

# **STAR: Distributed Secret Sharing for Threshold Aggregation Reporting**

PPM WG, IETF 116

Shivan Sahib

**Idea:**  $k$ -anonymity for clients reporting measurements to an untrusted server

# Goals

- **Cheap:** low computational overhead and network usage for clients and servers
- **Simple:** easy to implement, well-known crypto
- **Private:** practical privacy guarantees **for the client**

Client wants to send a telemetry value to the server,  
but only wants the server to see it if there are  $\geq K$   
submissions of the same value

# Implementations

- Shipping in Brave browser for telemetry
- Rust (Shamir): <https://github.com/brave/sta-rs>
- Rust (verifiable + benchmarks):  
<https://github.com/claucece/secret-sharing-extra>
- Go (verifiable + benchmarks):  
[https://github.com/chris-wood/star-go/](https://github.com/chris-wood/star-go)
- WASM bindings:  
<https://github.com/brave/sta-rs/tree/main/star-wasm>

<b>Secret Sharing Scheme</b>	<b>Signature Scheme/Protocol</b>	<b>Client threat mitigated</b>
Shamir Secret Sharing	OPRF	None
Verifiable Secret Sharing	OPRF	Bad shares (DoS)
Shamir Secret Sharing	Blind Signatures	Bad ciphertext
Verifiable Secret Sharing	Blind Signatures	Both

- **There seems to be strong interest in STAR**
- **We addressed feedback from the WG and it improved the document**
- **We should do this formally within the WG!**