Round-Robin is Optimal: Lower Bounds for Group Action Based Protocols

Daniele Cozzo[1], Emanuele Giunta[1, 2]

IMDEA Software Institute, Spain
{daniele.cozzo, emanuele.giunta}@imdea.org

Universidad Politecnica de Madrid, Spain.

Group Actions

$$\underbrace{\star}_{\text{Action}} : \underbrace{\mathbb{G}}_{\text{Group}} \times \underbrace{\mathcal{E}}_{\text{Set}} \to \underbrace{\mathcal{E}}_{\text{Set}}$$

$0 \star E = E$

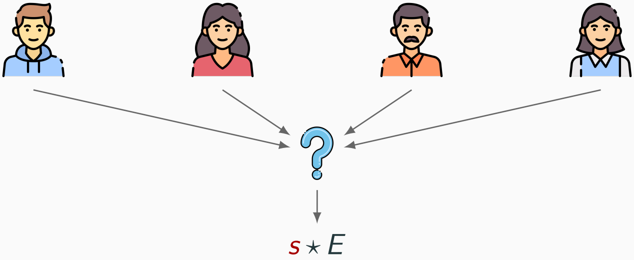
$(a + b) \star E \ = \ a \star (b \star E)$

$\star(\cdot, E)$ hard to invert

- ✓ Plausibly **post-quantum** problems.
- ✓ Concrete candidate instantiations (e.g. CSIDH).
- ✗ **Less structure** that prime-order groups.

Problem: Reconstructing Secrets in the Exponent

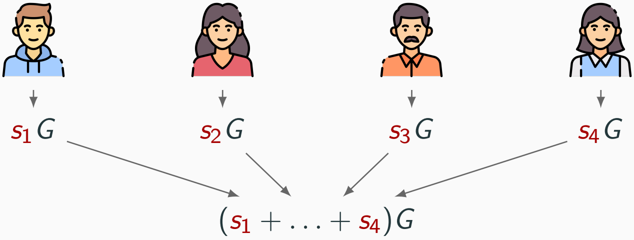
Given n parties with a secret sharing of $s \in \mathbb{G}$, they have to securely reconstruct $s \star E$ for some $E \in \mathcal{E}$.



Building Block for Distributed Key Generation and Threshold Decryption/Signature.

Warm up: Reconstructing Secrets in a Group

$\star : \mathbb{F}_q \times \mathbb{G} \to \mathbb{G}$ the scalar multiplication, $G \in \mathbb{G}$, $s = s_1 + \ldots + s_4$.



✔ Requires $O(1)$ **rounds**.

Round-Robin Protocol

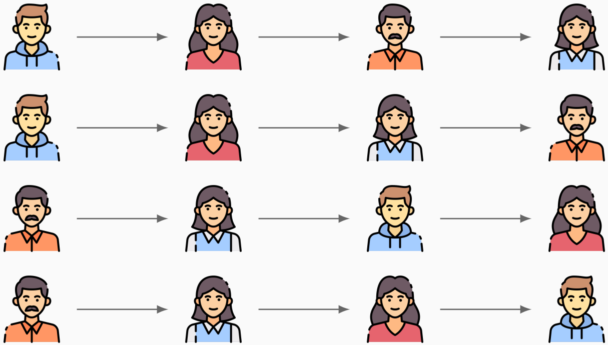
Given $E_0 \in \mathcal{E}$ and secret $s = s_1 + \ldots + s_4$.

$E_1 = s_1 \star E_0$ $\quad$ $E_2 = s_2 \star E_1$ $\quad$ $E_3 = s_3 \star E_2$

$E_4 = s_4 \star E_3$

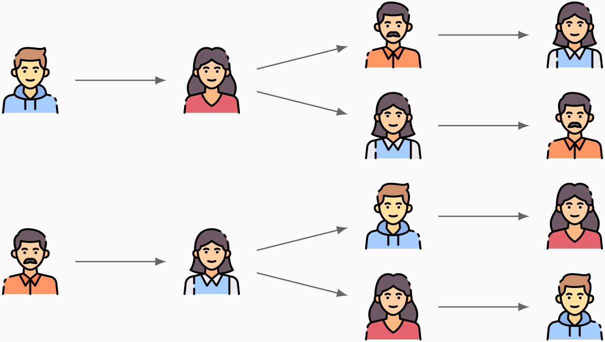
- ✖ Requires n **rounds**.
- ✖ Only the last user gets the result and is supposed to share it.

Round-Robin: Binary Splitting Strategy [DM20]



✖ Computation and communication complexity: $O(n^2)$.

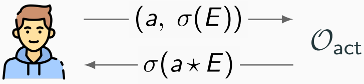
Round-Robin: Binary Splitting Strategy [DM20]



- Computation and communication complexity: $O(n \log_2 n)$.

Generic Action Model (GAM) [DHK+23]

Given $\sigma : \mathcal{E} \to \{0,1\}^{\mu}$ random **representation function**, the action is replaced by the oracle $\mathcal{O}_{\text{act}}$



Generic Action Model (GAM) [DHK+23]

Given $\sigma : \mathcal{E} \to \{0,1\}^\mu$ random **representation function**, the action is replaced by the oracle $\mathcal{O}_{\mathsf{act}}$

$$\xrightarrow{(a,\ \sigma(E))} \quad \mathcal{O}_{\mathsf{act}}$$
$$\xleftarrow{\sigma(a \star E)}$$

We **do not** model quadratic twists explicitly as in [DHK+23].

$$a_0 \star E_0 \xrightarrow{\text{twist}} (-a_0) \star E_0$$

Instead we allow the action to be **non-faithful** and $\mathbb{G}$ **not commutative** [BGZ23].

Our Results

In the **GAM**, given a t out of n secret sharing of s

Our Results

In the **GAM**, given a t out of n secret sharing of s

First Result: Any secure protocol computing $s \star E$ has round complexity $\geq t$.

Our Results

In the **GAM**, given a t out of n secret sharing of s

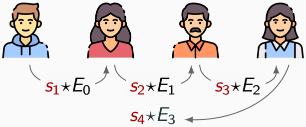
First Result: Any secure protocol computing $s \star E$ has round complexity $\geq t$.

Second Result: Any such t **round** protocol where t parties obtain the output after the $(t-1)$-th round requires to compute and communicate $\Omega(t \log_2 t)$ set elements.

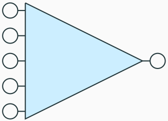
Consequences of Our Results

First Result. Any protocol computing $s \star E$ either:

Requires t rounds



Depends on a **circuit** evaluating $\star$

$\star(\cdot, \cdot) \ =$ 

Second Result. The binary splitting strategy [DM20] is optimal.

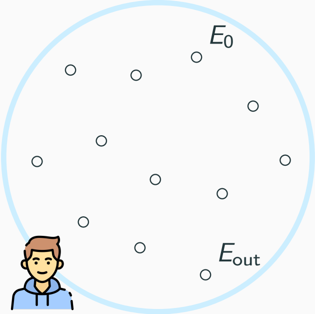
Round Lower Bound

Sequentiality Lemma (I)

Suppose $^{\mathcal{O}_{\mathsf{act}}}(E_0) \to (s, E_{\mathsf{out}})$ with $E_{\mathsf{out}} = s \star E_0$.

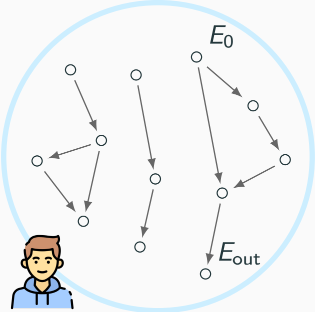
Sequentiality Lemma (I)

Suppose $^{\mathcal{O}_{\mathsf{act}}}(E_0) \to (s, E_{\mathsf{out}})$ with $E_{\mathsf{out}} = s \star E_0$.



Sequentiality Lemma (I)

Suppose  $^{\mathcal{O}_{\mathsf{act}}}(E_0) \to (s, E_{\mathsf{out}})$ with $E_{\mathsf{out}} = s \star E_0$.

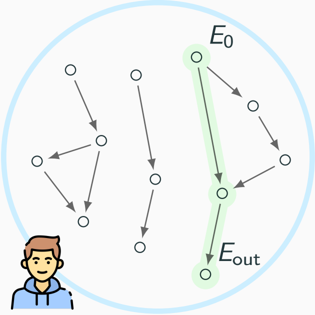


$D \to E$ if:

- $E = \mathcal{O}_{\mathsf{act}}(a, D)$ was queried for some $a \in \mathbb{G}$.
- D was observed *before* E.

Sequentiality Lemma (I)

Suppose  $^{\mathcal{O}_{\mathsf{act}}}(E_0) \to (s, E_{\mathsf{out}})$ with $E_{\mathsf{out}} = s \star E_0$.



$D \to E$ if:

- $E = \mathcal{O}_{\mathsf{act}}(a, D)$ was queried for some $a \in \mathbb{G}$.
- D was observed *before* E.

Then

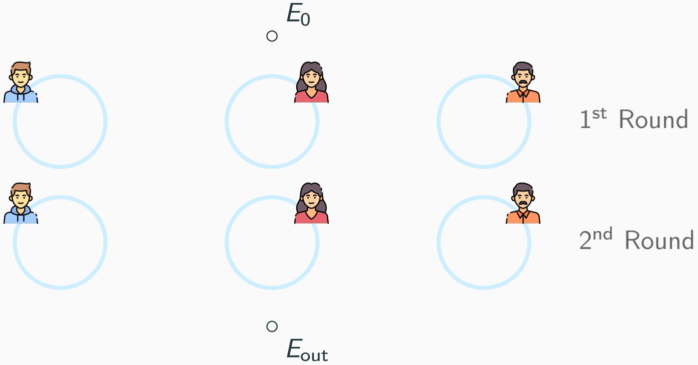
whp there exists a path from E_0 to E_{out}.

Sequentiality Lemma (II)

In a r rounds protocol computing $E_{\text{out}} = s \star E_0$, there exists a path "going through" at most r users.

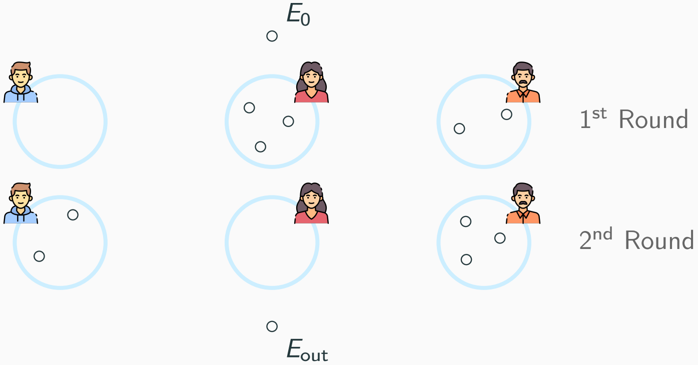
Sequentiality Lemma (II)

In a r rounds protocol computing $E_{\text{out}} = s \star E_0$, there exists a path "going through" at most r users.



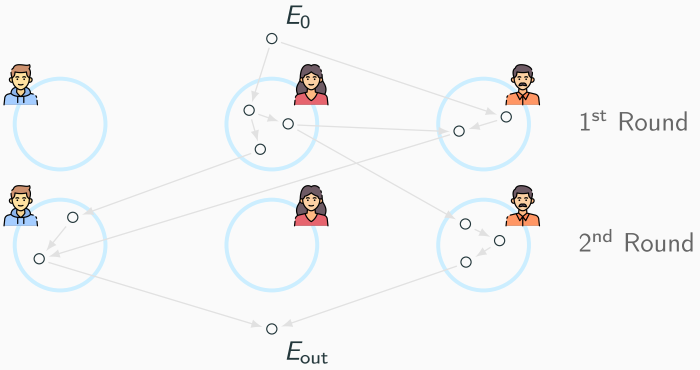
Sequentiality Lemma (II)

In a r rounds protocol computing $E_{\text{out}} = s \star E_0$, there exists a path "going through" at most r users.



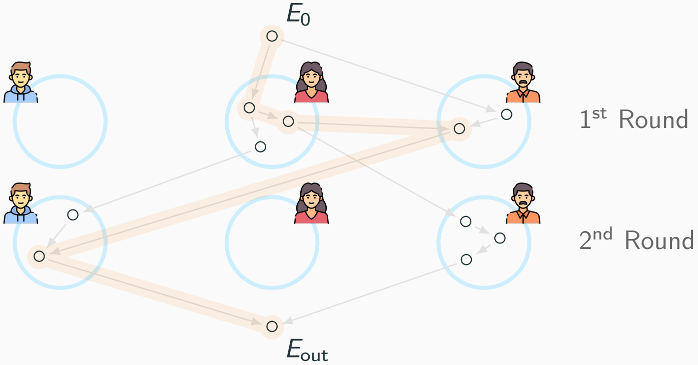
Sequentiality Lemma (II)

In a r rounds protocol computing $E_{\text{out}} = s \star E_0$, there exists a path "going through" at most r users.



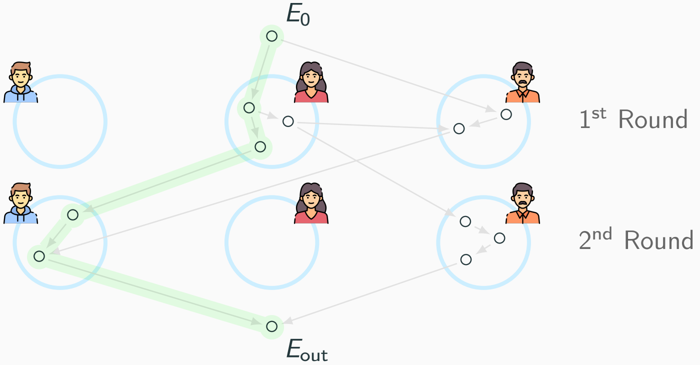
Sequentiality Lemma (II)

In a r rounds protocol computing $E_{\mathrm{out}} = s \star E_0$, there exists a path "going through" at most r users.



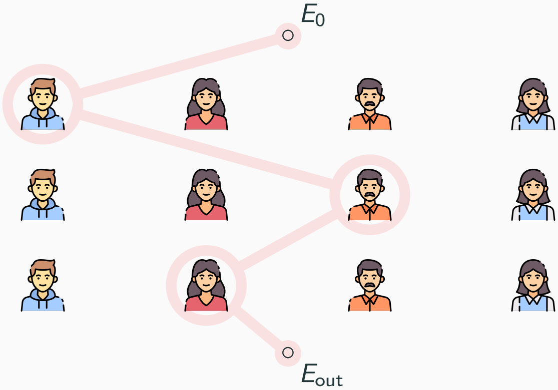
Sequentiality Lemma (II)

In a r rounds protocol computing $E_{\text{out}} = s \star E_0$, there exists a path "going through" at most r users.



Round Lowerbound

If there exists a $t-1$ rounds protocol to compute $s \star E_0$, then $t-1$ parties can recover s:



Thanks for your attention!