

CERIAS

The Center for Education and Research in Information Assurance and Security

Memory-Hard Proofs of Work

How can I charge a meaningful computation fee?

Jeremiah Blocki, **Nathan Smearsoll**
Purdue University

What is a Proof of Work?

The prover runs $\text{Prove}^H(\chi, N) \rightarrow c$

The verifier runs $\text{Verify}^H(\chi, N, c') \rightarrow \{\text{true}, \text{false}\}$

- H is a random oracle
- χ is an input string
- N is a security parameter
- c is the certificate
- c' is a potential certificate

What does it mean to be Memory-Hard?

$H: \{0,1\}^z \rightarrow \{0,1\}^\lambda$ is a random oracle/perfect hash function

Computation of algorithm A occurs over y rounds which make a batch of queries Q_i

Receive back $H(Q_i) = [H(x_{i,1}), \dots, H(x_{i,j})]$ and old state σ_i

We measure cumulative memory complexity:

$$cmc(A^H(\dots)) = \sum_{i=1}^y |\sigma_i|$$

Memory-Hardness is more egalitarian.

What is a Memory-Hard Proof of Work?

The prover runs $\text{Prove}^H(\chi, N) \rightarrow c$

The verifier runs $\text{Verify}^H(\chi, N, c') \rightarrow \{\text{true}, \text{false}\}$

Perfect Completeness:

$$\Pr[\text{Verify}^H(\chi, N, \text{Prove}^H(\chi, N)) = \text{true}] = 1$$

(ϵ, C)-Soundness:

$$\Pr[\text{Verify}^H(\chi, N, A^H(\chi, N)) \text{ and } cmc(A^H(\chi, N)) \leq C] \leq \epsilon$$

We show that:

Our protocol is sound when instantiated with a depth-robust graph.

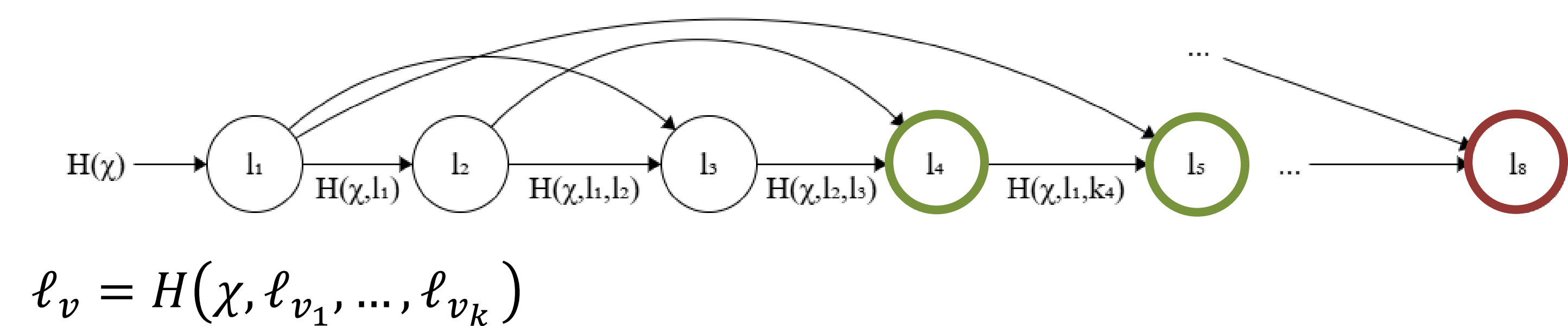
Instantiating with DRSample:

With high probability, any prover which outputs a valid certificate for our construction must have cumulative memory cost at least

$$O\left(\frac{N^2}{\log N}\right).$$

Honest Provers must:

Label a Graph

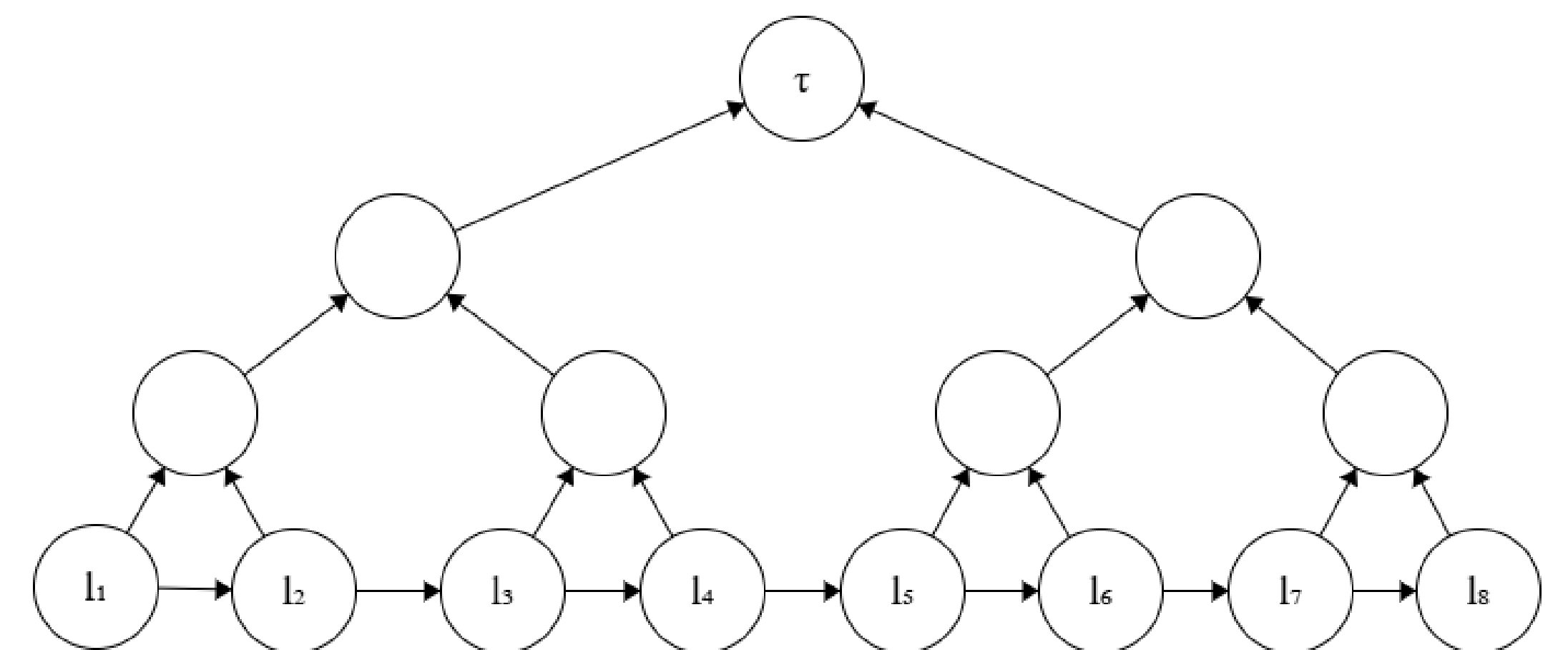


Green if internally consistent

Red otherwise

P_i pebbles the green graph

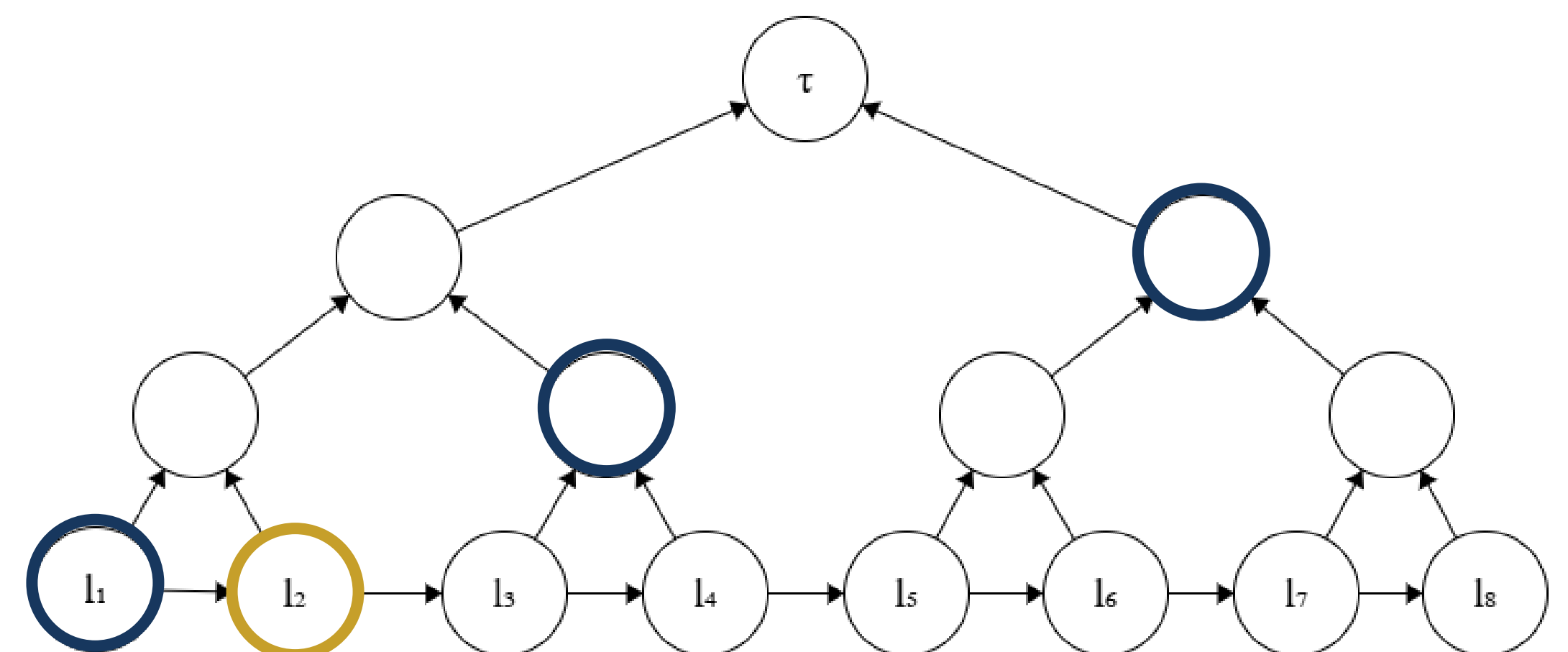
Label a Merkle Tree



$$\ell_s = H(s, \ell_{s||0}, \dots, \ell_{s||1})$$

Extract from a queries.
⊥ if no such query.

Answer Challenges



$$c_i = (H(\chi, i, \tau) \bmod N)$$

We prove that:

You can extract a prediction of $|P_i|$ oracle queries from any state σ_i of A , impossibly compressing the random oracle H .