Constant-Round Arguments for Batch-Verification and Bounded-Space Computations from OWF

CRYPTO, August 2024

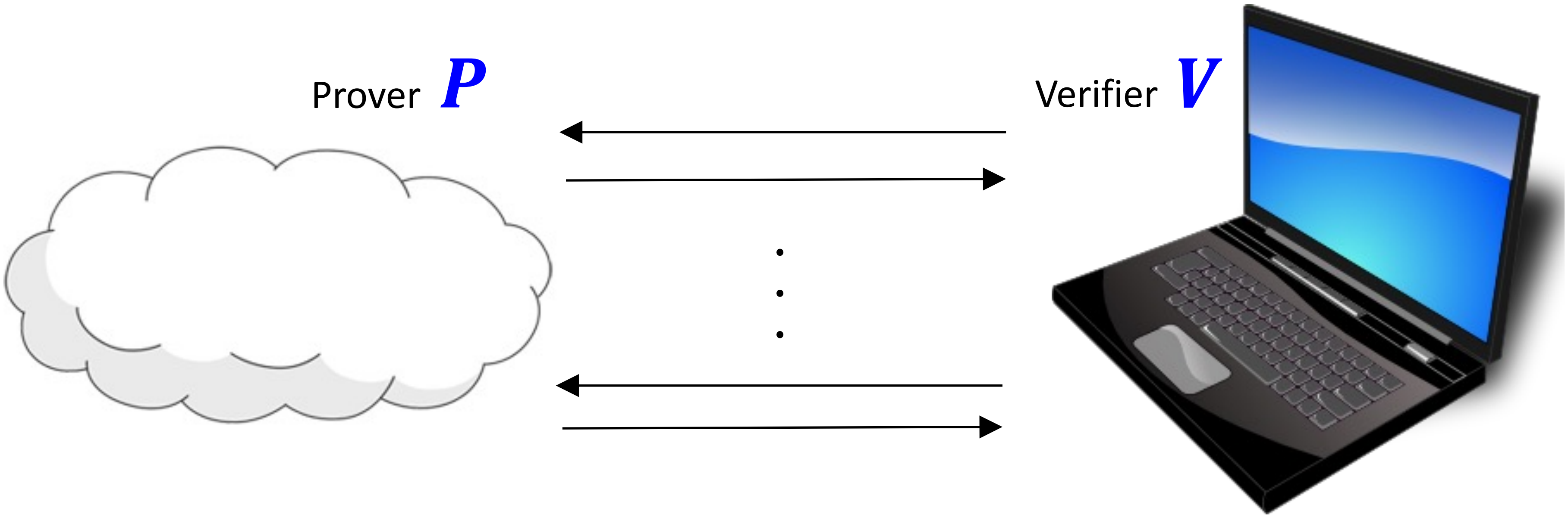
Noga Amit

UC Berkeley

Guy Rothblum

Apple

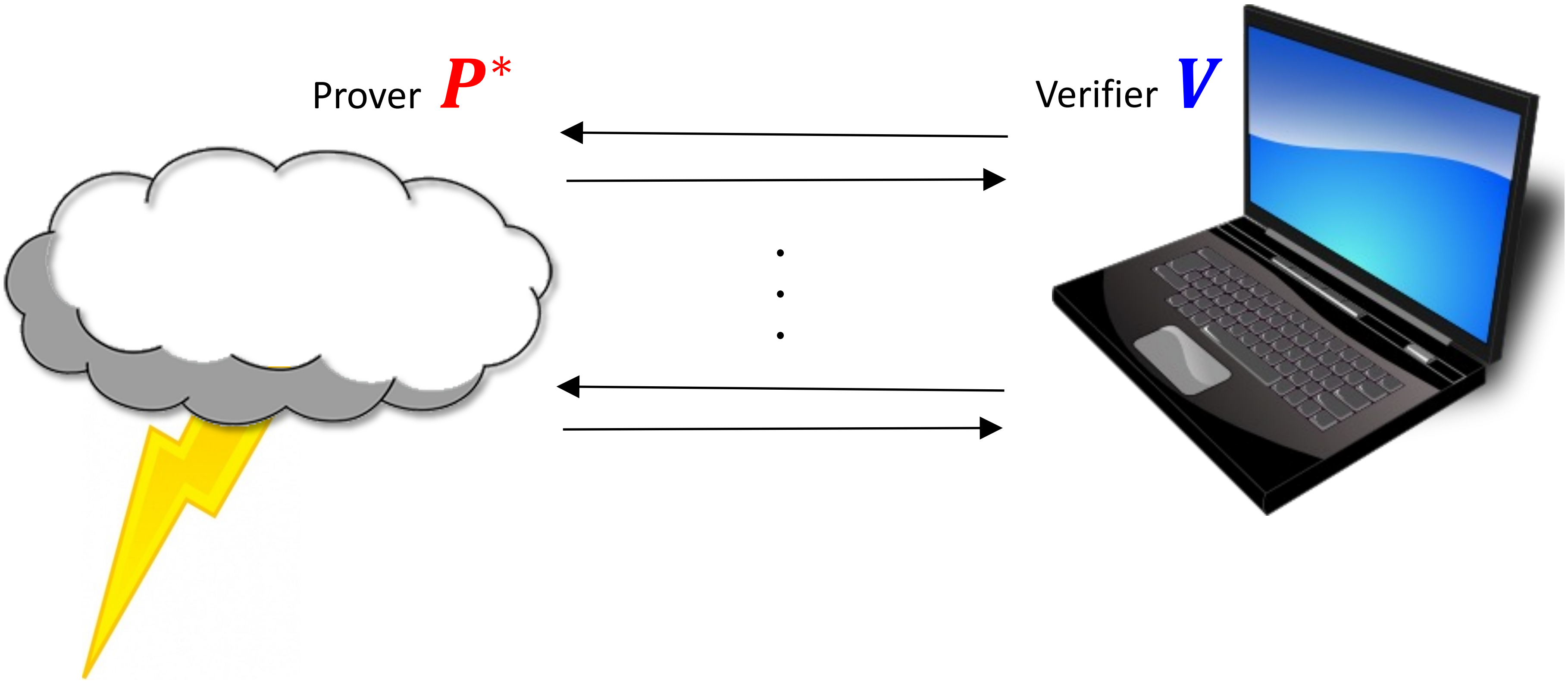
Interactive Proof / Argument



Untrusted P claims $x \in L$

Completeness $\forall x \in L,\ \Pr[\langle P, V\rangle \text{ accepts}] = 1$

Interactive Proof / Argument



Soundness $\forall x \notin L$, **unbounded/poly-time** P^*,

$$\Pr[\langle P^*, V\rangle \text{ accepts}] \leq 1/2$$

Interactive Proof / Argument

Complexity communication, rounds, V-time, P-time

Double efficiency (DE) for languages in **P**:

1. Verifier should be super efficient
   almost-linear V-time $\ll$ deciding $x \in L$?

2. Prover should be relatively efficient
   polynomial P-time $\approx$ deciding $x \in L$?

for languages in **NP**: given the **NP**-witness

Our Question

What assumptions are needed for constructing

- constant-round,
- almost-linear communication and V-time, DE

arguments?

- [Kil92] **CRH** $\Longrightarrow$ 2 rounds, sublinear communication, DE
  - For **NP**
- Can we replace **CRH** with **OWF**?
  - Equivalently [Rom90, KK08], with **UOWHF**? [NY89]
- [AR23] **OWF** $\Longrightarrow$ $O(1)$ rounds, DE for $\mathrm{Depth}(\boldsymbol{D})$, $\mathrm{Size}(poly(\boldsymbol{n}))$

First Result: Flat-RRR

Theorem:

Assume **OWF**s exist. $\forall \boldsymbol{\sigma} \in (0,1)$, every language in $\mathrm{Space}(\boldsymbol{S})$, $\mathrm{Time}(poly(\boldsymbol{n}))$ has a **constant-round, DE** interactive argument with:

Communication	$\boldsymbol{n}^{\sigma} \cdot O(\boldsymbol{S}^2)$
Rounds	$1 / \boldsymbol{\sigma}^4$
***V*-time**	$\boldsymbol{n}^{\sigma} \cdot O(\boldsymbol{S}^2 + \boldsymbol{n})$
***P*-time**	$poly(\boldsymbol{n})$

First Result: Flat-RRR

Theorem:

Assume **OWF**s exist. $\forall \boldsymbol{\sigma} \in (0,1)$, every language in $\mathrm{Space}(\boldsymbol{S})$, $\mathrm{Time}(poly(\boldsymbol{n}))$ has a **constant-round, DE** interactive argument with:

	This	**[RRR16]**
Communication	$\boldsymbol{n}^{\sigma} \cdot O(\boldsymbol{S}^2)$	$\boldsymbol{n}^{\sigma} \cdot poly(\boldsymbol{S})$
Rounds	$1 / \boldsymbol{\sigma}^4$	$exp(\tilde{O}(1/\boldsymbol{\sigma}))$
***V*-time**	$\boldsymbol{n}^{\sigma} \cdot O\left(\boldsymbol{S}^2 + \boldsymbol{n}\right)$	
***P*-time**	$poly(\boldsymbol{n})$	

UP Batch Verification

<u>**UP**</u>

- Given $\boldsymbol{N} \in \mathbb{Z}$, is there a *unique witness* $\boldsymbol{p}, \boldsymbol{q} \in \mathbb{Z}$ such that $\boldsymbol{N} = \boldsymbol{p} \cdot \boldsymbol{q}$?

<u>**UP** Batching</u>

- Given $\boldsymbol{N_1}, \dots, \boldsymbol{N_k} \in \mathbb{Z}$, are there $(\boldsymbol{p_i}, \boldsymbol{q_i})_{i \in [k]} \in \mathbb{Z}$ such that $\forall i, \boldsymbol{N_i} = \boldsymbol{p_i} \cdot \boldsymbol{q_i}$?

<u>**UP** Batch Verification</u>

- Given $\boldsymbol{N_1}, \dots, \boldsymbol{N_k} \in \mathbb{Z}$, *prover tries to convince a verifier* that there are $(\boldsymbol{p_i}, \boldsymbol{q_i})_{i \in [k]} \in \mathbb{Z}$ such that $\forall i, \boldsymbol{N_i} = \boldsymbol{p_i} \cdot \boldsymbol{q_i}$

UP Batch Verification

- **UP** Batch Verification
  - Given $N_1, \ldots, N_k \in \mathbb{Z}$, prover P tries to convince a verifier V that there are $(p_i, q_i)_{i \in [k]} \in \mathbb{Z}$ s.t. $\forall i, N_i = p_i \cdot q_i$

P gets the k witnesses

- <u>Naive solution</u>: P sends $(p_i, q_i)_{i \in [k]}$

- <u>Goal</u>: Achieving cc $\ll k \cdot |\text{witness}|$

Second Result: UP Batch Verification

Theorem:

Assume **OWF**s exist. $\forall \boldsymbol{\sigma} \in (0,1)$, every **UP** language with witness relation in $\text{Depth}(\boldsymbol{D})$, $\text{Size}(poly(\boldsymbol{n}))$ has a **constant-round, DE** interactive argument for batching $\boldsymbol{k}$ instances with:

Communication	$\tilde{O}(\boldsymbol{M} + \boldsymbol{k} \cdot \boldsymbol{n}^{\boldsymbol{\sigma}} \cdot \boldsymbol{D})$
Rounds	$O(1/\boldsymbol{\sigma}^3)$
$\boldsymbol{V}$**-time**	$\tilde{O}(\boldsymbol{M} + \boldsymbol{k} \cdot \boldsymbol{n}^{\boldsymbol{\sigma}} \cdot (\boldsymbol{n} + \boldsymbol{D}))$
$\boldsymbol{P}$**-time**	$poly(\boldsymbol{n})$ given the $\boldsymbol{k}$ witnesses

Second Result: UP Batch Verification

Theorem:

Assume **OWF**s exist. $\forall \boldsymbol{\sigma} \in (0,1)$, every **UP** language with witness relation in $\mathrm{Depth}(\boldsymbol{D}), \mathrm{Size}(poly(\boldsymbol{n}))$ has a **constant-round, DE** interactive argument for batching $\boldsymbol{k}$ instances with:

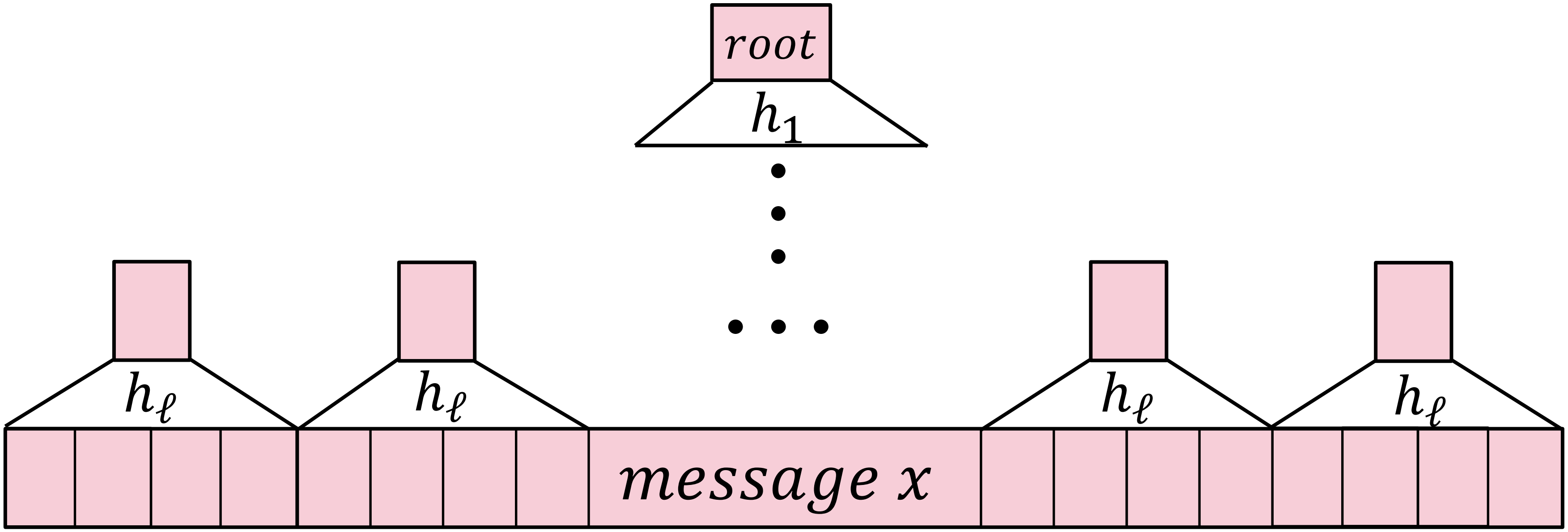
The first $O(1)$ rounds with quasi-linear cc!

Communication	$\tilde{O}(\boldsymbol{M} + \boldsymbol{k} \cdot \boldsymbol{n}^{\boldsymbol{\sigma}} \cdot \boldsymbol{D})$
Rounds	$O(1/\boldsymbol{\sigma}^3)$
$\boldsymbol{V}$**-time**	$\tilde{O}(\boldsymbol{M} + \boldsymbol{k} \cdot \boldsymbol{n}^{\boldsymbol{\sigma}} \cdot (\boldsymbol{n} + \boldsymbol{D}))$
$\boldsymbol{P}$**-time**	$poly(\boldsymbol{n})$ given the $\boldsymbol{k}$ witnesses

UOWHF tree

[AR23] **UOWHFs-based Merkel tree** is a *targeted collision-resistant* hash with local opening

- $\boldsymbol{n^{\sigma}}$-ary tree with $\ell + 1$ layers
- $\boldsymbol{h_i}$ are **UOWHF**s $\{0,1\}^{n^{2\sigma}} \to \{0,1\}^{n^{\sigma}}$



Targeted Collision-Resistance

Commit: S chooses $\boldsymbol{x} \in \{0,1\}^{\boldsymbol{M}}$

R sends hash functions $\boldsymbol{h}_1, \ldots, \boldsymbol{h}_\ell \in \boldsymbol{H}$

(the unique correct hash root $\boldsymbol{y}$ is defined)

S sends a commitment $\widetilde{\boldsymbol{y}}$

Local-Opening: S outputs a leaf index $\boldsymbol{q}$ and an opening for $\boldsymbol{q}$

Security: If $\widetilde{\boldsymbol{y}} = \boldsymbol{y}$,

$\mathbf{Pr}[$ the opening is *valid*

and (the opening for $\boldsymbol{q}$) $\neq \boldsymbol{x}[\boldsymbol{q}]$ $]$ $=$ negligible

UP Batch Verification: Overview

- Goal: Given k inputs $x_1, \ldots, x_k$,
  - V accepts if $x_1, \ldots, x_k \in L$
  - Rejects otherwise w.h.p.
- Protocol begins with P sending hash roots to $w_1, \ldots, w_k$
- Suppose that
  - all but one x_{i^*} are in L
  - P sends correct roots $\forall i \neq i^*$
- Targeted collision-resistance $\Longrightarrow$ P is committed to w_i

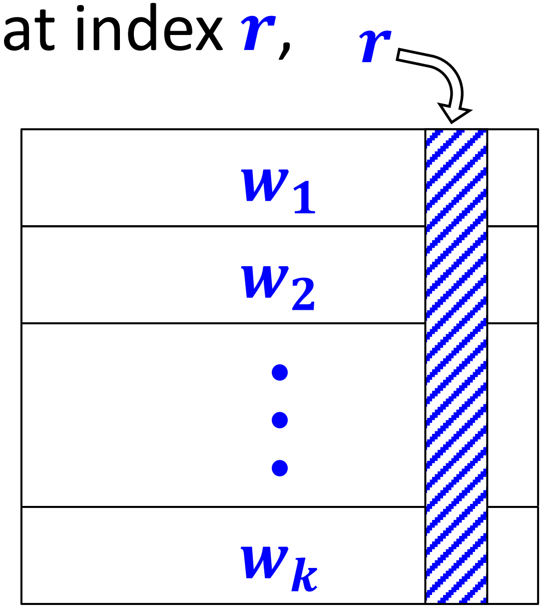
UP Batch Verification: Overview

- Then, $\boldsymbol{P}$ sends **XOR** of $\boldsymbol{w_1, \ldots, w_k}$

$\boldsymbol{w_1}$
$\boldsymbol{w_2}$
⋮
$\boldsymbol{w_k}$
XOR = $\bigoplus_{i \in [k]} \boldsymbol{w_i}$

UP Batch Verification: Overview

- Then, P sends **XOR** of $w_1, \dots, w_k$
- Whenever P is asked to locally-open w_i at index r, it locally-opens all k witnesses at r



- P is effectively committed to "$w_{i^*}[r]$" as well!

UP Batch Verification: Overview

[AR23] "**flat-GKR**"

- Running a protocol $\forall \boldsymbol{i}$ for checking $\boldsymbol{x_i} \in \boldsymbol{L}$
  - sound as long as $\boldsymbol{w_i}$ is fixed
  - makes a single query to (encoding) of $\boldsymbol{w_i}$

[RR19] "**code-switching**"
to obtain quasi-linear cc

- <u>Recall</u>: $\boldsymbol{P}$ is effectively committed to "$\boldsymbol{w_{i^*}[r]}$" → caught!

UP Batch Verification: Overview

- Getting rid of the assumptions
  - all but one x_{i^*} are in L
  - P sends correct roots $\forall i \neq i^*$
- V guesses a subset of $[k]$ where this holds w.h.p.

after P sends the commitment!

UP Batch Verification: The Protocol

1. V samples UOWHFs and sends them to P

2. P sends hash roots $y_1, \ldots, y_k$ for the k witnesses

3. V samples a subset $I \subseteq [k]$ and sends it to P

4. P sends the **XOR** of $w_{i_1}, \ldots, w_{i_{|I|}}$:

w_{i_1}
w_{i_2}
$\vdots$
$w_{i_{\vert I \vert}}$
XOR = $\bigoplus_{i \in I} w_i$

UP Batch Verification: The Protocol

1. V samples UOWHFs and sends them to P

2. P sends hash roots $y_1, \dots, y_k$ for the k witnesses

3. V samples a subset $I \subseteq [k]$ and sends it to P

4. P sends the **XOR** of $w_{i_1}, \dots, w_{i_{|I|}}$

5. P and V run a protocol $\forall i \in I$ that verifies w_i and y_i
   - V asks P to open y_i at r
   - V checks that the openings are (a) valid w.r.t. the UOWHFs

     (b) consistent with **XOR**

UP Batch Verification: The Protocol

1. V samples UOWHFs and sends them to P

2. P sends hash roots $y_1, \ldots, y_k$ for the k witnesses

3. V samples a subset $I \subseteq [k]$ and sends it to P

4. P sends the **XOR** of $w_{i_1}, \ldots, w_{i_{|I|}}$

the only dependence on $|\mathrm{witness}|$!

5. P and V run a protocol $\forall i \in I$ that verifies w_i and y_i
   - V asks P to open y_i at r
   - V checks that the openings are (a) valid w.r.t. the UOWHFs
     (b) consistent with **XOR**

Summary & Open Questions

OWF ⟹ targeted collision-resistant hash with local opening

⟹ constant-round arguments

Bounded-depth | Bounded-space | **UP** batching

for languages in **P**

- Arguments for **P** based on **OWF**? For **NP**?

Thank you!