Contextually Private Implementation

ANDREAS HAUPT and ZOË HITZIG

Consider a mechanism design environment in which a designer sequentially queries agents’ private information to determine the outcome of a choice rule. The designer’s social and technological environment constrains the set of access protocols that it can use. In high-tech environments, arbitrary cryptographic protocols are admissible, and so privacy concerns do not constrain the set of available choice rules. In other environments, privacy desiderata are needed to guide design. A protocol is contextually private for a choice rule if each piece of information learned about each participant is needed to determine the outcome. We characterize choice rules that can be implemented with a contextually private protocol under different assumptions about the class of admissible protocols. Under the assumption that private information must be elicited sequentially from uniquely-identified agents, the serial dictatorship and the first-price auction have contextually private implementations. However, no other \( k^{th} \)-price auction has a contextually private implementation, nor does any stable choice rule (in college assignment) or individually rational and efficient choice rule (in house assignment). Under a more generous assumption, which additionally allows the designer to anonymously count the number of agents whose private information has a certain property, the designer has wider scope: we describe a contextually private tâtonnement-like implementation of several choice rules that are not contextually private under the stricter assumption.
1 INTRODUCTION

Market participants supply vast amounts of information to firms, governments and other institutions that organize markets. New regulations, such as the European Union’s 2019 General Data Protection Regulation, aim to protect market participants’ privacy through laws that govern the use of information that participants supply. As a result, law-abiding market designers must increasingly design for privacy—that is, they must look for privacy-preserving implementations of their market rules.

In this paper, we define one notion of privacy-preserving implementation: A choice rule is contextually private if, under given social and technological constraints, there is a way to implement it in which each piece of information revealed to the designer is needed to determine the outcome. That is, information access is justified by the market context.

One issue that arose in a recent lawsuit against Google illustrates the potential value of contextual privacy for market design. The lawsuit claims that Google’s auctions for internet advertising on its exchanges (AdX) were “falsely represented” to be second-price auctions with pre-set floors. A complaint filed by the plaintiffs on January 14, 2022 explains how Google’s second-price auctions were not second-price auctions at all:

Google induced advertisers to bid their true value, only to override pre-set AdX floors and use advertisers’ true value bids against them... Google abused advertisers’ trust and secretly... generated unique and custom per-buyer floors depending on what a buyer had bid in the past. State of Texas et al. v. Google

Google used the history of advertisers’ losing bids in previous auctions to set personalized floors, which were then used as the “second-price” in customized auctions. The customized auctions forced advertisers to pay more than they would have if the floor had been pre-set.

Contextual privacy speaks to the core of the privacy problem in the Google case: Google learned information it didn’t need to know. In particular, Google did not need to know the identities and exact bids of losing bidders in order to carry out a second-price auction in good faith. Google’s information access was not appropriate to the context.

Contextual privacy is aligned with the concept of contextual integrity [Nissenbaum, 2004], which defines privacy preservation as ensuring appropriate information flows in a given social context. It thus contrasts with approaches that see privacy preservation as a matter of blocking information flows, and which accordingly see cryptography as a cure-all for privacy problems, regardless of context. In markets where high-tech cryptographic protocols are infeasible or costly for social or technological reasons, contextual privacy offers a formal notion of appropriate information flows between participants and the designer.

In principle, Google’s privacy problem could likely be solved with a high-tech cryptographic solution (such as secure multi-party computation, zero-knowledge proofs, hash functions, homomorphic encryption, etc.) which would block all information transmission [Alvarez and Nojoumian, 2020]. But Google’s auctions run in a fraction of a second—making any computational overhead, such as the overhead incurred through high-tech cryptographic calculations, particularly costly [Pachilakis et al., 2019]. Furthermore, the breach of trust may leave advertisers and regulators suspicious.¹ They might not believe Google’s claim that advertisers’ bids were cryptographically protected—and so regulators and participants would need to hire an expensive, trusted third-party specializing in high-tech cryptography to audit the auctions on a continual basis.

¹Even when there has not been a breach of trust, everyday users of cryptographic systems are suspicious of corporations claims about their privacy-preserving technology. A recent survey shows that only 61% of WhatsApp’s users believe the company’s claim that their messages are end-to-end encrypted [Alawadhi, 2021].
We ask whether contextual privacy, a weaker privacy desideratum, can be achieved with lower-tech (and thus lower cost) solutions. To formalize the process through which designers learn about agents’ private information, we define a general communication protocol through which agents reveal subsets of their private information. This perspective contrasts with much of direct mechanism design which assumes that agents reveal their private information in a single report. It aligns with the perspective in works such as Li [2017] and Akbarpour and Li [2020] which take the extensive-form of a dynamic mechanism to be primitive, and study formal properties of the resulting game tree.

1.1 Introductory Example

Suppose there are two agents, 1 and 2, and two objects, \(A\) and \(B\). The designer wants to choose a choice rule and a communication protocol to allocate the objects to the agents. An agent’s private information is her type, i.e. her preferred object (\(A\) or \(B\)). At the start of the protocol, the designer knows that the true type profile lies in the type space \(\{A, B\}\)\(^2\). In this example, we can visualize a protocol as consisting of \(2 \times 2\) boxes in which the rows are possible types for agent 1 and the columns are possible types for agent 2 (see Figure 1).

Protocols are made up of queries. Queries can be interpreted from a communication perspective or an access perspective: they can represent a live query to an agent (“communication”) or a query of a secure and monitored database that the designer can only access through such queries (“access”).\(^3\) At the start of a protocol, the designer knows that the true type profile of agents lies in the type space. Each query narrows down the set in which the true type profile lies. We can represent this learning process by shading in boxes in Figure 1 that the designer rules out with its queries.

We formalize the technological and social environment faced by a designer as restrictions on the set of queries that make up a protocol. We define and analyze three environments that vary in their degree of technological capacity and social trust. Roughly, these environments correspond to settings with low, medium and high degrees of technological capacity and social trust.

In environments with a low degree of technological capacity and social trust, only individual elicitation queries are available to the designer. These queries are direct questions about one agent’s type, as if the agent is being called to play in an extensive-form game, or as if the designer is querying an agent-identified entry in a database. We call a protocol made up of individual elicitation queries a sequential elicitation protocol.

Environments in which the designer is restricted to sequential elicitation protocols correspond to a low degree of technology and trust because the technology required to prove exactly what has been learned by the designer is extremely simple: all that is needed is a tamper-evident technology.\(^4\) Imagine that agents submit subsets of their private information in physical tamper-evident sealed envelopes. At the conclusion of the protocol, the designer can send back the envelopes that it has not opened. In this case, the agents have an exact record of what the designer learned, and do not have to trust the designer’s claim about what it learned.

An example of an individual elicitation query, shown on the left in Figure 1 is: “Is agent 1’s type \(A\)?” More generally, individual elicitation queries allow the designer to learn something

\(^2\)This paper is thus in the spirit of Brandt and Sandholm [2005, 2008], whose notion of unconditional full privacy for decentralized protocols is akin to contextual privacy for centralized protocols.

\(^3\)We treat the communication and access perspectives as equivalent throughout this paper. Clearly, the communication and access perspectives raise different strategic considerations which we discuss in subsection 2.2.

\(^4\)Tamper-evident technologies for protecting communications have existed for millennia, which confirms their technological primitiveness. Ancient Romans sealed letters with unique insignia pressed into wax seals so that others without their signet rings could not secretly reseal the letter. Since at least the 13\(^{th}\) century, writers of secure messages on paper have sealed their messages through an intricate series folds and cuts in a practice known as letterlocking.
about a single column—it can learn that agent 1’s type is either A or B. These two possibilities are represented by the “yes” arrow and the “no” arrow respectively. The “yes” arrow points to a refined type space in which the lower left cell is ruled out, while the “no” arrow points points to a refined type space in which the upper left cell is ruled out.

In environments with a medium degree of technological capacity and social trust, the designer additionally has access to anonymous sample queries. These queries are questions about how many agent types lie in a particular subset of the type space. Importantly, these queries are anonymous in that they do not identify which agents lie in the subset—they simply return an answer about how many agents do. We call a protocol made up of anonymous sample queries and individual elicitation queries a partially anonymous protocol.

Anonymous sample queries require some social trust and technological sophistication, but not too much. The only trusted technology needed is something that can de-identify the participants. Such technologies do exist, and are trusted, in both communication and access settings. In access settings, a range of trusted de-identification software programs are used to mask the identities of participants while gathering summary statistics about the sample of the population to which they belong. An example of an everyday anonymous sample technology in a communication setting is a secret ballot. In most elections in the U.S., voters have the right to a secret ballot, which means their vote is not learned by the government, other voters, or third parties. Notice that this requires trust in a de-identification technology, but the technology is not too sophisticated.\footnote{In the U.S., Kentucky was the first state to adopt a secret ballot in 1888. By 1950, secret ballots were in play nationwide.}

![Fig. 1. Example: Three types of queries](image)

An example of an anonymous sample query, shown on the right in Figure 1 is: “How many agents have type A?” The possible answers to this question are: neither agent prefers object A, one agent prefers object A, or both agents prefer object A. These three possibilities are represented by the “0”, “1” and “2” arrows respectively. The “0” arrow points to a refined type space in which the top row, corresponding to type profile (A, A), is ruled out. The “1” arrow points to a set of refined type spaces in which one agent has type A and the other has type B. The “2” arrow points to a refined type space in which the bottom row (type profile \((B, B)\)) is ruled out. Note that when the answer is 0 or 2, the designer learns the exact type profile with a single query, which illustrates how anonymous sample queries are more powerful than individual elicitation queries.

A protocol is contextually private for a choice rule \(\phi\) if each piece of information revealed through the protocol is necessary for determining the outcome of the choice rule. More precisely, a protocol is contextually private if the designer can only distinguish between possible types of agents in the event that the two types lead to different social outcomes. A choice rule is contextually privately implementable if there is an admissible protocol that implements it. The contextual privacy of a
choice rule thus varies depending on the technological and social environment, i.e. on the set of admissible protocols. Both sequential elicitation protocols and partially anonymous protocols are restrictive—some choice rules cannot be made contextually private.

To see how choice rules fail to be contextually private, suppose the designer wants to implement a simple efficient choice rule $\phi^\text{fair}$: give each agent their preferred object and break one of the possible ties in agent 1’s favor, and the other tie in agent 2’s favor.\footnote{Formally, this choice rule is}

When the designer must use elicitation queries, it cannot implement $\phi^\text{fair}$ in a contextually private way. For example, consider an individual elicitation query that asks “Is agent 1’s type $A$?” (shown on the left in Figure 1). If the answer is “yes”, then the designer knows that the true type profile $\theta$ is either $(A, A)$ or $(A, B)$, and for either of these type profiles, the outcome under $\phi^\text{fair}$ is $(1, A)$ and $(2, B)$. However, this query alone does not give the designer enough information to compute the choice rule. If the answer is “no” then the designer learns that the true type profile is either $(B, A)$ or $(B, B)$. In this event, the designer does not have enough information to compute the choice rule, because the two possible type profiles result in different outcomes under $\phi^\text{fair}$.

So the designer must pose another query: “Is agent 2’s type $A$?” While this second query, combined with the first, allows the designer to distinguish between type profiles $(B, A)$ and $(B, B)$ and therefore compute the choice rule, it violates contextual privacy for agent 2. To see this, suppose the true type profile is $(B, A)$. In this case, the protocol runs, and agent 1 gets object $A$ and agent 2 gets object $B$, and the designer knows that agent 2’s type is $A$ and not $B$. But, notice that holding agent 1’s type fixed at $A$, it did not matter whether agent 2 had type $A$ or $B$, the social outcome would have been $(1, A)$ and $(2, B)$ regardless. The designer did not need to know that agent 2 had type $A$ and not $B$, the social outcome would have been the same. So, under sequential elicitation protocols, $\phi^\text{fair}$ is not contextually private.

Under partially anonymous protocols, however, the designer can implement $\phi^\text{fair}$ in a contextually private way. Consider a protocol for $\phi^\text{fair}$ which begins with the query on the right in Figure 1: “How many agents prefer object $A$ to object $B$?” If the answer is 0, then the protocol stops, breaks the tie in favor of $B$ (assigning $B$ to 2 and 1 to $A$). If the answer is 2, the protocol stops, and breaks the tie in favor of $A$. If the answer is 1, then the designer learns that the type profile is either $(A, B)$ or $(B, A)$. In this event, the designer must ask pose another query, an individual elicitation query which asks “Is agent 1’s type $A$?” This query allows the designer to distinguish between the type profiles $(A, B)$ and $(B, A)$. But it still satisfies contextual privacy because for each agent, holding the other agent’s type fixed, the designer only learned to distinguish between an agent’s type if it made a difference to the outcome.

So, the choice rule $\phi^\text{fair}$ is contextually private under partially anonymous protocols (in “medium-tech environments”), but not under sequential elicitation protocols (in “low-tech environments”). This toy example therefore shows how the technological environment—that is, the set of protocols available—influence whether a choice rule has a contextually private implementation. Note that if the designer were operating in a high-tech environment with access to arbitrary (unrestricted) protocols, the choice rule $\phi^\text{fair}$ has a number of different contextually private implementations.

We introduce these restrictions on protocols to proxy for different kinds of technological environments, and choose these restrictions because they correspond to fairly primitive technologies that are and have been used widely in practice (tamper-evident envelopes, trusted anonymization). However, we note that there are many other kinds of protocols that could be considered, which
could lead contextual privacy to place different requirements on choice rules. It is instructive to compare our notion to differential privacy [Dwork et al., 2006], for example. Defining a differentially private implementation requires imposing a distributional assumption on types, which we have not needed here. Differential privacy would also accordingly define a statistical notion of indistinguishability of types, in contrast to our notion of exact indistinguishability. A differentially private implementation would also require types of queries that we do not study here. These queries would require a trusted technology that can add noise to query responses. While this article is not focused on contextual privacy for statistical indistinguishability, we view this as a fruitful avenue for future work. Contextual privacy will be compared more thoroughly to differential privacy in section 6.

1.2 Overview

In three different environments, we study whether common protocols and choice rules have contextually private implementations, and how contextual privacy interacts with other desirable properties of choice rules. Contextual privacy Table 1 summarizes our classification of common mechanisms in three environments.

| Choice Rule | "Low-Tech" (Sequential Elicitation) | "Medium-Tech" (Partially Anonymous) | "High-Tech" (Arbitrary) |
|-------------|-------------------------------------|-------------------------------------|-------------------------|
| SD          | yes                                 | yes                                 | yes                     |
| FP          | yes                                 | yes                                 | yes                     |
| SP          | no                                  | yes                                 | yes                     |
| kP          | no                                  | yes                                 | yes                     |
| Walras*     | no                                  | yes                                 | yes                     |
| DA          | no                                  | no                                  | yes                     |
| TTC         | no                                  | no                                  | yes                     |

*With additional conditions.

Table 1. Characterization results for common choice rules. Serial dictatorship (SD) and first-price (FP) auction have contextually private implementations under sequential elicitation protocols. If partially anonymous protocols are allowed, also second-price (SP), uniform k-th price (kP) and Walrasian (double) auctions have contextually private implementations. The top-trading cycles (TTC) choice rule and the deferred acceptance (DA) choice rule can be implemented in a contextually private way if arbitrary protocols are allowed.

In low-tech environments (when only sequential elicitation protocols are available), we find few contextually private choice rules. On the strict assignment domain (without transfers), we find that the serial dictatorship is contextually private and we prove two impossibility results. When agents begin with initial endowments of an object, no individually rational and efficient choice rule is contextually private. When objects have preferences over agents, as in the college assignment problem, no stable matching rule is contextually private. Turning to auction domains (with transfers), we find that the descending ("Dutch") protocol is a contextually private implementation for the first-price auction, and, under a mild condition, the unique efficient choice rule in which only the winner pays. Finally, we find that finding a market-clearing price in a double auction does not have a contextually private implementation.

In medium-tech environments, where the designer can use partially anonymous queries, many more common choice rules have contextually private implementations. We characterize a class of choice rules that can be contextually privately implemented with what we call tâtonnement protocols. The class of rules implementable with such protocols includes, for example, the second-price auction, and the Walrasian choice rule. We prove that the impossibilities from the pure assignment domain continue to hold when we allow partially anonymous protocols: contextual privacy is
incompatible with efficiency and individually rationality when agents have initial endowments, and it is incompatible with stability when agents have scores at different objects. We discuss how the results in the assignment domain may not extend to cases with an infinite set of agents.

The remainder of the paper proceeds as follows. We present the general model and key definitions in section 2. Then, we discuss contextually private implementation when: arbitrary (cryptographic) protocols are available (section 3), only sequential elicitation protocols (section 4) and only partially anonymous protocols are available (section 5). Section 6 discusses related literature and section 7 concludes. All omitted proofs can be found in the appendix.

2 MODEL
Consider a set \( \mathcal{N} = \{1, 2, \ldots, n\} \) of agents with private types \( \theta_i \in \Theta \) drawn from a distribution \( F \). We denote by \( \theta = (\theta_1, \theta_2, \ldots, \theta_n) \in \Theta^n \) the profile of agents’ types. Agents have preferences over outcomes in \( X \) which depend on their private types. The designer chooses an allocation rule \( \phi : \Theta^n \to X \) that assigns outcomes in \( X \).

2.1 Protocols
The designer also chooses a protocol to implement the chosen choice rule. For a choice rule \( \phi \), a protocol defines the process through which information is revealed about players’ private information.

**Definition 2.1 (Protocol).** A (deterministic) protocol \( P \) is a directed rooted tree with vertices \( V \) and edges \( E \). Each vertex is labelled with a non-empty subset of types \( \Theta^v = \times_{i=1}^n \Theta_{\theta_i}^v \). The root vertex \( v_0 \) corresponds to the full joint type space \( \Theta^n \). The labels of children \( (\Theta^w)_{\{w|(v,w) \in E\}} \) form a partition of the label of the parent node \( \Theta^v \).

We call nodes with zero out-degree *terminal*. All other nodes can be understood as questions about possible type profiles. For each type profile, there is a unique path through the tree \( P \) that leads to a terminal node. This definition is illustrated on the left in Figure 2.

We will study protocols implementing a social choice rule. We say that a protocol \( P \) implements a social choice rule \( \phi \) if \( P \) yields sufficient information to compute the choice rule, i.e. for any terminal node \( v \), and any distinct type profiles \( \theta \) and \( \theta' \)

\[
\phi(\theta) = \phi(\theta').
\]

In other words, the choice rule \( \phi \) is measurable with respect to the partition induced by terminal nodes of \( P \). When \( P \) certifies \( \phi \), we sometimes say \( P \) is a protocol for \( \phi \). We will also say that type profiles \( \theta, \theta' \) are separated at a node \( v \) if there are children \( w, w' \) of \( v \) such that \( \theta \in \Theta^w, \theta' \in \Theta^{w'} \).

**Definition 2.2 (Contextually Private Protocol).** A protocol \( P = (V, E) \) is contextually private for a social choice function \( \phi \) if for any \( (\theta_i, \theta_{-i}), (\theta'_i, \theta_{-i}) \in \Theta^n \), such that \( (\theta_i, \theta_{-i}) \in \Theta^v, (\theta'_i, \theta_{-i}) \in \Theta^v', \) \( v \neq v' \), we have

\[
\phi(\theta_i, \theta_{-i}) \neq \phi(\theta'_i, \theta_{-i}). \tag{1}
\]

Roughly, a protocol is contextually private if for all agents \( i \) and all types, if \( \theta_i \) is distinguishable from some \( \theta'_i \) for the designer at the conclusion of the protocol, it must be the case that \( \theta_i \) and \( \theta'_i \) result in different outcomes under \( \phi \). This criterion captures the idea that there must be a reason that the designer needed to know whether agent \( i \) had type \( \theta_i \) and not \( \theta'_i \). That reason, in particular, is that without distinguishing \( \theta_i \) from \( \theta'_i \), the designer could not have determined the overall allocation. This definition is illustrated on the right in Figure 2.

\footnote{We consider only deterministic rules in this article. For random rules, at least two definitions of contextual privacy, depending on whether randomization with public or with private sources of randomness is allowed, are possible.}
Definition 2.3 (Contextually Private Implementation). A choice rule $\phi$ is contextually privately implementable under a class of protocols $\mathcal{P}$ if there exists a protocol $P \in \mathcal{P}$ that implements $\phi$ and is contextually private.

Fig. 2. Definitions: Generic protocol (left), contextually private protocol (right)

To ease diction, we sometimes say that a choice rule is contextually private when it is contextually privately implementable. Contextually private implementation (or contextual privacy) is a property of a choice rule $\phi$ in a given environment characterized by protocols in class $\mathcal{P}$.

We define two types of queries which will be used to restrict the set of admissible protocols in different environments. Protocols can be understood as a sequence of queries, where a query for a non-terminal node $v$ is the partition of $\Theta^v$ induced by $\Theta^w$ for all children $w$ of node $v$.

Definition 2.4 (Individual Elicitation Query). Let $P = (V, E)$ be a protocol. A query for $v$ 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 $j \neq i$.

An individual elicitation query learns something about one agent at a time. For example, in an auction setting, an individual elicitation query could ask an agent $i$ whether their bid is above or below some value $x$.

Definition 2.5 (Anonymous Sample Query). A query for node $v$ is an anonymous sample query if there is a set $\tilde{\Theta} \subseteq \Theta$ (the so-called predicate) such that the children $\{w : (v, w) \in E\}$ correspond to the non-empty sets

$$\{\theta \in \Theta^v : |\{i \in N : \theta_i \in \tilde{\Theta}\}| = k\},$$

for $k \leq n \in \mathbb{N}$.

An anonymous sample query asks for the number of agents whose type lies in a certain subset of the type space. For example, in an auction setting, an anonymous sample query could ask how many agents have a bid above some value $x$.

We use these two types of queries to build protocols that correspond to different social and technological environments.

Definition 2.6 (Sequential Elicitation Protocol). A protocol $P$ is a sequential elicitation protocol if all its queries are individual elicitation queries.

A sequential elicitation protocol is a series of individual elicitation queries: it asks agents one after another for parts of their private information. Such a protocol can be realized live as an extensive-form game in which a single agent is called to play in each round (the communication perspective), or it can be realized as querying a data source (the access perspective).

Definition 2.7 (Partially Anonymous Protocols). A protocol $P$ is a partially anonymous protocol if all of its queries are individual elicitation queries or anonymous sample queries.
Sequential elicitation protocols and partially anonymous protocols express different technological and social constraints on the handling of information. Sequential elicitation protocols, as discussed in section 1, approximate the designer’s technological constraints in what we call “low-tech” environments. With simple technology—tamper-evident envelopes, for example, or a live extensive-form implementation—sequential elicitation protocols allow the designer to demonstrate to participants exactly what information it has learned or accessed. Participants do not have to trust the auctioneer or third party’s claim about what was learned, because they can see exactly for themselves.

Meanwhile, partially anonymous protocols require some amount of trust and technological capacity, so they approximate what is possible in what we call “medium-tech” environments. Some trusted de-identifier is required. For example, most everyday secret ballots for elections are run as one-step partially anonymous protocols. An anonymous sample query allows the electioneer to learn the number of agents that belong to the part of the space $\Theta$ that prefer a certain candidate. This is not a trustless environment: when voters vote, they have to trust that there is some technology that will keep their votes private.

2.2 Incentives and Equilibrium

In this paper, we deal only with “direct” mechanisms, in the sense that each mechanism we study is one in which agents submit subsets of their private information (“types”) to the designer. Often, studying the implementability of such mechanisms is without loss of generality, because of the revelation principle. The revelation principle states that any choice rule that can be implemented by an arbitrary mechanism can be implemented by a direct incentive-compatible mechanism with the same equilibrium outcome.

In this paper, we do not directly discuss the incentive compatibility of different protocols. However, depending on the relevant interpretation, incentive-compatibility results generated in other contexts apply directly here.

Recall the two interpretations of protocols: as access perspective and communication perspective. With the protocols as data access interpretation, agents’ truth-telling incentives remain intact. Taking on the access perspective, agents submit their reports (of types) using some pre-specified secure technology (e.g. tamper-evident envelopes in a low-tech environment, or anonymized ballots in a medium-tech environment). The protocol then describes how the designer accesses the pre-collected information. Their incentives are the same as they would be in a one-shot normal-form game in which they revealed all of their private information in a single report (as is standard in mechanism design).

With the protocols as live communication interpretation, however, agents’ truth-telling incentives will only remain intact for strategyproof choice rules, which can be implemented in dominant strategies. On this perspective, agents are called to submit pieces of their private information as the designer requests them as in an extensive-form game. It is easiest to imagine such a game for sequential elicitation protocols, since only one agent is called to play at a given time, and this type of game is canonical in game theory. When anonymous sample queries are included, there are stages of the extensive-form game in which all players are anonymously called to play. We do not model such dynamic incentives, and note that for choice rules that are not strategyproof, e.g. choice rules that are Bayesian incentive-compatible, the set of equilibria in the “communication”

---

8A social choice function $\phi$ is dominant-strategy incentive compatible or strategy-proof if

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

for any $\theta_i, \theta'_i, \theta_{-i}$. 
protocol dynamic game may differ from its static counterpart.\(^9\) This is because information about other agents’ types is revealed at each stage of the game.

When non-strategyproof choice rules are considered, the type and the report may not coincide. All choice rules we consider have Bayes-Nash equilibria with bijective strategies, so the conflation of types and reports is not too problematic—the type can be inferred from the report. In the rest of this article, we will write \(\theta_i\) to refer to the agent’s type or their type report. We use the notation \(\theta_{[k]}\) to denote the \(k\)-th highest element in \(\{\theta_i| i \in \mathcal{N}\}\) and call it the \(k\)-th order statistic.

### 3 HIGH-TECH ENVIRONMENTS

If there is no restriction on protocols, contextual privacy does not restrict the set of choice rules that are implementable. Denote \(\mathcal{P}\) the set of all protocols.

**Proposition 3.1.** Any choice rule \(\phi\) is contextually private under \(\mathcal{P}\).

**Proof.** Consider the protocol with one query, and partition of the space of type profiles \(\Theta^n\) into partition sets \(\phi^{-1}\{\{x\}\}, x \in X\). This clearly certifies the choice function \(\phi\). It also separates exactly the types that lead to different outcomes. \(\square\)

One technology that allows for near-arbitrary yet private access to information submitted to a mechanism is (mathematical) cryptography. Assuming a social environment in which participants believe that cryptography (which often relies on computational hardness properties) limits the amount of information learned about them, Lemma 3.1 shows that (nearly) arbitrary mechanisms are implementable. See the survey Alvarez and Nojoumian [2020] for a discussion of cryptographic implementations of auctions and mechanisms.

For the remainder of this article, we focus on environments in which social or technological constraints restrict the set of protocols that can be used by the designer.

### 4 LOW-TECH ENVIRONMENTS

In settings with low technological capacity and social trust, few choice rules are contextually private. We formalize the designer’s technological environment through restrictions on the protocols they can access: in “low-tech” environments, designers can use only sequential elicitation protocols. Sequential elicitation protocols are made up only of individual elicitation queries, which ask a single agent whether its private information lies in a subset of the type space. We call such protocols low-tech because of their easy live implementations: Participants are called one-by-one to reveal information, as if in an extensive-form game.

The following technical result will be useful for our characterization of contextually private choice rules in low-tech environments. Chor and Kushilevitz [1989] presents a similar result for decentralized protocols.\(^10\)

**Lemma 4.1 (Square Lemma).** Let \(\phi\) be contextually private under sequential elicitation protocols. Then, for any fixed \(\theta_{-i-j} \in \Theta^n\), for all types \(\theta_i, \theta'_i, \theta_j, \theta'_j \in \Theta\),

\[
\phi(\theta_i, \theta_j, \theta_{-i-j}) = \phi(\theta'_i, \theta_j, \theta_{-i-j}) = \phi(\theta_i, \theta'_j, \theta_{-i-j}) = x \implies \phi(\theta'_i, \theta'_j, \theta_{-i-j}) = x.
\]

\(^9\)Given independent and identically distributed types \(\theta_i \sim F\), choice rule \(\phi\) is Bayesian incentive-compatible if

\[
\mathbb{E}_{\theta_{-i-j}}[u(\phi_i(\theta_i, \theta_{-j}); \theta_i)] \geq \mathbb{E}_{\theta_{-i-j}}[u(\phi_i(\theta'_i, \theta_{-j}); \theta_i)].
\]

for a utility function \(u: X \times \Theta\) representing the agents’ preferences.

\(^{10}\)The condition of \(n\)-privacy in Chor and Kushilevitz [1989] is not directly related to our condition of contextual privacy under sequential elicitation protocols. In particular, it is about all information exchanged in an arbitrary decentralized protocol.
As $P$ is the set of agents and $x$ is the assignment.

That is, outcomes are pairs of agents and objects—an element of the outcome set is $\phi(\theta_i, \theta_j, \theta_{-i-j})$. In particular,

$$\phi(\theta_i, \theta_j, \theta_{-i-j}) = \phi(\theta'_i, \theta_j, \theta_{-i-j}) = \phi(\theta_i, \theta'_j, \theta_{-i-j}) = x$$

As $P$ certifies $\phi$, there must be a node separating types from the set

$$\{(\theta_i, \theta_j, \theta_{-i-j}), (\theta'_i, \theta_j, \theta_{-i-j}), (\theta_i, \theta'_j, \theta_{-i-j}), (\theta'_i, \theta'_j, \theta_{-i-j})\}.$$ 

By definition of sequential elicitation protocols, this node must be an individual elicitation query to agent $i$ or agent $j$. We treat the case of agent $i$, the case of agent $j$ is symmetric. Assume that the true type profile is $(\theta_i, \theta_j, \theta_{-i-j})$. In this case, the types

$$(\theta_i, \theta_j, \theta_{-i-j})$$

are separated, but $\phi(\theta_i, \theta_j, \theta_{-i-j}) = \phi(\theta'_i, \theta_j, \theta_{-i-j})$, a contradiction to contextual privacy. 

The Square Lemma is best understood graphically. Hold fixed the types of all agents who are neither agent $i$ nor agent $j$ (i.e., hold $\theta_{-i-j}$ fixed). Look only at the $|\Theta| \times |\Theta|$ square that represents the types of any two agents $i$ and $j$. A $2 \times 2$ sub-square is shown in Figure 1. If a choice rule $\phi$ is contextually private under sequential elicitation protocols, then it must be the case that, when three of the four quadrants in any such square result in outcome $x$, the fourth quadrant also results in $x$.

### 4.1 Assignment

In the assignment domain, we fix a set $C$ of objects. Then, the set of outcomes is $X = N \times (C \cup \{\emptyset\})$. That is, outcomes are pairs of agents and objects—an element of the outcome set is $x = (i, c)$ which says that agent $i$ is assigned to object $c$. It is possible for agents to get assigned to no object, which is represented by the outcome $x = (i, \emptyset)$.

In the standard object assignment setting, agents have ordinal preferences over objects, which are private information. So agents’ types $\theta \in \Theta$ are preference orders of $C$ where $>_i$ reference to agent $i$’s preference ordering. A choice rule $\phi$ is efficient if there is no outcome $x$ such that $x \succeq_i \phi_i(\theta)$ for all agents $i$ and $x >_j \phi_j(\theta)$ for some agent $j$.

Let $A \subseteq N \times (C \times \{\emptyset\})$ be an outcome. A partial assignment $N(A)$ is the set of agents who have an assigned object in $A$, i.e. $N(A) = \{i \in N | \exists c \in C : (i, c) \in A\} \subset N$. If $N(A) = N$, we call $A$ complete. For a partial assignment $A$, denote $A(i)$ the (at most one) object assigned to agent $i$.

The remaining objects $R(A)$ are the objects that do not have an assigned agent in $A$, i.e. $R(A) := \{c \in C | \exists i \in N : (i, c) \in A\}$ the remaining items.

We first study the serial dictatorship mechanism. To define the serial dictatorship protocol in our notation, we characterize the nodes and edges of the rooted tree. Fix a permutation of agents $\pi$. The serial dictatorship protocol with respect to $\pi$ has as nodes all partial assignments to agents in $N_{\pi}^i := \{\pi(i')|1 \leq i' \leq i\}$ for any $i \in N$. Edges are between partial assignments $A_i \in N_{\pi}^i$ and $A_{i+1} \in N_{\pi}^{i+1}$ such that agents $\pi(1), \pi(2), \ldots, \pi(i)$ are assigned the same objects. We define sets of type profiles associated to each node recursively. For an edge $(A_i, A_{i+1}), \Theta_{A_{i+1}} = \Theta_{A_i} \cap \{\theta \in \Theta| \max_{\theta_{\pi(i)}} R(i) = A_{i+1}(\pi(i))\}$. Here, $R(i)$ is the set of remaining objects when it is agent $i$’s turn in the partial order; $\max_{\theta_{\pi(i)}} R(i)$ is the maximal element of $R(i)$ with respect to the strict order $\theta_{\pi(i)}$. If a node is reached that is a complete assignment, the protocol ends, and the complete assignment is implemented.

**Proposition 4.2.** Serial dictatorships are contextually private under sequential elicitation protocols.
The proof of this statement is in the appendix. Similar, contextually private, protocols allow agents’ choice sets when they are called to choose to be subsets of the remaining objects. We call this serial dictatorships with constraints.

In addition to being contextually private, the serial dictatorship also has other appealing properties. It is strategyproof and efficient. Pycia and Troyan [2021] show that it is the unique obviously strategyproof and efficient assignment mechanism, and Bade [2020] shows that it is the unique strategyproof, efficient and nonbossy deterministic mechanism. The next example shows that for two agents, all contextually private social choice rules under sequential elicitation give the same assignment as a serial dictatorship.

**Example 4.3 (For \( n = 2 \), Contextual Privacy Coincides with Serial Dictatorship Outcomes).** Consider again the example from the introduction in Figure 1. There are two agents \( N = \{1, 2\} \) and two objects \( X = \{A, B\} \). Denote the two possible outcomes \( x = ((1, A), (2, B)) \) and \( x' = ((1, B), (2, A)) \). In the upper right box, efficiency requires that the outcome is \( x \). In the lower left box, efficiency requires that the outcome is \( x' \). In the top left and bottom right boxes, where both agents have the same type, efficiency allows either \( x \) or \( x' \).

|       | A     | B     |       | A     | B     |       | A     | B     | or    | A     | B     |
|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| A     | x or x' | x     | A     | x     | x     | A     | x     | x     | or    | A     | x     |
| B     | x'     | x or x' | B     | x     | x     | B     | x     | x     |       | B     | x     |

Table 2. Outcomes for Example in Figure 1 under an arbitrary efficient choice rule (left); under an efficient choice rule which breaks ties lexicographically (\( \phi_{\text{fair}} \)) (mid-left); under a serial dictatorship \( \phi_{\text{sd}} \) (mid-right, right)

Recall the choice rule \( \phi_{\text{fair}} \) from the introductory example. The rule \( \phi_{\text{fair}} \) is an efficient choice rule that breaks ties in favor of agent 1 when the type profile is \((A, A)\) and in favor of agent 2 when the type profile is \((B, B)\). Under this rule, the box of outcomes looks like middle-left box in the table above. Here, the square is not complete—three out of four corners result in outcome \( x \) while the fourth results in \( x' \). And so, the Square Lemma tells us immediately that the rule \( \phi_{\text{fair}} \) violates contextual privacy.

All contextually private social choice rules in this example give the same assignment as a serial dictatorship. If A is the dictator, the outcomes are given by the table in the middle-right. If B is the dictator, the outcomes are given by the table on the far right. By the Square Lemma, we know that the only other contextually private outcome would be to have either \( x \) in all type profiles, or \( x' \) for all type profiles. But, neither of these are efficient.

As soon as more complexity in the form of endowments or object-specific priority scores is introduced, standard market design desiderata become incompatible with contextual privacy under sequential elicitation protocols.

Consider first the house assignment problem [Shapley and Scarf, 1974]. All agents are initially endowed with an object from \( C \). Denote the initial assignment by an injective function \( e: N \rightarrow C \), where \( e(i) \in C \) refers to agent \( i \)'s initial endowment. For our result it will be irrelevant whether the endowments are private information or known to the designer. We call a choice rule \( \phi \) individually rational if for all \( i \in N \)

\[
\phi_i(\theta) \succ_i e(i).
\]

**Theorem 4.4.** Assume agents have initial endowments \( e(i) \). Then there is no individually rational, efficient and contextually private choice rule under sequential elicitation protocols.
Proof of Theorem 4.4. The proof uses the Square Lemma. Consider two agents $i$ and $j$ and two possible preference profiles for each agent. For agent $i$, consider a type $\theta_i$ which contains $e(i) \succ_{i} e(j)$, and a type $\theta'_i$ which contains $e(j) \succ_{i} e(i)$. For agent $j$, consider $\theta_j$ which contains $e(j) \succ_{j} e(i)$, and a type $\theta'_j$ which contains $e(i) \succ_{j} e(i)$. Hold fixed all other types $\theta_{-i,j}$, and assume without loss that each agent has a preference profile with the feature that their own endowment is preferred to all other objects, i.e. $\theta_{-i,j} = \{ \theta \in \Theta^{n-2} | e(k) \succ_k c \text{ for all } c \in C \setminus \{e(k)\} \}$.

When the type profile is $(\theta_i, \theta_j, \theta_{-i,j})$, the agents both prefer their own endowment to the other’s. When the profile is $(\theta'_i, \theta_j, \theta_{-i,j})$, or $(\theta_i, \theta'_j, \theta_{-i,j})$, they both prefer $i$’s endowment and $j$’s endowment, respectively. When $(\theta'_i, \theta'_j, \theta_{-i,j})$, they each prefer the other’s endowment to their own. Let $x$ be the outcome in which both agents retain their endowment, i.e. $x = (i, e(i)), (j, e(j))$. Let $y$ be the outcome in which each agent gets each other’s endowment $y = (i, e(j)), (j, e(i))$. Then, individual rationality makes the requirements shown on the mid-left in Figure 3: $\psi(\theta_i, \theta_j, \theta_{-i,j}) = (\theta'_i, \theta'_j, \theta_{-i,j})$. Meanwhile, efficiency requires $\psi(\theta_i, \theta_j, \theta_{-i,j}) = y$ (shown on the mid-right in Figure 3).

![Fig. 3. Applying the Square Lemma for house assignment. Type profiles $\{\theta_i, \theta'_i\} \times \{\theta_j, \theta'_j\}$ used in the proof (left, arrows denote whether agent prefers own or other’s endowed object); required outcomes for each type profile under individual rationality (mid-left), under efficiency (mid-right), and under both efficiency and individual rationality (right).](image)

So, by the Square Lemma, no individually rational and efficient choice rule is contextually private under sequential elicitation protocols.

In another extension of the object assignment domain, two-sided matching, contextual privacy is incompatible with stability (no justified envy) under sequential elicitation. In this extension, every agent is matched to at most one object, and at most $\kappa(c)$ agents are matched to school $c$, for every $c \in C$, for some capacities $\kappa(c)$. That is, the set of outcomes is

$$X = \{ \mu \subseteq N \times C \text{ s.t. } \forall i \in N \{ c \in C \mid (i, c) \in \mu \} \leq 1 \text{ and } \forall c \in C \{ i \in N \mid (i, c) \in E \} \leq \kappa(c) \}$$

We say there is no oversupply if there are exactly as many “spots” as there are agents, i.e. $\sum_{c \in C} \kappa(c) = n$.

We assume that objects have preferences over agents, which are given by priority scores. We assume the scores for different objects are private information of the agents. This matches the college assignment problem with standardized test scores [Balinski and Sönmez, 1999, Sönmez and Unver, 2010]. We assume that each agent (student) has a vector of scores $s_c$, representing their score at each object (school) $c \in C$. Objects prefer agents with higher scores. Agent $i$ has private information $\theta_i = (\prec_i, s_i)$, where $\prec_i$ is $i$’s preference ranking over schools, and $s_i : C \rightarrow \mathbb{R}$ maps objects to scores.

In such school choice settings, a desirable property of choice rules is stability. A choice rule $\phi$ is stable if there is no pair $(i, c), i \in N, c \in C$ such that $c \succ_i \phi_i(\theta)$ and $s_i(c) > s_i(\phi_i(\theta))$. 

Andreas Haupt and Zoë Hitzig

12
We next consider single-item auctions and double auctions. Our results that pertain to the first-price and second-price rules, respectively, include the descending (“Dutch”) protocol and the ascending (“English”) protocol. Formally, the second-price auction is a choice rule \( \phi_{S}^{FP}(\theta) \) given by

\[
\phi_{i}^{SP}(\theta) = \begin{cases} 
(1, \theta_{i}) & \text{if } \theta_{i} = \min \arg \max_{j \in \mathcal{N}} \theta_{j} \\
(0, 0) & \text{otherwise.}
\end{cases}
\]

Both of these auction rules can be implemented via a number of different protocols. Commonly studied protocols for the first-price and second-price rules, respectively, include the descending (“Dutch”) protocol and the ascending (“English”) protocol. The ascending protocol for the second-price auction is celebrated because it is not only efficient but also strategyproof [Vickrey, 1961, Wilson, 1989] and credible [Akbarpour and Li, 2020]. We show that the ascending auction protocol is not contextually private, and furthermore, that the second-price choice rule does not have a contextually private implementation.

**Proposition 4.6.** Assume \( n \geq 3 \) agents. Under sequential elicitation, the second-price choice rule \( \phi_{S}^{SP} \) is not contextually private. If \( n \geq k + 2 \), the uniform \( k \)-th price auction is not contextually private.

The proof of this statement is in the appendix.

We now consider first-price choice rules. Note that first-price choice rules can be implemented with descending protocols. A descending protocol queries, for each element of the type space \( \tilde{\theta} \),
decreasing order, each agent 1 to n on whether their type \( \theta_i \) is above \( \theta \). Formalized as a protocol, this leads to a set of nodes \( \Theta \times N \times \{0, 1\} \) and edges from \( ((i, \hat{\theta}, 0)) \) to \((i + 1, \theta, 0))\) if \( \theta_i \neq \theta \) for any \( \theta \in \Theta \) (asking the next agent then no agent is the type just asked). There are also edges from \( ((n, \theta, 0)) \) to \((1, \text{max}_{\theta' < \theta} \theta', 0)) \) if \( \theta_n \neq \theta \) (going to the next lower type). Furthermore, there are edges \( ((i, \theta, 0), (i, \theta, 1)) \) for all \( i \in N \) and \( \theta \in \Theta \) corresponding to an agent stating that they have a type \( \theta \), which leads to them being allocated the good. Hence, the set of terminal nodes is \( \Theta \times N \times \{1\} \). The associated set of type profiles is recursively defined as

\[
\Theta_i^{(i+1, \theta, 0)} = \Theta_i^{(i, \theta, 0)} \setminus \{\theta\}
\]
\[
\Theta_n^{(1, \theta, 0)} = \Theta_n^{(n, \text{min}_{\theta' > \theta} \theta', 0)} \setminus \{\theta\}
\]
\[
\Theta_i^{(i, \theta, 1)} = \{\theta\}.
\]

The first line rules out the type \( \theta \) for type \( i \) when they claim that they are not this type. The next line does this for type agent \( n \). The last identifies an agent’s type exactly when they claim they are a type.

**Proposition 4.7.** The first-price rule \( \phi^{FP} \) is contextually private under sequential elicitation protocols.

The proof of this statement is in the appendix.

Hence, the first-price choice rule is contextually private under sequential elicitation. The next example gives insight into the other kinds of standard auction choice rules that have contextually private implementations under sequential elicitation protocols.

**Example 4.8.** Consider a standard auction rule in which the agent with the highest type wins and pays a price \( t \) where \( t : \Theta^n \rightarrow \mathbb{R} \) is an injective function. That is, the payment \( t \) that the winner pays is different for every type profile \( \theta \in \Theta^n \). In this case, the outcome \( \phi(\theta) = (q, t) \) is different for every type profile. Hence, contextual privacy is an empty condition, as \( \phi(\theta) = \phi(\theta') \) for \( \theta \neq \theta' \), \( \theta, \theta' \in \Theta^n \) is impossible. Hence, any protocol that implements this auction rule is automatically contextually private.

The example above shows that when the winner’s payment can depend in an arbitrary way on the profile of bids, many exotic standard auction choice rules are contextually private. However, with an additional condition on how the payment depends on the bid distribution, the first-price choice rule is the unique contextually private choice rule. We say that payments in an auction depend only on rank if the payment is a function of an order statistic, \( t = f(\theta_{[k]}) \) where \( k \in N \) is a quantile of the empirical bid distribution and \( \theta_{[k]} \) denotes the \( k \)-th order statistic of the set \( \{\theta_i| i \in N\} \).

**Proposition 4.9.** Consider the class of choice rules \( \Phi \) that consists only of standard auctions where the payment \( t \) depends only on rank. Under sequential elicitation protocols, the first-price choice rule \( \phi^{FP} \) is the unique efficient and contextually private standard auction rule in \( \Phi \).

The proof of this statement is in the appendix.

We conclude this section with an observation on standard double auctions. Suppose \( m \) agents are buyers and \( m \) agents are sellers, and \( n = 2m \). The \( m \) sellers are endowed with one indivisible object each (all seller’s objects are identical), and the buyers have unit demand for the object. Formally, agents have initial endowments \( e(i) \in \{0, 1\} \) where \( e(i) = 0 \) for buyers and \( e(i) = 1 \) for sellers. The preferences are

\[
u_i((q, t), \theta) = -e(i)\nu_i(\theta_i)q_i + (1 - e(i))\nu_i(\theta_i)q_i + t_i.
\]
An efficient double auction price rule seeks to find a price \( t \) that maximizes \( \sum_{i \in N} u_i((q, t), \theta) \) if buyers with types \( \theta_i \geq t \) buy a good at price \( t \), and sellers with value \( \theta_i \leq t \) sell their good at price \( t \), and agents with \( \theta_i = t \) sell or buy in order to match supply to demand. Efficient price rules set prices that are medians of the empirical type distribution of types, \( \phi(\theta) \in [\theta_{[m]}, \theta_{[m+1]}] \).

**Proposition 4.10.** Assume there are \( n > 3 \) agents. There is no efficient, uniform-price contextually private double auction price rule under sequential elicitation protocols.

The proof of this statement is in the appendix.

A natural choice rule for auction protocols includes the allocations and payments for agents directly in the choice function. Whether there is a contextually private protocol implementing such a choice rule is an interesting question for future research.

## 5 MEDIUM-TECH ENVIRONMENTS

Sometimes, social and technological constraints restrict the designer to a degree that falls somewhere in between the permissiveness of high-tech environments (in which arbitrary protocols are possible) and the restrictiveness of low-tech environments (in which only sequential elicitation protocols are possible). In medium-tech environments, we allow for partially anonymous protocols. These protocols contain anonymous queries of the form: “How many agents have types that lie in subset \( \theta \in \Theta \)?” The designer can count how many agents have types that lie in a particular subset without learning the identities of those agents. Such queries could be enabled through a trusted de-identification software, or process. Anonymous sample queries are ubiquitous in real world mechanisms: political elections and raffles are implemented through a series of anonymous sample queries that participants in these settings trust.

We show that lifting some but not all restrictions on the designer’s available protocols enables contextually private implementations of a wider class of choice rules, especially in the auction domain.

### 5.1 Auctions

We show that a wider class of auction rules are contextually private under partially anonymous protocols than are contextually private under sequential elicitation protocols.

Consider market-clearing choice rules. A choice rule with private allocations is called market-clearing with respect to quantile \( k \) if \( \phi_i(\theta) \) can be implemented as a serial dictatorship with an object set only depending on the \( k \)-th highest type \( \theta_{[k]} \).

We call type profiles \( \theta \) \( k \)-dispersed, for \( k = 2, 3, \ldots, n - 1 \) if \( \theta_{[k]} \notin \{\theta_{[1]}, \theta_{[n]}\} \). They are called 1- and \( n \)-dispersed if \( \max_{i \in N} \theta_i \neq \min_{i \in N} \theta_i \). We denote the set of \( k \)-dispersed type profiles by \( \hat{\Theta}_k \). These are type profiles in which there are types above and below the quantile \( k \).

Any market-clearing choice rule can be implemented by a protocol we call the tâtonnement protocol. This protocol uses anonymous sample queries to determine the “price” \( \theta_{[k]} \), and then individual elicitation queries to determine allocations. At each possible price \( \tau \in \Theta \), the auctioneer poses an anonymous sample query of the form: “How many agents have types greater (less) than or equal to \( \tau \)?” When the answer to this query is some \( k \), set \( \tau = t \). Then, in order to determine allocations, the auctioneer asks the agents to select objects from objects depending on this type.

Many choice rules are implementable with tâtonnement protocols. For example, the second-price choice rule is implementable with a tâtonnement protocol: set \( \tau = t \) when the answer to the partially anonymous protocol is \( k = 1 \), and let agents choose to buy at that price.\(^{12}\)

\(^{12}\)We assume that this breaks ties for indifferent agents in that they choose not to buy the good.
Tâtonnement protocols are contextually private. In order to prove this, we define tâtonnement more formally. The tâtonnement protocol first determines the order statistic $\theta[k]$ using anonymous sample queries, and then determines the individual allocations using sequential elicitation queries. This fits into the metaphor of the Walrasian auctioneer: a price is determined, which agents use to make transactions.

**Theorem 5.1.** Under partially anonymous protocols and $k$-dispersed type spaces, market-clearing rules for quantile $k$ are contextually private.

The proof of this statement is in the appendix.

This implies that all the auction rules studied in section 4 are contextually private under partially anonymous elicitation (with respect to $k$-dispersed type profiles). Also, the first-price rule is contextually private under sequential elicitation which means it is also contextually private under partially anonymous protocols.

**Corollary 5.2.** Under partially anonymous protocols and $k$-dispersed type spaces, the following choice rules are contextually private:

- Second-price rule
- Uniform $k$-th price rule

The proof of this statement is in the appendix.

For the double auction, we found in Proposition 4.10 that finding an efficient price is not contextually private under sequential elicitation protocols. Under partially anonymous protocols, it is clearly possible to locate an efficient price in a contextually private way: Using an upward pass of anonymous sample queries through the type space, stop as soon as the median is reached. This protocol does not distinguish any types when types are restricted to be in the set of $k$-dispersed types $\Theta_k$. We can consider the full uniform-price double auction environment, in which not just a price, but the allocations and transfers for agents are determined. Under an additional condition, we arrive at a positive result for efficient implementations in this environment. The condition is that there is a unique median agent, i.e. the type space is $\{\theta||i \in N|\theta_i = \theta[m] = 1\}$.

**Proposition 5.3.** Under partially anonymous protocols and $k$-dispersed type spaces, when there is a unique median agent, an efficient uniform-price double auction rule is contextually private.

The proof of this statement is in the appendix.

### 5.2 Assignment

By definition, under partially anonymous queries and without transfers, the Serial Dictatorship rule still remains a contextually private mechanism. In finite domains, the two extensions to settings with endowments (“house assignment”) or scores (“college assignment”), do not give positive results.

**Theorem 5.4.** Assume $|C|, |N| \geq 2$ and agents have initial endowments $e(i)$. Under partially anonymous elicitation, there is no efficient, individually rational and contextually private choice rule.

The proof of this statement is in the appendix.

This implies that there is no way to implement the same choice rule as top trading cycles with partially anonymous protocols.

Similarly, in the “college-assignment” problem, where agents (students) have private scores that represent the objects’ (colleges) preferences over them, stability and contextual privacy are incompatible even under partially anonymous elicitation.
Theorem 5.5. Assume that there are at least two agents and objects, agents have scores $s_i$, and there is no oversupply. There is no stable and contextually private choice rule under partially anonymous protocols.

The proof of this statement is in the appendix. Hence, the often deployed deferred acceptance rule leads to an outcome that does not coincide with the outcome of any contextually private choice rule. A search for a contextually private protocol for deferred acceptance is hence sure to fail even if partially anonymous queries are allowed.

5.3 Tâtonnement and Contextual Privacy in the Large

In large ($n \to \infty$) economies, it may be possible to implement a wider class of choice rules under partially anonymous protocols. While a formal discussion is beyond the scope of this paper, we give intuition for why partially anonymous protocols may be especially powerful for achieving contextual privacy when the number of agents and/or objects is large.

We call the protocols used in Theorem 5.1 tâtonnement protocols because they resemble Walras’ famous description of the trial-and-error processes through which prices equalize supply and demand. First, these protocols query “demand” and “supply” through partially anonymous queries, and stop when the market-clearing price has been found. Second, the agents choose their allocations given prices.

In finite economies, the first stage anonymous sample queries can pose problems for contextual privacy. It is often necessary, in this stage, to distinguish between two (or more) possible type profiles for a given agent in order to certify a choice rule, even when doing so won’t ultimately make a difference to the outcome. We saw that stable matching rules, for instance, do not have contextually private implementations (Theorem 5.5). In large economies, however, individual agents might not affect the overall response to an anonymous sample query, hence it is possible that no information is revealed in this phase.

This suggests that in large economies, choice rules characterized by supply-demand equations may have contextually private tâtonnement implementations. For instance, the general “price mechanism” for large economies (with $n \to \infty$ agents and multiple goods) praised for its communication tractability in Hayek [1945] (see also Nisan and Segal [2006]), may also have a privacy rationale. Also, supply-demand formulations of high-dimensional social choice problems may admit contextually private tâtonnement implementations. Azevedo and Leshno [2016] gives such an interpretation for large matching markets.

6 RELATED LITERATURE

This paper brings privacy considerations into the tradition of dynamic mechanism design, which analyzes the ways an extensive-form mechanism differs from its normal-form counterparts. Obvious strategyproofness Li [2017] helped to emphasize the importance of the extensive-form implementation of a mechanism, and has been widely studied, often in conjunction with other normative properties of mechanisms [Ashlagi and Gonczarowski, 2018, Bade and Gonczarowski, 2016, Golowich and Li, 2021, Mackenzie, 2020, Pycia and Troyan, 2021].

A more closely related extensive-form criterion is credibility [Akbarpour and Li, 2020], which requires incentive compatibility for the auctioneer. Credibility offers a different diagnosis of the Google case discussed in the introduction. While contextual privacy tells us that the second-price auction is not private, and thus needs to be implemented with a privacy-preserving protocol, credibility would say that the problem is that the second-price auction is not credible—the auctioneer has an incentive to deviate from it’s stated plan. Though the two diagnoses coincide in the case of
the second-price auction, they point in different directions in other cases—there are protocols that are credible but not contextually private, and some that are contextually private but not credible.

Contextual privacy generalizes unconditional full privacy [Brandt and Sandholm, 2005, 2008], which is itself a generalization of unconditional winner privacy [Milgrom and Segal, 2020]. Unconditional full privacy requires that the only information revealed through a market protocol is the information contained in the outcome. Brandt and Sandholm defined unconditional winner privacy separately for the auction domain [Brandt and Sandholm, 2008], and a voting domain [Brandt and Sandholm, 2005]. Further, Brandt and Sandholm’s formalism is derived from the premises of cryptography and computing, and is not readily incorporated into economic environments. We present a single definition for contextual privacy in a formal framework amenable to economic analysis.

Beyond unconditional full privacy, the most closely related concept in computer science and cryptography, lies an extensive literature on privacy preserving protocols for auctions and allocation. The literature on cryptographic protocols for auctions, going back to Nurmi and Salomaa [1993] and Franklin and Reiter [1996] is too vast to summarize here—the main point is that there are many cryptographic protocols that do not reveal any private information to a designer. Such protocols allow participants to jointly compute the outcome without relying on any trusted third party. To this literature we bring a degree of realism about the social and technological environments in which many designers operate: when cryptographic protocols are not available, we need some other privacy desiderata to guide design. Thus, we align with the tradition of contextual integrity Nissenbaum [2004] which contrasts with traditions that view cryptography as a go-to solution for all privacy problems [Benthall et al., 2017].

An influential privacy desideratum that also does not rely on cryptographic techniques is differential privacy [Dwork et al., 2006]. Contextual privacy sharply diverges from interpretations of differential privacy in mechanism design contexts. Differential privacy, as adapted for mechanism design contexts, says that the report of a single agent should have a negligible effect on the outcome. (This idea also has a precedent in the concept of “informational smallness” studied in Gul and Postlewaite [1992] and McLean and Postlewaite [2002].) To illustrate the sharp contrast between differential privacy and contextual privacy, suppose some bit of information is revealed through the mechanism. Differential privacy says that this bit can be revealed if it does not have an effect (or has a negligible effect) on the outcome. Contextual privacy says that this bit can be revealed if it does have an effect on the outcome—it can be revealed if the designer needed to know it. Whether contextual or differential privacy is a more appropriate notion of privacy will depend on context. Note that differential privacy would have no bite in articulating the way in which Google’s ad auctions represented a breach of privacy.14

7 CONCLUSION

In 2008, a coalition of sugar beet farmers in Denmark teamed up with agricultural titan Danisco to implement the first large scale use of secure multiparty computation: they ran a cryptographic auction to clear the market for sugar beets while protecting the firm’s and the farmers’ valuations of that year’s crop Bogetoft et al. [2009]. Detailing the results of the 2008 sugar beet auction, Bogetoft et al. [2009] acknowledges that the high-tech cryptographic solution may have been overkill: “One might also ask if the full power of multiparty computation was actually needed?” They respond by

---

13Differential privacy was originally proposed as a tool for database management. For a survey of its incorporation into mechanism design, see Pai and Roth (2013)).
14Differential privacy has also been microfounded with privacy concerns in agent utility functions, [Ghosh and Roth, 2013, Ligett and Roth, 2012, Nissim et al., 2012, Roth and Schoenebeck, 2012], and has been shown to be compatible with truthfulness [McSherry and Talwar, 2007, Xiao, 2013].
noting that a deviation from the level of privacy afforded by cryptographic solutions demands an answer to an intricate normative question: what constitutes an acceptable deviation from perfect privacy in this particular social environment? “Using full-blown multiparty computation,” they conclude, “is a better solution because it frees us from even having to consider the question.”

Contextually private implementations offer an answer that can guide design when cryptographic solutions are not available or excessively costly: a protocol is contextually private in a given social context if each piece of information revealed is needed to determine the outcome. We study the demands of contextual privacy in low-, medium- and high-tech environments. We find that few choice rules have contextually private implementations in low-tech environments: among common choice rules, serial dictatorships and first price auctions are exceptions. When designers operate in medium-tech environments, with access to trusted or easily auditable de-identification software, many more choice rules have contextually private implementations.

Contextually private implementation raises a number of avenues for further research. In particular, this paper did not discuss stochastic protocols or choice rules, which would dramatically change the set of contextually private choice rules—though also may occasion a modified definition of contextually privacy to preserve its spirit in the face of randomness. Relatedly, we did not introduce statistical queries on protocols, which would allow, for example, an articulation of—and more direct comparison to—differential privacy within our framework. In addition, we hope to further explore relative notions of contextual privacy which would allow for ordering the degree to which different mechanisms violate contextual privacy in a given context.

REFERENCES
Mohammad Akbarpour and Shengwu Li. 2020. Credible auctions: A trilemma. *Econometrica* 88, 2 (2020), 425–467.
Neha Alawadhi. 2021. Only 1 in 250 understand role of encryption in securing messaging: Study. *Business Standard* March 21 (2021).
Ramiro Alvarez and Mehrdad Nojoumian. 2020. Comprehensive survey on privacy-preserving protocols for sealed-bid auctions. *Computers & Security* 88 (2020), 101502.
Itai Ashlagi and Yannai A Gonczarowski. 2018. Stable matching mechanisms are not obviously strategy-proof. *Journal of Economic Theory* 177 (2018), 405–425.
Eduardo M Azevedo and Jacob D Leshno. 2016. A supply and demand framework for two-sided matching markets. *Journal of Political Economy* 124, 5 (2016), 1235–1268.
Sophie Bade. 2020. Random serial dictatorship: the one and only. *Mathematics of Operations Research* 45, 1 (2020), 353–368.
Sophie Bade and Yannai A Gonczarowski. 2016. Gibbard-Satterthwaite success stories and obvious strategyproofness. *arXiv preprint arXiv:1610.04873* (2016).
Michel Balinski and Tayfun Sönmez. 1999. A tale of two mechanisms: student placement. *Journal of Economic theory* 84, 1 (1999), 73–94.
Sebastian Benthall, Seda Gürses, Helen Nissenbaum, et al. 2017. *Contextual integrity through the lens of computer science*. Now Publishers.
Peter Bogetoft, Dan Lund Christensen, Ivan Damgård, Martin Geisler, Thomas Jakobsen, Mikkel Krøigaard, Janus Dam Nielsen, Jesper Buus Nielsen, Kurt Nielsen, Jakob Pagter, et al. 2009. Secure multiparty computation goes live. In *International Conference on Financial Cryptography and Data Security*. Springer, 325–343.
Felix Brandt and Tuomas Sandholm. 2005. Unconditional privacy in social choice. In *TARK*. 207–218.
Felix Brandt and Tuomas Sandholm. 2008. On the existence of unconditionally privacy-preserving auction protocols. *ACM Transactions on Information and System Security (TISSEC)* 11, 2 (2008), 1–21.
B Chor and E Kushilevitz. 1989. A zero-one law for Boolean privacy. ACM Press.
Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. 2006. Calibrating noise to sensitivity in private data analysis. In *Theory of cryptography conference*. Springer, 265–284.
Matthew K Franklin and Michael K Reiter. 1996. The design and implementation of a secure auction service. *IEEE Transactions on Software Engineering* 22, 5 (1996), 302–312.
David Gale and Lloyd S Shapley. 1962. College admissions and the stability of marriage. *The American Mathematical Monthly* 69, 1 (1962), 9–15.
Arpita Ghosh and Aaron Roth. 2015. Selling privacy at auction. *Games and Economic Behavior* 91 (2015), 334–346.
Louis Golowich and Shengwu Li. 2021. On the computational properties of obviously strategy-proof mechanisms. *arXiv preprint arXiv:2101.05149* (2021).

Faruk Gul and Andrew Postlewaite. 1992. Asymptotic efficiency in large exchange economies with asymmetric information. *Econometrica: Journal of the Econometric Society* (1992), 1273–1292.

Friedrich August Hayek. 1945. The use of knowledge in society. *The American Economic Review* 35, 4 (1945), 519–530.

Shengwu Li. 2017. Obviously strategy-proof mechanisms. *American Economic Review* 107, 11 (2017), 3257–87.

Katrina Ligett and Aaron Roth. 2012. Take it or leave it: Running a survey when privacy comes at a cost. In *International workshop on internet and network economics*. Springer, 378–391.

Andrew Mackenzie. 2020. A revelation principle for obviously strategy-proof implementation. *Games and Economic Behavior* 124 (2020), 512–533.

Richard McLean and Andrew Postlewaite. 2002. Informational size and incentive compatibility. *Econometrica* 70, 6 (2002), 2421–2453.

Frank McSherry and Kunal Talwar. 2007. Mechanism design via differential privacy. In *48th Annual IEEE Symposium on Foundations of Computer Science (FOCS’07)*. IEEE, 94–103.

Paul Milgrom and Ilya Segal. 2020. Clock auctions and radio spectrum reallocation. *Journal of Political Economy* 128, 1 (2020), 1–31.

Noam Nisan and Ilya Segal. 2006. The communication requirements of efficient allocations and supporting prices. *Journal of Economic Theory* 129, 1 (2006), 192–224.

Helen Nissenbaum. 2004. Privacy as contextual integrity. *Washington Law Review* 79 (2004), 119.

Kobbi Nissim, Claudio Orlandi, and Rann Smorodinsky. 2012. Privacy-aware mechanism design. In *Proceedings of the 13th ACM Conference on Electronic Commerce*. 774–789.

Hannu Nurmi and Arto Salomaa. 1993. Cryptographic protocols for Vickrey auctions. *Group Decision and Negotiation* 2, 4 (1993), 363–373.

Michalis Pachilakis, Panagiotis Papadopoulos, Evangelos P Markatos, and Nicolas Kourtellis. 2019. No more chasing waterfalls: a measurement study of the header bidding ad-ecosystem. In *Proceedings of the Internet Measurement Conference*. 280–293.

Mallesh M Pai and Aaron Roth. 2013. Privacy and mechanism design. *ACM SIGecom Exchanges* 12, 1 (2013), 8–29.

Marek Pycia and Peter Troyan. 2021. A theory of simplicity in games and mechanism design. *University of Zurich, Department of Economics, Working Paper* 393 (2021).

Aaron Roth and Grant Schoenebeck. 2012. Conducting truthful surveys, cheaply. In *Proceedings of the 13th ACM Conference on Electronic Commerce*. 826–843.

Lloyd Shapley and Herbert Scarf. 1974. On cores and indivisibility. *Journal of Mathematical Economics* 1, 1 (1974), 23–37.

Tayfun Sönmez and M Utku Ünver. 2010. Course bidding at business schools. *International Economic Review* 51, 1 (2010), 99–123.

William Vickrey. 1961. Counterspeculation, auctions, and competitive sealed tenders. *The Journal of Finance* 16, 1 (1961), 8–37.

Robert Wilson. 1989. Game Theoretic Analysis of Trading. In *Advances in Economic Theory: Fifth World Congress*. CUP Archive, 33.

David Xiao. 2013. Is privacy compatible with truthfulness?. In *Proceedings of the 4th conference on Innovations in Theoretical Computer Science*. 67–86.
A ADDITIONAL PROOFS

A.1 Low-Tech Environments

Proof of Proposition 4.2. Consider \( \theta_i, \theta'_i \in \Theta \) and a partial type profile for other agents \( \theta_{-i} \in \Theta^{n-1} \) such that \((\theta_i, \theta_{-i}) \) is separated from \((\theta'_i, \theta_{-i}) \). We will show that

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

Denote \( A \) the node of separation. By definition of sequential elicitation, this must be a query to agent \( i \). By definition of serial dictatorship, the children of \( A \) are given by \( \{ \theta | \theta_{\pi(i)} \in \max_{\theta_{\pi(i)}} R(i) = c \} \) for some \( c \in R(A) \). Hence, if \( \phi(\theta_i, \theta_{-i}) \) and \( \phi(\theta_i, \theta_{-i}) \) are separated from each other, agent \( i \) must get a different assignment under \( \theta_i \) and \( \theta'_i \), hence \( \phi(\theta_i, \theta_{-i}) \neq \phi(\theta_i, \theta_{-i}) \). \( \square \)

Proof of Theorem 4.5. The proof uses the Square Lemma. We first choose the type profile for \( n-2 \) agents that are not labelled \( i \) or \( j \). Then we construct a square representing possible types for agents \( i \) and \( j \).

Consider the type profile of all \( n-2 \) agents that are not \( i \) or \( j \) to be \( \theta_{-i,-j} \) where each agent has a score of 1 for their top choice object, and their top choice object has capacity to accommodate them. Denote \( C \) there is no oversupply, i.e. \( \sum_{c \in C} k(c) = n \), the number of remaining spots is \( n - (n - 2) = 2 \). Assume without loss of generality that the remaining spots are for different objects. Label these objects with remaining spots \( a \) and \( b \).

Consider the final two agents \( i, j \in N \). Two possible (partial) types for agent \( i \) are:

- \( \theta_i : (a \succ_i b, s_i(a) = \tilde{s}, s_j(b) = \bar{s}) \)
- \( \theta'_i : (b \succ_i a, s_i(a) = \tilde{s}, s_j(b) = \bar{s}) \)

and two possible types for agent \( j \) are

- \( \theta_j : (b \succ_j a, s_j(a) = \tilde{s}, s_j(b) = \bar{s}) \)
- \( \theta'_j : (a \succ_j b, s_j(a) = \tilde{s}, s_j(b) = \bar{s}) \)

where we assume that scores \( s_c \) belong to the interval \([\tilde{s}, \bar{s}]\) for all \( c \in C \). The parts of agent \( i \) and \( j \)’s types that do not pertain to school \( a \) and school \( b \) can be arbitrary.

Let \( x \) be the outcome in which agent \( i \) is matched to school \( a \) and \( j \) is matched to \( b \). Let \( y \) be the outcome in which agent \( i \) is matched to \( b \) and \( j \) is matched to \( a \). In both \( x \) and \( y \), all agents not \( i \) or \( j \) are assigned to their top choice object at which they have a high score.

![Fig. 4. Applying the Square Lemma to college assignment. Agent types \( \theta_i, \theta'_i, \theta_j, \theta'_j \) (left, arrows from agents denote favored object, arrows from objects denote high score); outcomes under any stable choice rule (right, where \( x = ((i, a), (j, b)) \) and \( y = ((j, a), (i, b)) \)).

Stability requires that \( \phi(\theta_i, \theta_j, \theta_{-i,-j}) = (\theta_i, \theta'_j, \theta_{-i,-j}) = (\theta'_i, \theta_j, \theta_{-i,-j}) = x \) while \( \phi(\theta_i, \theta_j, \theta_{-i,-j}) = y \).

We have chosen a particular \( \theta_{-i,-j} \in \Theta^{n-2} \), and particular \( \theta_i, \theta'_i, \theta_j, \theta'_j \in \Theta \) such that the condition (2) does not hold for any stable choice rule. So, by the Square Lemma, no stable choice rule is contextually private under sequential elicitation protocols. \( \square \)
Proof of Proposition 4.6. The proof uses the Square Lemma. Consider the agents with types $\theta_{[2]}$ and $\theta_{[3]}$ i.e. the agents with the 2nd and 3rd highest types. Call these two agents $i$ and $j$. Consider (without loss) two possible types $\theta < \bar{\theta}$, with $\bar{\theta}, \theta \in (\theta_{[4]}, \theta_{[1]})$. Hold fixed all other agents’ types $\theta_{-i,-j}$.

Consider the square that encodes two possible types for agent $i, \bar{\theta}_i$ and $\theta_i$ as well as two possible types for agent $j, \bar{\theta}_j$ and $\theta_j$ holding all other types $\theta_{-i,-j}$ fixed. That is, the four boxes of the square represent the type profiles $(\bar{\theta}_i, \bar{\theta}_j, \theta_{-i,-j})$, $(\bar{\theta}_i, \theta_j, \theta_{-i,-j})$, $(\theta_j, \bar{\theta}_j, \theta_{-i,-j})$, $(\theta_j, \theta_j, \theta_{-i,-j})$. See Figure 5.

![Figure 5. Applying the Square Lemma to the second-price auction. Type profiles for agent i and agent j (left, agent j’s type is represented by a dot, and agent i’s type is represented by a dash); required outcome under the second-price auction rule $\phi^{SP}$.](image)

Let $x$ be the outcome in which the highest type wins ($q_i = 1$ for $\theta_i = \theta_{[1]}$, $q_i = 0$ otherwise) and pays the price $t_i = \bar{\theta}$. Let $x'$ be the outcome under which the highest type wins and pays the price $t_i = \theta$. Note that $\phi^{SP}((\bar{\theta}, \bar{\theta}, \theta_{-i,-j})) = \phi^{SP}((\bar{\theta}, \theta, \theta_{-i,-j})) = \phi^{SP}((\theta, \bar{\theta}, \theta_{-i,-j})) = x$. But, under $\phi^{SP}$, it must be the case that $\phi(\bar{\theta}, \theta, \theta_{-i,-j}) = x'$. Since $x \neq x'$, the Square Lemma is violated, and thus the second-price choice rule is not contextually private under sequential elicitation protocols.

The construction given here extends straightforwardly to a uniform multi-unit auction with a single seller and $k$ unit-demand buyers.

Proof of Proposition 4.7. It suffices to show that the descending protocol is contextually private. Let $(\theta_i, \theta_{-i})$ and $(\theta'_i, \theta_{-i})$ be separated. By definition of sequential elicitation, this must happen when agent $i$ is queried. Note that terminal nodes cannot separate type profiles. Hence, $(\theta_i, \theta_{-i})$ and $(\theta'_i, \theta_{-i})$ are separated at a node of the form $(i, \bar{\theta}, 0)$. By definition of the descending protocol, the children of the node $(i, \bar{\theta}, 0)$ are associated to sets

$$\{\theta\} \text{ and } \{\theta' \in \Theta | \theta' < \bar{\theta}\}.$$

Let, without loss, $\theta_i = \bar{\theta}$ and $\theta'_i < \bar{\theta}$. In the former case, the outcome is that agent $i$ gets the good at price $\bar{\theta}$. By definition of the descending protocol, in the latter case, it is that either agent $i$ does not get the good, or they get it at a price $\theta' < \bar{\theta}$.

Note that by construction of the protocol, the first query leading to a singleton possible type space must be a type $\theta_i$ attaining $\max_{i \in \mathbb{N}} \theta_i$. This implies that the descending protocol implements a first-price choice rule (with tie-breaking according to the order $1, 2, \ldots, n$).

Proof of Proposition 4.10. Since every efficient uniform-price choice rule is a Walrasian choice rule, it suffices to show that no Walrasian choice rule is contextually private.

We use the Square Lemma. Consider four agents $i, j, k,$ and $\ell$ who have the types $\{\theta_{[m-1]}, \theta_{[m]}, \theta_{[m+1]}, \theta_{[m+2]}\}$.

For ease of exposition (and without loss of generality), suppose these middle four types are belong to the set $\{\bar{\theta}, \theta\}^4$ with $\theta < \bar{\theta}$. Consider arbitrary endowments.
We construct two squares: a square that holds agents $k$ and $\ell$’s types fixed at $(\theta_k, \theta_\ell) = (\theta, \theta)$ and considers all possible combinations in $(\theta, \theta)^2$ for agents $i$ and $j$; a square that holds $i$ and $j$’s types fixed at $(\theta_i, \theta_\ell) = (\bar{\theta}, \bar{\theta})$ and varies $k$ and $\ell$ in the same manner. See Figure 6.

![Fig. 6. Applying the Square Lemma to the double auction. Combinations of types for agents $i, j, k, \ell$ (left); required prices $t$ in an efficient choice rule.](image)

Let $x$ be the outcome in which the market clearing price is $t = \theta$ and let $x'$ be the outcome in which the market clearing price is $t = \bar{\theta}$. Consider first the top square which holds the types of agents $k$ and $\ell$ fixed and varies the types of agents $i$ and $j$. Efficiency requires $\phi(\theta_i', \theta_j', \bar{\theta}, \bar{\theta}) = \phi(\theta_i, \theta_j, \bar{\theta}, \bar{\theta}) = x$. Efficiency also requires that $\phi(\theta_i', \theta_j', \theta, \theta) \in \{x, x'\}$.

Now consider the bottom square which holds the types of agents $i$ and $j$ fixed and varies the types of agents $k$ and $\ell$. Efficiency requires $\phi(\bar{\theta}, \bar{\theta}, \theta_k, \theta_\ell) \in \{x, x'\}$. It also requires that $\phi(\bar{\theta}, \bar{\theta}, \theta_k', \theta_\ell') = \phi(\bar{\theta}, \bar{\theta}, \theta'_k, \theta'_\ell) = x'$.

The outcome under the type profile in the box that conjoins the two squares $(\bar{\theta}, \bar{\theta}, \bar{\theta}, \bar{\theta})$ must be either $x$ or $x'$ (it cannot be both). If it is $x$, then the Square Lemma is violated in the bottom $(k - \ell)$ square. If it is $x'$, then the Square Lemma is violated in the top $(i - j)$ square. So, there must be a violation of the Square Lemma, and any efficient uniform-price rule is not contextually private under sequential elicitation protocols.

**Proof of Proposition 4.9.** A similar construction as in the proof of Theorem 4.6. The quantile that the price depends on is chosen by two types. The square lemma can be similarly applied. □

### A.2 Medium-Tech Environments

**Proof of Theorem 5.1.** Denote by $s: \Theta \rightarrow \Theta$ the successor function for the order. We will propose only the cases $k = 1, 2, \ldots, n - 1$, which can be obtained by partially anonymous queries in ascending order. The case $n$, which requires descending queries, is symmetric. Formally, the protocol has nodes of two types. Nodes in $\Theta$ correspond to partially anonymous queries to elicit the order statistic, other types for an element of the type space $\theta$ and a partial assignment correspond to sequential elicitation queries. This corresponds to a type space

$$\Theta \cup \Theta \times \left(\bigcup_{i=1}^{n} C^{i-1}\right),$$
The edge set encodes an upwards pass through the types until the $k$-th order statistic is reached (first two types of edges) and a pass through a serial dictatorship given feasible sets $f(\tilde{\theta},\theta_i)$. Formally,
\[
(\tilde{\theta},s(\tilde{\theta})),\tilde{\theta} \in \Theta \setminus \{\text{max } \Theta \}
\]
\[
(\tilde{\theta},(\tilde{\theta},\emptyset)),\tilde{\theta} \in \Theta
\]
\[
((\tilde{\theta},c_1,c_2,\ldots,c_{i-1}),(\tilde{\theta},c_1,c_2,\ldots,c_i))\tilde{\theta} \in \Theta,c_1,c_2,\ldots,c_i \in C.
\]
To complete the description of the protocol, the type spaces associated with the nodes are
\[
\Theta^{\tilde{\theta}} = \{\theta \mid \{i \in N|\theta_i \geq \tilde{\theta}\}| \geq k\}
\]
\[
\Theta^\tilde{\theta}_{c_1,c_2,\ldots,c_i} = \{\theta||\{i \in N|\theta_i \geq \tilde{\theta}\}| = k,f(\theta_j,\tilde{\theta}) = c_j,j = 1,2,\ldots,i-1\}.
\]
We show that this protocol is contextually private under partially anonymous elicitation with respect to $\Theta_k$. Let $(\theta_i,\theta_{-i})$ be separated from $(\theta'_i,\theta_{-i})$. Let $A$ be a node of separation. There are two possible types of nodes that $A$ can be.
Case $A \in \Theta$: By definition of the protocol, it must then be that $\max\{\theta_i|i \in N\} < \theta'_i$. Note that this is not possible by the definition of $\Theta_k$ as there must be types above $\theta_k$.
Case $A = (\tilde{\theta},c_1,c_2,\ldots,c_{i-1})$: In this case, since $f$ is a function, it must be that there is $c_i,c'_i$ such that
\[
f(\theta_i,\tilde{\theta}) = c_i
\]
\[
f(\theta'_i,\tilde{\theta}) = c'_i.
\]
In this case, the outcome for type profile $(\theta_i,\theta_{-i})$ and $(\theta'_i,\theta_{-i})$ must be different as the type for agent $i$ is different. In other words, $\phi(\theta_i,\theta_{-i}) \neq \phi(\theta'_i,\theta_{-i})$, which implies that the protocol is contextually private.\footnote{A slightly more complicated proof also allows for ties in the protocol, which we omit. In this case, the second stage of the mechanism is a serial dictatorship instead of the rule outlined here.}

PROOF OF COROLLARY 5.2. We show that these rules are market-clearing rules. The second- resp. uniform $k$-th price auction are market-clearing with respect to 2 resp. $k$ and
\[
f(\tilde{\theta},\theta_i) = \begin{cases} (1,\tilde{\theta}) & \theta_i > \tilde{\theta} \\ 0 & \text{else}. \end{cases}
\]

\begin{flushright} \Box \end{flushright}

PROOF OF THEOREM 5.4. Our proof uses a Square Lemma-like construction. Assume there was a contextually private partially anonymous protocol $P$. We will derive a contradiction.

Fix an enumeration of $C$ and $N$. Let agent $i$ be endowed with object $i$. Furthermore, let object $j$ be the most preferred object for agent $j$ for $j \in N \setminus \{1,2\}$. Consider the four types given in
1. Agent 1’s most preferred item is 1; Agent 2’s most preferred item is 2;
2. Agent 1’s most preferred item is 2; Agent 2’s most preferred item is 2;
3. Agent 1’s most preferred item is 1; Agent 2’s most preferred item is 1;
4. Agent 1’s most preferred item is 2; Agent 2’s most preferred item is 1.

We will use the numbers 1 to 4 to refer to these type profiles. Note that in the former three cases, the only individually rational outcome is to assign agent $i$ to object $i$, $i \in N$. In the last case, the only assignment is to assign agent 1 to object 2 and agent 2 to object 2. As the outcomes are different, there must be a node in the protocol that separates types in the set of these types. We consider different cases depending on the query $A$ separating the types.
Case $A$ is a sequential elicitation query. Without loss, assume that this is a query to agent 1, the case of a query to agent 2 is symmetric. If agent 1’s preference is elicited, then type profiles 1 and 3
are separated from 2 and 4. This, however, implies that profiles 1 and 3 are separated from each other but lead to the same outcome. As 1 and 3 only differ in agent 2’s type, this is a contradiction to contextual privacy.

Case A is a counting query. Note that the only queries separating the agents are counting the number of agents that most prefer agent 1’s or agent 2’s endowment. We consider the case of preference for agent 1’s endowment, the case for agent 2’s endowment is symmetric. In this case, the type profiles are partitioned as \{1, 4\}, \{2\} and \{3\}. In particular, 1 and 3 are separated, lead to the same outcome, and differ only in agent 2’s type, which is again a contradiction to contextual privacy.

We hence showed that any query separating types (1), (2), (3), (4) leads to a violation of contextual privacy. As such separation is needed to certify an individually rational, efficient choice rule, this implies that no such choice rule is contextually private.

\[ \square \]

**Proof of Theorem 5.5.** Assume there was a partially anonymous, contextually private protocol \( P \).

We consider type profiles in which students \( i = 3, 4, \ldots n \) are assigned to schools. As we assume no oversupply, a partition where all but two colleges, which we call \( a \) and \( b \) have exactly as many students assigned as their capacity is. Assume that assigned students list the school as their highest priority, and that all other students have low scores at the school. Assume that agents 1 and 2 each have school \( a \) as their most preferred school. Assume that \( s_1 > s''_2 > s'_2 > s_2 \) are scores at school \( a \), which are lower than all other students’ scores at \( a \). We consider four different type profiles for the scores at school \( a \):

1. Agent 1 has score \( s_1 \), Agent 1 has score \( s_2 \);
2. Agent 1 has score \( s'_1 \), Agent 2 has score \( s_2 \);
3. Agent 1 has score \( s_1 \), Agent 1 has score \( s'_2 \);
4. Agent 1 has score \( s'_1 \), Agent 1 has score \( s'_2 \).

Note that in these type profiles, stability demands that the first three type profiles lead to an assignment of agent 1 to school \( a \) and agent 2 to school \( b \); the last needs to assign student 1 to school \( b \) and student 2 to school \( a \). Hence, there must be a node separating these type profiles. We show that for any query \( A \) that separates these types, there is a violation of contextual privacy.

Case 1: \( A \) is a sequential elicitation query. Without loss, consider the case that a sequential elicitation query to agent 1 is asked. This separated type profiles \( \{(1), (3)\} \) from \( \{(2), (4)\} \). Note that type profiles 1 and 2 only differ in the type of agent 1 and lead to the same outcome, which is a contradiction to contextual privacy.

Case 2: \( A \) is an anonymous sample query. In this case, the following is an exhaustive list of partitions that can be reached through counting queries, which we list with their potential predicates. Note that this list can be obtained by considering all 16 possible subsets of \( \{s_1, s_2, s'_1, s'_2\} \). Observe that \( \bar{\Theta} = \emptyset \) and \( \bar{\Theta} = \{s_1, s_2, s'_1, s'_2\} \). Observe that \( \bar{\Theta} = \{s_1, s_1\} \), and \( \bar{\Theta} = \{s_2, s'_2\} \) are unable to separate the types from 1 to 4.

- \( \{(1), (2)\}, \{(3), (4)\} \) (for \( \Theta \in \{s_1, s'_1, s_2\}, \{s_1, s'_1, s'_2\}, \{s_1\}, \{s'_1\}\))
- \( \{(1), (3)\}, \{(2), (4)\} \) (for \( \Theta \in \{s_1, s_2, s'_2\}, \{s'_1, s_2, s'_2\}, \{s_1\}, \{s'_1\}\))
- \( \{(1), \{(2), (3)\}, \{(4)\} \) (for \( \Theta \in \{s_1, s_2\}, \{s'_1, s'_2\}\))
- \( \{(3), \{(1), (4)\}, \{(2)\} \) (for \( \Theta \in \{s_1, s'_2\}, \{s'_1, s_2\}\))

In the first, third and fourth case, type profiles 1 and 3 are separated, lead to the same outcome, and only differ in agent 2’s type, hence contradict contextual privacy. In the second case, type profiles 1
and 2 are separated, lead to the same outcome, and only differ in agent 1’s type. Hence, in any case, we arrive at a contradiction to contextual privacy.

Hence, for any possible query separating any of the types (1), (2), (3), (4) from any of the other possible profiles, a violation of contextual privacy results. As such separation is needed to certify a stable choice rule, a contextual private implementation is not possible. □

Proof of Proposition 5.3. We consider a similar protocol as in the proof of Theorem 5.1, which we do not formally define for brevity. First, we pass upwards through the type space with partially anonymous queries \( \{\theta|\{i \in N|\theta_i \geq \theta\} = k\} \). As soon as a query results in \( m \), a serial dictatorship round is introduced. Given that there is a unique type that would be indifferent between selling and buying, we can ask each seller whether they are weakly below the quantile \( \tilde{\theta} \) and every buyer whether they are weakly above the quantile \( \tilde{\theta} \).

This is a contextually private protocol. By our restriction to \( ^\wedge \Theta_k \), a partially anonymous query is unable to distinguish any agent types without affecting the price, and hence, the outcome. By our restriction to a single median type, it is possible to certify the uniform-price efficient double auction at the minimum efficient price through queries for sellers that are weakly below the median or sellers that are weakly above the value. Sequential elicitation queries, also, cannot separate types. Indeed, the only information learned about an agent determines their outcome, either through the transfer (the endowment) or the allocation (which is through the type). □