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.

![Diagram showing the process of aggregating measurements securely to the aggregation server.](image-url)
Distributed Point Functions (DPFs)
Distributed Point Functions (DPFs)
Distributed Point Functions (DPFs)
One-hot Verifiability

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

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

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

One-hot Verifiability

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

One-hot Verifiability

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

\[
\begin{align*}
\text{Evaluate}(\text{Prefix}, \text{key}_0) &= (Y, \pi_0) \\
Y &= \{ y_1, y_2, ..., y_m \} \\
\text{Evaluate}(\text{Prefix}, \text{key}_1) &= (Z, \pi_1) \\
Z &= \{ z_1, z_2, ..., z_m \}
\end{align*}
\]

Vectors of Secret Shares for a level

One-hot Verifiability:

\[
\text{if } \pi_0 = \pi_1 \text{ then } Y + Z \text{ is one-hot!}
\]

One-hot Verifiability

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

Path Inconsistency: $\beta$ values are different and not on the same path!
Path Verifiability

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

Path Verifiability

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


Path Verifiability

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

---


Path Verifiability

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

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

*This is not possible with Poplar.*


Thwarting Malicious Clients

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

**Path Verifiability:** Asserts that $\beta$ 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 $T$.

![Graphs showing runtime for different threshold values](image_url)

- a) Threshold = 1% of $l$
- b) Threshold = 5% of $l$
- c) Threshold = 10% of $l$

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 $T$.

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

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