IPA Update

Feb 2023 - PATCG Face-to-Face

Previous Update Recap (Aug 2022)

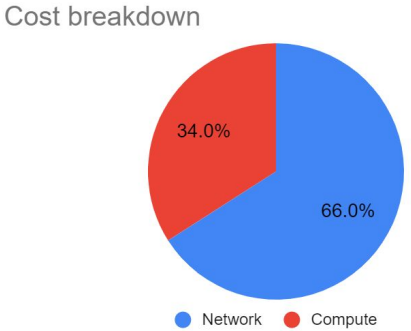
Cost is mostly Network
Network is mostly Sort

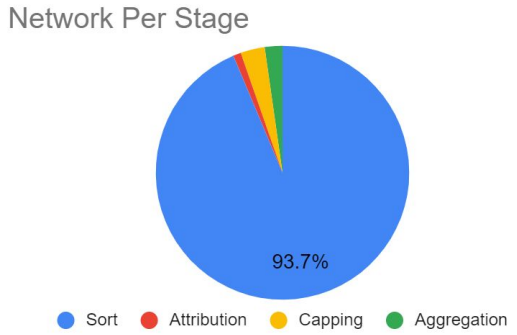
In summer 2022, we prototyped IPA using MP-SPDZ, an MPC engine built for benchmarking. Here are some figures we shared with the PATCG at that time.

Estimated Cost for 1M events:

Network: $31 ($0.08/GB * 390 GB)

Compute: $16 (100 min * $3.2/hr * 3 machines)





IPA *from scratch* Prototype

Why

MP-SPDZ is useful for benchmarking, it's not *production ready*. Additionally, it's an added layer of complexity for security analysis.

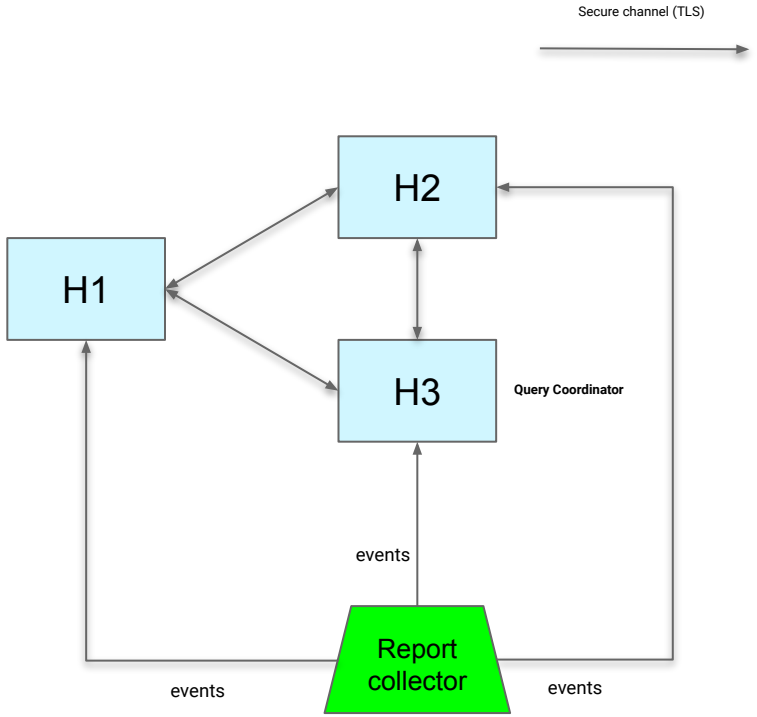
What

github.com/private-attribution/ipa is an open source implementation of IPA, built from scratch in Rust.

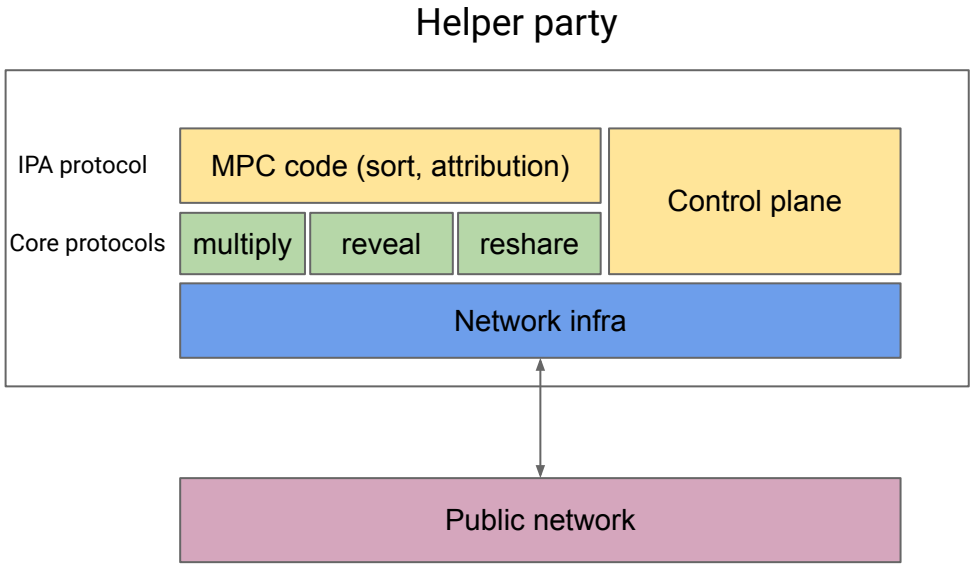
It is intended to be a **functional**, **performant**, and **comprehensible** implementation of the core IPA protocol.

IPA *from scratch* implementation architecture and overview

- IPA is implemented in Rust
- 3 servers, HTTP frontend



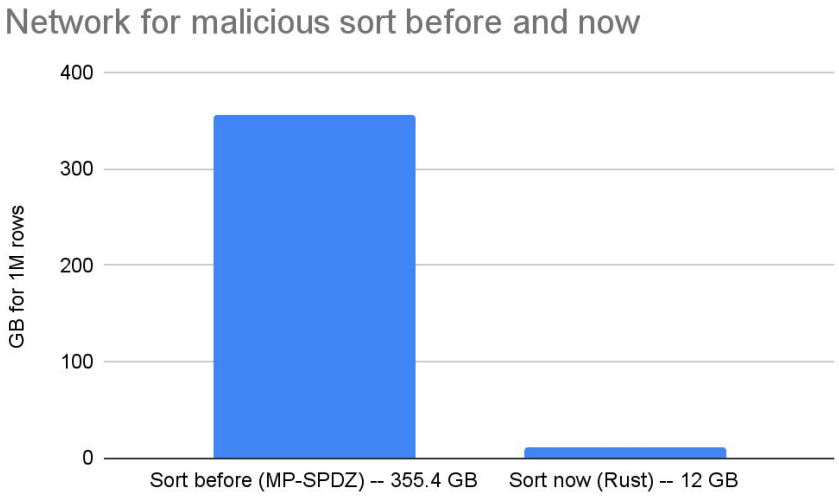
IPA *from scratch* implementation architecture and overview



IPA “from scratch” performance benchmarks

Our work on the current implementation has focused primarily on **reducing the overall bandwidth for the sorting stage**, as this drove most of the cost.

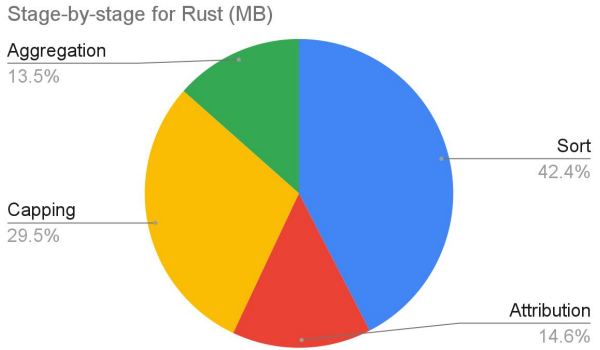
- We have achieved a 32-45x reduction in network usage for malicious sort
- Sorting 1M records with malicious security now uses 8-12 GB of total network



IPA “from scratch” performance benchmarks

Here is a stage-by-stage comparison

malicious 10k, 40 bit matchkey, 16 breakdowns		
Stage	**Rust (MB)**	**MP-SPDZ (MB)**
Modulus Conversion	38	not implemented
Sort	79	3,554
Attribution	27	38
Capping	55	118
Aggregation	25	131
Total	223	3,841



IPA “from scratch” performance benchmarks

Total predicted network costs for malicious

- Predicted total network for 1M: 22-32GB
  - Linear scaling from 10k to 22GB
- **Predicted total network cost for 1M: ~$2.56**
  - $2.56 = 32 GB * ($0.08/GB)
- Many of our algorithmic improvements to sort will also benefit compute but we are still working to be able to test that fully.

Malicious upgrade factor

- Our upgrade from semi-honest to malicious increases network by a factor of 2.44x

Exploring an *In-Market Test* of IPA

We are exploring the possibility of running an *in-market test* of IPA, using the *from scratch* prototype.

We aim for this test to include:

- Real ads
- Real advertisers
- Real publisher(s)
- Real measurement company(ies)
- Real helper parties

It will (likely) not include an actual client side IPA match key implementation, and instead focus on leveraging surfaces where individual identifiers currently exist (e.g., Android.)

Exploring an *In-Market Test* of IPA

By doing this test, we're hoping to:

1. Demonstrate viability and affordability of the proposed IPA system
2. Validate and compare the IPA measurement results against existing measurement results
3. Gather learnings about usability

Also, get more information on the following questions:

1. Optimal number of breakdowns keys
2. Optimal amount of trigger value entropy
3. Assessing the risk of match key collision

Exploring an *In-Market Test* of IPA

This is still in very early planning stages, but if you are interested in participating, please reach out to:

richaj@meta.com

Further IPA references:
https://github.com/patcg-individual-drafts/ipa

https://github.com/private-attribution