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**

### PROTOCOL DESIGN

1. **Randomness phase**
   - Client $(x, aux)$
   - Randomness Server
   - Aggregation Server
   - Request $(x, epoch)$
   - Response $(rand)$

2. **Message phase**
   - Generate message
   - Key rotation
   - $OHAI(message)$

3. **Aggregation phase**
   - Reveal $(x, aux)$ from each message if $x$ sent by $k$ clients.
Randomness sampling (in epoch $\epsilon$):

- **Local:** $\text{rand} \leftarrow H(x, \epsilon)$
- **Remote:** $\text{rand} \leftarrow \text{OPRF}(sk_\epsilon, x)$

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

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

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

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

**KEY POINTS**
- Stronger privacy guarantees
- For high-entropy measurement distributions
- Puncturable POPRF for verifiable key rotations
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.
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.
Helpers do not exist

Same entity (aggregation server)
::: 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?