Distributed Aggregation Protocol
Draft and implementation updates

Tim Geoghegan
PPM - IETF 117 - San Francisco

- **DAP-05: "Ping-pong" topology**
  - DAP is now specialized to exactly two aggregators (one Leader, one Helper)
  - Simplifies protocol and implementations
  - Enables performance improvement: aggregators now take turn combining prepare messages and evaluating proofs, cutting Leader<->Helper HTTP round trips **by half** for Prio3 VDAFs
  - See discussion [back at IETF 116](https://datatracker.ietf.org/meetings/116/) and the protocol change in [PR#393](https://datatracker.ietf.org/prs/drafts/pr393/)
  - VDAF still allows arbitrarily many aggregators
  - Better names than "ping-pong" welcome!

- **VDAF-06:**
  - VDAF-06 adds interfaces to support DAP-05 ping-pong topology
  - Prio3Histogram is now parameterized by # of buckets instead of bucket boundaries
    - Much more efficient since some applications use Prio3Histogram to represent vectors with 100s, even 1,000s of dimensions!
Implementations

- **libprio-rs**
  - Implements Prio3 and Poplar1 VDAF families and VDAF abstraction
  - VDAF-06 in [prio-0.13.x](https://prio-0.13.x)
  - We'd (still) love to see more implementations – Go would be great

- **Daphne**
  - Helper implementation targeting Cloudflare Workers
  - Moving to DAP-05 soon

- **Janus**
  - Client, Leader, Helper, Collector implementations
  - DAP-05 "ping-pong" implementation is prototyped, will be merged soon

- **divviup-ts**
  - Typescript Client implementation
  - DAP-04 implementation complete (Prio3 only)
  - Only [minor changes](https://example.com) needed for DAP-05/VDAF-06 (domain separation strings)
  - Ongoing integration test against Janus

- **Firefox**
  - DAP-05 client coming
Upcoming work

- Server differential privacy (more imminently)
- Overhaul the security considerations
- Trim error code to the bare essentials
- Poplar1 changes will emerge as we accumulate operational experience with that VDAF