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

Dimitris Mouris\textsuperscript{1}, Pratik Sarkar\textsuperscript{2}, Nektarios G. Tsoutsos\textsuperscript{1}

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

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

[Diagram showing a tree with leaf values and a double-vote scenario]
Verifiable DPF (VDPF)

- **Public inputs for evaluation** (i.e., vector of data-points to evaluate): $X = \{x_1, x_2, \ldots, x_m\}$
- **Private clients’ inputs** (i.e., secret data-point): $(a, 1) \ a \in X \rightarrow (\text{key}_0, \text{key}_1)$
- **Private outputs obtained by servers** (i.e., vector of secret shared outputs): $\{0, 0, \ldots, 1, \ldots, 0\}$

Evaluate($X$, key$_0$) = ($Y$, $\pi_0$)

$Y = \{y_1, y_2, \ldots, y_m\}$

**Correctness:** $Y + Z = \{0, 0, \ldots, 1, \ldots, 0\}$

$Z = \{z_1, z_2, \ldots, z_m\}$

Verifiability: $\pi_0 = \pi_1$ if $Y + Z$ is non-zero at a single point (Valid DPF)

Non-zero leaf value is 1: Verify: $H(\sum_{i \in [m]} y_i) = H(1 - \sum_{i \in [m]} z_i)$
Tackling Malicious Client

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

Disproportionate voting:
Leaf value is greater than 1!

Taken care by verifiability property of vDPF

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

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

One additional server
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

- 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\textsuperscript{1}, Pratik Sarkar\textsuperscript{2}, Nektarios G. Tsoutsos\textsuperscript{1}

\texttt{jimouris@udel.edu, pratik93@bu.edu, tsoutsos@udel.edu}

https://eprint.iacr.org/2023/80
Roadmap of PLASMA

Verifiable DPF ⟷ Incremental DPF

Verifiable Incremental DPF (Tackles malicious clients) ⟷ Replicated secret sharing in the three server setting (Tackles malicious servers)

Basic Version of PLASMA (with large communication) + Client Batch Verification using Merkle Trees

PLASMA (with small communication)

+