Concurrent Zero Knowledge in the Bounded Player Model

Vipul Goyal – Microsoft Research, India
Abhishek Jain – MIT and Boston University
Rafail Ostrovsky – UCLA
Silas Richelson – UCLA
Ivan Visconti – University of Salerno, Italy

Introductions

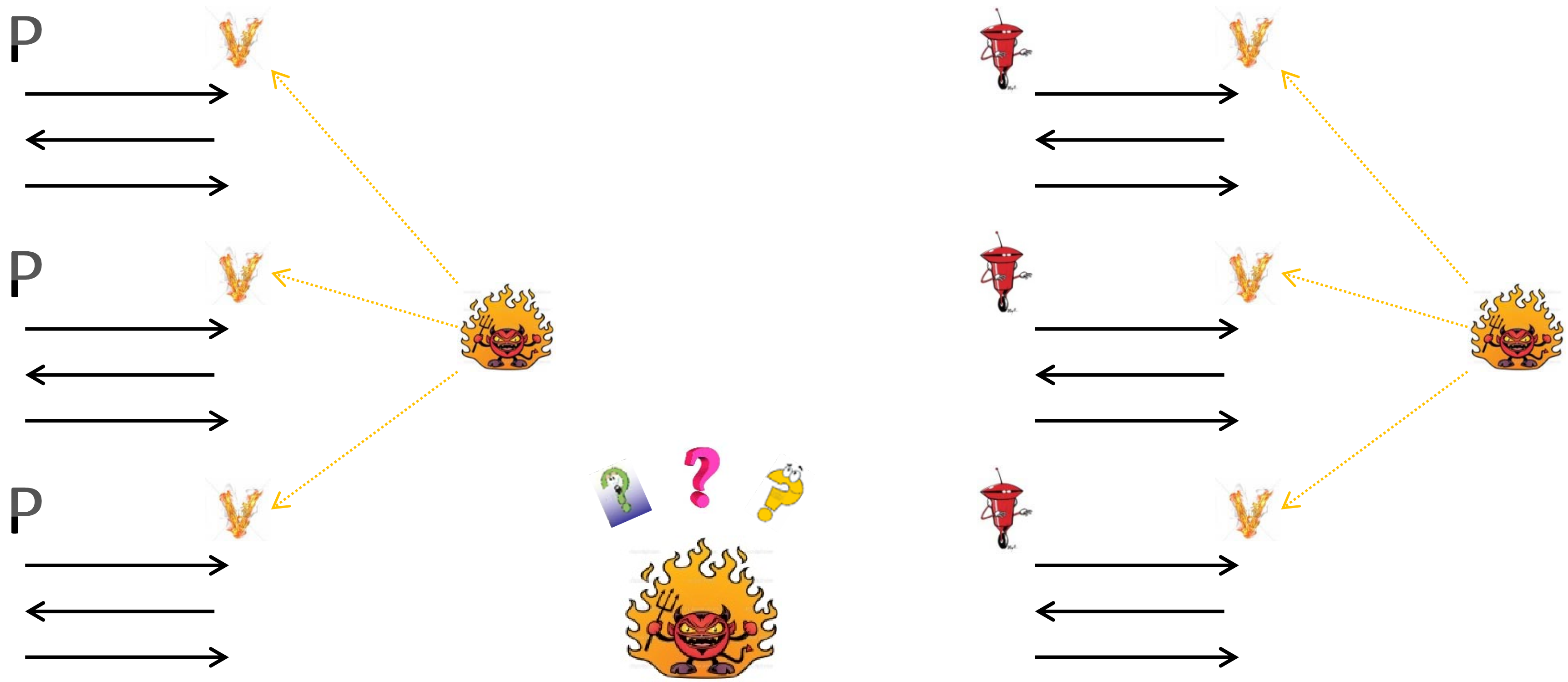
- Meet

and

- (P, V) is **zero knowledge** if: there exists  which can emulate 's interaction with P.

Concurrent Zero Knowledge

- (P, V) is **concurrent zero knowledge** [DNS98] if ZK holds when V* may run many instances of protocol concurrently.



cZK in the Plain Model

- cZK exists in the plain model – [RK99].
- Nearly logarithmic round complexity – [KP01], [PRS02].
- Black box cZK requires almost logarithmically many rounds [R00], [CKPR01].
- Impossibility of cMPC – [CF01], [CKL03], [L03], [L04]

- **Open Problem:** Is cZK possible in sublogarithmically many rounds?

Constant Round cZK in Other Models

- Timing Models – [DNS98]
- Super Polytime Simulation – [P03]
- Common Reference String – [BSMP91]
- Bare Public Key – [CGGM00], [SV12]
- Bounded Concurrency – [B01]

- Constant Round cMPC exists in most of the above models.

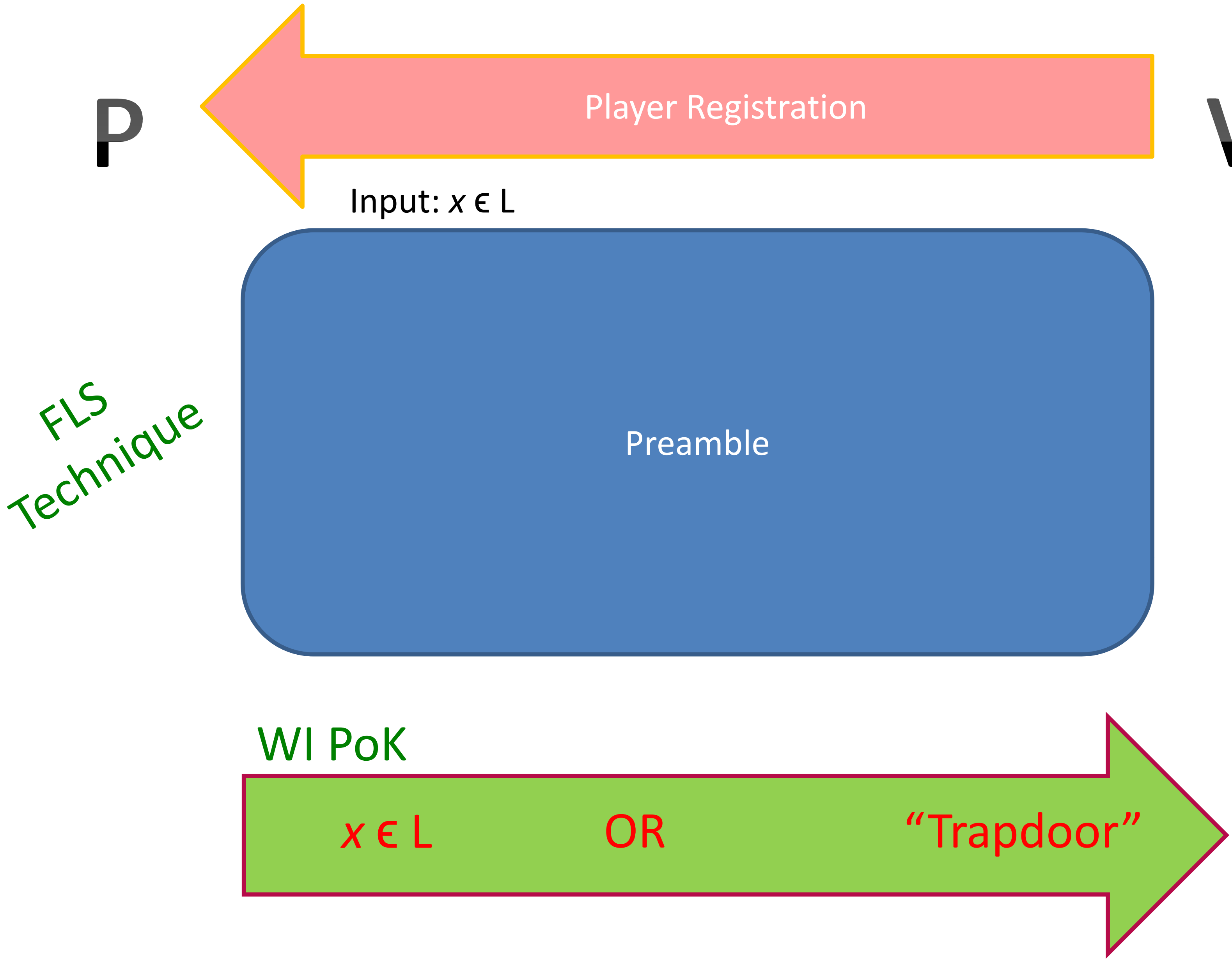
Our Model – Bounded Player Model

- A **bounded number of players** will ever engage in the protocol.
  - Each player may play unbounded number of sessions.
- Relaxation of bounded concurrency model.
- Improvements over Bare Public Key model.
  - No preprocessing phase.
  - Non-blackbox simulation needed for cZK with sublogarithmically many rounds.
- **cMPC impossible**.
  - Evidence that BP model is close to plain model.

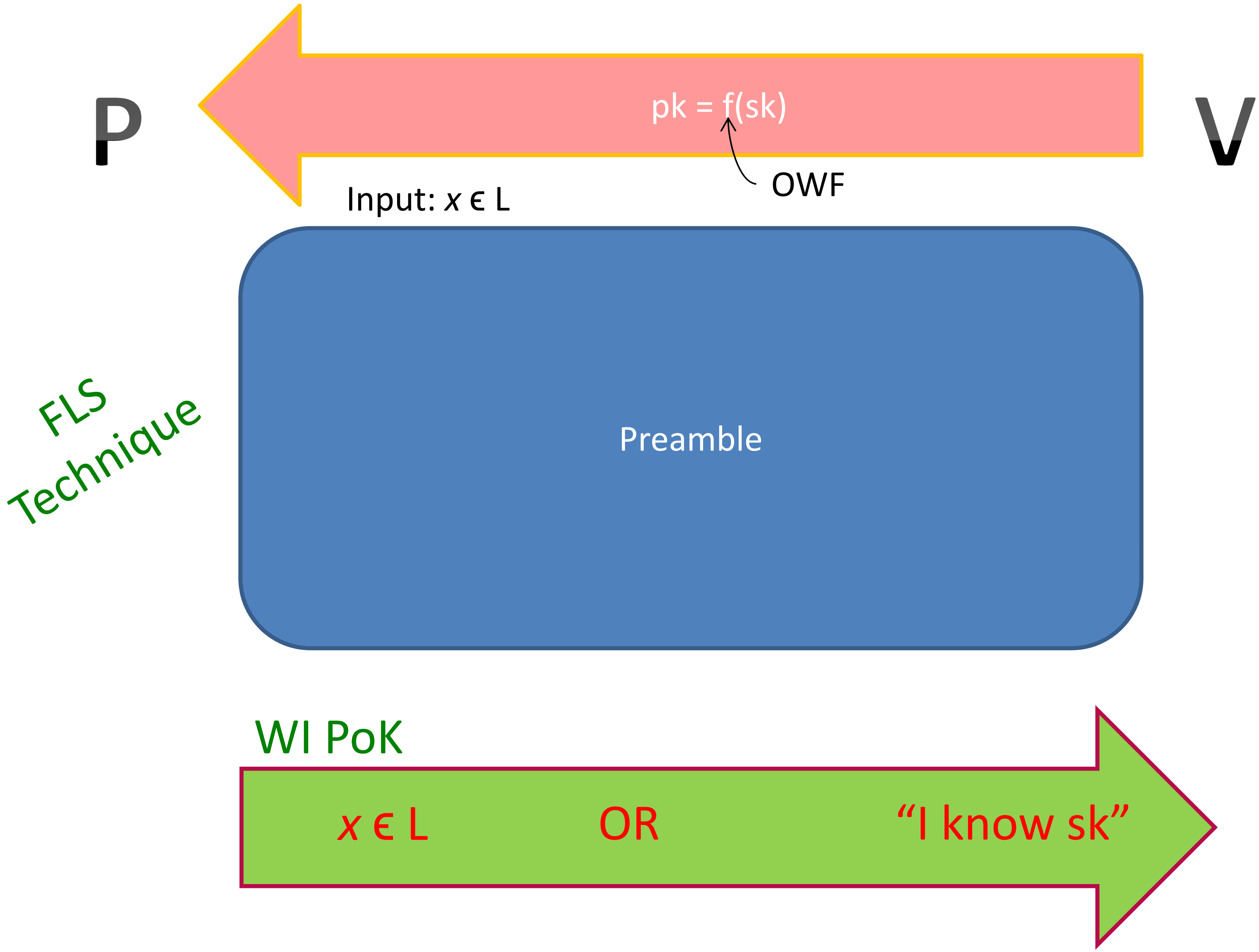
Main Theorem

- Assuming standard complexity theoretic assumptions there exists a cZK argument in the BPM.
  - Slightly super-constant round complexity ($\omega(1)$)
  - Straight-line non-blackbox simulator.

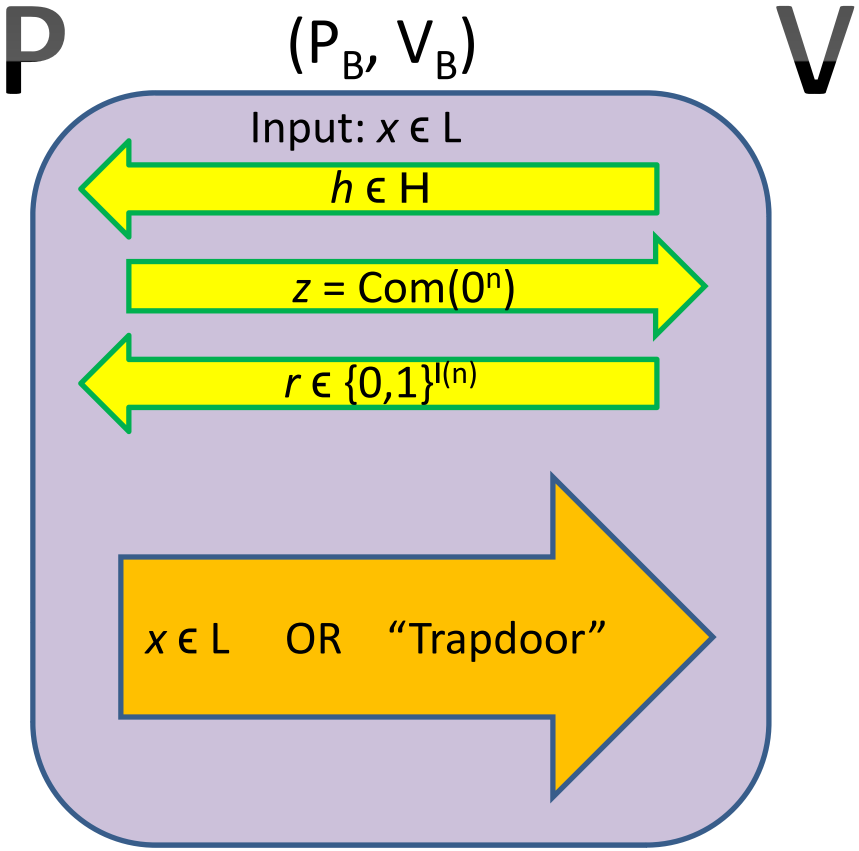
Building the Protocol (Informal)



Building the Protocol (Informal)



Barak's Protocol – A Building Block



- Non-blackbox simulator obtains trapdoor by sending *z*, a commitment to a machine Π which predicts *r*.

- Achieves bounded concurrency. Our model allows for unbounded concurrency (bound is on number of players).

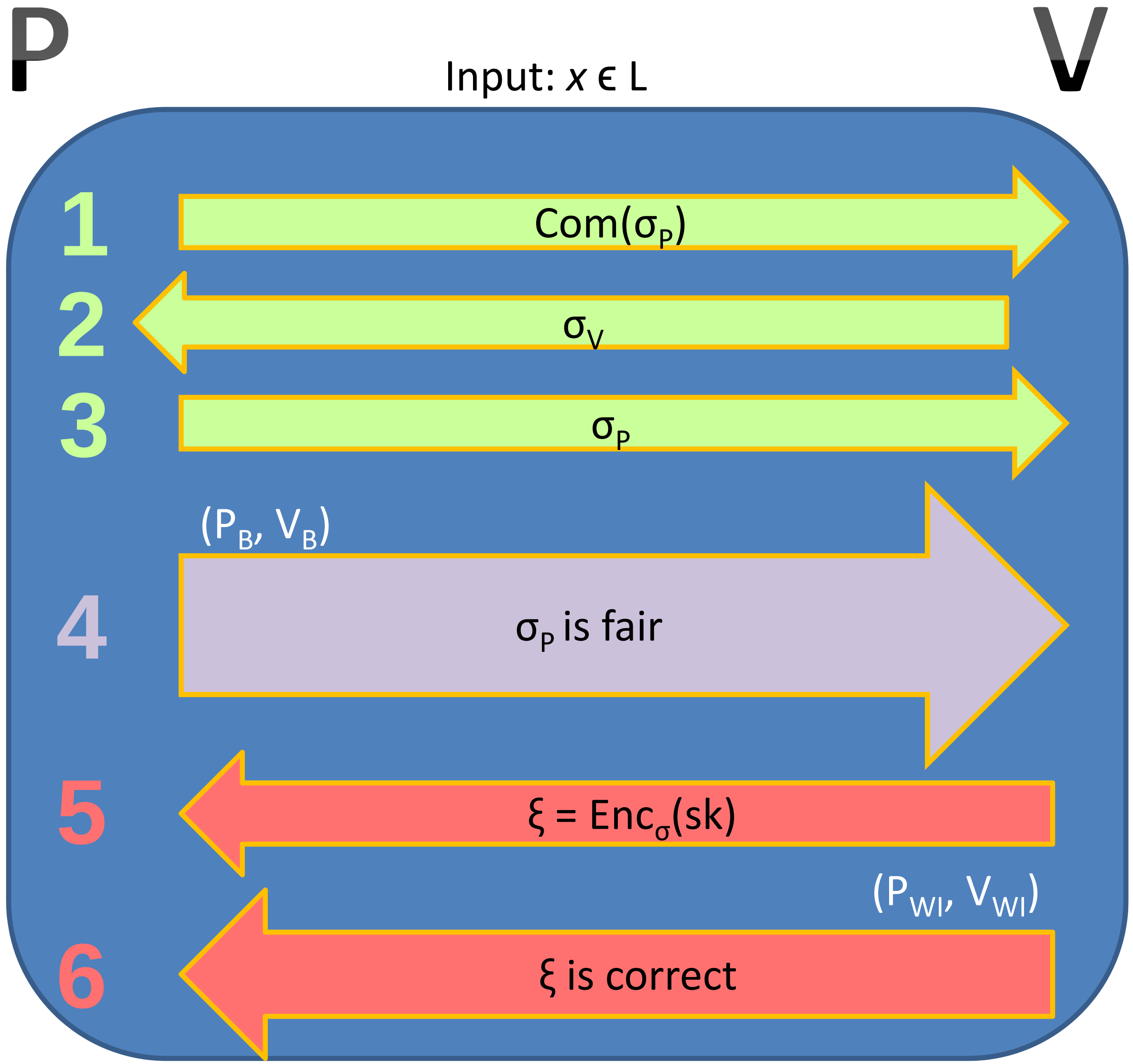
Our Starting Idea

- Can we bound the number of non-blackbox simulations required to learn each player's identity?

- Then we could use bound on total number of players to reduce to case of bounded concurrency.

The Preamble (informal)

We need to devise a way for the simulator to learn the secret key.

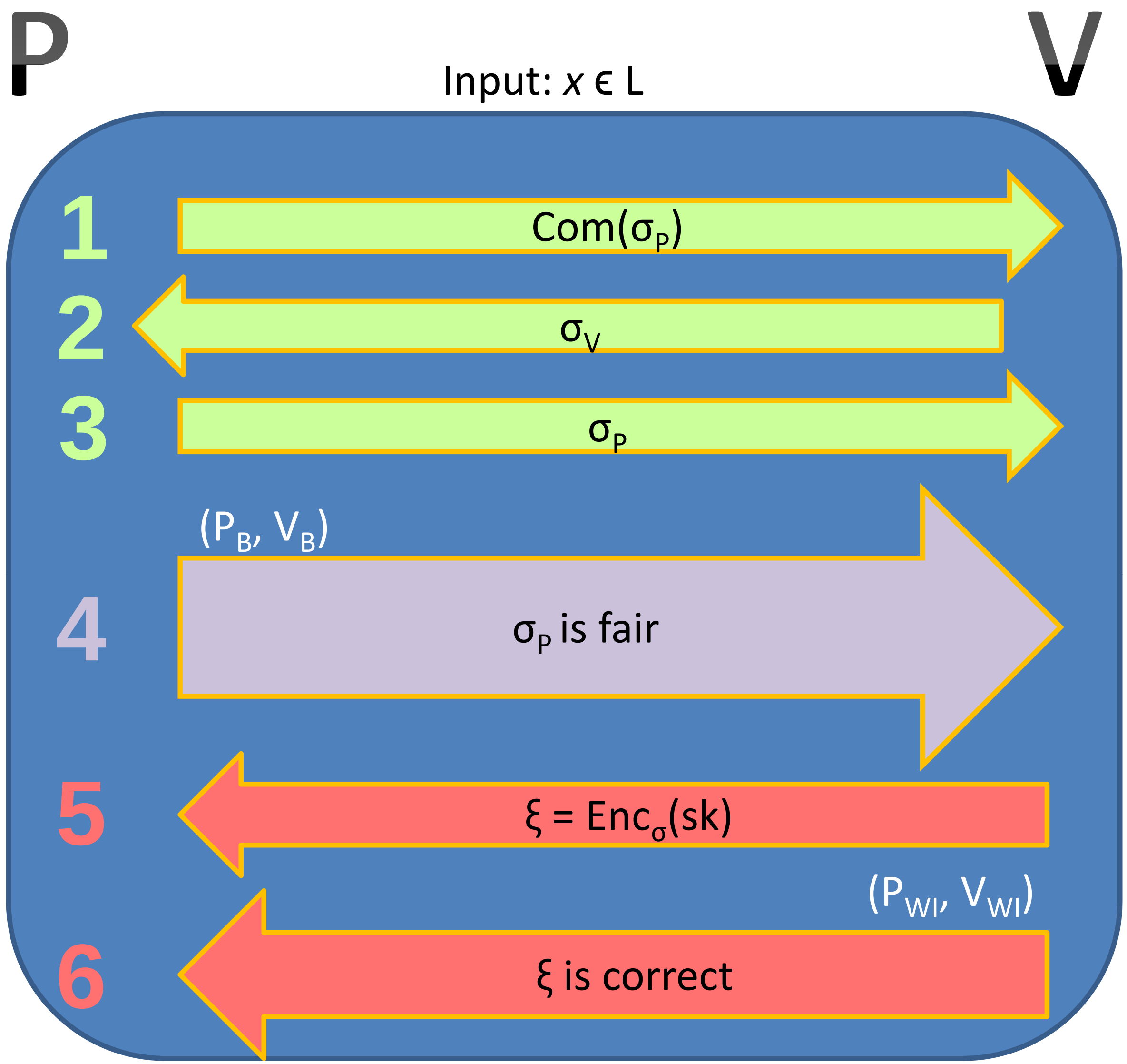


- Unfair coin flipping protocol obtaining $\sigma = \sigma_P + \sigma_V$
  - ➢ P never decommits.
- P proves that σ_P is fair using Barak's protocol.
- V sends encryption of sk under public key σ.
- Proves correctness of ξ using WI.

The Preamble (informal)

Soundness:

- Soundness of (P_B, V_B) forces P* to send same value in (3) that he committed to in (1).
- Public key used by V to encrypt is random and so P* cannot know corresponding private key.
- Semantic security means P* learns nothing about secret key.



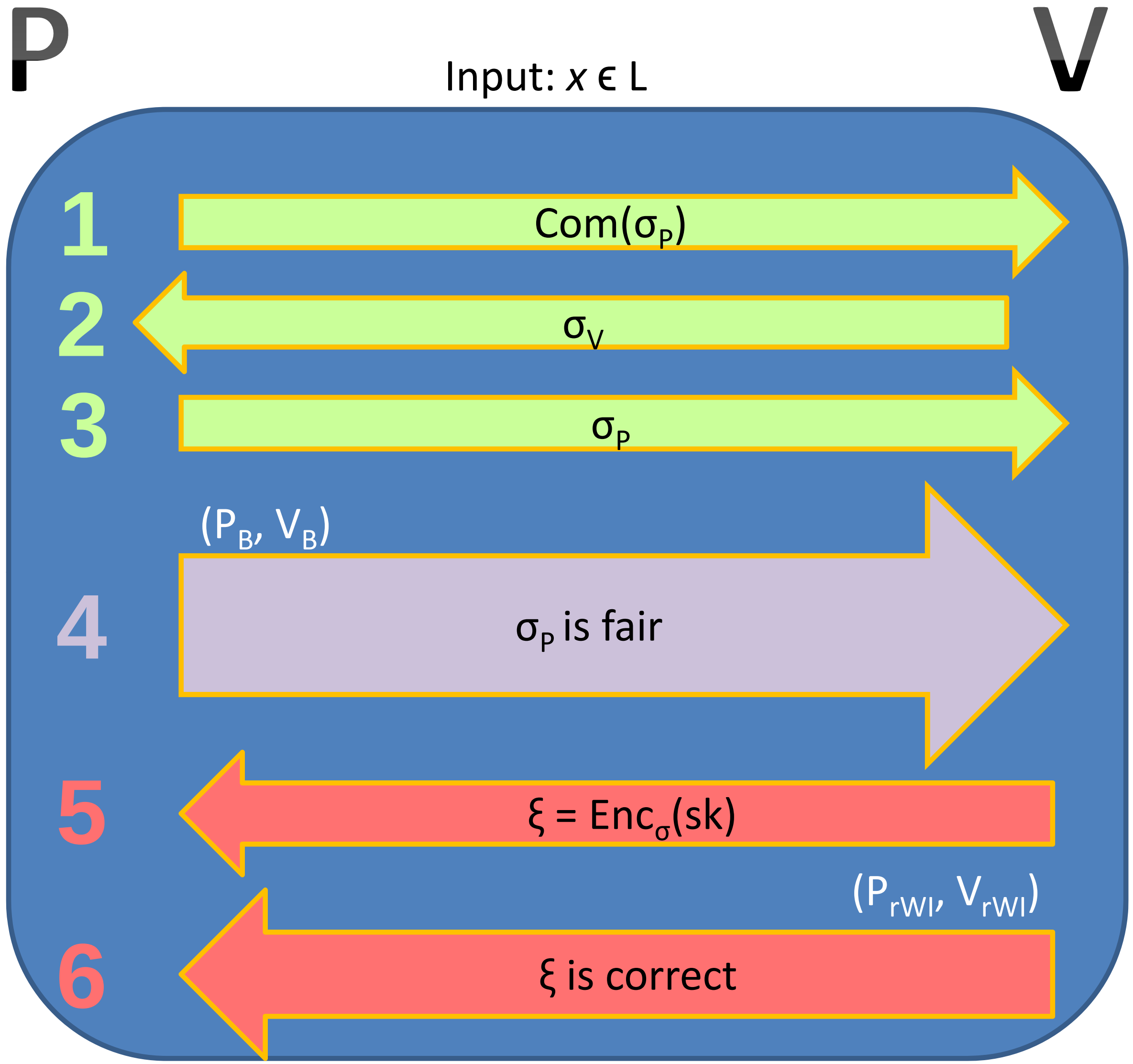
The Preamble (informal)

Zero Knowledge:

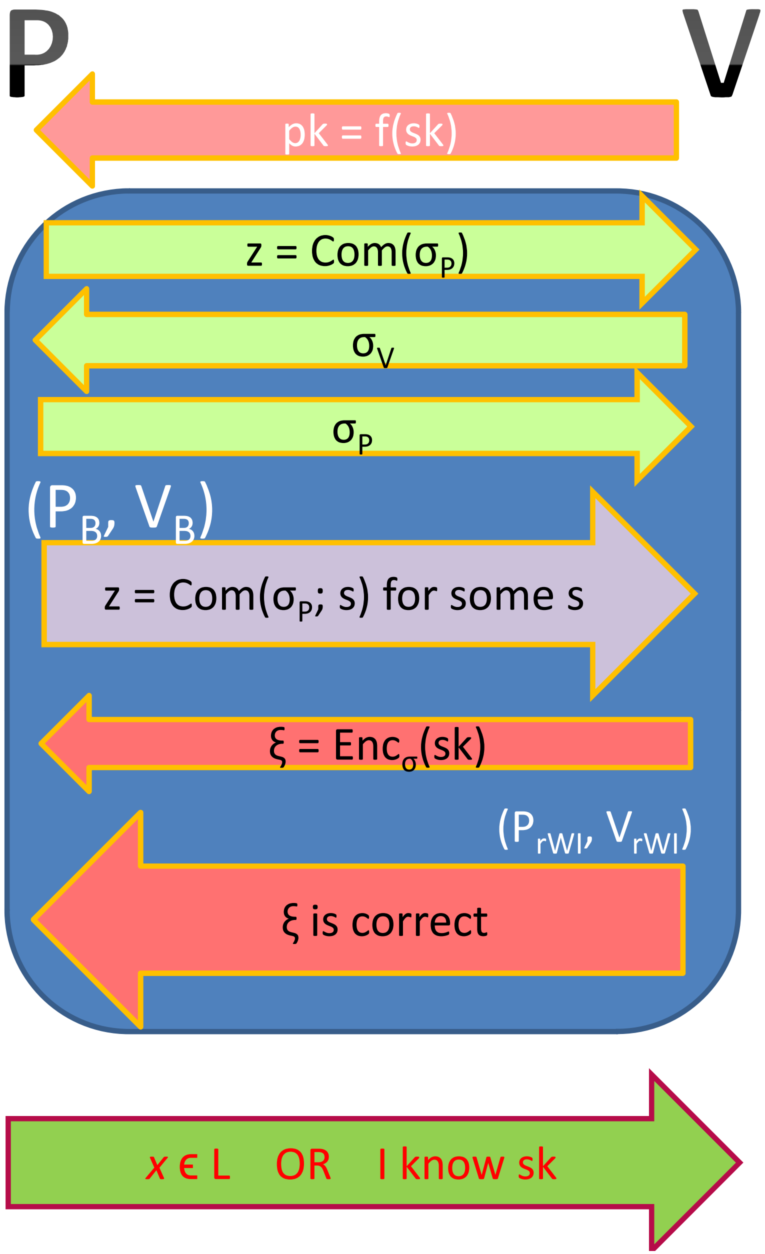
- Simulator can use trapdoor in Barak's protocol to prove a false theorem to V*.

Simulator:

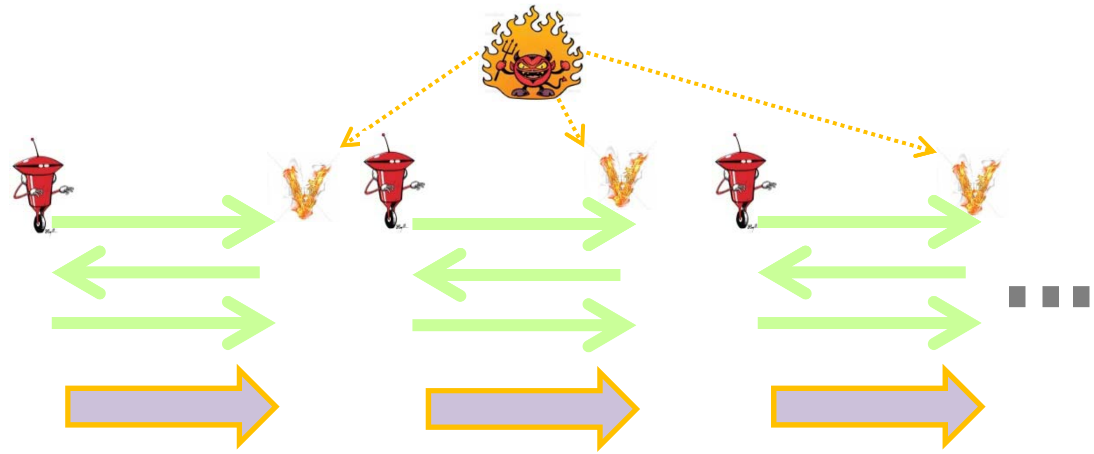
- Send Com(0^n)
- Run **Gen** obtaining key pair (σ, τ)
- Send $\sigma_P = \sigma + \sigma_V$.
- Use trapdoor to prove false theorem in (P_B, V_B).
- Receive ξ, verify correctness and recover sk = $\mathbf{Dec}_\tau(\xi)$.



Main Problem

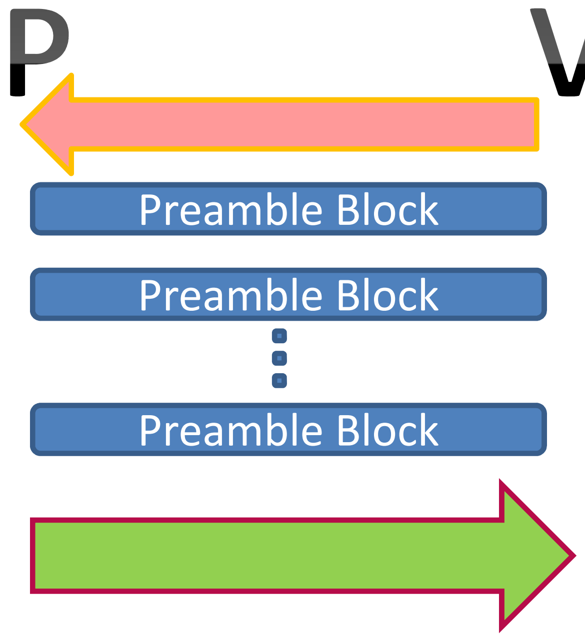


Problem: Adversarial verifier can interleave sessions.



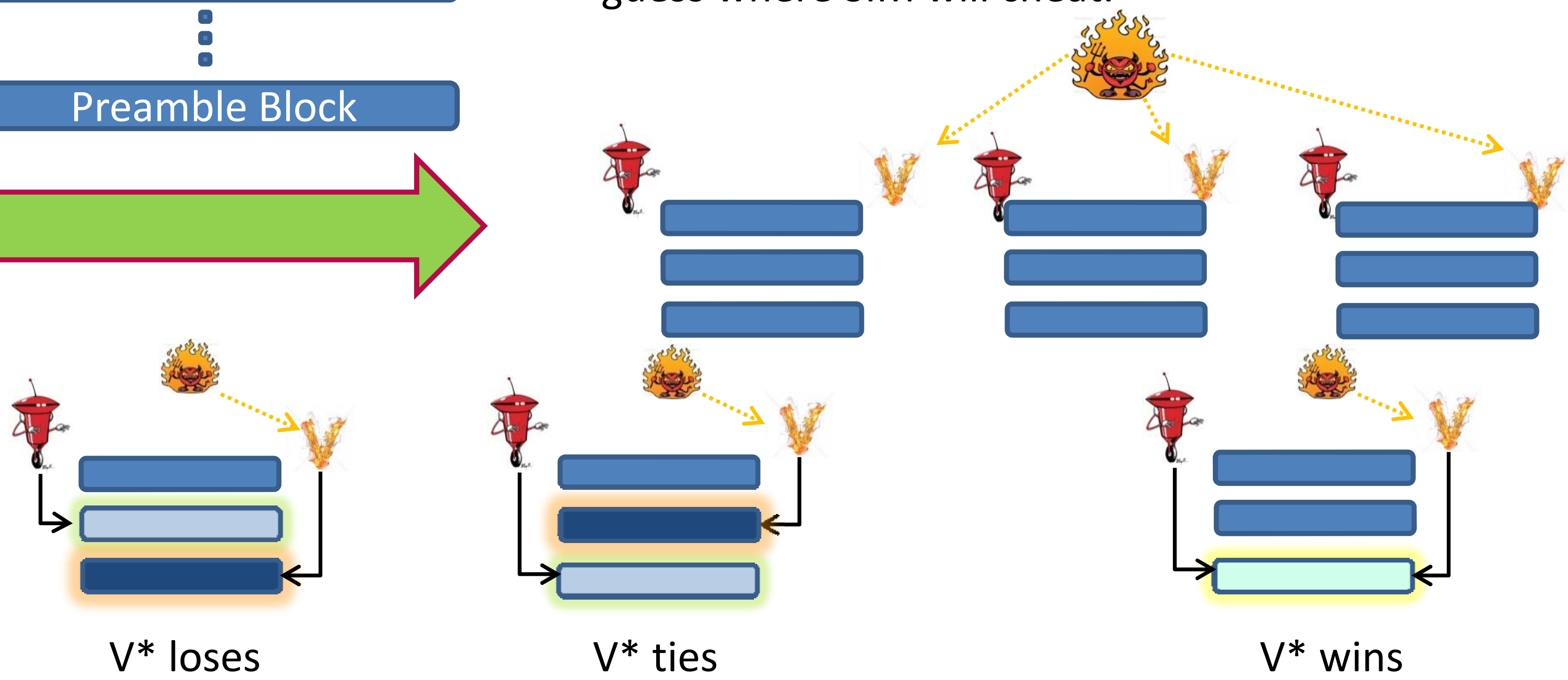
We encounter the same issue as someone attempting to extend (P_B, V_B) to the setting of unbounded concurrency.

Main Idea – Many Preamble Blocks

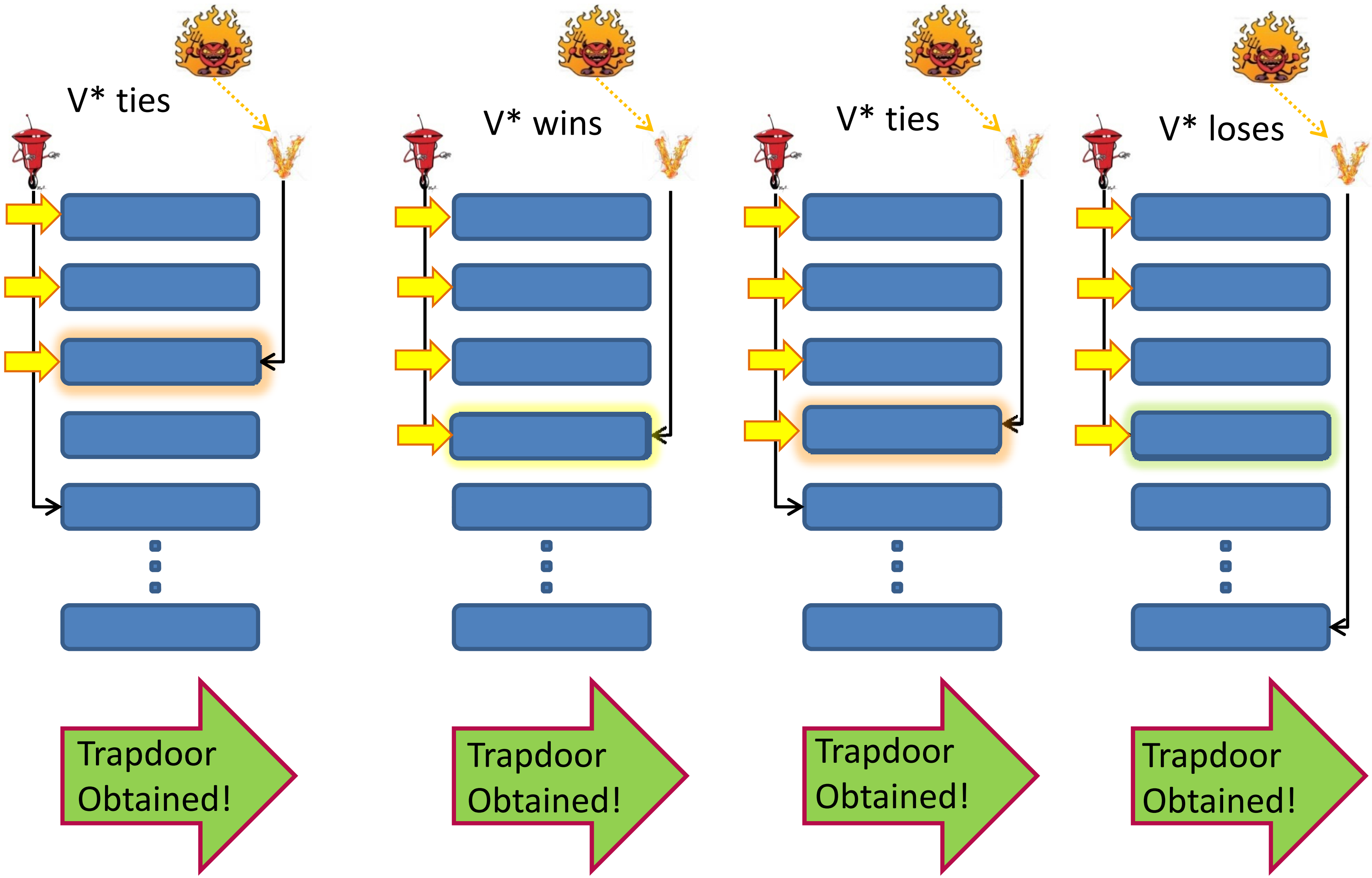


Advantages: Simulator only needs to extract the secret key once *per player*.

Interleaving attack is now less dangerous: V* must guess where SIM will cheat.



A Sample Simulation



Where to Cheat?

- At least $\omega(1)$ preamble blocks are needed per session.
- **Theorem (Main Technical Lemma):**
  $\omega(1)$ preamble blocks are sufficient.
- **We will**:
  - ➢ Construct distribution on {preamble blocks} describing where SIM will cheat.
  - ➢ Prove that SIM will have to cheat at most a bounded polynomial number of times per player.

The Distribution

- Fix $k = \omega(1)$. Consider the protocol with k preamble blocks.

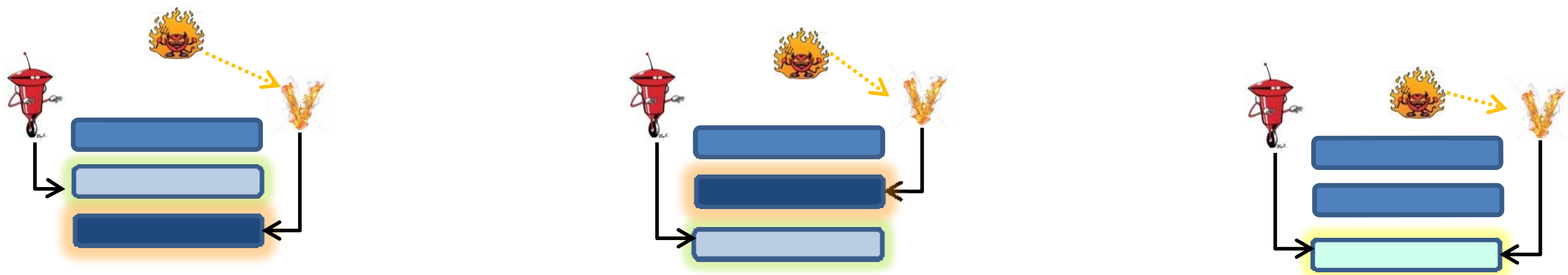
- Note the uniform distribution: $p_i = \frac{1}{k}$ does not work (V* always picks first preamble block).

- We use instead: $p_i = \varepsilon n^i$,
  where ε is such that $\sum_i p_i = 1$.

Proof Intuition of MTL (1/2)

- Recall we must bound the number of non-blackbox simulations required to learn sk.

- In light of the terminology:



V* **loses** session V* **ties** session V* **wins** session

It suffices to show that V* cannot win p(*n*) times without losing.

Proof Intuition of MTL (2/2)

- We bound Prob(V* wins) in terms of Prob(V* loses).
  - **P(W) ≤ 2*n* P(L).**
- We bound P(W) in terms of *n*.
  - **P(W)** $\leq \left(\mathbf{1} - \frac{\mathbf{1}}{\mathbf{2}n\mathbf{+1}}\right)$
- Given n^3 sessions, can bound Prob(V* wins all).
  - P(V* wins all) $\leq \left(1 - \frac{1}{2n+1}\right)^{n^3} \leq e^{-n}$.
  -  succeeds with high probability.

Conclusion

- We define **the bounded player model**.
  - ➢A natural model – can bound players, not sessions.
  - ➢Seemingly closer to the plain model than other existing models.
- We construct a cZK protocol in the BP model.
  - ➢Sublogarithmic round complexity.
  - ➢Straight line non-blackbox simulator.
- We construct a PDF with appealing properties.
  - ➢Possible applications elsewhere.

Questions?