Privacy-Preserving Market Design*

Mariann Ollár
University of Pennsylvania, Economics Department and Warren Center

Marzena Rostek
University of Wisconsin-Madison, Department of Economics

Ji Hee Yoon
University of Wisconsin-Madison, Department of Economics

November 9, 2015

Abstract

Preserving privacy is, increasingly, a concern in auctions and exchanges. To examine the role of privacy in markets, this paper suggests an alternative to “differential privacy” (Dwork (2006)) that accommodates settings in which outcomes of a mechanism respond to incentives. We formulate a class of mechanism design problems based on the uniform-price market clearing to study the joint design of (i) bids schedules (contingent variables); (ii) transparency settings for auction outcomes (observables); and (iii) the timing of market clearing. A design preserves privacy if the publicly observable outcome is not sufficient to recover the participants’ private information. We show that this privacy requirement can be necessary for the viability of the market – if violated, equilibrium may not exist. There need not be a trade-off between privacy preservation and welfare, in general. In particular, privacy-preserving design can be efficient. Common market mechanisms (i.e., an anonymous uniform-price auction protocol, a dark pool, and certain types of intermediation) are privacy-preserving designs that can also be efficient.

Keywords: Privacy, Uniform Price Auction, Divisible Goods, Market Design, Dark Pools, Observables, Contingent Variables

*We thank Paul Klemperer and Balazs Szentes for feedback, Rakesh Vohra and Aaron Roth for helpful conversations. Rostek gratefully acknowledges the financial support from the WARF Research Grant.
1 Introduction

Market participants are concerned about revealing information on their past trades, purchases, income, or liquidity needs. Designers of public auctions and sellers in online markets understand that bidders’ preferences for a design that preserves the privacy of their private information may critically affect behavior and participation. In financial markets, institutional buyers and sellers choose alternative trading venues, such as online marketplaces or dark pools (where identity is hidden behind an account number and trade transparency to other participants is limited)\(^1\) seeking to avoid exposure of their orders and front running. Privacy preservation is a major concern in financial exchanges, online auctions, benchmarking, electricity markets, agricultural markets, and has created a market for privacy. (Section \(^5\) provides an overview of the privacy practices that have developed.)

The goal of this paper is to understand the relevance of and the possibility for privacy-preserving market design: one in which the output of a market mechanism (e.g., prices or quantities) that is observable to market participants or an outside observer (e.g., a seller, a market maker, an intermediary) does not allow for recovering any trader’s private information. Despite its practical relevance for market design, privacy has only recently received attention in economics. The problem of privacy was first introduced in computer science, where a large literature has developed based on the concept of differential privacy (Dwork (2006))\(^2\) Take two databases that differ only in the participation of one individual and consider a function of a database. A differentially private mechanism selects its output using randomness so that the probability of any given outcome for participants is similar under any two such databases. Hence, the outcomes of the mechanisms that are differentially private cannot respond too much to any individual agent’s behavior. This restricts the class of environments in which differentially private implementation is possible, for instance, by requiring the number of participants to be sufficiently large\(^3\) The concept of differential privacy aptly captures privacy concerns in settings such as consumer markets – associated with purchases, credit history, or demographic data. However, in market or auction settings, successful design that enhances efficiency often entails that outcomes respond to behavior. This paper complements the study

\(^1\) About 30% of volume in U.S.-listed equities is executed in non-public markets that do not display traders’ positions and identities. This percentage has been increasing nearly every month. Over the past few years, liquidity pool trading (which involves trading of publicly listed stocks) in the U.S. has grown by more than 50%, while in Europe, the volume traded in liquidity pools relative to order-book activity has more than doubled. (Financial Times (2013)).

\(^2\) E.g., recent surveys by Dwork (2008); Pai and Roth (2013); Dwork and Roth (2014); and Heffetz and Liegett (2014).

\(^3\) While differential privacy allows reporting outcomes that can significantly change the observer’s posterior, the outcomes cannot be sensitive to the presence or absence of any individual in the database. The possibility of differentially private designs has been established for settings where an individual agent’s action does not significantly change the outcome for other agents, for example in large games or in games with the \(\mu\)-sensitivity property, which restricts how each agent’s strategy affects the utility of other players (Kearns et al. (2014)).
of privacy by considering such strategic settings.

The task of information collection and computation – by the seller or the market maker – can be relegated to an auction issuer, who, using cryptographic tools, can collect and store the reported information without observing it and determine the allocations without disclosing the collected information to the seller or buyers. Such cryptographic tools, and even self-destroying hardware for auctions or exchanges, are widely available. Cryptographic design defines what information and when is hidden. Nevertheless, they are not used in a variety of market settings, including online auctions and exchanges. This paper considers when the rules of the market themselves shall be defined to preserve privacy, what role privacy serves in markets, and how the privacy properties of a design interact with efficiency. Specifically, we consider a class of mechanisms for divisible goods based on the uniform price market clearing to study the joint design of

(i) bid space: to be realized market statistics for the domain of bid functions (contingent variables);

(ii) transparency settings: outcomes realized during the course of the auction (such as prices, individual or aggregate quantities, other statistics) to be made observable to bidders (observables);

(iii) static vs. dynamic auctions and the timing of market clearing.

Variants of market clearing based on the uniform price are used in many financial exchanges as well as auctions for commodities or assets. The mechanism design problem takes efficiency as the objective, subject to the incentive and participation constraints of the bidders.

We study markets for divisible goods with quasilinear-quadratic utilities and arbitrary Gaussian information structures. Our main results characterize the role of privacy preservation for equilibrium and the possibilities of enhancing efficiency while preserving privacy.

For static or dynamic designs based on the uniform-price mechanism with one round of market clearing after trade, we establish that preserving privacy with respect to other strategic bidders – in the sense that no trader’s valuation can be observed by the other bidders – is necessary for bidding according to true values. We further show that, in this class of designs, preserving privacy with respect to other bidders is necessary for equilibrium existence when bidder values are interdependent. Thus, outside of independent private value settings, privacy affects the viability of certain types of trading arrangements. The tight link between preserving privacy and truth telling properties of a design as well as equilibrium existence suggests why cryptographic implementation may not be applicable universally and when it might be useful.

Likewise, the task of verification of execution of the market protocol is often relegated to algorithmic tools – a function traditionally played by the price itself.

See, e.g., Thorpe and Parkes (2007); Flood, Katz, Ong, Smith (2014).

E.g., auctions of government bonds, emission permits, spectrum, electricity exchanges, refinancing (repo) markets, commodity markets, wholesale markets.

The main conclusions carry over to maximization of revenue in one-sided auctions or liquidity.
We then show that the rules of market design can be defined to preserve privacy while not compromising efficiency, informational or allocative. Privacy preserving designs, with a single or multiple rounds of market clearing, can enhance learning about payoff relevant information if bids are based on and, hence, learning occurs through contingent variables rather than observables. In addition, in dynamic auctions, a privacy preserving design ought to be non-transparent about outcomes or bids both pre-trade and throughout trading. The designs that satisfy these privacy requirements (in the class considered) include (i) static designs (essentially, the anonymous uniform-price auction protocol and the dark pool) and (ii) dynamic auctions (ascending, batch) in which outcomes of market clearing are observable only after the final trading round, and (iii) certain forms of intermediation. Thus, the designs that are commonplace if not dominate market design in exchange and auction settings appear as solutions to the privacy-preserving design problem. Finally, we characterize the efficiency properties of the privacy-preserving designs. A privacy-preserving design can be both informationally and ex post efficient (i.e., informationally and allocatively efficient). With the – common in practice – bid space of price contingent schedules (or combinations of limit and market orders), dynamic privacy-preserving designs with multiple trading rounds followed by market clearing do not aggregate information beyond what static markets do. For general information structures, efficiency can be achieved with richer contingent orders.

One insight from our analysis is that in divisible-good markets with interdependent values, design requires different privacy settings than with independent private value environments. Even with the standard price contingent schedules, privacy preservation is not a concern in general only if values are independent private. With divisible goods, interdependent values are precisely those for which designs based on a “mediator” or cryptographic tools may not be viable.

Let us highlight additional properties of our approach to privacy, relevant for implementation and market design. Differential privacy is a property of the mechanism (often, a randomized

---

8 While high levels of transparency are often perceived as pro efficiency, we show that they may be inconsistent with market viability, for both participation and incentive reasons, and can lower efficiency. In their analysis of market practice and regulation concerning transparency settings, Flood, Katz, Ong, and Smith (2013) argue that limited information sharing could be welfare improving through appropriate disclosure rules, and how cryptography could be useful.

9 Dark pools (e.g., internal crossing networks in large banks) typically do not use an internal price setting mechanisms for publicly traded stocks, but rather execute orders at the best price currently available at the public exchange ("price matching" or "best execution" practice). Dark pools were originally created to enable institutional investors to buy and sell large orders anonymously and avoid the trading ahead that moves the stock price and effectively taxes returns.

10 We are the first to characterize equilibrium in dynamic (without assuming stationarity) uniform-price auctions with interdependent values and information aggregation in markets. The literature on dynamic uniform-price auctions has considered independent private value settings. (Vayanos (1999) studies stationary (infinite horizon) markets with private and public aggregate endowment; Rostek and Weretka (2013) characterize non-stationary markets with public aggregate endowment). Du and Zhu (2014) and Kyle, Obzhihaeva and Wang (2013) allow for interdependent values in stationary (infinite horizon) uniform-price markets.
mapping from data into observable outcomes) and not of the outcome of strategic interaction in
the mechanism. Our notion of privacy concerns a property of the outcomes of a deterministic
mechanism. Indeed, in the differential privacy approach, randomness is what makes the direct
mechanism differentially private and, therefore, approximately incentive compatible. We show
that in divisible good settings, market designs based on the classic uniform-price mechanism
may not even induce bidding according to true values, unless they preserve privacy. Unlike
under differential privacy, the agents’ incentives to tell the truth are not weakened in a privacy
preserving designs we examine.

When, as the literature does, we quantify agents’ privacy with respect to the information
disclosed in equilibrium in the privacy-preserving designs, we show that, in a strategic market
context, there generally need not be a trade-off between privacy preservation and efficiency.
In particular, a dark pool can be more efficient than an auction. This contrasts with the
common view in the literature that privacy and welfare tradeoff.

Additionally, the literature commonly takes as a premise that privacy or withheld infor-
mation is valued by agents. In consumer markets, agents may have an intrinsic preference
for privacy. We do not assume that privacy is valued, but demonstrate its value (in utility
terms). Concerns about front running, commonplace in financial markets, give rise to the

---

11 Differential privacy so far has only been applied to settings with direct mechanisms. If a direct mechanism
is also differentially private (i.e., it defines a differentially private function from reports to outcomes), then
incentive compatibility will hold, yet only in an approximate sense. This follows from the interpretation that
the output of a differentially private function should be approximately unaffected by one particular individual’s
data (see Kasiviswanathan and Smith (2008), Dwork et al. (2006)). Recently, several authors relax the privacy
requirement; that is, instead of requiring differential privacy for the full outcome, they only require that the
joint output of other agents or the agent-by-agent outputs stay approximately unaffected by one particular
agent’s report.

12 In addition, applying randomness in the differential privacy approach may itself conflict with efficient
allocation, and strong privacy guarantees obscure information.

13 Studies of privacy treat it as an exogenous constraint, or incorporate it as an argument in the utility’s
domain (directly or via beliefs; e.g., Augenblick and Bodoh-Creed (2014)) or as a reduced-form argument in
the utility function (e.g., Gradwohl (2013); see also the survey by Pai and Roth (2013)). The exponential
mechanism, a classic tool to achieve differential privacy, is the solution to the optimization problem of a
designer who trades off efficiency and privacy, measured by the information theoretic Shannon measure (see,
e.g., Pai and Roth (2013). In this sense, differential privacy is optimal when privacy is valued intrinsically by
agents or by the designer. In our analysis, privacy is a necessity, rather than an objective.

The assumption that revealing less information is better is common in the privacy literature (see, e.g.,
Echenique, Cummings, and Wierman (2014) who examine testable implications of privacy-aware preferences,
adapting revealed preference analysis). Likewise, a rich literature encompassing cryptographic securities ex-
changes and differentially private release mechanisms offers practical tools to achieve privacy; however, the
reasons why privacy is a valid and desirable objective are less understood. Our analysis motivates privacy as
essential for incentivizing agents to act according to their actual private information; moreover, in its absence,
a market may fail to develop.

14 Our notion of an agent’s privacy is not information-theoretic and is defined in a strategic context. For a
trader, a loss of information about his signal is a concern to the extent that it can be used in a payoff-relevant
way by others. This need not be the case even if the statistic on which all bidders can condition their strategies
is informationally equivalent to the full signal vector.
value of privacy; Pai and Roth (2013) also observe this. More novelty, we show that privacy has value even in one-shot markets, thus when privacy-related consequences for future utility are absent. Namely, the possibility of nonexistence of equilibrium, even in static designs, points to a separate reason why privacy has value.

Privacy and incentives are attracting growing interest in the economics literature, notably by Gradwohl (2013), Augenblick and Bodoh- Creed (2014), Dziuda and Gradwohl (2014), Cummings, Echenique, and Wierman (2014). The main differences are that our analysis does not assume that privacy is intrinsically valued, that reports about private information are verifiable, and implementation does not rely on the direct mechanism. In the computer science literature on mechanism design based on differential privacy, agents’ incentives to misreport are limited, as the effect on the outcome would be limited, as the effect on the outcome would be limited; differential privacy implies approximate truthfulness (McSherry and Talwar (2007)). So are agent’s incentives to tell the truth (Nissim, Smorodinsky and Tennenholtz (2012); Xiao (2013)). Finally, there is renewed interest in the computer science and economics research in the interaction between mechanism design and bidder inference (e.g., Chawla, Hartline, Nekipelov (2014)). In the context of divisible good markets, this paper contributes the idea of designing the conditioning variables in bidders’ inference – the observables and contingent variables – to prevent market participants from recovering the unobservables (private information) while possibly enhancing inference about payoff relevant variables to achieve certain design objectives, such as efficiency.

2 Markets and Privacy

We describe the standard, Gaussian model for a divisible-good setting, present an example and the formulation of the market design problem.

2.1 Market

TRADERS AND INFORMATION STRUCTURE. Consider a market for a divisible good or asset with \( I \geq 2 \) traders indexed by \( i \) and an outside observer (e.g., a designer, a seller, an intermediary, an outside market participant) indexed by \( 0 \). Trader \( i \) has a quasilinear utility function, which is linear in money, and quadratic in quantity given by

\[
U_i(q_i) = \theta_i q_i - \frac{\mu_i}{2} q_i^2 ,
\]

15 Large investors, whose individual trades are large enough to move the price, typically do not place their orders at once, but instead, break up their orders and place them sequentially. Making the prices and quantities public exposes subsequent trades to front running by participating or outside investors.
where $q_i$ is the obtained quantity of the good traded and $\mu_i > 0$ can be interpreted as risk aversion.

Each trader is uncertain about how much the good is worth to him; this uncertainty is captured by randomness of the intercept of marginal utility $\{\theta_i\}_i$ and represents shocks to preferences, endowments or liquidity. Each trader $i$ observes a noisy signal about his own true value $\bar{\theta}_i$, $s_i = \theta_i + \varepsilon_i$. Random vector $\{\theta_i, \varepsilon_i\}_i \in I$ is jointly normally distributed, noise $\varepsilon_i$ is mean-zero and independent across traders with variance $\sigma^2_{\varepsilon}$, and value $\theta_i$ has expectation $E_i(\theta_i)$ and variance $\sigma^2_{\theta}$ the same for all $i$. Let $\sigma^2 \equiv \sigma^2_{\varepsilon}/\sigma^2_{\theta}$ denote the variance ratio. The $I \times I$ variance-covariance matrix of the joint distribution of values, normalized by variance $\sigma^2_{\theta}$, defines the matrix of correlations,

$$
IS \equiv \begin{bmatrix}
1 & \rho_{12} & \ldots & \rho_{1I} \\
\rho_{21} & 1 & \ldots & \rho_{2I} \\
\vdots & \vdots & \ddots & \vdots \\
\rho_{I1} & \rho_{I2} & \ldots & 1
\end{bmatrix},
$$

(2)

which, with a slight abuse, we will refer to as information structure (IS), as our analysis will explore the role of interdependence in $\{\theta_i\}_i$. One expects the privacy properties of design to depend on the interdependence among traders’ values. We consider the following types of interdependence, encompassed by the Gaussian model above with arbitrary $\{\rho_{ij}\}_{j \neq i}$:

- *independent (private) value model*: $\rho_{ij} = 0$ for all $i \neq j$;
- *fundamental value model*: $\rho_{ij} = \bar{\rho}$ for all $j \neq i$: e.g., $\theta_i = \theta + \tilde{\theta}_i$, where $\{\tilde{\theta}_i\}_i$ are independent across $i$, $\bar{\rho} = Var(\theta)/(Var(\theta) + Var(\tilde{\theta}_i))$; with only idiosyncratic shocks $\theta_i = \theta'_i$, this nests the independent private value model, and with only common shocks, the pure common value model obtains, $\rho_{ij} = 1$ for all $i \neq j$;
- *equicommonal model*: each trader is correlated with the market in the same way, on average, $\bar{\rho} \equiv \frac{1}{I-1} \sum_{j \neq i} \rho_{ij}$, for all $i$.

**MARKET-CLEARING MECHANISM.** Market clearing is based on a uniform-price mechanism. While later in the analysis, we use a more general definition, let us recall that of the standard uniform-price auction. Traders submit downward-sloping (net) demand schedules $\{q_i(p)\}_{i \in I}$; the part of a bid with negative quantities is interpreted as a supply schedule. We consider

---

16 In the fundamental value model, value correlations are the same for all trader pairs; e.g., all traders’ values are affected by only common or idiosyncratic shocks – the prevalent assumption in the asset-pricing or macroeconomic literature to study the impact of aggregate shocks to fundamentals. We also leverage recent equilibrium characterizations in divisible-good auctions, with the information structures that admit heterogeneity in interdependence among trader values, and show that the (as)symmetry properties they exhibit determine the privacy properties of design. The characterizations of equilibrium in divisible good auction models for the fundamental value, equicommonal and Gaussian model with a finite number of participants were developed, respectively, by Vives (2011), Rostek and Weretka (2012), and Rostek and Yoon (2014). The classic model of Kyle (1989) with $\rho_{ij} = \bar{\rho} = 1$, assumes the presence of noise traders apart from strategic traders. Vives (2011) allowed $\rho_{ij} = \bar{\rho} < 1$. 

---
one-sided auctions with \( I \) strategic buyers and a strategic seller who submits a supply schedule \( Q_0(p) \) or a nonstrategic seller of a fixed or stochastic quantity \( Q_0(p) = Q_0 \) as well as double auctions with \( I \) strategic buyers and sellers, \( Q_0(p) = 0 \). We consider static and dynamic auctions with \( T \) stages indexed by \( t \). In a one-stage auction, the market-clearing price \( p^* \) is one for which aggregate demand \( Q(p) = \sum q_i(p) \) equals total supply \( Q_0(p) = Q_0(p^*) \). Trader \( i \) obtains the quantity determined by his submitted bid evaluated at the market clearing price, \( q_i^* = q_i(p^*) \), for which he pays \( q_i^* p^* \). Each trader’s payoff is given by the utility function \( \Pi \) evaluated at \((q_i^*, p^*)\).

EQUILIBRIUM. We study linear\(^{17}\) bid function equilibrium for static auctions and dynamic linear bid function equilibrium for dynamic auctions (hereafter, “equilibrium”).

2.2 Example

We begin with a motivating example that explains the uniform-price mechanism and equilibrium and introduces privacy considerations.

Example 1 (Privacy in a Static Double Auction). Consider the standard one-stage double auction with equicommonal information structure. The necessary (and sufficient) optimization condition of bidder \( i \) (Appendix B) equalizes his expected marginal utility with his marginal expenditure, for any \( p \),

\[
E(\theta_i|s_i,p) - \mu q_i = \frac{\partial(q_i \cdot p(q_i))}{\partial q_i},
\]

given the conditional expectations

\[
E(\theta_i|s_i,p) = c_\theta E(\theta_i) + c_s s_i + c_p p
\]

with inference coefficients \( c_s, c_p \) and \( c_{\theta} \). One can show (Appendix B) that, in the symmetric linear Bayesian Nash Equilibrium, bidding strategies and market clearing price are given by

\[
q_i(p) = \frac{\gamma - c_p c_{\theta}}{1 - c_p \mu} E(\theta_i) + \frac{\gamma - c_p c_s}{1 - c_p \mu} s_i - \frac{\gamma - c_p}{\mu} p,
\]

\[
p^* = \frac{c_\theta}{1 - c_p} E(\theta_i) + \frac{c_s}{1 - c_p} \bar{s},
\]

where \( \gamma \equiv 1 - \frac{1}{T-1} \) is the index of market size and \( \bar{s} \equiv \frac{1}{T} \sum s_i \) is the average signal. Thus, assume that after the auction is completed, quantities, \( \{q_i\} \), are observed to each \( i \) and the

\(^{17}\)Equilibrium is linear if bids have the functional form \( q_i(p) = \alpha_0 i + \alpha_s s_i + \alpha_p p \); it is symmetric linear if the coefficients \( \alpha_0 i, \alpha_s i, \) and \( \alpha_p i \) are the same across traders.
designer. The coefficients in the symmetric bid functions are common knowledge. Let $\tilde{q}_i \in \mathbb{R}$ denote the observed quantity allocated to agent $i$. Let $\tilde{s}_i$ denote the realized (privately observed) signal of agent $i$.

Substituting 6 into 5, we find each equilibrium quantity as a function of realized signals, $\tilde{q}_i = \frac{\gamma - c_p c_s}{1 - c_p \mu} (\tilde{s}_i - \bar{s})$. Write the equation system for the realized signals as

$$\tilde{q} = \frac{\gamma - c_p c_s}{1 - c_p \mu} \begin{bmatrix} 1 - \frac{1}{I} & -\frac{1}{I} & \cdots & -\frac{1}{I} \\ -\frac{1}{I} & 1 - \frac{1}{I} & \cdots & -\frac{1}{I} \\ \vdots & \ddots & \ddots & \vdots \\ -\frac{1}{I} & \cdots & 1 - \frac{1}{I} \end{bmatrix} \tilde{s}. \quad (7)$$

What can an outside observer infer by observing the quantities on the market? Note that (7) does not have a unique solution; whenever $s$ is a solution, then $s + \beta 1$ is a solution as well for any $\beta \in \mathbb{R}$. At the same time, agent $i$ knows his own signal $\tilde{s}_i$ and faces the system of $I - 1$ equations (with the l.h.s. observable to him and the r.h.s. variables unknown to him)

$$\left\{ \tilde{q}_j + \frac{\gamma - c_p c_s}{1 - c_p \mu} \tilde{s}_i = \frac{\gamma - c_p c_s}{1 - c_p \mu} \left( \tilde{s}_j - \frac{\sum_{k \neq i} \tilde{s}_k}{I} \right) \right\}_{j \neq i}. \quad (8)$$

Subtracting the equation for $\tilde{q}_i$ from the equation for $\tilde{q}_j$ and solving for $\tilde{s}_{-i}$, we obtain

$$\tilde{s}_j = \tilde{s}_i + \frac{\tilde{q}_i - \tilde{q}_j}{\kappa} \text{ for } j \neq i \text{ and } \kappa \equiv \frac{\gamma - c_p c_s}{1 - c_p \mu}. \quad (9)$$

Thus, when observing the vector of quantities, each agent $i$, who also knows his own private signal $\tilde{s}_i$, is able to uniquely recover the full signal vector of private information.

This example illustrates the difference between a trader’s privacy with respect to other auction participants versus an outsider observer (e.g., an auctioneer, a designer, an intermediary). As we will show, it is the former type of privacy that is critical for the incentive properties of a design. The possibility for a bidder to take advantage of the inferred signals of other bidders alters the bidder’s incentives – preserving privacy becomes necessary. Given that the auction outcome contains payoff-relevant information, can a design that enables conditioning on (some statistic of) that outcome when bidding improve efficiency?

### 2.3 Preserving Privacy: A Market Design Approach

To characterize implications of privacy in markets, let us formalize the notion of a design and privacy-preserving. We first define observables and contingent variables, which will be elements of a design.
Definition 1 (Observables). Let $O_i$ denote the variables that are functions of bids submitted in the auction and are observable to trader $i$ during the auction. In a $T$-stage auction, let $O_{i,t-1}$ denote the observables to bidder $i$ in stage $t$. $O_{i,0}$ denotes the initial private information of trader $i$ ($O_{i,0} = \{s_i\}$), $O_{i,T}$ denotes the observables after the last round $T$; and $O_i \equiv \times_t O_{i,t}$ where $t \in \{0,1,\ldots,T\}$.

Observables $O_{i,t-1}$ list the new variables that become available (or inferable) at $t$, with variables in $O_{i,t-1}$ understood to be available at $t$. Observables represent transparency settings and may include any feedback about behavior – such as any function of the realized outcomes (prices, all or some traders’ quantities, trading volume), identities, and any function of the submitted bids – and the timing of disclosure (prior to, during, after bidding). The observables can accommodate mandatory disclosure of bids for some or all traders, or of realized prices or quantities.

Bidders’ strategies can also be expressed in the outcomes to be realized; for example, in a one-stage auction, bid schedules of all bidders are price-contingent orders. The conditioning possibilities determine the bidders’ strategy space. To encode its richness in the conditioning possibilities, it is useful to define contingent variables.

Definition 2 (Contingent Variables). Let $C_i$ denote the variables that are functions of outcomes to be realized in the auction and on the realizations of which trader $i$ can condition his strategies. Let $C_0$ denote the contingent variables for the auctioneer. In a $T$-stage auction, let $C_{i,t}$ denote the contingent variables for $i$ in stage $t$; $C_i \equiv \times_t C_{i,t}$.

We refer to $(O;C)$, $O \equiv \{O_{i,t}\}_{i,t}$ and $C \equiv \{C_{i,t}\}_{i,t}$, as conditioning variables. The strategy space $A_{i,t}$ of bidder $i$ in stage $t$ comprises all functions $f: C_{i,t} \rightarrow \mathbb{R}$; and let $A_i \equiv \times_t A_{i,t}$. Both contingent variables and observables can differ across participants; may include only public observables (i.e., $O_i \equiv O_j$ for all $i, j \in I \cup \{0\}$), or may be common to traders but not the auctioneer. We assume that when an observable variable is informationally equivalent to a contingent variable (as is the case, e.g., with the average signal and price in the equicommonal model), a bidder relies on the contingent variable.

Definition 3 (Outcome Function). Let $g_t$ be a function that maps strategies to prices and quantities in stage $t$, $g_t : \times_i A_{i,t} \rightarrow \mathbb{R}^I \times \mathbb{R}^I$ and let $g_t(a) = (\{q_{i,t}\}_i, p_t)$. The outcome function $g = (g_1, g_2, \ldots, g_T)$ allows for stages in which no allocation occurs, $g_t \equiv 0$, or allocates according to the uniform-price market clearing. Assume that the last round $T$ is an allocative round.

The design represents the choices of a designer.

---

18 With a common for all bidders contingent variable, this corresponds to a babbling equilibrium.

19 For a richer set of contingent variables, we define the generalized uniform price market clearing (Definition 8).
Definition 4 (Design). A design is a tuple

\[ D = \{ O; C, g \}, \]  

where the set of contingent variables \( C_i \) defines the strategy space of bidder \( i \), \( O_i \) is the set of observables of bidder \( i \), and \( g \) is the outcome function that determines quantities and prices at each stage.

Choosing a design corresponds to the joint choice of observables, contingent variables and the outcome function (the timing of market clearing, given the uniform-price mechanism for every round of trade). Together with utility functions (1) and information structure (2), design \( D \), which is a utility free concept, defines an auction.

Our definition of privacy preservation requires that the observables are insufficient for inferring any bidder’s private information.

Definition 5 (Privacy Preservation). An auction with design \( D \) preserves privacy if no bidder \( i \) learns the signal \( s_j \) of some other bidder, \( j \neq i \) from observables \( O_i \) before the final bidding stage, \( t < T \). An auction with design \( D \) strictly preserves privacy if no bidder \( i \) learns information that is not contained in his own signal \( s_i \) from observables \( O_i \) before the final bidding stage, \( t < T \).

Definition 6 (Ex Post Privacy Preservation). An auction with design \( D \) preserves privacy ex post with respect to bidders if no bidder \( i \) learns the signal \( s_j \) of some other bidder, \( j \neq i \). An auction preserves privacy ex post with respect to the outside observer if he does not learn the signal of any bidder \( i \). An auction preserves privacy ex post if it does so with respect to bidders and the outside observer.

In Example 1 privacy with respect to observables is preserved in the sense of Definition 5 in a one-shot design, own signal is the only observable prior to the bidding stage. In Example 4 if the final observables are quantities, then while each market participant can recover all private information, ex post privacy is preserved with respect to the outside observer in the sense of Definition 6. Ex post privacy is not preserved with respect to other bidders – a potential challenge for ex post participation. If the designer chooses the to disclose as final outcomes \( O_T \) to be the price and a bidder’s own quantity, then ex post privacy is preserved and ex post participation is guaranteed.

---

\(^{20}\) If allocations \( g_T \) are all either cheap talk or based on the standard uniform price market clearing, then \( D \) is both payoff-free (well-defined regardless of preferences) as well as, prior-free (well-defined regardless of the information structure). If in some allocative stage, \( q_t \) is determined by bids based on richer than price contingent variables, if these variables are optimally chosen, then this optimal choice is a function on the information structure; thus, \( D \) might be prior-dependent.
While no individual trader’s privacy is compromised in Example 1 at the same time, the mechanism releases information about traders’ values. Hence, the auction with data \( \tilde{q} \) observable to both the participants and an outside observer is not secure in the information theoretic sense. Indeed, information about the signals gets revealed to an outside observer who, knowing vector \( \tilde{q} \), can eliminate any signal vector \( s \) that would have generated a different \( \tilde{q} \) vector. We will show that, in divisible good markets, certain equilibrium implications of preserving privacy are independent of how much information is revealed. We thus adopt a definition of “privacy-preservation” that is not information-theoretic. This also allows us to develop implications of privacy itself, separate from those of “how much privacy” is revealed.21 22

The goal of this paper is to characterize privacy-preserving designs based on the uniform-price mechanism: Maximization of efficiency (both informational and allocative, defined below) subject to incentive constraints (IC) and participation constraints (IR), which depend on \( (O; C) \). The choice variables of the designer specify the variables \( C \) on which bidders can condition their schedules and transparency settings embodied in \( O \), in static and dynamic uniform-price auctions.

We will evaluate efficiency of privacy-preserving designs with respect to the first best allocation, which maximizes total welfare of the traders subject to the market clearing constraint, given the private information of the traders, i.e. the profile of all bidders’ signals, \( s \equiv \{ s_i \}_i \). The first best efficient allocation solves the following optimization problem

\[
\max_{\{q_i\}} \sum_i \left( E(\theta_i|s) q_i - \frac{\mu}{2} q_i^2 \right), \text{ such that } \sum_i q_i = Q_0. \tag{11}
\]

Letting \( e_i \equiv E(\theta_i|s_1, s_2, \ldots, s_I) \) and \( \bar{e} \equiv \frac{1}{I} \sum_i e_i \), the efficient allocation is given by

\[
q_i^* = \frac{Q_0}{I} + \frac{e_i - \bar{e}}{\mu}, \text{ for all } i \in I, \tag{12}
\]

where the conditional expectations vector is, by the projection theorem, \( e = C_\theta (C_\theta + \sigma^2 C_\varepsilon)^{-1} s \); each \( e_i \) is a linear combination of the signals. Adopting the standard definition, we will say that equilibrium is informationally efficient (price is privately revealing) if, for any bidder \( i \), the posterior of \( \theta_i \) satisfies \( F(\theta_i|s_i, p^*) = F(\theta_i|s) \) for every state \( s \), given the equilibrium price \( p^* = p^*(s) \). In Example 1, the one-shot design with uniform price market clearing does not

21 For instance, in the fundamental value model, in the standard double auction (with \( (O_i, C_i) = (s_i, p) \)), price is informationally equivalent to the full signal vector, but conditioning on the price statistic does not allow recovering the vector. Quantifying “how much privacy” is revealed is relevant for problem of data privacy and pricing data (e.g., Ghosh and Roth (2013)).

22 Differential privacy requires privacy for all strategies. Definition 3.1 concerns equilibrium strategies. Indeed, conceptually, privacy loss of an agent is relevant if his report impacts inference of other agents – this is another sense in which, in contrast to differential privacy, the concept of privacy that is relevant in the strategic context studied in this paper is not a statistical one.
implement the efficient allocation \( q_i^* \); the distortion can be due to informational inefficiency (i.e., when equilibrium price does not aggregate the information contained in the signal vector \( s \)) and price impact.

3 Privacy-Preserving Designs

Why should one be concerned about privacy? This paper shows that privacy is relevant to design performance for both incentive- and participation-related reasons. This section contains the main results of the paper; it demonstrates the role of privacy for incentives, characterizes the privacy-preserving designs (given by the choice of observables, contingent variables, static and dynamic allocation rules) and their informational and allocative efficiency properties.

3.1 Necessity of Privacy: Observables and Incentives

In the standard uniform-price auction (i.e., with \((O_i; C_i) = (O_{i,0}; C_{i,1}) = \{s_i\}; \{p\})\), by conditioning on price, bidders can incorporate information about their own values that is contained in others’ signals. With the efficiency objective in mind, suppose that prior to the auction, bidders have an opportunity to indicate their willingness to pay and that a statistic of these reports, e.g. the average report, is made available to all before the actual bids are submitted. In divisible good markets, inference affects bidding, and hence efficiency, in two ways: it affects (1) inference about values and (2) price impact. A design that elicits from bidders information about the signal vector \( s \) beyond that contained in the one-shot auction’s price and makes this information available to all bidders before submitting schedules may potentially improve the informational efficiency of the auction, despite no binding payoff consequences. In addition, availability of information before bidding may lower traders’ price impact – conditioning on price no longer affects bid slopes, only bid intercepts. The liquidity benefit would be available even in markets where the static auction price aggregates all information contained in \( s \). To consider the impact of such richer conditioning possibilities, compared to the standard uniform-price auction, we consider a two-stage design, with a pre-trade bidding stage.

Definition 7 (A Two-Stage Design with Pre-trade Bidding). In the first stage of a two-stage design, each bidder submits a (net) demand schedule \( q_{i,1}(p) \); that is, \( C_{i,1} = \{p\} \), for all \( i \).

Instead of letting the bidders observe the statistics of the pre-trade reports, the designer could reward bidders for making predictions close to the second-stage bids, thus incentivizing the bidders to submit reports close to their true values, as in McLean and Postlewaite (2002). However, in the divisible settings we examine, the signal space and utility space are unbounded; hence, so is the informational size, in the sense of McLean and Postlewaite (2002), unbounded. A large informational size either necessitates large efficiency losses or requires large side payments. A randomized design akin to differential privacy would fail for the same reason; the impact of bidders’ realized signals on the efficient allocation is not bounded. A differentially private allocation mechanism could have an arbitrary large impact on (in)efficiency, at least for some realizations of signals.
Prior to bidding in the second stage, statistic $f_i(\{q_{i,1}\})$ of the submitted bids is announced to all bidders; $O_{i,1} = \{f_i(\{q_{i,1}\})\}$ for all $i$. Then, in the second stage, the uniform-price auction takes place: each bidder $i$ submits a bid function $q_{i,2}(p)$, after he observed the statistic $f_i$, and quantities $\{q^*_i\}_i$ and price is determined by market clearing $\sum_i q_{i,2}(p^*) = Q_0$ and allocations by the bids are $q^*_{i,2} = q_{i,2}(p^*)$ for all $i$.

The first-stage bidding is equivalent to submitting by each bidder a report $r_i$ about his signal $s_i$; the statistic observable before stage two is then one of the submitted reports, $f_i : \mathbb{R}^I \rightarrow \mathbb{R}; \mathcal{O}_i^1 = \{f_i(r)\}$ for all $i$, where $r \equiv \{r_i\}_i$. Given the equivalence, we say that a two-stage design has a truth-telling equilibrium if the bidder’s reports submitted in the first stage are their true signals. Theorem 1 shows that releasing private information in the pre-trade stage creates incentives to misreport the true value and equilibrium fails to exist. We consider linear feedback statistics $f_j(r) = \sum_{k \neq j} \beta_{jk} r_k$. Lemma 1 in the Appendix characterizes equilibrium with linear feedback statistics.

**Theorem 1 (Privacy is Necessary).** Consider a two-stage design with pre-trade bidding with observables $O_{i,1} = \{f_i\}$, contingent variables $C_{i,2} = \{p\}$, for all $i$. A two-stage design with a truth-telling equilibrium exists if, and only if, either

(i) the design strictly preserves privacy, that is, $O_{i,1} = \emptyset$, for all $i$; or

(ii) the feedback statistics $\{f_i\}_i$ are such that the market-clearing price is not affected at the margin by a misreport at the truth-telling profile: $\frac{\partial p^*(s_{-i})}{\partial r_i} = 0$ for all $i$. Here, truth-telling is weak best reply only.

Intuitively, if price were affected by a (mis)report, then a bidder could benefit from manipulating his report to affect the bids submitted by others through their beliefs. The incentives to manipulate are present for any statistic of reports from the pre-trade stage that does not strictly preserve the bidders’ privacy. Thus privacy-preservation is necessary in the strict sense unless price is unaffected by misreports (case (ii)). The condition that the price is unaffected by a misreport of any bidder is equivalent to

$$\sum_{j \neq i} \frac{c_{fj}}{\lambda_j + \mu_j} \beta_{ji} = 0 \text{ for all } i.$$  

In case (ii), for any report, the marginal effect of a misreport in a bidder’s first order condition is 0; bidders are indifferent between reporting their true signals and misreporting. In addition, the condition required for truth-telling is a joint restriction on the information structure $\mathcal{IS}$ and the observables $\{f_i\}_i \in \mathcal{L}$ in the design. To specify the feedback statistics, the designer must know the details of $\mathcal{IS}$. Moreover, the designer must know the $\mathcal{IS}$ exactly – a given profile of feedback statistics that admits truth-telling is not robust to small changes in the information structure.
Example 2 illustrates Theorem 1. We consider a design with a simple feedback statistic: all reports from the pre-trade stage are observable to all bidders. We first show that unless price is unaffected by misreports, then bidders are always strictly better off by misreporting. We then show the possibility of a weak truthtelling equilibrium for certain information structures. In the context of the example, we give a necessary and sufficient condition on the information structures for which price remains unaffected by a misreport of any bidder.

Example 2 (All Pre-trade Bids are Observable). Consider the two-stage design in which all submitted bids from the first stage are observable to all bidders before the second stage. Let $r_i$ denote the report (possibly a misreport) of $i$ in the first stage. We show that if values are interdependent, then there exists no such equilibrium where reports in the first stage are $r_i = s_i$ for all $i$. Assume, that there exists a truthtelling equilibrium. Then, bidders are able to recover the full signal vector $s = (s_1, s_2, \ldots, s_I)$ from the first stage. By first order condition, the optimal bids in the second stage are

$$q_j(p) = \left(\frac{E(\theta_j|s_1, s_2, \ldots, s_I)|_{s_i=r_i}}{\lambda + \mu}\right) - p, \text{ for all } j \neq i \quad (13)$$

and the best reply of bidder $i$ is

$$q_i(p) = \left(\frac{E(\theta_i|s_1, s_2, \ldots, s_I)}{\lambda + \mu}\right) - p. \quad (14)$$

Then by market clearing, the price is

$$p = \frac{E(\theta_i|s) + \sum_{j \neq i} E(\theta_j|s_{-i}, r_i)}{I}. \quad (15)$$

By the projection theorem, $E(\theta_i|s_1, s_2, \ldots, s_I)$ is given by a linear function of the signals, the vector $E(\theta|s) = Ds$ with $D = C_\theta (C_\theta + \sigma^2 I)^{-1}$, from which price is

$$p = d_i^T s + \sum_{j \neq i} \left(d_i^T s - d_{ij} (s_i - r_i)\right) = \frac{1}{I} d_i^T D s - \sum_{j \neq i} d_{ij} (s_i - r_i), \quad (16)$$

where $d_i$ denotes the $i$th column of $D$.

From the ex-post utility, $u_i = \theta_i q_i - \frac{\mu}{2} q_i^2 - p q_i$, the interim utility of $i$ is

$$E(u_i|s_i) = E\left((\theta_i - p) \left(\frac{E(\theta_i|s) - p}{\lambda + \mu}\right) - \frac{\mu}{2} \left(\frac{E(\theta_i|s) - p}{\lambda + \mu}\right)^2 \big| s_i\right), \quad (17)$$

from which the first order condition (FOC) of the first stage is

$$0 = \frac{\partial E(u_i|s_i)}{\partial r_i} = E\left(-\frac{\theta_i}{\mu + \lambda} - \frac{E(\theta_i|s)}{\mu + \lambda} + \frac{2p}{\mu + \lambda} + \frac{\mu}{\mu + \lambda} \left(\frac{E(\theta_i|s) - p}{\mu + \lambda}\right)\right) \frac{\partial p}{\partial r_i}|_{s_i}. \quad (18)$$
Price impacts satisfy the fixed point condition \( \lambda = \frac{\lambda + \mu}{1-I} \), from which \( \lambda = \frac{\mu}{1-I} \).

Consider equation 18.

(i) If there is a bidder \( i \) such that \( \frac{\partial p}{\partial r_i} \neq 0 \) then, the second order condition for optimality requires that

\[
0 > \frac{\partial^2 E(u_i|s_i)}{\partial^2 r_i} = \left( \frac{\partial p}{\partial r_i} \right)^2 \frac{\lambda + 2\mu}{\mu + \lambda} = \left( \frac{\partial p}{\partial r_i} \right)^2 \frac{2I - 3}{I - 1},
\]

which does not hold for any market size, the extremal point is a minimizer. The convexity of the expected utility implies that bidder \( i \) always has an incentive to manipulate his first stage report to infinity so as to drive up both the price and other bidders’ demand for in the second stage, he can submit his final bid so as to become a seller and realize large revenues over small marginally diminishing costs.

(ii) On the other hand, there is a possibility that \( \frac{\partial p}{\partial r_i} = 0 \) for all \( i \), which ensures that all bidders are indifferent between truthtelling or submitting other reports, given that other bidders report their true signals. Thus truthtelling is part of an equilibrium in which telling a truth is a best reply although only a weak best reply. When is it possible that \( \frac{\partial p}{\partial r_i} = 0 \) for all \( i \)? The price is unaffected by \( i \)'s marginal misreport at the truthtelling profile, \( \frac{\partial p}{\partial r_i} = 0 \), if and only if \( \sum_{j \neq i} d_{ij} = 0 \), so by Equation 16. As \( D \) is a deterministic function of the information structure, this gives a necessary and sufficient condition on the prior, which if holds then price is marginally unaffected by misreports at the truthtelling profile.

Let us give an example which satisfies the equation system. Consider 4 bidders, \( \sigma^2 = 0.3267 \) and the following correlation matrix with respect to values:

\[
C_\theta = \begin{bmatrix}
1.0000 & 0.6337 & -0.8515 & -0.4554 \\
0.6337 & 1.0000 & -0.4554 & -0.8515 \\
-0.8515 & -0.4554 & 1.0000 & 0.6337 \\
-0.4554 & -0.8515 & 0.6337 & 1.0000
\end{bmatrix}.
\] (19)

This value correlation structure generates \( D \), defined by projection theorem as \( D = C_\theta (C_\theta + \sigma^2 E)^{-1} \), such that

\[
D = \begin{bmatrix}
0.5000 & 0.2000 & -0.3000 & 0.1000 \\
0.2000 & 0.5000 & 0.1000 & -0.3000 \\
-0.3000 & 0.1000 & 0.5000 & 0.2000 \\
0.1000 & -0.3000 & 0.2000 & 0.5000
\end{bmatrix},
\] (20)

which satisfies the condition and price is unaffected by the misreport of any bidder.

Beyond this example, it is clear that the sufficient and necessary condition for unaffected price holds only for some special information structures. For example, if \( C_\theta \) exhibits funda-
mental values (all pairwise correlations are the same), then by the relationship between \( C \) and \( D \), i.e. by \( D = \left( E + \sigma^2 C_g^{-1} \right)^{-1} \), \( D \)'s entries are positive. Thus, \( \sum_{j \neq i} d_j = 0 \) can not hold for information structures with fundamental values.

In light of Theorem 1, information generically cannot be conveyed by allowing bidders to observe a feedback about each others’ signals, before market clearing without leading to instability. Truth-telling strong equilibrium does not exist for any feedback rule; no indicative bids or cheap talk reports may enhance informativeness if observable. Moreover, the necessity of privacy preservation extends to feedbacks in designs with multiple non-allocative stages. For practical market design, it is valuable to identify the stages of markets where cryptography shall necessarily be used; even with the existence of certain cryptographic implementations, exploitations of them are known to be costly. Our results suggest that submitted bids shall be kept secure and confidential up until the point at which market clearing is executed.

3.2 Privacy-Preserving Designs: Contingent Variables

In light of the necessity for privacy with respect to observables, let us consider how an expanded set of contingent variables, \( C \), richer than just the price, change possibilities in one-stage auctions. The standard double auction allows bidders to condition on price, suppose that bidders can condition on other, potentially more informative variables; for instance, quantities to be allocated in the auction to bidders or statistics of other bidders’ submitted bids. For which such designs for what information structures of the primitive values of the bidders can bidding admit equilibrium? For which such privacy-preserving designs can equilibrium be more efficient informationally?

First, let us consider market clearing for a bid space that is richer than the standard bid space with price dependent orders in that bids can be expressed in more variables than just the to-be-realized price. We define a generalization of the uniform price market clearing for such enriched bid schedules.

**Definition 8 (Generalized Uniform-Price Market Clearing).** In a static generalized uniform-price market clearing with contingent variables \( \{ C_i \}_{i} \), where \( C_{i,1} = (p, c_{-p,i}) \) for all \( i \), each bidder submits a bid function \( q_i(C_{i,1}) \). Then, the vector \( \tilde{c}_{-p} \) is determined by some transformation of the submitted bids, \( \tilde{c}_{-p} = T(\{ q_i \}_{i \in I}) \), and \( p^* \) is then determined as a fix point of the market clearing equation \( \sum_i q_i(p, \tilde{c}_{-p,i}) = 0 \). Based on \( p^* \), the submitted bid functions give quantities \( q_i^* := q_i(p^*, \tilde{c}_{-p,i}) \) for all \( i \).

A natural example for such a generalized market clearing is the one that allows for bid schedules that express demand in terms of price and intercepts of other bidders´ schedules. Such a one-shot design trivially preserves privacy.

---

24 If there is no such a price that solves the equation or there are multiple solutions, then we assume that no trade takes place.
Example 3 (Market Clearing for Bids with others’ Intercepts and Price). Let \( a_i \) represent the constant part of \( i \)'s bid function. Bidders are asked to submit bids of the form \( q_i(a_{-i}, p) = \alpha_i + \sum_{j \neq i} \beta_{ij} a_j - \gamma_i p \). The market is cleared by, first, setting \( \tilde{a}_i := \alpha_i \) for all \( i \), second, substituting these values into the bid functions to derive the price-dependent bids \( q_i(p) = \alpha_i + \sum_{j \neq i} \beta_{ij} \tilde{a}_j - \gamma_i p \), third, applying the standard uniform price market clearing to find \( p^* \) as a solution to \( \sum_{i \in I} q_i(p) = Q_0 \) and then quantities as \( q_i^* := q_i(\tilde{a}_{-i}, p^*) \).

To illustrate market clearing for intercept-dependent bids, consider \( Q_0 = 0 \) and two bidders. If bidder 1 submits the bid function \( q_1 = 8 + 2a_2 - 2p \) and bidder 2 submits \( q_2 = 5 - a_1 - 3p \), then first, by reading off the intercepts \( a_1 = 8 \) and \( a_2 = 5 \). Second, substituting these into the bids, the price-dependent orders are \( q_1(p) = 18 - 2p \) and \( q_2(p) = -3 - 3p \), from which the aggregate demand is \( 15 - 5p \) and, by the market clearing condition \( 15 - 5p = 0 \), thus \( p^* = 3 \) and \( q_1^* = q_2^* = 12 \).

Example 4 (Market Clearing for Bids with Average Intercept and Price). Bidders are asked to submit bids of the form \( q_i(\tilde{a}, p) \), where \( \tilde{a} \) represents the average bid intercept to-be-submitted. Then first, the market maker solves for the average intercept, second, plugs the calculated \( \tilde{a} \) into the submitted bids and third, applies uniform price market clearing so as to find \( p^* \) such that it solves \( \sum_{i \in I} q_i(\tilde{a}, p^*) = Q_0 \) and then quantities as \( q_i^* := q_i(\tilde{a}, p^*) \).

To illustrate market clearing for bids that depend on the average intercept, consider \( Q_0 = 0 \) and two bidders. If bidder 1 submits the bid \( q_1 = 8 + 2\tilde{a} - 2p \) and bidder 2 submits \( q_2 = 4 - \tilde{a} - 3p \), then in the first step the market maker computes the average intercept \( \tilde{a} = \frac{4 + 8}{2} = 6 \), second, he plugs the calculated \( \tilde{a} \) into the submitted bids to get \( q_1 = 20 - 2p \) and \( q_2 = -2 - 3p \) and third, applies uniform price market clearing so as to find the market clearing price \( p^* = 3.6 \) and the corresponding quantities \( q_1^* = -q_2^* = 12.8 \).

Our designs with enriched contingent variables are reminiscent to the designs considered in Dasgupta and Maskin (2000) for efficiency in unit-demand auctions. Dasgupta and Maskin (2000) shows that efficient allocation is possible even in interdependent value cases, by asking bidders to submit bids that are functions of other bidders bids. Theorem 2 is the counterpart to this result for divisible good auctions with uniform price. Similarly to our design with intercept-dependent demand as in Example 3, the bids in Dasgupta and Maskin (2000) become more and more complicated with market size. The required dimensionality of the submitted bids is linear in the number of bidders in both cases. Yet, the unit-demand framework does not capture the allocative effect that in our setting is clearly captured by price-impact. In Dasgupta and Maskin (2000), informational efficiency is equivalent to welfare efficiency, while in our setting with divisible goods one can identify when it is the case that more informativeness is accompanied by increased welfare and what are the information structures for which informativeness and market power are in conflict and the tradeoff is such that market power, which is due to the competition of finitely many bidders, outweighs improved informativeness.
Theorem 2 (Privacy-Preserving Design via Enriched Conditionals). There exists a generalized one-stage uniform price auction such that (1) privacy is preserved (2) an equilibrium exists which is informationally efficient, regardless of the particular information structure $I S$.

Proof. The proof is constructive and informational efficiency is shown for the design with Bids that are Contingent on others’ Intercepts as in Example 3. Let us look for equilibrium in linear strategies such that $q_i = \alpha_i s_i + \sum_{j \neq i} t_{ij} a_j - \beta_i p$ for all $i$. Assume that such an equilibrium exists. Then, from the submitted orders, the intercepts are

$$\tilde{a}_i = \alpha_i s_i,$$

for all $i$, plugging them into the submitted orders gives $q_i = \alpha_i s_i + \sum_{j \neq i} t_{ij} \alpha_j s_j - \beta_i p$ for all $i$ and the market clearing price is $p^* = \frac{\sum_{i \in I} \left( \alpha_i s_i + \sum_{j \neq i} t_{ij} \alpha_j s_j \right)}{\sum_{i \in I} \beta_i} = \frac{\sum_{i \in I} \left( \sum_{j \neq i} \epsilon_i \right) \alpha_i s_i}{\sum_{i \in I} \beta_i}$. Although in equilibrium price is informative, the vector $\tilde{a}_i$ conveys all information that is present in the environment, therefore price is ignored for inference. The first order condition of the bidders is

$$E(\theta_i|s_i, \tilde{a}_i (s), p^*(s)) - \mu q_i - \lambda_i q_i - p = 0,$$

which implies that

$$E(\theta_i|s_i, \{\alpha_j s_j\}_{j \neq i}) - \mu q_i - \lambda_i q_i - p = 0.$$

By the projection theorem $E(\theta_i|s_i, \{c_{s_j} s_j\}_{j \neq i}) = d_i^T s$ for all $s$ and for all $i$, where $d_i$ is the $i$th column of $D = \left( I + \sigma^2 C_\theta^{-1} \right)^{-1}$. Thus in equilibrium, the bid coefficients must be such that $\alpha_i = \frac{d_i}{\mu + \lambda}$ and $t_{ij} \alpha_j = \frac{d_{ij}}{\mu + \lambda}$ for all $i$, from which $t_{ij} = \frac{d_{ij}}{d_j}$. With notation $\gamma := \frac{1 - 2}{1 - 1}$, the first order condition and the fix point condition for price impacts\(^\text{25}\) give the equilibrium bid functions such that

$$q_i(p) = \gamma \frac{d_i}{\mu} s_i + \sum_{j \neq i} \frac{d_{ij}}{d_j} a_j - \gamma \frac{p}{\mu}$$

for all $i$.

From the bid functions, the equilibrium allocation as a function of signals is

$$q_i(\tilde{a}_{-i}, p^*) = \frac{\gamma}{\mu} \left( d_i s_i + \sum_{j \neq i} d_{ij} s_j \right) - \frac{\gamma}{\mu} \frac{\sum_{i \in I} \left( d_{ii} s_i + \sum_{j \neq i} d_{ij} s_j \right)}{I}.$$

Observe that the latter expression shows that informativeness is perfect. In fact, $q_i(\tilde{a}_{-i}, p^*) = \left( \mu + \gamma \right)^{-1} \sum_{j \neq i} \left( \gamma \lambda_j - \gamma \lambda_i \right) s_j$ for all $i$, which implies that $\lambda_i = \lambda = \mu (I - 2)^{-1}$ for all $i$.\(^\text{25}\)

\(^{25}\)The fix point condition for price impacts is $\lambda_i^{-1} = \sum_{j \neq i} (\lambda_j + \mu)^{-1}$ for all $i$, which implies that $\lambda_i = \lambda = \mu (I - 2)^{-1}$ for all $i$.\(^\text{25}\)
Thus the design with intercept-dependent bidding improves learning on the market thereby improves informational efficiency, yet does not provide solution for the inefficiency that stems from market competition. Moreover, depending on the information structure there might be a tradeoff between the improved informativeness and the changed competitive effect – i.e. for example changing the effective price impact from $\frac{\gamma - cp}{1 - cp}$ as in the uniform price static equicommonal auction to $\gamma$ here might outweigh improved informativeness and result in overall lower efficiency. Clearly, this tradeoff might only hold for the small market and disappears as the market gets large, $\gamma \to 1$, or when dynamic designs are possible and the allocative inefficiency can be traded away in multiple rounds. Especially in the latter case, it is compelling to first focus on improvements regarding informational efficiency and then correct the remaining allocative inefficiency by multiple subsequent rounds during which further learning does not take place.

**Theorem 3 (Privacy-Preserving Dynamic Design).** There exists a generalized multi-stage uniform price auction such that (1) privacy is preserved (2) an equilibrium exists which is efficient, regardless of the particular information structure $IS$.

*Proof.* Consider the dynamic design such that the first stage is as in Example 3 and each subsequent stage is a retrade stage that allows for trading away the competition effect that arises from market power on the small market with finitely many traders. Informational efficiency is a consequence of Theorem 2, thus efficiency follows in the limit.

It turns out that the class of designs which involves bid spaces based on intercept-contingent demand and weighted versions of intercept-contingent bidding constitute a base in the class of designs with generalized market clearing rules, in that, if a generalized market clearing rule achieves certain informational efficiency for given information structure, then there exists a weighted intercept-contingent bid space and the corresponding generalized market clearing rule that guarantee the same informativeness. Note that perfect informational efficiency, requires full dimensionality of the bid schedules, in that the submitted bids in the privacy-preserving design with intercept-dependent bidding, see in Example 3 as used in the Proof of Theorem 2, must be a function from $\mathbb{R}^{I+1}$ to $\mathbb{R}$, which might be overly complicated even for moderate market sizes. The required bid complexity is proportional to the number of traders, thus larger markets require more complex bidding. What are the possibilities of enhancing informational and allocative efficiency when complexity of bid schedules is restricted?

Privacy-Preserving Designs with Constrained Bid Complexity can be informationally efficient for given information structure $IS$. For example, if the bid space is constrained to...
bid functions that are at most 2-dimensional, \( q_i(a_i, p) \), then for each bidder one can find the right linear combination of other bidders’ intercepts so that in equilibrium full informational efficiency is achieved. Note that such a design would be a design that is no longer prior-free, in that, it depends on the particular correlation matrix of the information structure \( IS \) whereas the design with full bid complexity in Example 3 is well defined and guarantees informational efficiency for any information structure.

4 Privacy as a Participation Constraint

It is common practice to make the auction outcomes \((q, p)\) available to all bidders after the auction is conducted. Our results are consistent with this practice, the classic double auction corresponding (with price as the contingent variable) to a restriction of the strategy space to one-dimensional bid schedules \( R \to R \); that is, the contingent variables do not include the quantity vector along with the price. Even though the outcomes of the auction become available to bidders after market clearing occurs, the strategies do not allow to condition on the (quantity) outcomes, thus making the classic auction design immune to manipulation.

Transparency rules in markets have received increased attention after the crisis. The question is what should traders in markets be allowed to observe before \((O_0)\), during \((O_t, t = 1, ..., T - 1)\) and after \((O_T)\) the auction about the terms of trade, the allocations or the orders placed in the market they participate and in other markets from the same asset. Our results about privacy and incentives suggest that transparency before trading should be limited. On the other hand, post-trade transparency (obligation to disclose trades already executed or their terms of trade) is consistent with incentives and participation, provided the design allows exhausting gains to trade among the participants – essentially, a design based on repeated trading in dark pools, identified by Theorem 3 on dynamic trading designs. Indeed, concerns about front running are the primary reason for choosing to trade in dark pools. Post-trade transparency settings that preclude disclosure of the auctions’ outcomes or impartial intermediation can serve as solutions to potential privacy loss.

---

26 Note that publicly announcing the outcome of a dynamic auction after the last round is consistent with the traders’ concern about front running, which applies given the gains to trade – in the model, for a given realization of \( \{s_i\}_i \), that is, within our dynamic auction, where the gains to trade are determined by the realization of \( \{s_i\}_i \) prior to round one.

27 Note that publicly announcing the outcome of a dynamic auction after the last round is consistent with the traders’ concern about front running, which applies given the gains to trade – in the model, for a given realization of \( \{s_i\}_i \), that is, within our dynamic auction, where the gains to trade are determined by the realization of \( \{s_i\}_i \) prior to round one.

28 Disclosure of outcomes may affect not only ex ante but also ex post participation decisions. Cryptographic tools, and especially multiparty computation, which facilitate secure feedback and verification of the execution, are one solution markets have developed to address the protocol completion issue – the incentive to revise the submitted bids by the bidders upon learning the outcome of the auction which can be seen in Example 1; here, protocol completion can be addressed with price transparency without allocation transparency, or bid...
The idea that privacy may challenge participation motivates the study of privacy in most of the literature. Our analysis so far suggests that even if privacy concerns are not binding for the (ex ante or ex post) participation constraints\textsuperscript{29} privacy preservation with respect to auction participants is, in fact, necessary for both incentive compatibility and viability of an auction. Additionally, the remarks on the interaction between privacy and participation in this section are based on the utility-based rather than intrinsic value of privacy.

5 Privacy in Practice

We report how privacy affects trading arrangements in many markets, including financial markets, electricity markets, and exchange of agricultural contracts.\textsuperscript{30}

Financial markets. Arguments pro transparency or privacy have been widely discussed in financial markets context. Cases of front running and penny jumping have been investigated by the SEC and other regulatory bodies of trading agencies. Thorpe and Parkes (2007) and Thorpe and Parkes (2009) propose cryptographic methods for securities exchanges that allow for a variety of settings of transparency versus privacy.

The exchange of baskets of securities is an example where the problem of privacy is particularly important for large institutional traders. These traders often intend to exchange or liquidate fully a baskets that contains many different securities. Finding a matching order for the entire basket is time-costly and the information contained in the particular assembly of the basket exposes a trader to the risk of price impact before the actual trade takes place. Thorpe and Parkes (2009) introduce cryptographic tools that can be used by the designer set the desired levels of privacy versus transparency.\textsuperscript{31}

Privacy concerns related to ex post participation are also common in financial markets. Thorpe and Parkes (2009) discuss protocol completion incentive problems in the exchange of baskets of securities. By the time the institutional trader who placed the basket on the market gets an offer, he might no longer be willing to execute the trade, as the offer itself represents new information which might as well change the trade preferences of the owner of the basket.

Electricity markets. Application of cryptographic tools in electricity markets is fairly new. Transparency. Cryptography is what enabled privacy with respect to the outside observer. Facilitating secure feedback and verification of the promised execution brings a possibility of a variety of transparency settings, which was not considered in the standard mechanism design setting.

\textsuperscript{29} As is presumably the case in settings with the practice of announcing the outcomes \((q,p)\) after the auction.

\textsuperscript{30} Bonneau and Preibusch (2010) provide an overview of privacy practices and policies in online social networks.

\textsuperscript{31} Thorpe and Parkes (2009) emphasize that their cryptographic solution allows for publishing the changes in risk measures of liquidity providers, instead of properties of the baskets directly. As additional possibilities, the designer could choose to reveal information about portfolio value and dividends (long and short sides of the portfolio, the skew) or portfolio composition statistics only (market sector, market capitalization, index membership, dividend per share price, average daily trading volume, historical price volatility).
The software company Partisia provides cryptographic solutions for electricity procurements and collects bids that might come at different time points without disseminating any information about the encrypted bids before the auction is executed. One of the electricity procurement applications of Partisia aims to encourage participation of a segment of the electricity market that traditionally does not switch providers often. Further, in the applied auction system, a buyer can reject or accept the best price offer that he gets from the auction system. This also points to *ex post* participation, which is better resolved here by ensuring privacy and allowing for rejections.

Another practical example of where privacy affected design in electricity markets is the Nordic Electricity Exchange. Participants are traders, dealers, producers, consumers. The exchange features futures markets as well (for day-ahead and intraday trading). Bidding is anonymous, hinting at privacy issues, and clearing house is compulsory, hinting at protocol completion / *ex-post* participation issues otherwise. Indeed, Nordpoolspot states guaranteeing settlement and delivery as one of its core functions. Concerning transparency, Nordpoolspot emphasizes the importance of price transparency besides anonymity.

**Agricultural markets.** The exchange of beet farming contracts in Denmark provides a famous example of how privacy impacted design. This exchange is the first where cryptographic tools (secure multiparty computing) were implemented not to compromise bidders’ private information and encourage participation. In the exchange of beet farming contracts, farmers were concerned about their private information being revealed to the monopolist Danisco. In particular, the farmers expressed concerns that their bid information could be exploited in the future when decision will be made about new quota allocations or delivery conditions. The cryptographic solution – via an intermediary – that was implemented clearly encouraged participation and resulted in more contract trade than voluntary bilateral trades facilitated previously.

**References**


32 “Bids clearly reveal information, e.g., on a farmer’s economic position and their productivity, and therefore farmers would be reluctant to accept Danisco acting as auctioneer, given its position in the market. Even if Danisco would never misuse its knowledge of the bids in the ongoing renegotiation of the contracts (including the pricing scheme), the mere fear of this happening could affect the way farmers bid and lead to a suboptimal result of the auction.” (Bogetoft et al. (2009)).


Appendix A: Proofs

Proof of Theorem 1. There are two stages in the market; the communication stage in which each trader \( i \in I \) reports his signal \( r_i \) to the market designer who announces to \( i \) message \( g(r) \), which is calculated from the report vector \( r \) (\( g(\cdot) \) can be a vector-valued function); and
the trading stage in which trader $i$ submits a bidding function $q_i(\cdot)$ conditional on $(O_i \cup C_i) = (s_i, g(r); p)$, and the market clears.

In order to find the necessary and sufficient condition for the existence of a truth-telling equilibrium, in which all agents choose to report the true signal ($r_i = s_i$ for all $i \in I$), we will first characterize the choice of agent $i$ at the communication stage, assuming that all other traders $j \neq i$ report truthfully $r_j = s_j$. Also, all traders $j \neq i$ believe that $r_j = s_j$ for all $j \in I$, as in the truth-telling equilibrium.

In the Gaussian setting where $g(r)$ is a linear function of $r_i$ and $(r_j = s_j)_{j \neq i}$, equilibrium bidding function of each bidder $j \neq i$ can be characterized as

$$q_j(p) = \frac{1}{\mu_j + \lambda_j} (c_{sj}s_j + c_{gj} \cdot g(r_i, s_{-i}) - (1 - c_{pj})p + c_{gj}\theta) \equiv A_j(s_{-i}) + B_jp + C_jr_i, \forall j \neq i,$$

where $(\lambda_j, c_{sj}, c_{gj}, c_{pj})_{j \in I}$, and then $(B_j, C_j)_{j \in I}$, are constants independent of $r_i$ or $s_i$. Report $r_i$ of agent $i$ parallelly shifts the bidding functions of others, with coefficient $C_j = c_{gj} \cdot (\partial g/\partial r_i)$. On the other hand, the bidding function of agent $i$ is calculated based on the true value of $s_i$, since $i$ knows his own private signal $s_i$ and report $r_i$, and can recover the true value of $g(s)$ from the observed message $g(r_i, s_{-i})$.

$$q_i(p) = \frac{1}{\mu_i + \lambda_i} (c_{si}s_i + c_{gi} \cdot g(s) - (1 - c_{pi})p + c_{gi}\theta) \equiv A_i(s_{-i}) + B_ip + C_is_i. \quad (22)$$

Furthermore, the equilibrium price is characterized by

$$p^* = \left(\sum_{j \in I} \frac{1 - c_{pj}}{\mu_j + \lambda_j}\right)^{-1} \left(\sum_{j \in I} \frac{1}{\mu_j + \lambda_j} (c_{sj}s_j + c_{gj} \cdot g(s) + c_{gj}\theta) + \sum_{j \neq i} \frac{c_{gj}}{\mu_j + \lambda_j} \cdot (\partial g/\partial r_i)\right)$$

$$\equiv D^*(s_{-i}) + E^*r_i + F^*s_i. \quad (24)$$

That is, the bid functions of $j \neq i$ and the equilibrium price are linear functions of $r_i$ with constant coefficients, given the Gaussian information structure and the linearity of messages. In particular, $E^* = \partial p^*/\partial r_i = \left(\sum_{j \in I} \frac{1 - c_{pj}}{\mu_j + \lambda_j}\right)^{-1} \left(\sum_{j \neq i} \frac{c_{gj}}{\mu_j + \lambda_j} \cdot \partial g/\partial r_i\right)$ is a constant as long as $g(\cdot)$ is linear. The interim utility of bidder $i$ in the beginning of the communication stage is

$$E[U_i|s_i; r_i] = E[\theta_iq_i(p^*) - \frac{\mu_i}{2}q_i^2(p^*) - p^*q_i(p^*)|s_i; r_i]. \quad (25)$$

The first order condition with respect to $r_i$ is

$$0 = E[(\theta_i - p^*) \frac{\partial q_i(p^*)}{\partial r_i} - \mu_i q_i(p^*) \frac{\partial q_i(p^*)}{\partial r_i} - q_i(p^*) \frac{\partial p^*}{\partial r_i}] | s_i; r_i$$

$$= - \left(\frac{\lambda_i(1 - c_{pi})}{\mu_i + \lambda_i} + 1\right) E[q_i(p^*)|s_i; r_i] \frac{\partial p^*}{\partial r_i}. \quad (27)$$
and the second order condition with respect to \( r \) is
\[
-2 \frac{\partial^2 p^*}{\partial r^2} \frac{\partial q_i(p^*)}{\partial r_i} = \frac{\mu_i}{\mu_i + \lambda_i} \left( 1 - c_{gi} \right) \left( 1 + c_{gi} \right) \mu_i + 2 \lambda_i \left( \frac{\partial p^*}{\partial r_i} \right)^2 \geq 0.
\]

**Proof.** Assume that the information structure is one of independent private values \((C = \text{Id})\) or \( g \) is not more informative than \((s_i, p)\). Lemma 1 implies that \( c_{gi} = 0 \) for all \( i \in I \). Then,
\[
\frac{\partial p^*}{\partial r_i} = \left( \sum_{j \in I} \frac{1 - c_{pj}}{\mu_j + \lambda_j} \frac{\partial q_j(p^*)}{\partial r_j} \right)^{-1} \left( \sum_{j \neq i} \frac{c_{pj}}{\mu_j + \lambda_j} \frac{\partial q_j(p^*)}{\partial r_j} \right) = 0
\]
and, hence, the first order condition is satisfied for any \( r_i \in \mathbb{R} \). Bidder \( i \) is indifferent to report truthfully \( r_i = s_i \).

**Only If** Assume the message \( g \) is more informative than \((s_i, p)\) and values are not independent private. Then, by Lemma 1 there exists \( j \in I \) such that \( c_{gj} \neq 0 \). It follows that there exists a bidder \( i \in I \) such that \( \frac{\partial p^*}{\partial r_i} \neq 0 \). The second order condition for such bidder \( i \) is strictly positive, and the optimal choice of report is \( r_i = \infty \); that is, he does not report truthfully.

Therefore, the truth-telling equilibrium exists, if and only if, the information structure is one of independent private values or the message \( g \) is not more informative than \((s_i, p)\). \(\square\)

**Lemma 1.** \( c_{gi} = 0 \) for all \( i \in I \) if, and only if, the information structure is one of independent private values \((C = \text{Cov}(\theta_i; i \in I) = \text{Id})\) or that the message is not more informative than \((s_i, p)\) \( (g = \kappa p \text{ for a constant } \kappa \in \mathbb{R}) \).

**Proof.** Assume that in equilibrium \( p^* = \sum_{j \in I} \alpha_j s_j \) and \( g = \sum_{j \in I} \beta_j s_j \) for some constants \( \alpha = (\alpha_j)_{j \in I}, \beta = (\beta_j)_{j \in I} \). From the projection theorem,
\[
0 = c_{gi} \quad (29)
\]
\[
0 = \begin{bmatrix}
\text{Cov}(s_i, \theta_i)(\text{Cov}(g, p^*)\text{Cov}(s_i, p^*) - \text{Cov}(s_i, g)\text{Var}(p^*)) \\
+ \text{Cov}(g, \theta_i)(\text{Var}(s_i)\text{Var}(p^*) - \text{Cov}(s_i, p^*)^2) \\
+ \text{Cov}(p^*, \theta_i)(\text{Cov}(s_i, p^*)\text{Cov}(s_i, g) - \text{Cov}(p^*, s_i)\text{Var}(s_i))
\end{bmatrix} \quad (30)
\]
\[
0 = \left[ (\alpha \gamma + \alpha \sigma^2) \{ (\alpha_i - \alpha \gamma \gamma_i) \beta - (\beta_i - \beta \gamma \gamma_i) \alpha \} + (\alpha \gamma \gamma_i + \alpha \sigma^2) (\beta_i - \beta \gamma \gamma_i) \right] \\
0 = \text{Cov}(p^*, \alpha_i - \alpha \gamma \gamma_i)(g - \beta_i s_i) - (\beta_i - \beta \gamma \gamma_i)(p^* - \alpha_i s_i) \quad (32)
\]
The above equation holds for all \( i \in I \). To consider the whole system of equations, we can rewrite the second term in the above covariance operator as follows;
\[
((\alpha_i - \alpha \gamma \gamma_i)(g - \beta_i s_i) - (\beta_i - \beta \gamma \gamma_i)(p^* - \alpha_i s_i))_{i \in I} = (\alpha - C \alpha)m - (\beta - C \beta)p + ((\alpha \gamma \gamma_i(\alpha_i - \beta \gamma \gamma_i))_{i \in I} = ((\text{Id} - C)(\alpha \beta i - \beta \alpha i) + \text{diag}((\text{Id} - C)\alpha_i(\alpha_i - \beta_i))s_i_{i \in I} \quad (33)
\]
\[
= [(\text{Id} - C)(\alpha \beta i - \beta \alpha i) + \text{diag}((\text{Id} - C)\alpha_i(\alpha_i - \beta_i))] (\text{Id} + \sigma^2 \text{Id}) \alpha.
\]
Hence, the necessary and sufficient condition for \( c_{gi} = 0 \) for all \( i \in I \) is
\[
0 = [(\text{Id} - C)(\alpha \beta i - \beta \alpha i) + \text{diag}((\text{Id} - C)\alpha_i(\alpha_i - \beta_i))] (C + \sigma^2 \text{Id}) \alpha.
\]

27
There are two possible cases that satisfy the above equation: (1) \( C = Id \), so that the information structure is one of independent private values. (2) \( \alpha \beta i = \beta \alpha i \), that is \( \alpha_i \beta_j = \alpha_j \beta_i \) for any \( i, j \in I \). Hence, \( \beta = \frac{\beta_i}{\alpha_i} \alpha \equiv \kappa \alpha \) for a constant \( \kappa \in \mathbb{R} \), which means that the message \( g \) is informationally equivalent to the equilibrium price \( p^* \).

Appendix B: Derivation of Equilibrium

GAUSSIAN INFORMATION STRUCTURE

Derivation of linear equilibrium in the general model:

In the symmetric linear equilibrium, bids have functional form \( q_i(p) = \alpha_0 + \alpha_s s_i + \alpha_p p \), where constants \( \alpha_0, \alpha_s, \) and \( \alpha_p \) are the same across all traders. The (net) demand functions of bidders \( j \neq i \) define the residual supply for bidder \( i \) with a slope \( \lambda_i \) and a stochastic intercept which is a function of other bidders’ signals \( \{s_j\}_{j \neq i} \). The slope \( \lambda_i \) is \( i \)'s price impact, which measures a price increase resulting from a marginal increase in the quantity demanded by \( i \).

The best response of trader \( i \) to the residual supply is given by the first-order (necessary and sufficient) condition: for any \( p \),

\[
E(\theta_i|p, s_i) - \mu_i q_i = p + \lambda_i q_i, \tag{36}
\]

Using (36), the equilibrium bid is

\[
q_i(p) = \frac{1}{(\mu_i + \lambda_i)} [E(\theta_i|p, s_i) - p]. \tag{37}
\]

Aggregating, for each \( i \), the bids submitted by \( j \neq i \), gives the residual supply for \( i \), the slope of which defines \( i \)'s price impact. We obtain the following fixed point for the price impacts

\[
\lambda_i = - \left( \sum_{j \neq i} (\partial q_j(p)/\partial p) \right)^{-1} = \left( \sum_{j \neq i} \frac{1-c_{pj}}{\mu_j + \lambda_j} \right)^{-1} = \left( \sum_{j \neq i} \gamma_j (1-c_{pj}) \right)^{-1}, \quad i \in I, \tag{38}
\]

where \( \gamma_i \equiv (\mu_i + \lambda_i)^{-1} \). Given an affine information structure, the conditional expectation is linear, \( E(\theta_i|p, s_i) = E(\theta_i) + c_{si}(s_i - E(s_i)) + c_{pi}(p - E(p)) = E(\theta_i)(1-c_{si} - c_{pi}) + c_{si}s_i + c_{pi}p \), using \( E_i(\theta_i) = E(\theta_i) \) for all \( i \). Hence, \( c_{\theta i} = 1-c_{si} - c_{pi} \) and the equilibrium bid is

\[
q_i(p) = \frac{1}{(\mu_i + \lambda_i)} [c_{\theta i} E(\theta_i) + c_{si} s_i - (1-c_{pi})p] \tag{39}
\]

This is based on Rostek and Yoon (2014) who characterize equilibria in divisible auctions in the general Gaussian model.
Aggregating bid functions \( q_i(p) \) through market clearing gives the equilibrium price

\[
p^* = \left( \sum_{i \in I} \frac{1 - c_{pi}}{\mu_i + \lambda_i} \right)^{-1} \sum_{i \in I} \frac{1}{\mu_i + \lambda_i} [c_{qi}E(\theta_i) + c_{si}s_i].
\]  

(40)

The price impact of agent \( i \), defined as the slope of the residual inverse supply, is

\[
\lambda_i = -\frac{1}{\sum_{j \neq i} (\partial q_j(p)/\partial p)} = \frac{1}{\sum_{j \neq i} \frac{1 - c_{pj}}{\mu_j + \lambda_j}}.
\]

(41)

Given (40), random vector \((\theta_i, s_i, p^*)\) is jointly normally distributed\(^ {34}\)

\[
\begin{pmatrix}
\theta_i \\
s_i \\
p^*
\end{pmatrix} = \mathcal{N} \left( \begin{pmatrix}
E(\theta_i) \\
E(s_i) \\
E(p^*)
\end{pmatrix}, \begin{pmatrix}
\sigma^2_{\theta} & \sigma^2_{\theta} & \text{cov} (\theta_i, p^*) \\
\sigma^2_{\theta} & \sigma^2_{\theta} + \sigma^2_{\varepsilon} & \text{cov} (s_i, p^*) \\
\text{cov} (p^*, \theta_i) & \text{cov} (p^*, s_i) & \text{Var} (p^*)
\end{pmatrix} \right).
\]  

(46)

Applying the Projection Theorem\(^ {35}\) gives the system of equations for inference coefficients. Let \( \gamma_i \equiv \frac{1}{\mu_i + \lambda_i}, \Gamma_i \equiv \gamma_i c_{si}, \Gamma \equiv \{ \Gamma_i \}_{i \in I} = \{ \gamma_i c_{si} \}_{i \in I} \in \mathbb{R}^I \), and let \([.].i\) and \([.].ij\) denote the \( i \)-th element of a vector and the \((i,j)\)-element of a matrix. Define the following statistic

\[
\bar{p}_i \equiv \frac{1}{I - 1} \sum_{j \neq i} \gamma_j c_{sj} \rho_{ij} = \frac{1}{I - 1} \left( \frac{1}{I - 1} \left[ (C - \text{Id}) \Gamma \right]_i \right) = \frac{1}{c_{si} \gamma_i} \left( \frac{1}{I - 1} \sum_{j \neq i} \gamma_j c_{sj} \rho_{ij} \right),
\]

(48)

\( ^{34}\)The covariances in (46) are given by

\[
cov (\theta_i, p^*) = \left( \sum_{i \in I} \frac{1 - c_{pi}}{\mu_i + \lambda_i} \right)^{-1} \left( \gamma_i c_{si} + \sum_{j \neq i} \gamma_j c_{sj} \rho_{ij} \right) \sigma^2_{\theta} = \frac{1}{G} \left( \gamma_i c_{si} + \sum_{j \neq i} \gamma_j c_{sj} \rho_{ij} \right) \sigma^2_{\theta}
\]

(42)

\[
cov (s_i, p^*) = \frac{1}{G} \left( \gamma_i c_{si} \left( 1 + \sigma^2 \right) + \sum_{j \neq i} \gamma_j c_{sj} \rho_{ij} \right) \sigma^2_{\theta}
\]

(43)

and

\[
\text{Var} (p^*) = \frac{1}{G^2} \left( 1 + \sigma^2 \right) \sum_i \gamma_i^2 c_{si}^2 + \sum_i \gamma_i c_{si} \sum_{j \neq i} \gamma_j c_{sj} \rho_{ij} \right) \sigma^2_{\theta}.
\]

(44)

\[
E (p^*) = \frac{1}{G} \sum_{i \in I} \frac{1 - c_{pi}}{\mu_i + \lambda_i} \frac{1}{\mu_i + \lambda_i} \left[ c_{qi}E(\theta_i) + c_{si}E(s_i) \right] = \frac{\sum_{i \in I} \frac{[c_{si} + c_{si} \mu_i]}{\mu_i + \lambda_i}}{\sum_{i \in I} \frac{1 - c_{pi}}{\mu_i + \lambda_i}}.
\]

(45)

\( ^{35}\)Let \( \theta \) and \( s \) be random vectors such that \((\theta, s) \sim N(\mu, \Sigma)\), where

\[
\mu \equiv \begin{pmatrix} \mu_{\theta} \\ \mu_s \end{pmatrix} \quad \text{and} \quad \Sigma \equiv \begin{pmatrix} \Sigma_{\theta, \theta} & \Sigma_{\theta, s} \\ \Sigma_{s, \theta} & \Sigma_{s, s} \end{pmatrix},
\]

(47)

are partitional expectations and variance covariance matrix and \( \Sigma_{s, s} \) is positive definite. The distribution of \( \theta \) conditional on \( s \) is normal and given by \((\theta | s) \sim N(\mu_{\theta} + \Sigma_{\theta, s} \Sigma_{s, s}^{-1} (s - \mu_s), \Sigma_{\theta, \theta} - \Sigma_{\theta, s} \Sigma_{s, s}^{-1} \Sigma_{s, \theta})\).
while still allowing for a symmetric equilibrium. In more general (asymmetric) information structures, equilib-
common in the information aggregation literature, in order to accommodate heterogeneous interdependence
where

\[
\bar{\rho}_i^2 \Gamma_i^2 + \frac{1 + \sigma^2}{(T-1) \rho_i} \bar{\rho}_i \Gamma_i^2 \]

The equicommonality assumption relaxes the stronger symmetry assumption of \( \rho_{i,j} = \rho \) for all \( i \neq j \)
common in the information aggregation literature, in order to accommodate heterogeneous interdependence
while still allowing for a symmetric equilibrium. In more general (asymmetric) information structures, equilib-
rium bids depend on the information structure \( \mathcal{C} \) not just through commonality; the dependence is a function
of the information structure, risk aversion \( \mu_i \) and, hence, price impact \( \lambda_i \).

\[
\frac{\partial c_p}{\partial \rho} = (2 - \gamma) \sigma^2 \frac{(1-\gamma)(1+\sigma^2)+\bar{\rho}^2}{(1-\gamma+\rho)(1-\rho+\sigma^2)}
\]

The explicit formula for \( c_{pi} \) is obtained using \( \sum_{j \in I} \gamma_j (1 - c_{pj}) = \frac{1}{\lambda_i} + \gamma_i (1 - c_{pi}) \).

**EQUICOMMONAL INFORMATION STRUCTURE.** In the equicommunal model, \( \bar{\rho}_i = \frac{1}{T-1} \sum_{j \neq i} \rho_{ij} \)
is constant across agents \( i \in I \). The symmetric equilibrium\(^{36}\) bid of trader \( i \) is

\[
q_i (p) = \frac{\gamma - c_p c_s}{1 - c_p} E (\theta_i) + \frac{\gamma - c_p c_s}{1 - c_p} s_i - \frac{\gamma - c_p c_s}{1 - c_p} p,
\]

where the inference coefficients in the conditional expectation \( E (\theta_i | s_i, p) \) are given by

\[
c_s = \frac{1 - \bar{\rho}}{1 - \bar{\rho} + \sigma^2}, \quad c_p = \frac{(2 - \gamma) \bar{\rho} \sigma^2}{1 - \gamma + \rho \bar{\rho} \sigma^2}, \quad c_\theta = 1 - c_s - c_p. \tag{54}
\]

The inference coefficient \( c_s \) is decreasing and \( c_p \) is increasing in the value of \( \bar{\rho} \). Price impact
is given by \( \lambda_i = -\frac{(\partial q_i (p) / \partial p)^{-1}}{T-1} = \frac{(1-\gamma) \mu}{\gamma - c_p} \), for all \( i \). The equilibrium price is

\[
p^* = \frac{c_m E (\theta_i)}{1 - c_p} + \frac{c_s}{1 - c_p} \bar{s}, \tag{55}
\]

where \( \bar{s} = \frac{1}{T} \sum_{i \in I} s_i \).

\(^{36}\) The equicommonality assumption relaxes the stronger symmetry assumption of \( \rho_{i,j} = \rho \) for all \( i \neq j \)
common in the information aggregation literature, in order to accommodate heterogeneous interdependence
while still allowing for a symmetric equilibrium. In more general (asymmetric) information structures, equilib-
rium bids depend on the information structure \( \mathcal{C} \) not just through commonality; the dependence is a function
of the information structure, risk aversion \( \mu_i \) and, hence, price impact \( \lambda_i \).
Appendix C: Other Arguments

Efficiency via a Direct Revelation Mechanism. Define \( D \equiv \sigma^2_\theta \mathcal{C}_\theta (\sigma^2_\theta \mathcal{C}_\theta + \sigma^2_\varepsilon \mathcal{C}_\varepsilon)^{-1} \). Write the efficient allocation as

\[
q^*_i(s) = \frac{e_i - \bar{e}}{\mu} = \frac{d^T_i s - \sum_{j \in I} d^T_j s}{\mu}.
\]

We show that the efficient allocation can be implemented via a direct revelation mechanism \((q^* (m), t(m))\) with incentive compatible transfers \(t_i\) for all \(i\). The well known method of constructing dominant strategy incentive compatible transfers – or VCG transfers for efficient implementation – can be extended to the linear-normal environment. For arbitrary transfer scheme \(t_i(m)\), the interim expected utility in the revelation mechanism that implements \(q^*\) is

\[
EU_{s_i}(m_i) = E \left( \theta_i q^*_i(m) - q^*_i(m)^2 - t_i(m) | s_i \right).
\]

A trader’s first order condition is

\[
\frac{\partial EU_{s_i}(m_i)}{\partial m_i} = E \left( \theta_i d_{ii} - \frac{\sum_{j \in I} d_{ij}}{\mu} - \left( d^T_i - \frac{\sum_{j \in I} d^T_j}{I} \right) m \cdot \frac{d_{ii} - \sum_{j \in I} d_{ij}}{\mu} - \frac{\partial t_i(m)}{\partial m_i} | s_i \right) = 0.
\]

Therefore, if transfers match the remaining terms in the previous expression, namely if

\[
\frac{\partial t_i(m)}{\partial m_i} = \frac{\sigma^2_\theta}{\sigma^2_\theta + \sigma^2_\varepsilon} m_i \frac{d_{ii} - \sum_{j \in I} d_{ij}}{\mu} - \left( d^T_i - \frac{\sum_{j \in I} d^T_j}{I} \right) m \cdot \frac{d_{ii} - \sum_{j \in I} d_{ij}}{\mu},
\]

then \(m_i = s_i\) is always a best response for trader \(i\), regardless the strategies played by other traders. These transfers, letting \(K_i \equiv \frac{d_{ii} - \sum_{j \in I} d_{ij}}{\mu}\), are

\[
t^*_i(m) = \frac{\sigma^2_\theta}{\sigma^2_\theta + \sigma^2_\varepsilon} m_i^2 K_i - \left( d^T_i - \frac{\sum_{j \in I} d^T_j}{I} \right) m \cdot m_i K_i + \left( d_{ii} - \frac{\sum_{j \in I} d_{ij}}{I} \right) m_i^2 |_i,
\]

which depend on the details of the information structure through the \(d_{ij}\) coefficients. Hence, although the efficient allocation can be implemented in an ex post equilibrium via a direct revelation mechanism, yet notice that this mechanism can not be rewritten into a uniform price auction, moreover the transfers are a function of the information structure \(\mathcal{IS}\).