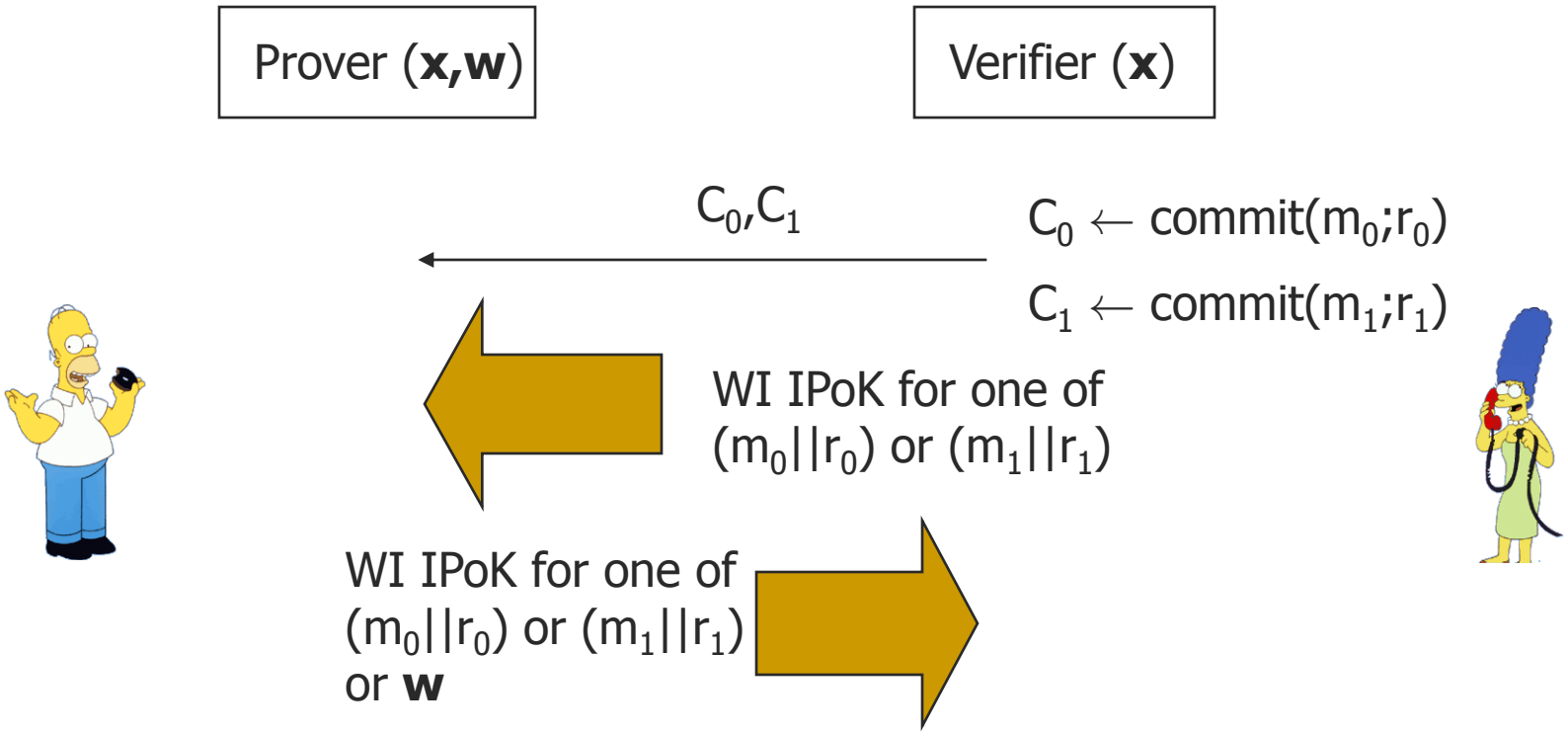
Environment cannot distinguish left from right.

Just like Knowledge Soundness, ℓ-IZK is impossible if C<ℓ.



IZK + IPoK from WI IPoK

- Use FLS paradigm to go from WI to IZK
- Use your favorite WI IPoK, Perfectly Binding Commitments



Applications of IPoK and IZK

- Can prevent man-in-the-middle attacks on identification schemes when the prover is partially isolated (use a WI IPoK).
- UC secure MPC under a “cave” assumption. We can implement ideal ZK PoK in such a cave and so can do arbitrary UC-MPC using [CLOS02].
- Would like to do UC-MPC when only one party is partially isolated at a given time. This is needed for tamper-proof hardware. Can be accomplished using a WI-IPoK (see ePrint 2007/332).

Thank You!

QUESTIONS?