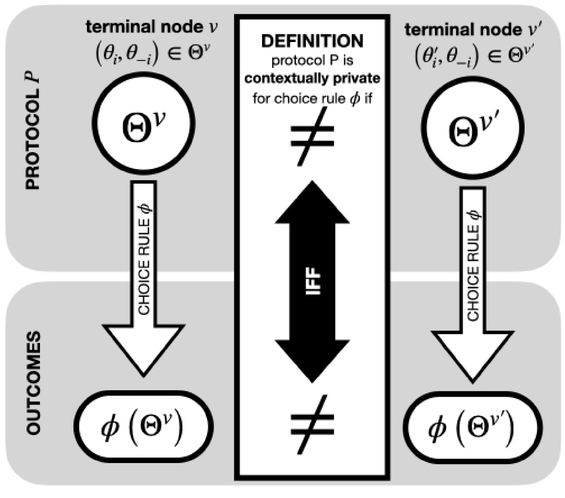
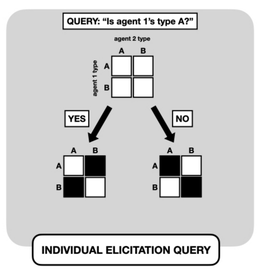
Contextual Privacy

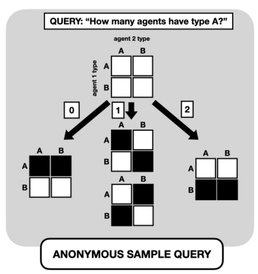
Andreas Haupt
Massachusetts Institute of Technology

Zoë Hitzig
Harvard University

Definition 1 (Protocol). *A (deterministic)* protocol P *is a directed rooted tree with vertices* V *and edges* E*. Each vertex ("query") is labelled with a non-empty subset of types* $\Theta^v \subseteq \Theta^n$*. The root vertex* v_0 *corresponds to the full joint type space* Θ^n*. The labels of children* $(\Theta^w)_{\{w|(v,w)\in E\}}$ *form a partition of the label of the parent node* Θ^v*.*







Social Choice Function	Sequentially		Anonymous	
	CP?	How?	CP?	How?
SD	yes	SD	yes	SD
FP	yes	DESC	yes	DESC
SP	**no**		yes	Tâtonnement (ASC)
kP	**no**		yes	Tâtonnement
Walras*	**no**		yes	Tâtonnement
DA	**no**		**no**	
TTC	**no**		**no**	

*add. conditions.

A mechanism is

contextually private

if it only elicits

what it **needs to know.**

Which choice functions can **implemented** by contextually private mechanisms?

arxiv:2112.10812

Definitions

Definition 2 (Contextual Privacy). *Protocol* $P = (V, E)$ *is* contextually private *(CP) for SCF* ϕ *if for all terminal nodes* $v, v' \in V$ *and all* $(\theta_i, \theta_{-i}) \in \Theta^v$, $(\theta'_i, \theta_{-i}) \in \Theta^{v'}$,

$$\phi(\theta_i, \theta_{-i}) \neq \phi(\theta'_i, \theta_{-i}).$$

SCF ϕ *is CP under* $\mathcal{P}$ *if there exists a CP protocol* $P \in \mathcal{P}$ *implementing it.*

Definition 3 (Queries). *A query* v *is an* individual elicitation query *if there is an agent* $i \in [n]$ *such that for all edges* $e = (v, w) \in E$, $\Theta^v_j = \Theta^w_j$ *for any* $j \neq i$*. A node* v *is an* anonymous sample query *if there is a set* $\tilde{\Theta} \subseteq \Theta$ *such that the children* $\{w : (v, w) \in E\}$ *correspond to the non-empty sets* $\{\boldsymbol{\theta} \in \Theta^v : |\{i \in N : \theta_i \in \tilde{\Theta}\}| = k\}$*, for* $k = 1, \ldots, n$*.*

Definition 4 (Protocols). *A protocol is sequential if all of its queries are individual elicitation queries. A protocol* P *is a* anonymous *if all of its queries are individual elicitation queries or anonymous sample queries.*

Proofs