March 31, 2023

PLASMA: Private, Lightweight Aggregated Statistics against Malicious Adversaries with Full Security

Dimitris Mouris[1], Pratik Sarkar[2], Nektarios G. Tsoutsos[1]

jimouris@udel.edu, *pratik93@bu.edu*, *tsoutsos@udel.edu*

https://eprint.iacr.org/2023/80

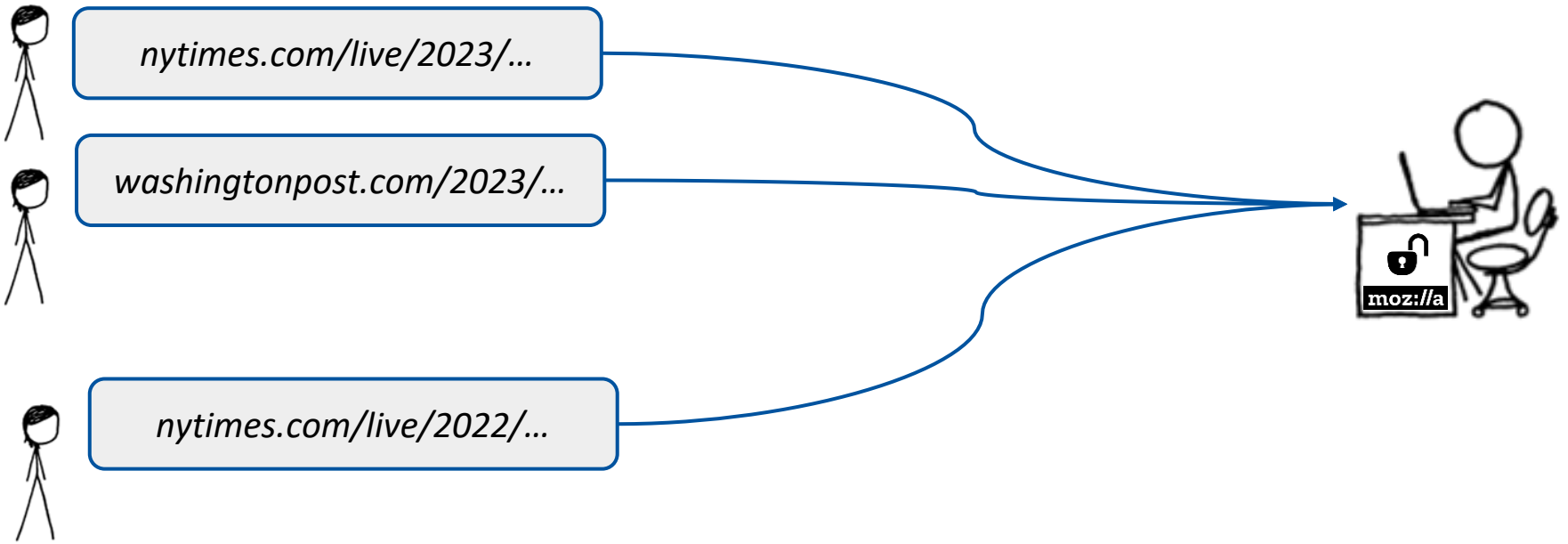
Trustworthy Computing Group

[1] University of Delaware

[2] Boston University

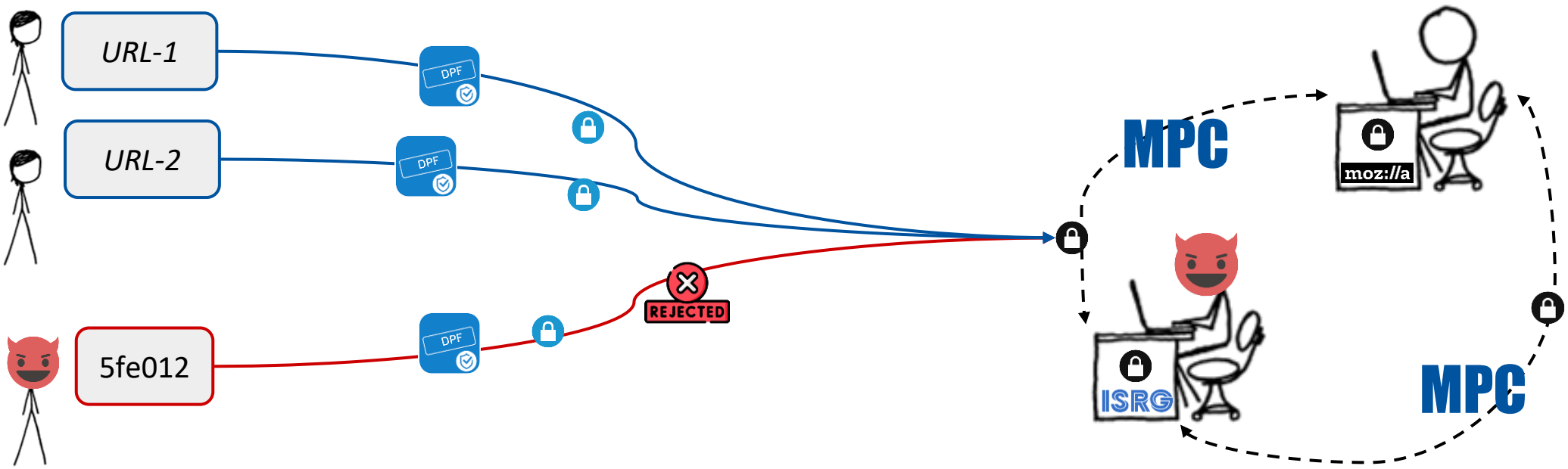
Heavy-Hitters – Popular URLs

- Heavy-hitters computes the most popular client submissions.
- Today, a server can see the clients' submissions and find the heavy-hitters.
- No privacy guarantees.



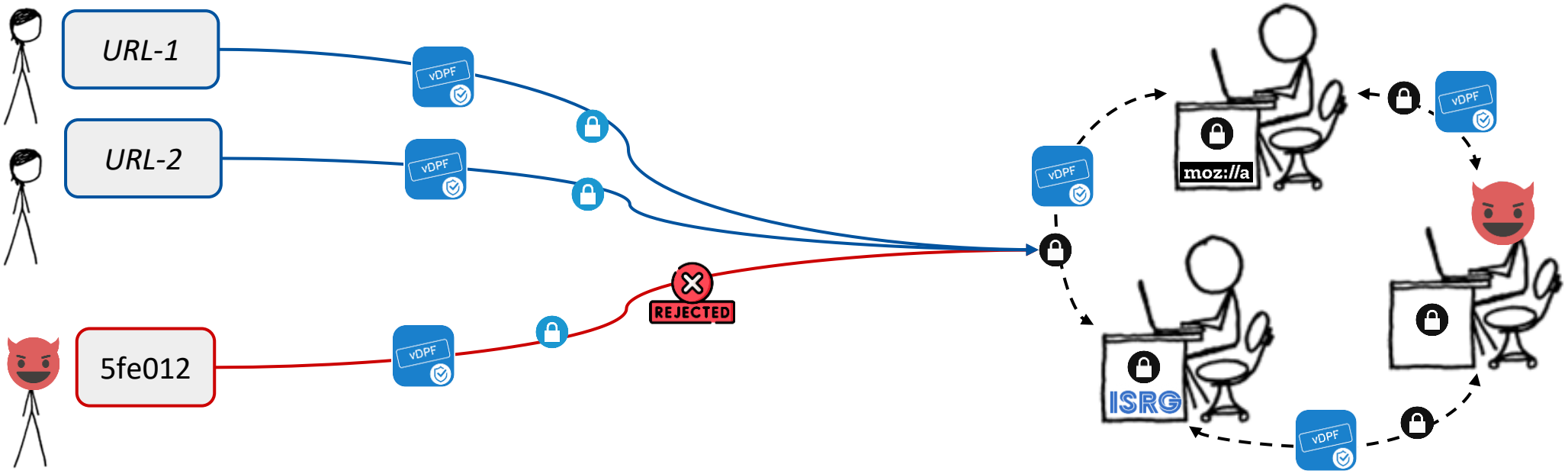
Poplar for Private Heavy-Hitters

- **Threat Model:**
  - **Correctness + Privacy against malicious clients.** – (using expensive MPC checks)
  - Two non-colluding servers.
  - Only guarantees **privacy** against one malicious server, ***not correctness.***

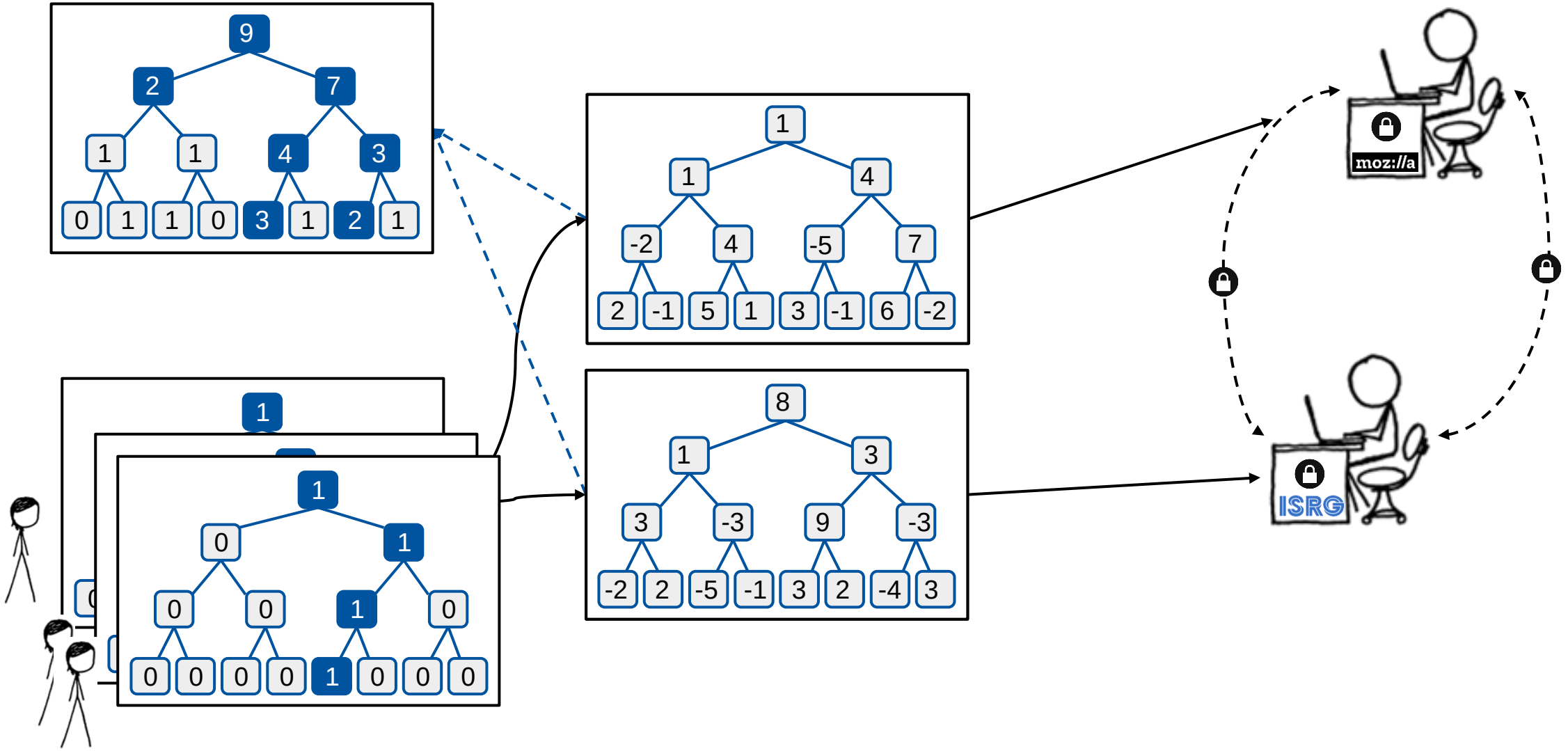


PLASMA for Private Heavy-Hitters

- **Threat Model:**
  - **Correctness and privacy against malicious clients .** – (lightweight symmetric primitives)
  - Three non-colluding servers.
  - Full Security **against malicious server** (i.e., privacy and correctness)



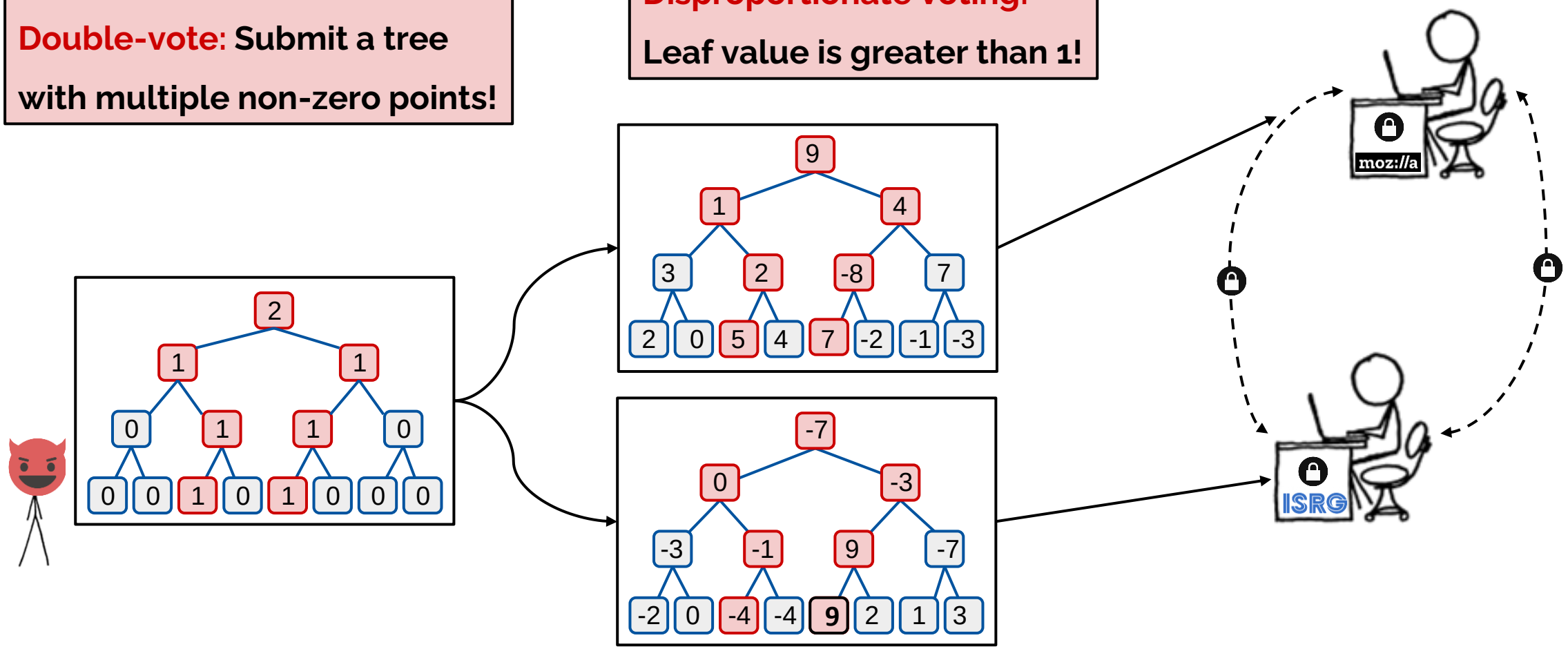
Distributed Point Functions (DPFs)



Malicious Client

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

Disproportionate voting: Leaf value is greater than 1!



Verifiable DPF (VDPF)

- **Public inputs for evaluation** (i.e., vector of data-points to evaluate): **X** = { x_1, x_2,... ,x_m }
- **Private clients' inputs** (i.e., secret data-point): **(*α* , 1)** ***α*** **ε X** → (key_0 , key_1)
- **Private outputs obtained by servers** (i.e., vector of secret shared outputs): { [0], [0], …, [1], …, [0] }

Evaluate(**X**, key_0) = **(Y, π_0)**

Y = { y_1, y_2, …, y_m }

Evaluate(**X**, key_1) = **(Z, π_1)**

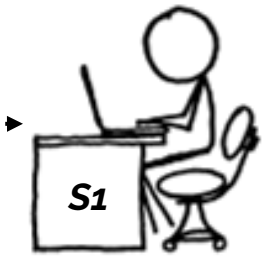
Z = { z_1, z_2, …, z_m }

Correctness: **Y** + **Z** = [0, 0, … , **1**, …, 0]

***α**th point*

Verifiability: **π_0 = π_1** if **Y+Z** is non-zero at a single point (Valid DPF)

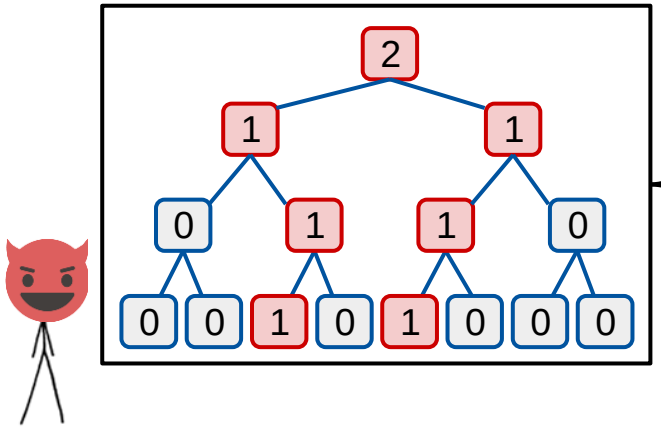
Non-zero leaf value is 1: Verify: **H($\Sigma_{i \varepsilon [m]}$ y_i) = H(1 - $\Sigma_{i \varepsilon [m]}$ z_i)**



Tackling Malicious Client

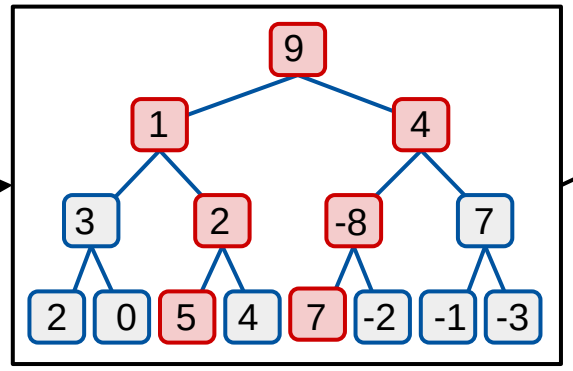
Double-vote: Submit a tree with multiple non-zero points!

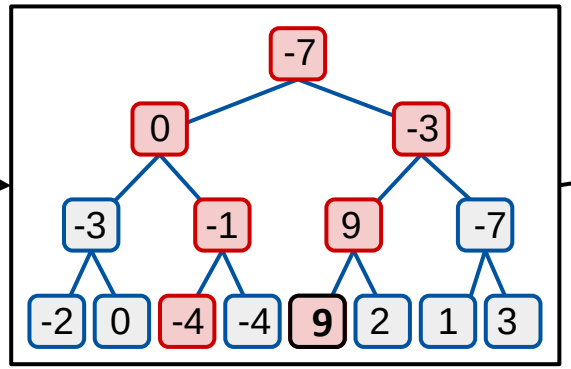
Taken care by verifiability property of vDPF

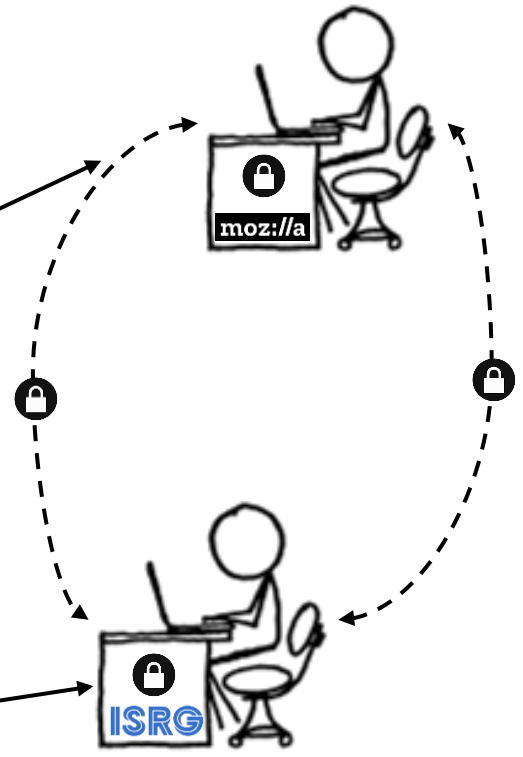


Disproportionate voting: Leaf value is greater than 1!

Taken care by ensuring non-zero leaf value is 1

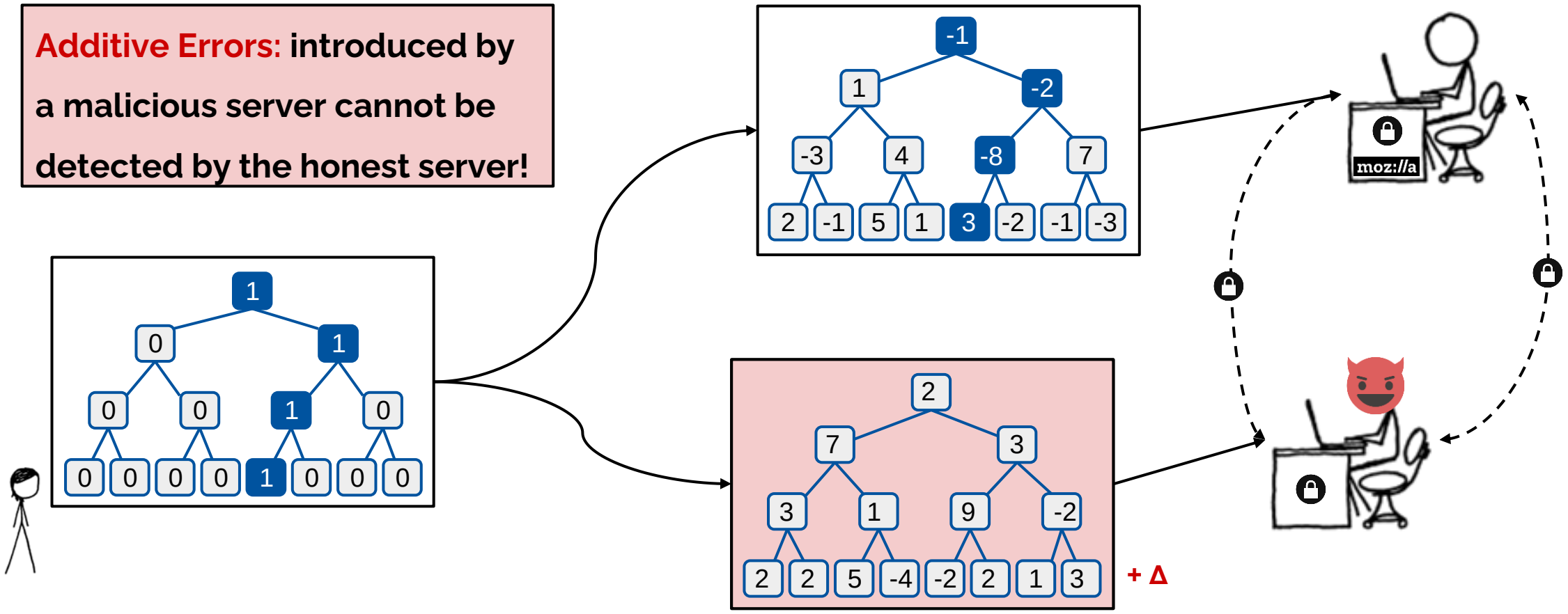






Malicious Server

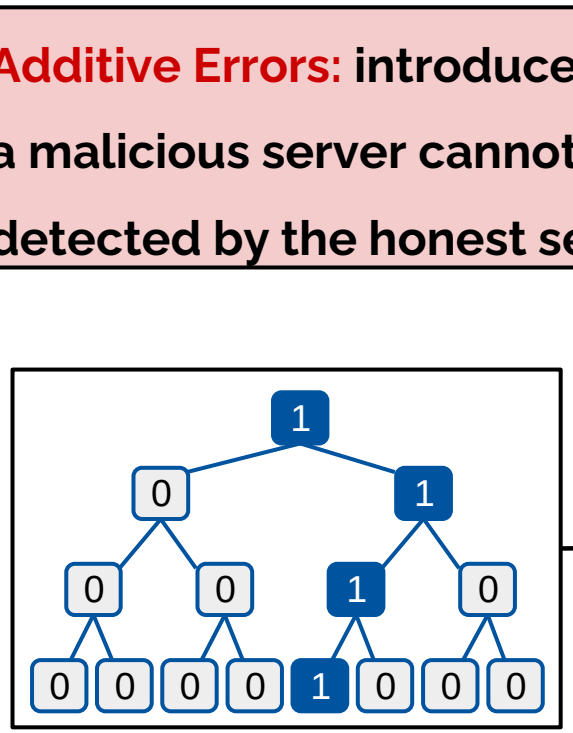
Additive Errors: introduced by a malicious server cannot be detected by the honest server!

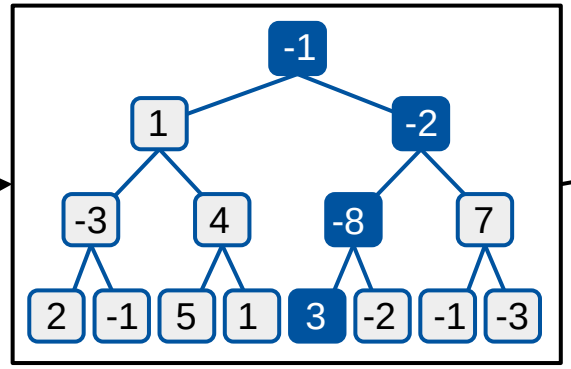


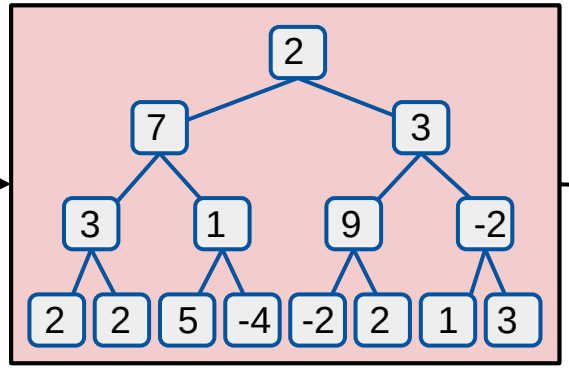
Tackling Malicious Server

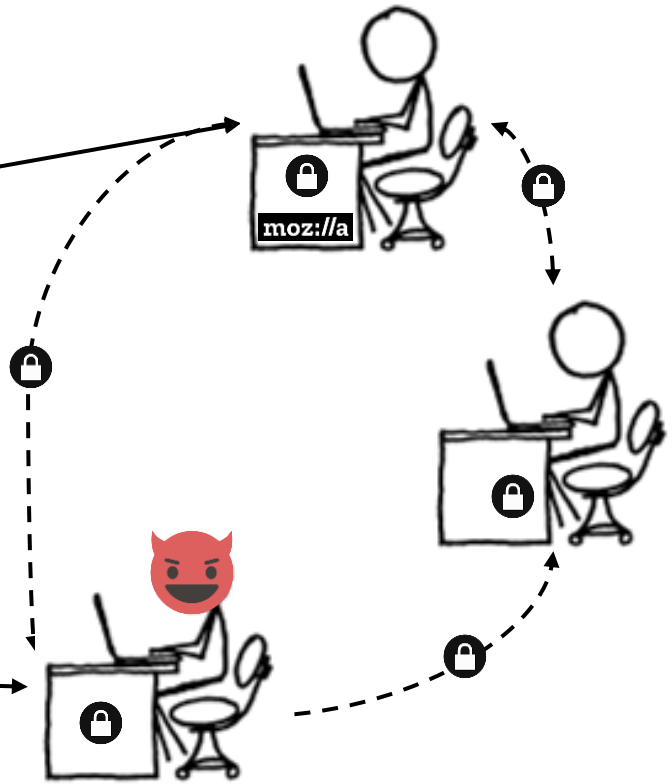
One additional server

Additive Errors: introduced by a malicious server cannot be detected by the honest server!





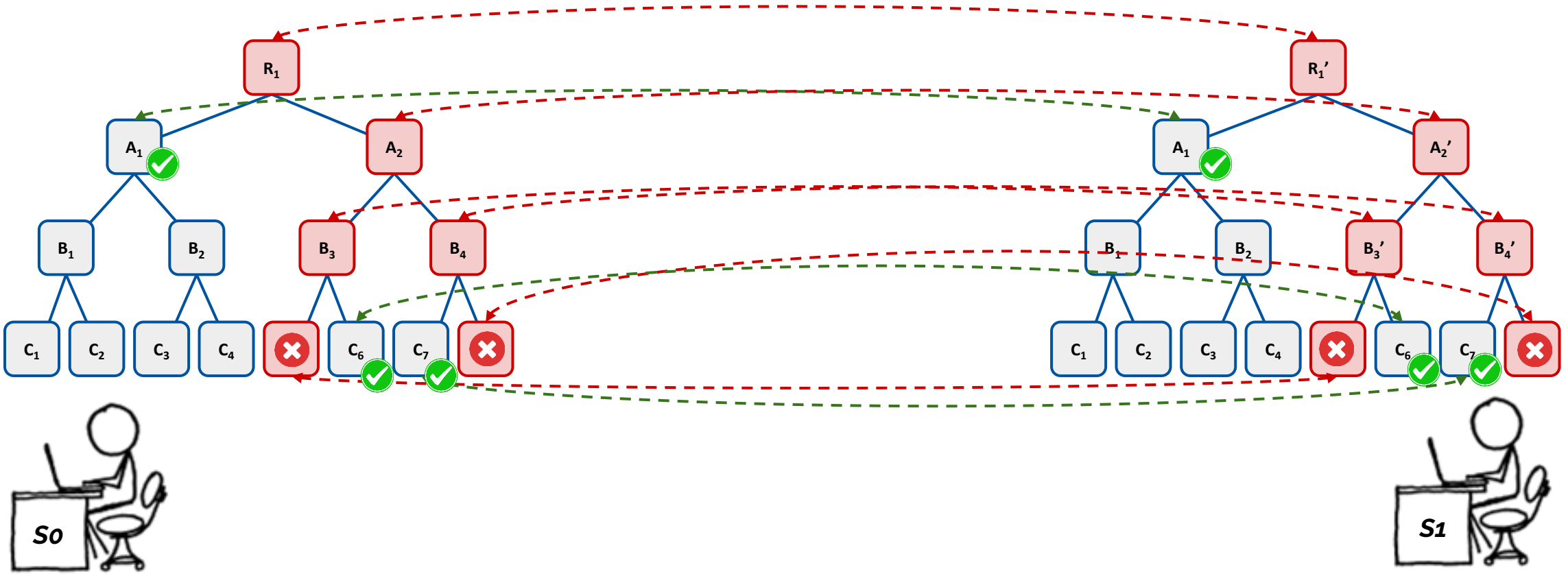




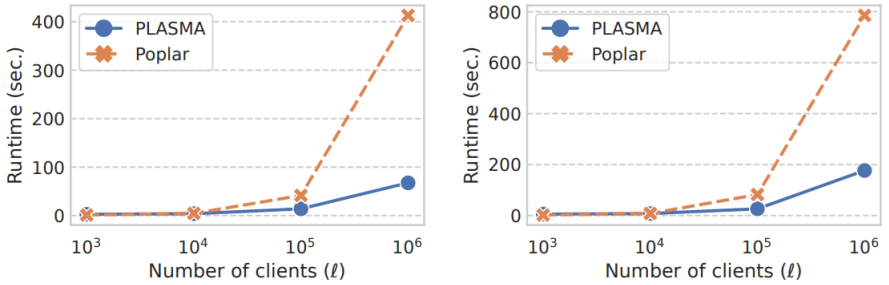
Used replicated secret sharing over vDPFs in the three server setting

Client Batch Verification using Merkle Trees

- Server-to-Server communication depends on the number of malicious clients.
- Depends logarithmically on the total number of clients.

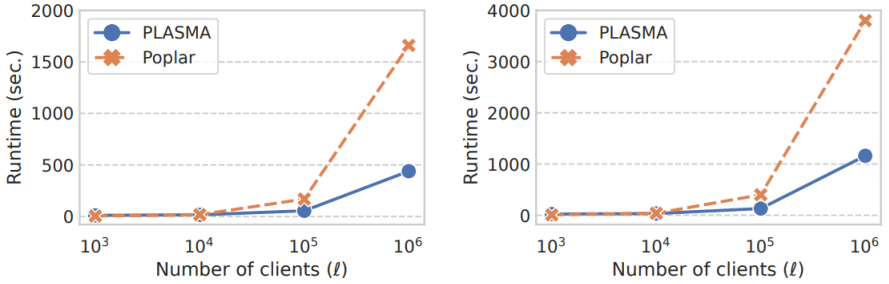


Experimental Evaluations



(a) Bit-string size ($n = 32$)

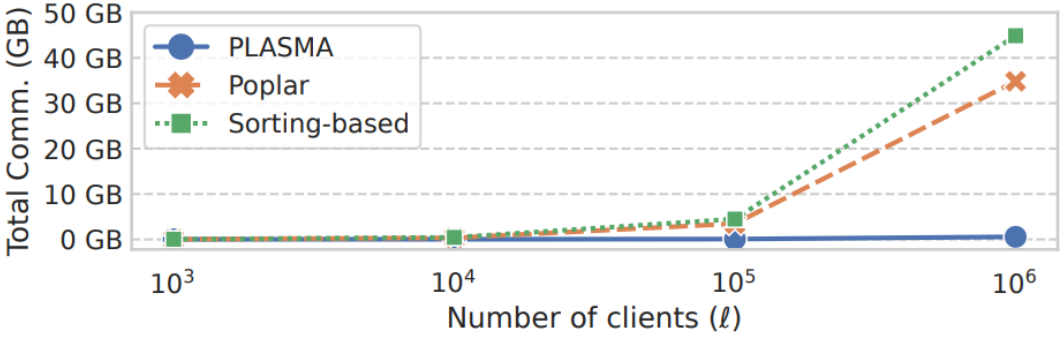
(b) Bit-string size ($n = 64$)



(c) Bit-string size ($n = 128$)

(d) Bit-string size ($n = 256$)

- PLASMA is 3-6x faster than Poplar for 1M clients
- PLASMA requires communication:
  - 182x less than Poplar
  - 235x less than sorting-based protocols



Questions?

PLASMA: Private, Lightweight Aggregated Statistics against Malicious Adversaries with Full Security

Dimitris Mouris[1], Pratik Sarkar[2], Nektarios G. Tsoutsos[1]

jimouris@udel.edu, pratik93@bu.edu , tsoutsos@udel.edu

https://eprint.iacr.org/2023/80

Trustworthy Computing Group

[1] University of Delaware

[2] Boston University

Roadmap of PLASMA