DRAFT-DSS-STAR-00

Alex Davidson Shivan Sahib Peter Snyder

Brave Software

PPM WG ::: IETF113, Vienna

2022-03-25

STAR| Distributed Secret Sharing for Threshold Aggregation Reporting.

Idea| Providing *k*-anonymity for client-side measurement reporting.

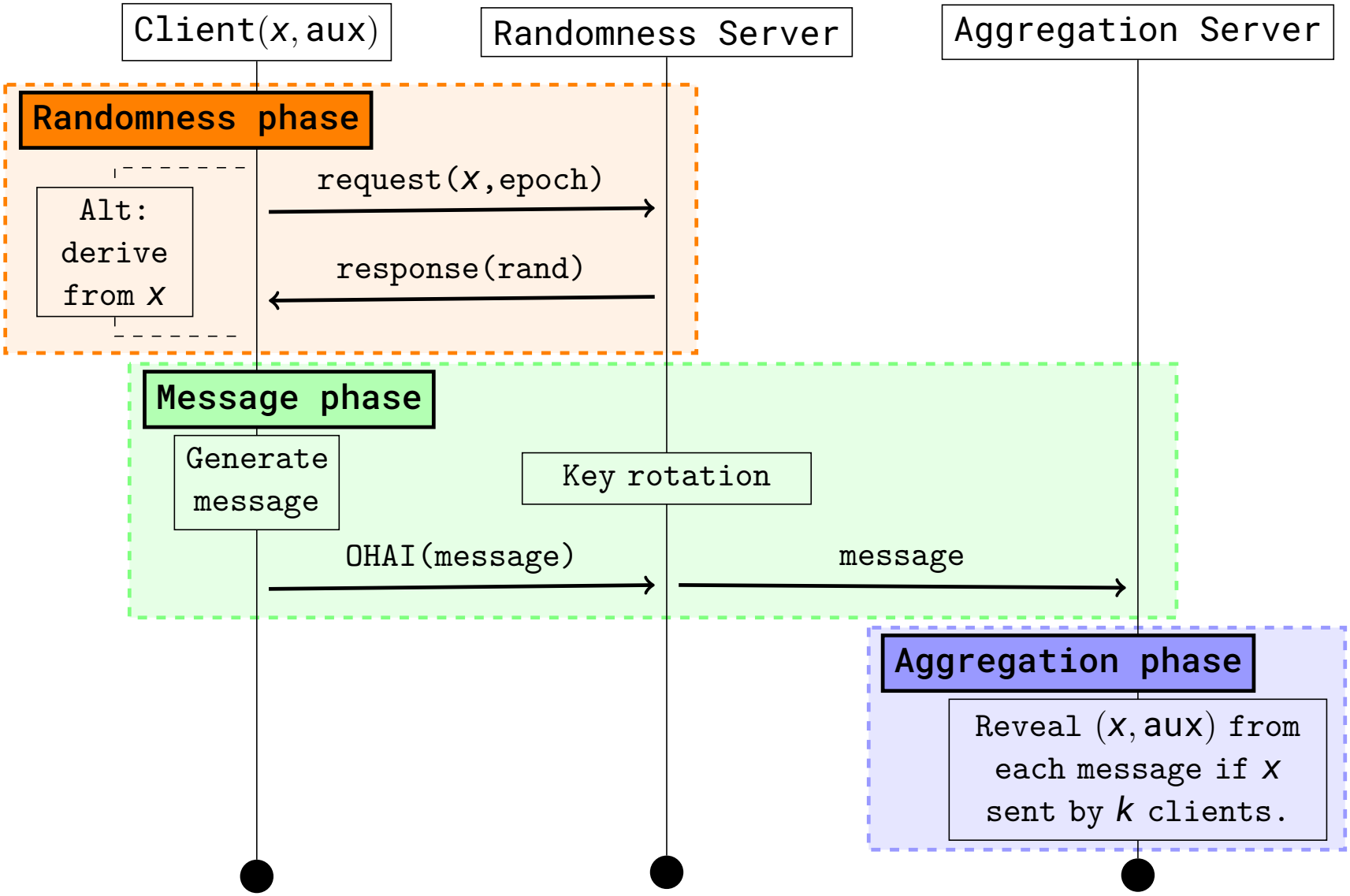
Aims|

:: *Cheap*: Low computational and network usage overheads for clients and servers.

:: *Simple*: Short path to implementation, well-known cryptographic techniques.

:: *Privacy*: Practical privacy guarantees for client measurements.

STAR DESIGN GOALS



PROTOCOL DESIGN

::: Randomness sampling (in epoch ϵ):

- Local: $\mathsf{rand} \leftarrow H(x, \epsilon)$
- Remote: $\mathsf{rand} \leftarrow \mathsf{OPRF}(\mathsf{sk}_\epsilon, x)$

Stronger privacy guarantees

For high-entropy measurement distributions

::: Message format: $\mathtt{msg} = (c, s, t)$

- $c \leftarrow \mathsf{Enc}(key, x \| \mathsf{aux})$; $key \leftarrow \mathsf{derive}(\mathsf{rand}[0])$
- $s \leftarrow \mathsf{share}(\mathsf{rand}[0]; \mathsf{rand}[1])$
- $t \leftarrow \mathsf{rand}[2]$

Puncturable POPRF for verifiable key rotations

::: Aggregation: (for $\geq k$ msgs with common t)

- $r \leftarrow \mathsf{recover}(\mathtt{messages})$; $key \leftarrow \mathsf{derive}(r)$
- $(x \| \mathsf{aux}) \leftarrow \mathsf{Dec}(key, c)$

KEY POINTS

Comparable with `poplar1`:

::: **Non-collusion**: Randomness and Aggregation servers are disallowed from colluding.

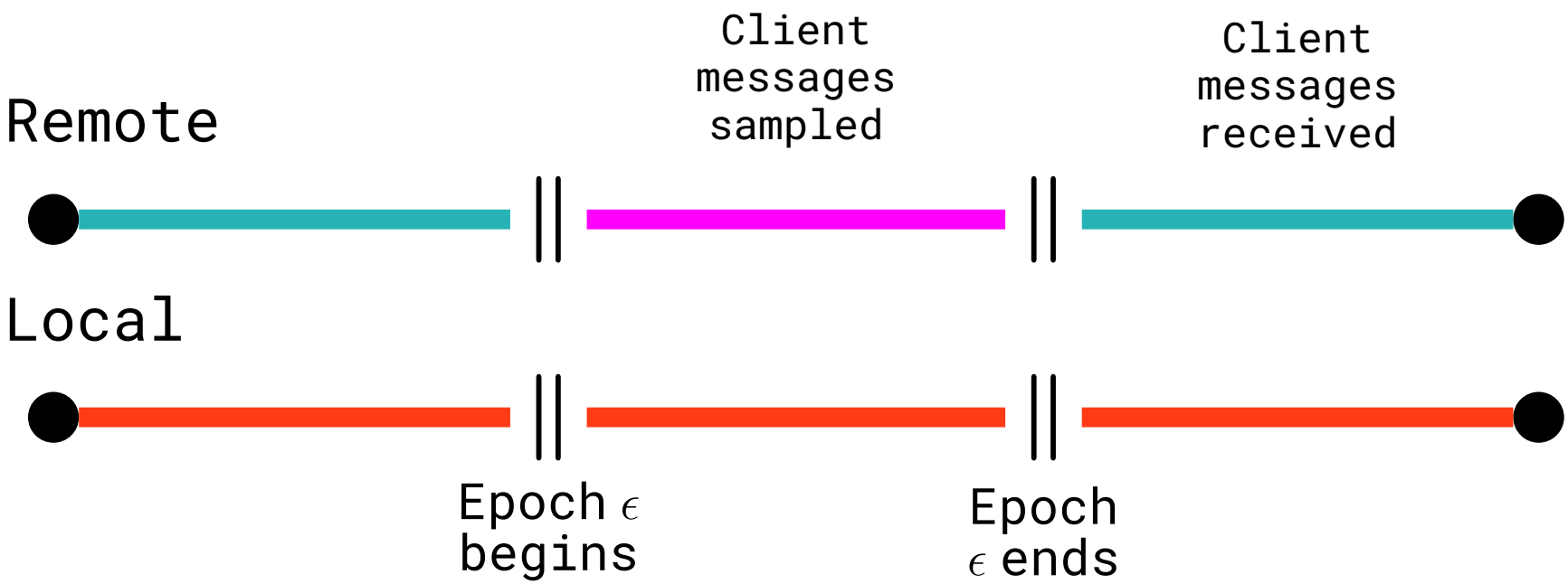
::: **Malicious adversary**: Controls one server and a subset of clients.

::: **Leakage**: Messages that encode the same measurements.

::: **Goals**: *Confidentiality* of measurements sent by $\leq k$ clients, and aggregation *robustness*.

SECURITY MODEL

- Client measurements are safe
- Online attack is possible
- Offline attack is possible



CLIENT PRIVACY: SYBIL ATTACK WINDOW

STAR provides very similar functionality to heavy-hitter protocols, such as `poplar1`.

Comparison with `poplar1`:

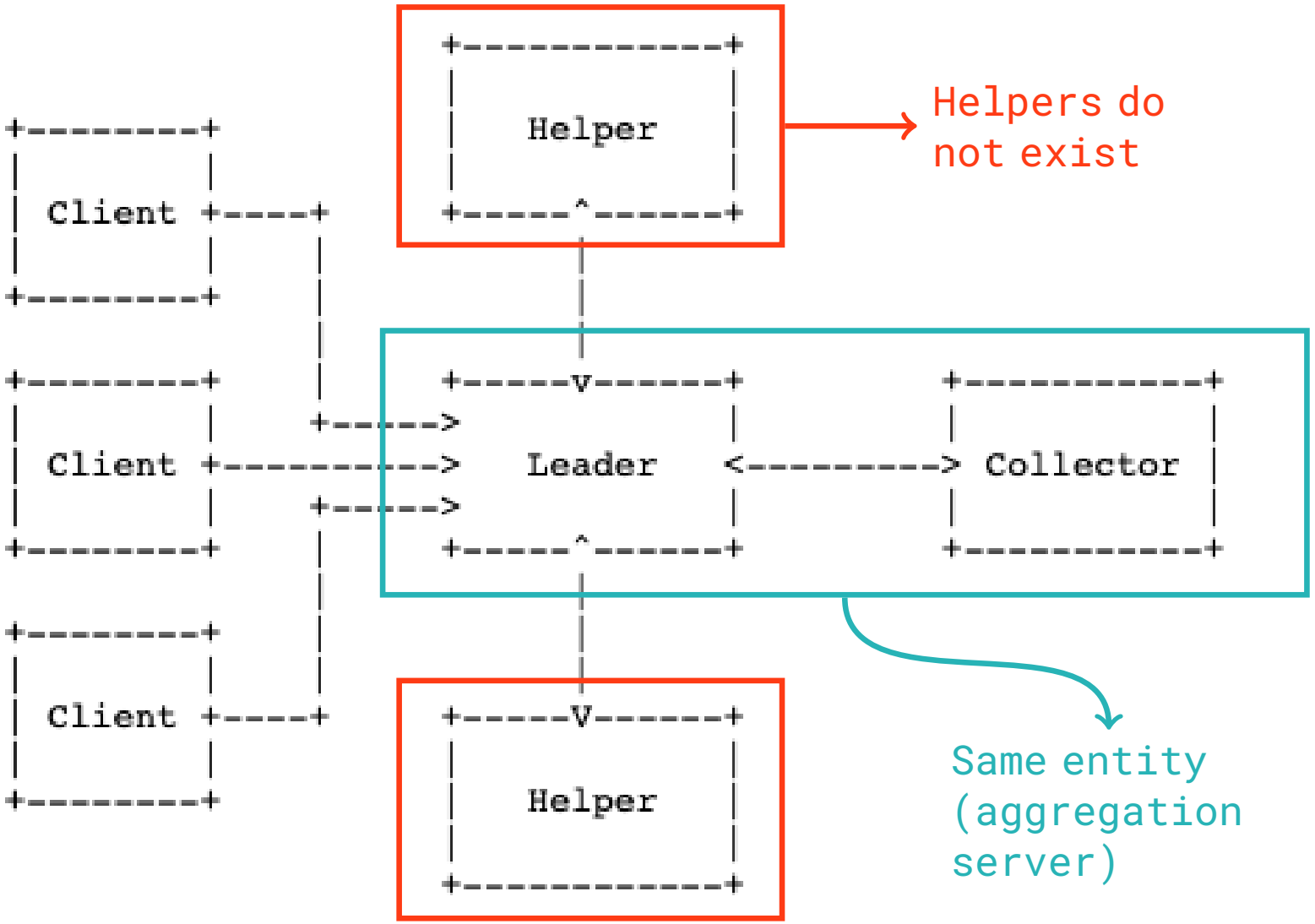
::: Clients can send auxiliary information.

::: STAR leakage reveals all the subsets of messages that hide the same measurement (even if threshold is not satisfied).

::: `poplar1` leakage reveals heavy-hitting prefixes.

::: Requires only a single aggregation server.

FUNCTIONAL COMPARISON WITH `poplar1`



PPM FRAMEWORK COMPATIBILITY

::: **Trust assumptions**: No additional non-colluding entities on top of OHAI.

::: **Financial costs**: No bandwidth usage and minimal computation during aggregation; ensures cheap operating costs (see https://arxiv.org/abs/2109.10074).

::: **Privacy**: Concrete guarantees for client privacy, and a limited leakage profile.

::: **Functionality**: Allows auxiliary data to be provided by clients.

::: **Simple cryptography**: No usage of novel primitives.

BENEFITS OF STAR

::: We think that STAR provides:

- A privacy-preserving reporting mechanism for those with limited resources, and without expert implementation knowledge.
- Trust assumptions that are preferable to those made by `prio3` and `poplar1`.

::: Questions:

- Is the WG interested in alternative protocol specs?
- Does the STAR draft fit into the WG charter?