November 9, 2023

The Mastic Verifiable Distributed Aggregation Function (VDAF)

Hannah Davis, **Dimitris Mouris**, Christopher Patton,

Pratik Sarkar, Nektarios G. Tsoutsos

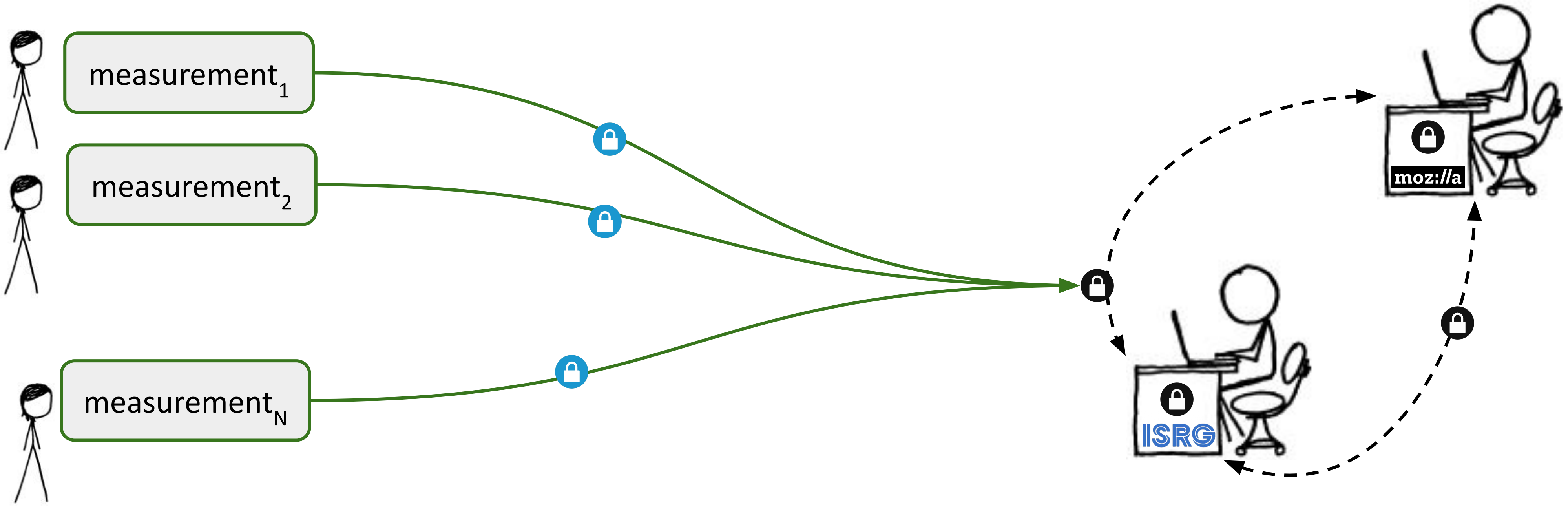
*hannahedavis@protonmail.com, **jimouris@udel.edu**, cpatton@cloudflare.com,*

pratik93@bu.edu, tsoutsos@udel.edu

https://datatracker.ietf.org/doc/draft-mouris-cfrg-mastic

Verifiable Distributed Aggregation Functions

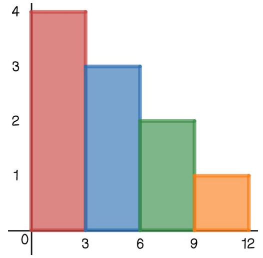
Securely compute aggregation functions over client measurements.

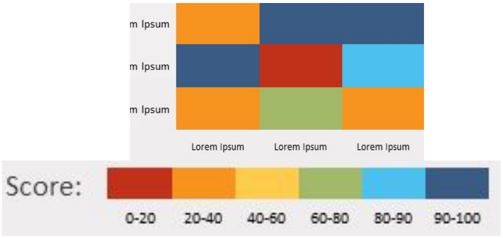


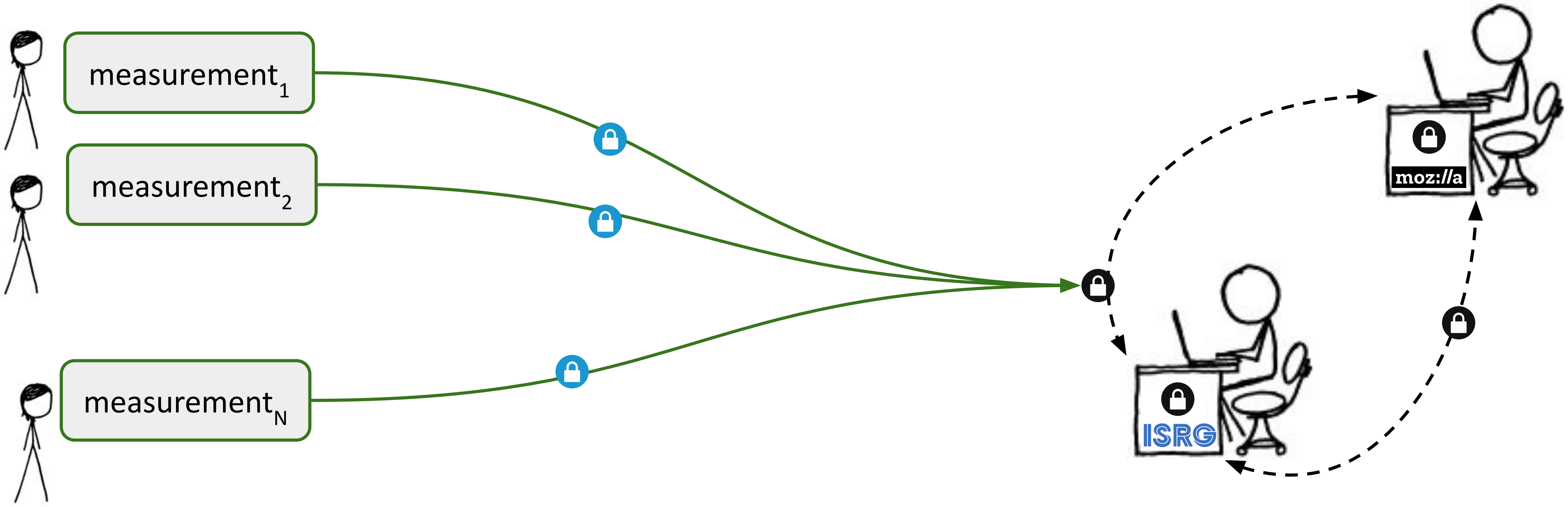
Verifiable Distributed Aggregation Functions

Securely compute aggregation functions over client measurements.

- **Counts:** Add client measurements.
- **Histograms:** Add client measurements by category.
- **Heatmaps:** Add client measurements by categories.
- **Heavy-hitters:** Find most popular client submissions.





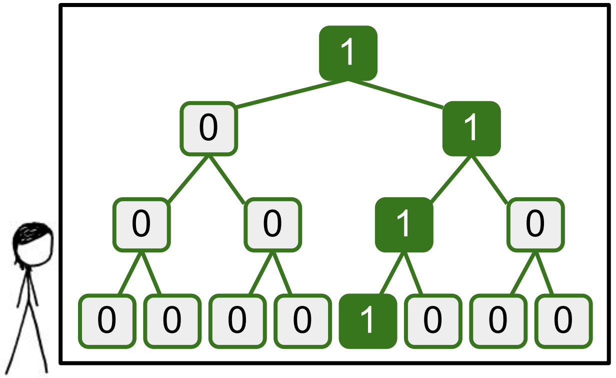


measurement$_1$

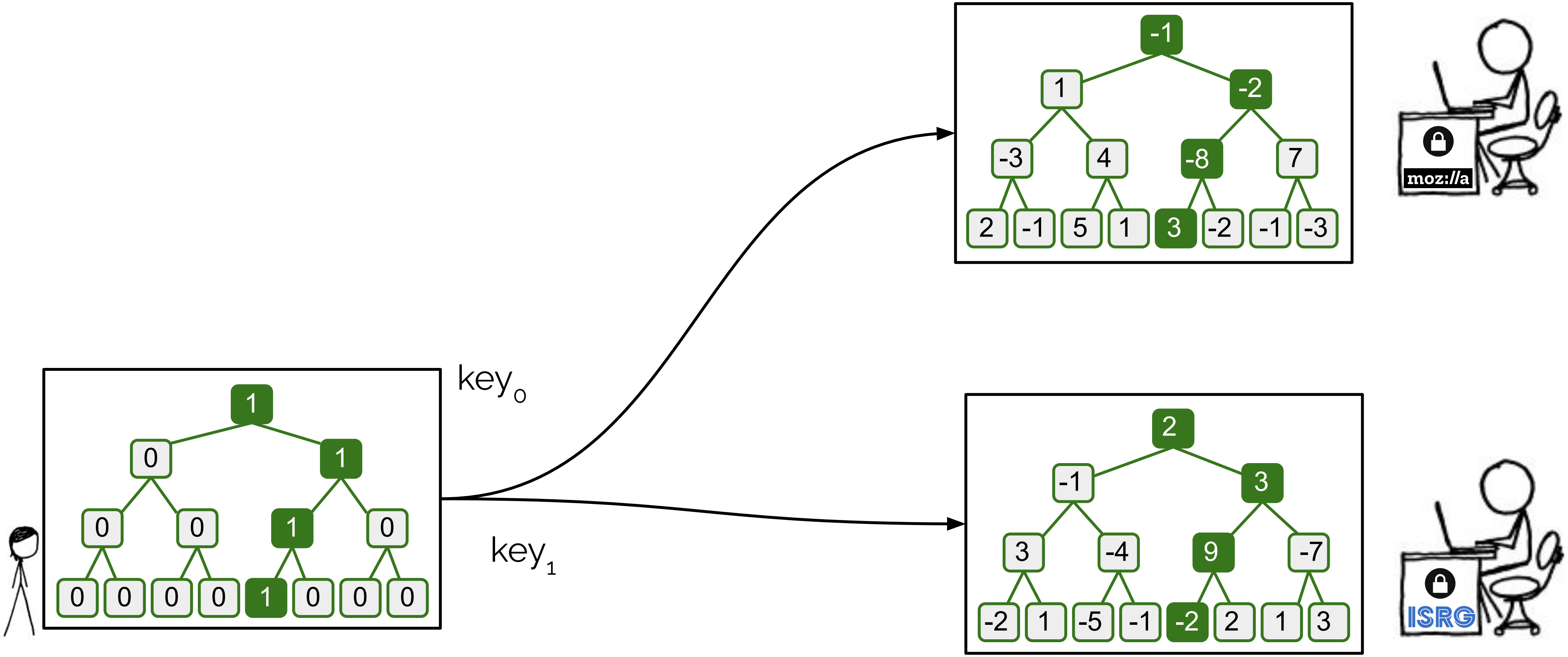
measurement$_2$

measurement$_N$

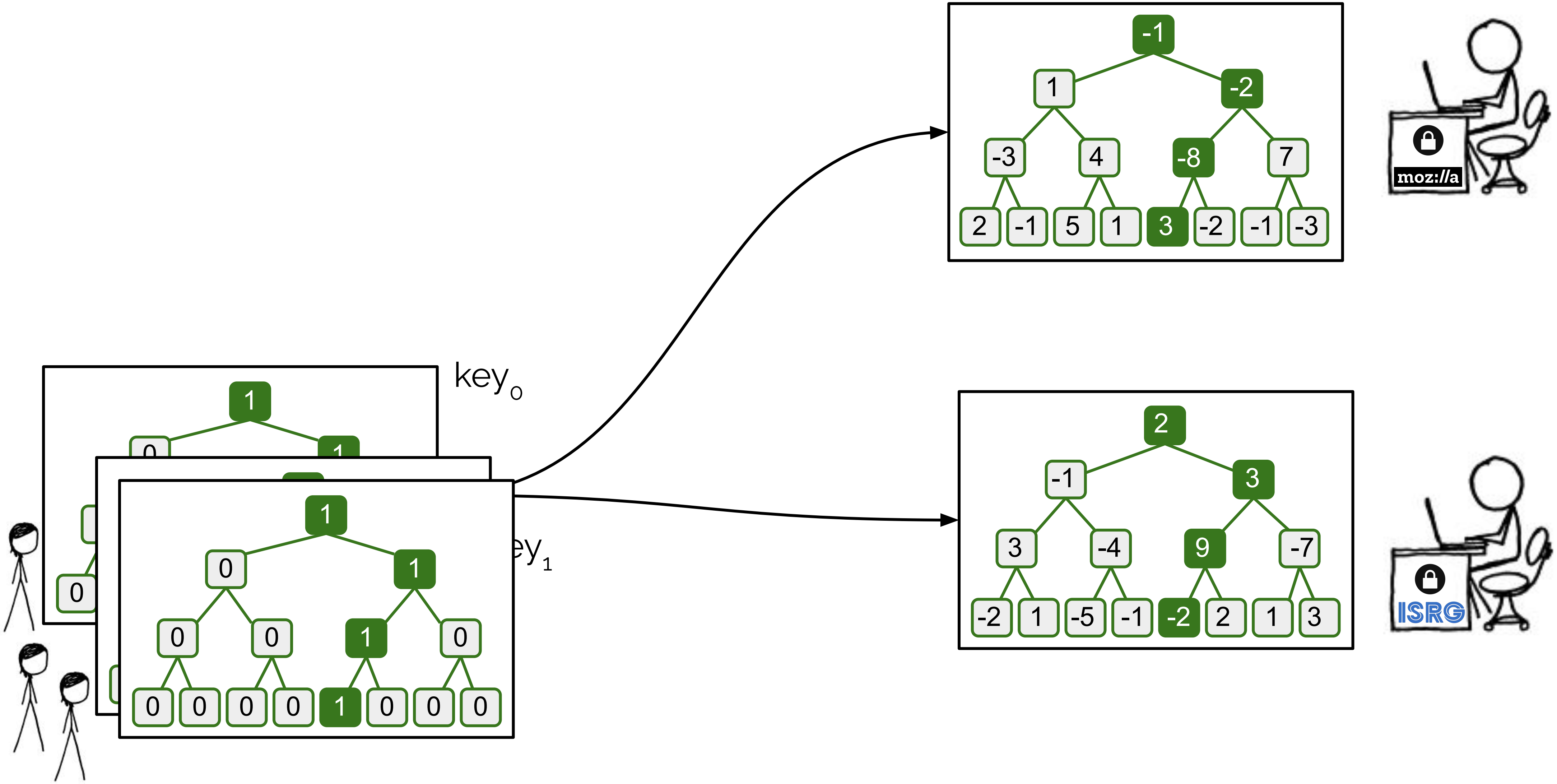
Distributed Point Functions (DPFs)



Distributed Point Functions (DPFs)



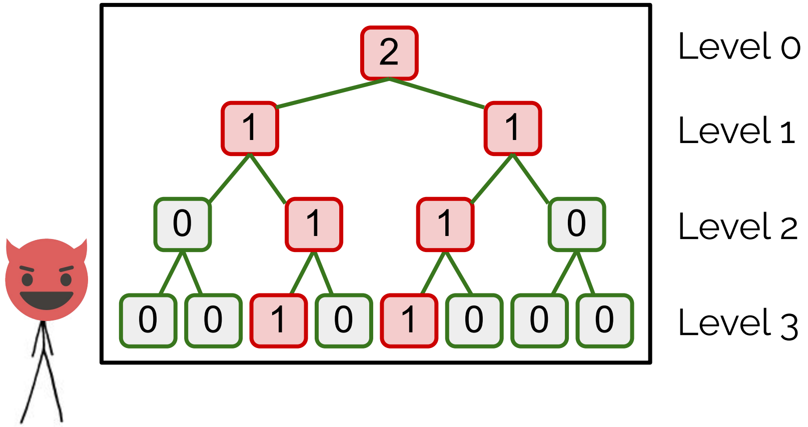
Distributed Point Functions (DPFs)



One-hot Verifiability

Each level of the tree needs to be one-hot!

Double-vote: Submit a tree with multiple non-zero points!

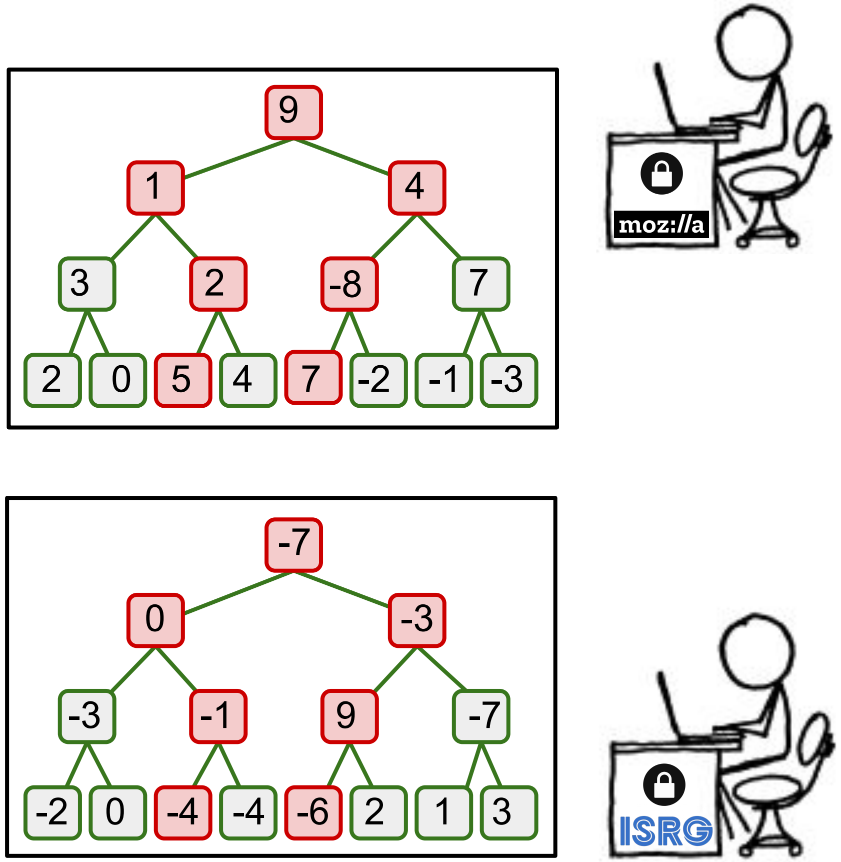


Level 0

Level 1

Level 2

Level 3



One-hot Verifiability

- **One-hot Verifiability:** Each level has *at most one* non-zero value β.
    - We get this property from the VIDPF of PLASMA [1].

[1] Mouris, D., Sarkar, P., & Tsoutsos, N. G. *PLASMA: Private, Lightweight Aggregated Statistics against Malicious Adversaries.* https://ia.cr/2023/080

One-hot Verifiability

- **One-hot Verifiability:** Each level has *at most one* non-zero value *β*.
  - We get this property from the VIDPF of PLASMA [1].

Evaluate(**Prefix**, key$_0$) = $(\mathbf{Y}, \boldsymbol{\pi}_0)$

$\mathbf{Y} = \{ \mathbf{y}_1, \mathbf{y}_2, \dots, \mathbf{y}_m \}$

Evaluate(**Prefix**, key$_1$) = $(\mathbf{Z}, \boldsymbol{\pi}_1)$

$\mathbf{Z} = \{ \mathbf{z}_1, \mathbf{z}_2, \dots, \mathbf{z}_m \}$

Vectors of Secret

Shares for a level

[1] Mouris, D., Sarkar, P., & Tsoutsos, N. G. *PLASMA: Private, Lightweight Aggregated Statistics against Malicious Adversaries.* https://ia.cr/2023/080

One-hot Verifiability

- **One-hot Verifiability:** Each level has *at most one* non-zero value *β*.
  - We get this property from the VIDPF of PLASMA [1].

Evaluate(**Prefix**, key$_0$) = **(Y, π_0)**

Y = { y$_1$, y$_2$, …, y$_m$ }

One-hot Verifiability:

if **π_0 = π_1**

then **Y+Z** is one-hot!

Evaluate(**Prefix**, key$_1$) = **(Z, π_1)**

Z = { z$_1$, z$_2$, …, z$_m$ }

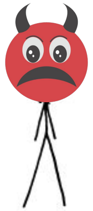
Vectors of Secret

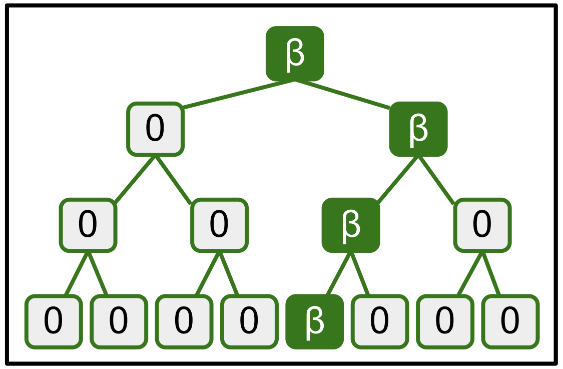
Shares for a level

[1] Mouris, D., Sarkar, P., & Tsoutsos, N. G. *PLASMA: Private, Lightweight Aggregated Statistics against Malicious Adversaries.* https://ia.cr/2023/080

One-hot Verifiability

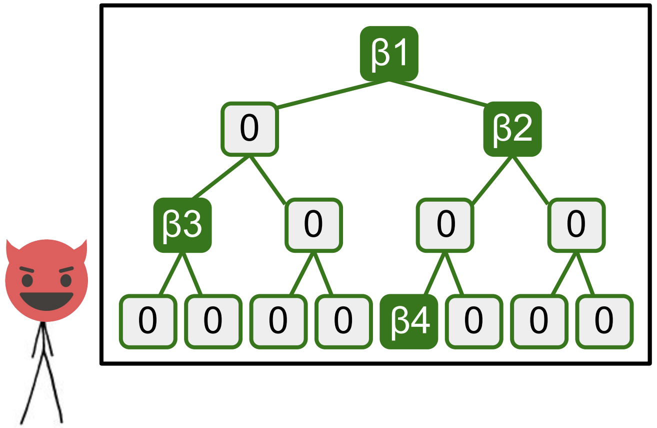
One-hot Verifiability: Asserts that each level has at most one non-zero value

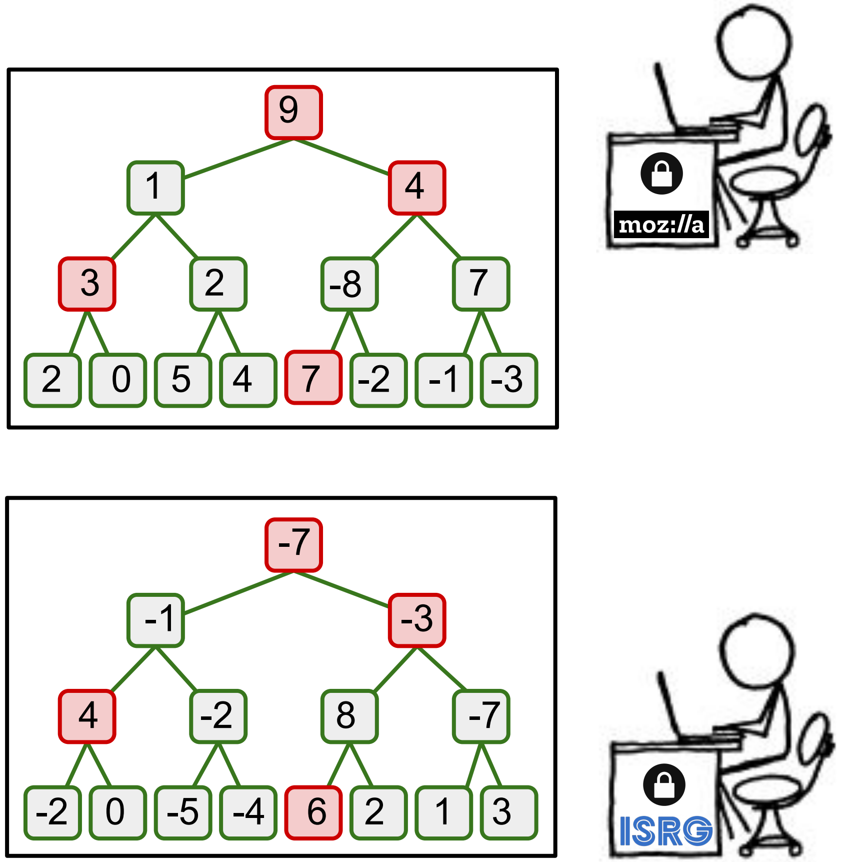




Path Verifiability

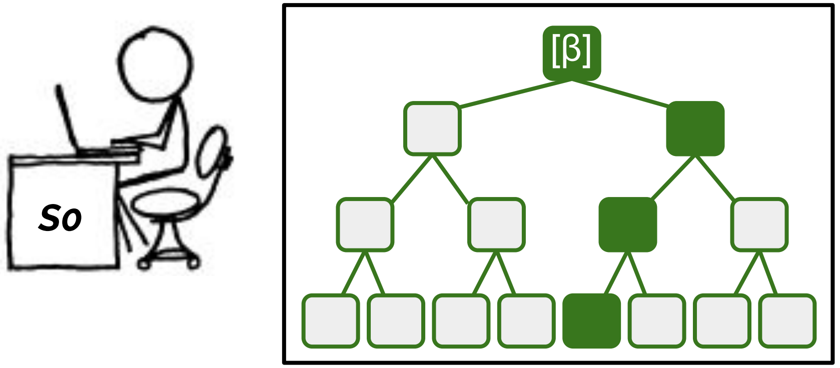
Path Inconsistency: β values are different and not on the same path!

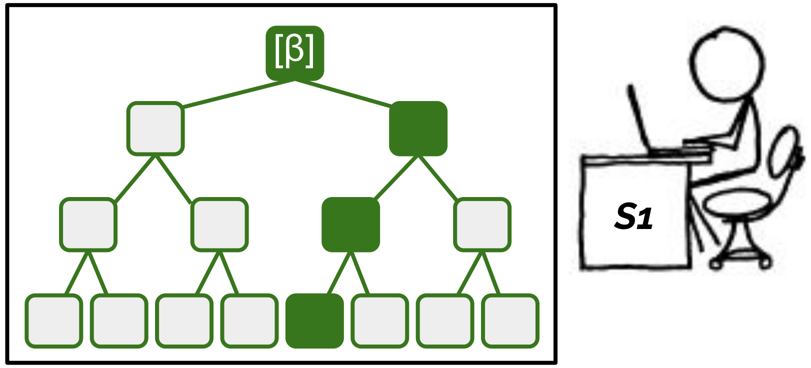




Path Verifiability

- **Path Verifiability:** Asserts that *β values* are the same and they are in one path.
  - **Step 1:** Verify that β is valid at the root using an FLP [2].



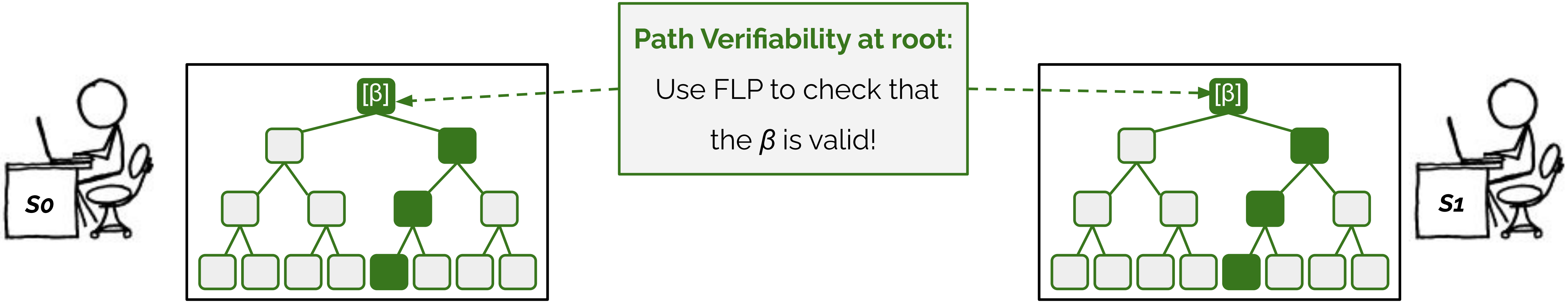


[1] Mouris, D., Sarkar, P., & Tsoutsos, N. G. *PLASMA: Private, Lightweight Aggregated Statistics against Malicious Adversaries.* https://ia.cr/2023/080

[2] Davis, H., Patton, C., Rosulek, M., & Schoppmann, P. *Verifiable Distributed Aggregation Functions.* https://ia.cr/2023/130

Path Verifiability

- **Path Verifiability:** Asserts that *β values* are the same and they are in one path.
  - **Step 1:** Verify that β is valid at the root using an FLP [2].



Path Verifiability at root:

Use FLP to check that

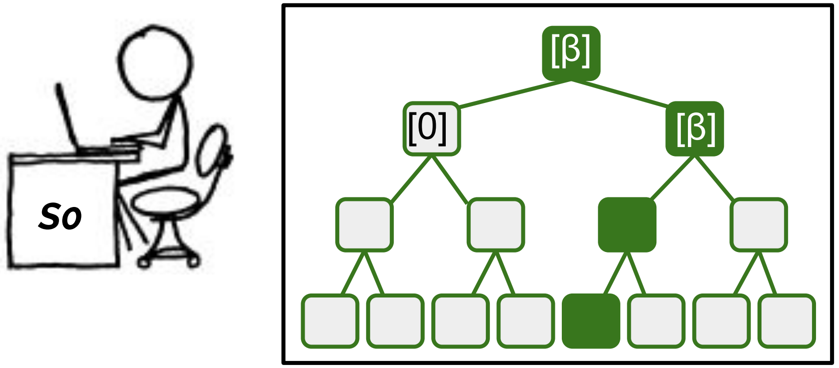
the *β* is valid!

[1] Mouris, D., Sarkar, P., & Tsoutsos, N. G. *PLASMA: Private, Lightweight Aggregated Statistics against Malicious Adversaries.* https://ia.cr/2023/080

[2] Davis, H., Patton, C., Rosulek, M., & Schoppmann, P. *Verifiable Distributed Aggregation Functions.* https://ia.cr/2023/130

Path Verifiability

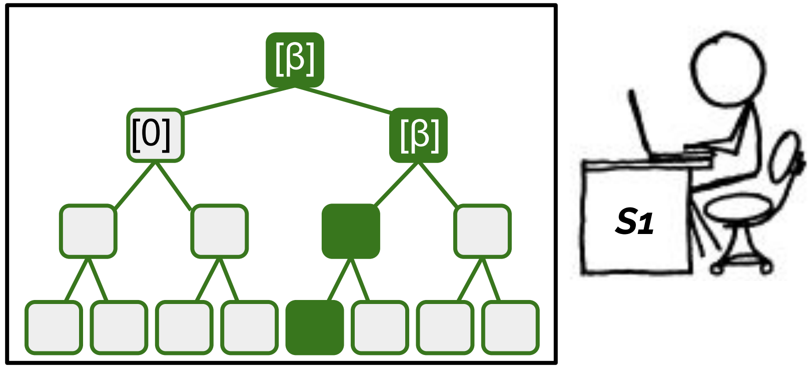
- **Path Verifiability:** Asserts that *β values* are the same and they are in one path.
  - **Step 1:** Verify that β is valid at the root using an FLP [2].
  - **Step 2:** Verify that β is correctly propagated down the tree *a la* PLASMA.



Path Verifiability:

at each level check

that $y^p = y^{p||0} + y^{p||1}$

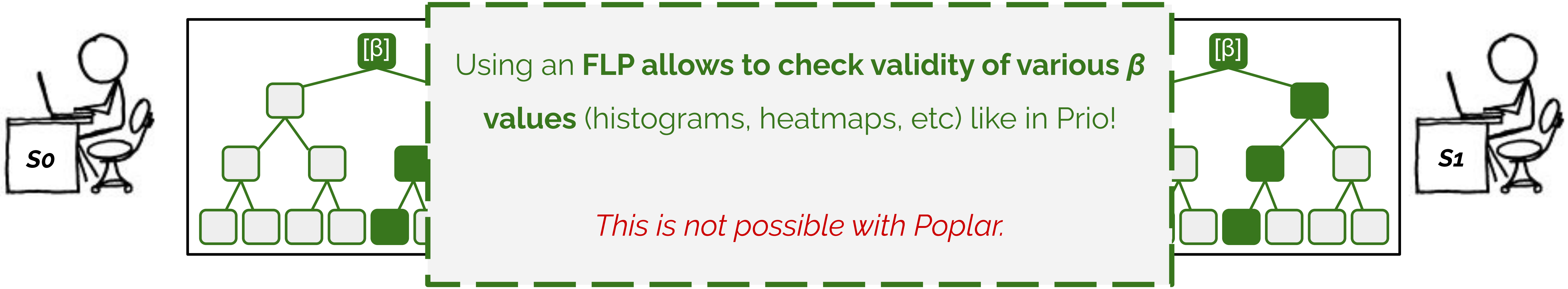


[1] Mouris, D., Sarkar, P., & Tsoutsos, N. G. *PLASMA: Private, Lightweight Aggregated Statistics against Malicious Adversaries.* https://ia.cr/2023/080

[2] Davis, H., Patton, C., Rosulek, M., & Schoppmann, P. *Verifiable Distributed Aggregation Functions.* https://ia.cr/2023/130

Path Verifiability

- **Path Verifiability:** Asserts that *β values* are the same and they are in one path.
  - **Step 1:** Verify that β is valid at the root using an FLP [2].
  - **Step 2:** Verify that β is correctly propagated down the tree *a la* PLASMA.



Using an **FLP allows to check validity of various *β* values** (histograms, heatmaps, etc) like in Prio!

This is not possible with Poplar.

[1] Mouris, D., Sarkar, P., & Tsoutsos, N. G. *PLASMA: Private, Lightweight Aggregated Statistics against Malicious Adversaries.* https://ia.cr/2023/080

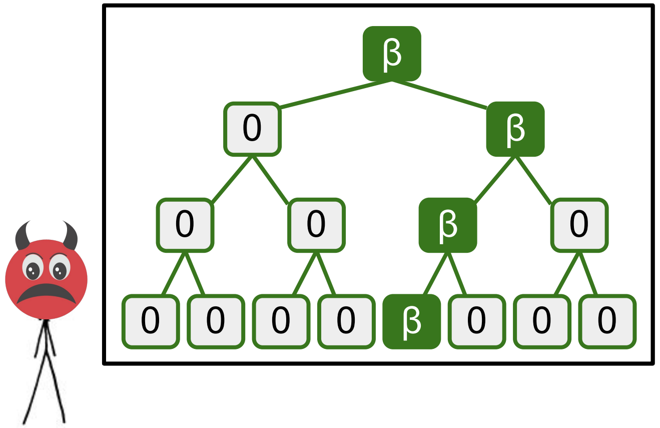
[2] Davis, H., Patton, C., Rosulek, M., & Schoppmann, P. *Verifiable Distributed Aggregation Functions.* https://ia.cr/2023/130

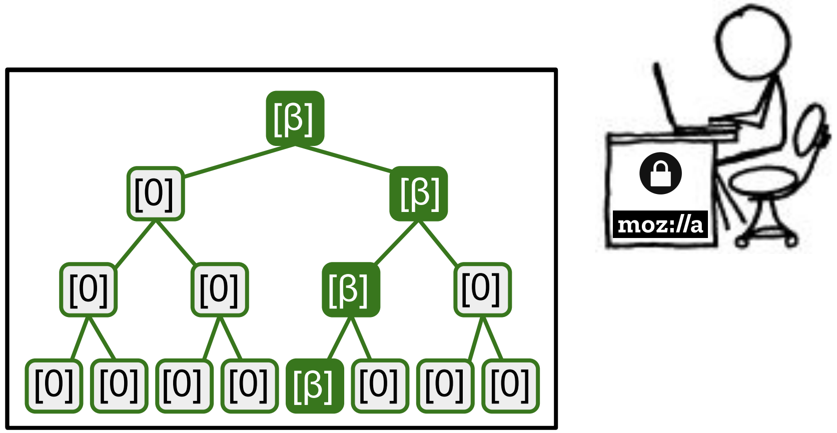
Thwarting Malicious Clients

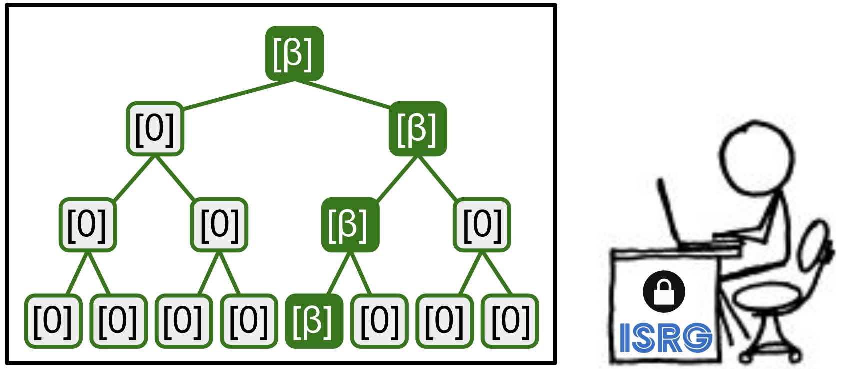
One-hot Verifiability: Asserts that each level has at most one non-zero value

+

Path Verifiability: Asserts that β values are the same and they are in one path

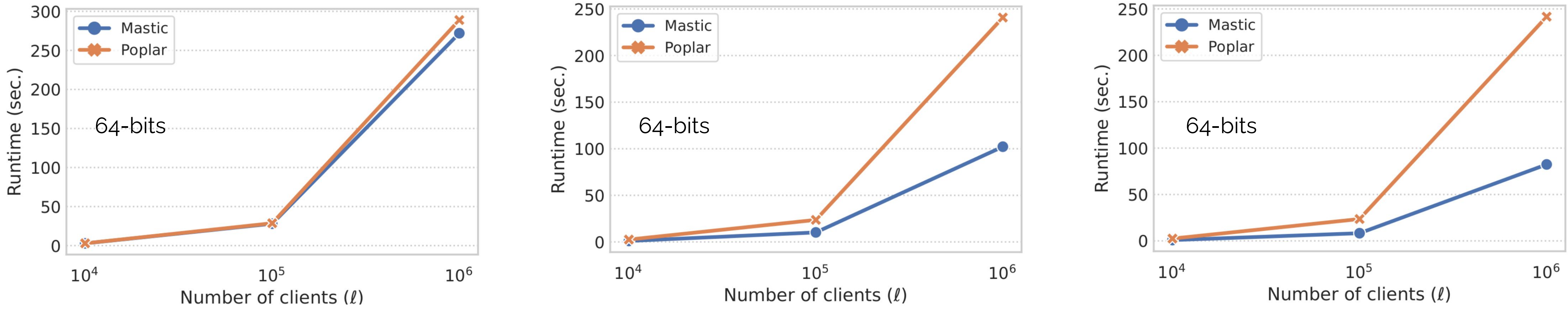






Preliminary Results for Heavy-Hitters

- **Mastic** is faster than Poplar [3] while ***enabling more elaborate statistics*** (Prio-like).
- **Mastic** becomes even faster for bigger thresholds T.



a) Threshold = 1% of ℓ

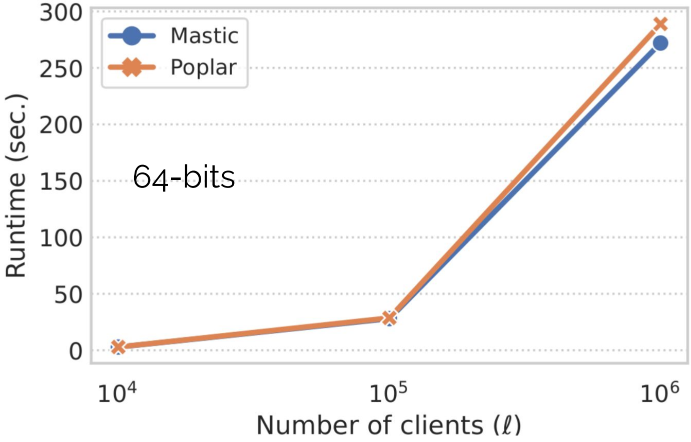
b) Threshold = 5% of ℓ

c) Threshold = 10% of ℓ

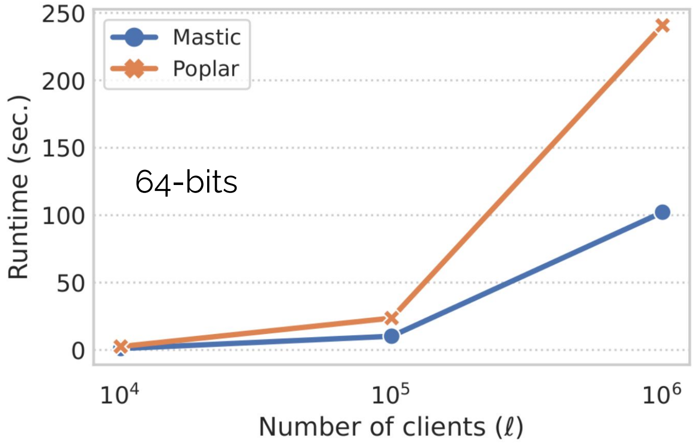
[3] D. Boneh, E. Boyle, H. Corrigan-Gibbs, N. Gilboa and Y. Ishai, *Lightweight Techniques for Private Heavy Hitters*. https://ia.cr/2021/017

Preliminary Results for Heavy-Hitters

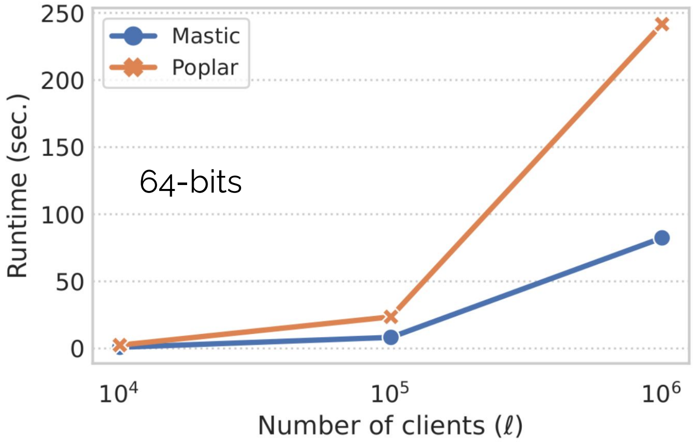
- **Mastic** is faster than Poplar [3] while ***enabling more elaborate statistics*** (Prio-like).
- **Mastic** becomes even faster for bigger thresholds T.



a) Threshold = 1% of ℓ



b) Threshold = 5% of ℓ



c) Threshold = 10% of ℓ

*Stay tuned for a **full security analysis** and **more evaluations** (paper coming soon)*

[3] D. Boneh, E. Boyle, H. Corrigan-Gibbs, N. Gilboa and Y. Ishai, *Lightweight Techniques for Private Heavy Hitters*. https://ia.cr/2021/017

Questions?

The Mastic Verifiable Distributed Aggregation Function (VDAF)

Hannah Davis, **Dimitris Mouris**, Christopher Patton,

Pratik Sarkar, Nektarios G. Tsoutsos

*hannahedavis@protonmail.com, **jimouris@udel.edu**, cpatton@cloudflare.com,*

pratik93@bu.edu, tsoutsos@udel.edu

https://datatracker.ietf.org/doc/draft-mouris-cfrg-mastic