Privacy Preserving Tâtonnement

A Cryptographic Construction of an Incentive Compatible Market

John Ross Wallrabenstein and Chris Clifton

Dept. of Computer Science, Purdue University, USA
{jwallrab,clifton}@cs.purdue.edu

Abstract. Léon Walras' theory of general equilibrium put forth the notion of *tâtonnement* as a process by which equilibrium prices are determined. Recently, Cole and Fleischer provided tâtonnement algorithms for both the classic One-Time and Ongoing Markets with guaranteed bounds for convergence to equilibrium prices. However, in order to reach equilibrium, trade must occur outside of equilibrium prices, which violates the underlying Walrasian Auction model. We propose a cryptographic solution to this game theoretic problem, and demonstrate that a secure multiparty computation protocol for the One-Time Market allows buyers and sellers to jointly compute equilibrium prices by *simulating* trade outside of equilibrium. This approach keeps the utility functions of all parties private, revealing only the final equilibrium price. Our approach has a real world application, as a similar market exists in the Tokyo Commodity Exchange where a trusted third party is employed. We prove that the protocol is inherently *incentive compatible*, such that no party has an incentive to use a dishonest utility function. We demonstrate security under the standard semi-honest model, as well as an extension to the stronger Accountable Computing framework.
Keywords. Secure Multi-Party Computation, Privacy Preserving Protocol, Tâtonnement, Game Theory.

1 Introduction

Open markets balance supply and demand by converging to a price where the two are equal. For example, oil is a commodity where increasing supply becomes progressively more expensive, and increasing price reduces demand. Absent other disturbing factors, oil supply and demand would eventually stabilize. However, this takes time, and in the meantime prices rise and fall, leading to unnecessary investment in uneconomical production based on an expectation of high prices, or investment in consumption based on expectation of low prices. Faster convergence or lower volatility in prices can have significant benefits.

Economic models generally accepted as valid representations of real-world market behavior tend to have underlying computationally tractable algorithms. It follows naturally to propose that these algorithms could be evaluated by parties to arrive at the result deemed to accurately reflect the outcome of a given

market phenomenon. The work of Cole and Fleischer studies the market equilibrium problem from an algorithmic perspective, and they give tractable price update algorithms that do not rely on global information [7].

The algorithms of Cole and Fleischer [7] follow the Walrasian Auction model: prices are adjusted according to a tâtonnement process, where prices iteratively rise or fall in response to changes in demand [27]. In the Walrasian Auction model, *trade occurs only once equilibrium has been established.* In real-world markets, it is trade that dictates demand and, thus, how prices are adjusted to converge toward equilibrium. However, Cole and Fleischer's algorithms allow trade outside of equilibrium.

As specified, the Walrasian Auction model is limited to the theoretical domain unless a trusted third party is invoked to serve as a mediator between the buyers and sellers. Not only must the mediator be trusted to faithfully represent the interests of all parties involved, it must be trusted with substantial information about each party's private utility function. As a utility function defines a party's preferences over goods with respect to both quantity and price, it reveals valuable information that parties would prefer to keep private. Further, there are no guarantees that the parties will truthfully report their valuations of the good. This problem becomes particularly pronounced when independent buyers collude to reduce the final equilibrium price.

The recent work of Dodis et al. [10] considered a similar game theoretic problem: implementing the mediator for rational players to arrive at a *correlated equilibrium.* In game theory, a correlated equilibrium is selected when a mediator recommends a strategy to each player such that, given the recommended strategy, no player can improve their utility[1] by choosing a different strategy. Further, the payoff may exist outside the convex hull of standard Nash equilibria, yielding more utility than when a mediator is not present. Dodis et al. demonstrate that secure multiparty computation (SMPC) can replace the mediator with a protocol among the players, removing the necessity of a trusted third party. In this work, we use SMPC to find Walrasian equilibria *without* invoking a mediator or allowing trade to occur prior to arriving at a stable price.

Further, we are able to make strong claims of *incentive compatibility.* In the standard security model, a monolithic adversary $\mathcal{A}$ corrupts a subset of the participants. In rational cryptography, each player acts solely in their own self-interest, and thus have an associated *local* adversary controlling their deviations [5]. The move to local adversaries has important consequences on the stability of coalitions for rational player. Not even protocols secure in the malicious model cannot guarantee that a malicious party will not manipulate its input to the protocol, as a monolithic adversary may force the equilibrium price to be deflated through centralized control of corrupted parties. We demonstrate that our protocols are resilient against this behavior in the presence of local, independent rational adversaries seeking to maximize their utility.

[1] A utility function describes an agent's preferences over outcomes, and can informally be considered a mapping between events and agent happiness.

2 Our Contribution

Drawing on recent work from both the cryptographic and game theoretic literature [1, 16–18, 20–22], we propose a privacy preserving protocol that allows buyers and sellers to arrive at an equilibrium price using the tâtonnement process *without* trade occurring outside of equilibrium. This approach has the auxiliary benefit of keeping the utility functions of all parties private; only the final equilibrium price is revealed. Further, we show that our construction is *incentive compatible*: the strategy of reporting truthful private valuations weakly dominates all other strategies for both buyers and seller.

A protocol that arrives at the equilibrium price for a good is beneficial to both the buyers and sellers involved. A participant's utility function must be evaluated many times throughout the tâtonnement process in order for appropriate price updates to occur. This is a potential disincentive to engaging in the protocol, as the participant's utility function contains their preferences for a good, and many individual points from their utility function are evaluated and publicly disclosed. A malicious agent could use this information to alter their behavior for personal gain. SMPC allows two or more mutually distrustful parties to engage in a collaborative protocol to compute the result of a function securely [14, 28]. Our approach allows the tâtonnement process to be evaluated privately, revealing *only* the final equilibrium price.

SMPC has had real-world use, very much in the scenario we suggest. Bogetoft et al. [3] deploy a privacy preserving protocol to evaluate a double auction model for Danish commodity trading. However, they assume that all parties behave honestly in using the system, and do not explore the possibility that a malicious party could manipulate the equilibrium price to its advantage. In fact, they state *"we did not explicitly implement any security against cheating bidders"*, although they were only discussing semi-honest vs. malicious behavior in the traditional sense. Further, the authors surveyed the farmers' views on the privacy of their utility functions, and found that nearly all preferred that information to remain private.

We go well beyond this, exploring *lying about the input to the protocol itself*: a behavior that even the malicious model does not prevent. Previous work has demonstrated this idea, although the authors only consider a two-party protocol, and showed incentive compatibility only for an approximation of the real-world problem [6]. We show that this approach can be used to enable SMPC to address the full range of malicious behavior in a real-world, multi-party problem.

As another example, the Tokyo Commodity Exchange uses the *itayose* mechanism, similar to tâtonnement, to reach equilibrium. In fact, this existing market circumvents the restriction of disallowed trade until equilibrium is reached by invoking a trusted third party: an auctioneer that adjusts prices based on excess demand [11]. Our approach requires no trusted third party, resulting in the minimum possible disclosure of information regarding each party's utility function. Thus, there is clear real-world application and tangible benefit from our results, similar to those of Bogetoft et al. [3].

Note that our model makes a stronger statement than that of a Bayes-Nash equilibrium, where participants have an incentive to be truthful if and only if others are acting truthfully as well. We show that acting honestly is the dominant strategy in our protocol *regardless of the actions of the other players*. The work by Eaves et al. [11] provides further evidence for our claims of incentive compatibility, based on the fact that agents engage in the protocol repeatedly. However, our results hold without the assumption of repeated interaction.

To ensure parties deviating from the protocol will be caught, it is secure under the accountable computing (AC) framework proposed by Jiang and Clifton [19]. Note that we first show security under the standard semi-honest model, and then extend this to the AC-framework. The AC-framework provides the ability to verify that a party correctly followed the protocol; contractual penalties can then be used to ensure that correctly following the protocol is incentive compatible. Typical semi-honest protocols provide no such guarantee; a malicious party may be able to manipulate the protocol to their benefit. Protocols secure under the malicious model (forcing participants to correctly follow the protocol) typically have much greater computational cost. By demonstrating security under the AC-framework, detected deviations are punishable by other participants forcing the *minmax utility*[2] on the deviating parties [10]. We also use commitments to ensure that parties use their true utility function with the protocol; this prevents parties from supplying one input to the protocol (e.g., a low demand) to give an artificially beneficial price, then purchasing greater quantities at the resulting price.

We show that the utility functions and actions of all agents remain private, with the equilibrium price revealed to all agents at the conclusion of the protocol. The knowledge gain is only the information that can be derived from the result of the function, and knowledge of the function itself. This satisfies the standard definition of semi-honest security in that the protocol emulates the existence of a trusted third party, *without* actually requiring such an entity [13]. This property is ideal, as a universally trusted third party rarely exists for a given set of parties. Our work considers only the case of the *oblivious One-Time Market* setting. That is, we consider the market where all parameters are assumed *not* to be global information. Rather, agents compute the price updates based solely on local information.

We begin by defining the market problem and reviewing the oblivious One-Time Market algorithm in Section 3. We review the cryptographic primitives used in Section 4, and give a construction[3] based on an additively homomorphic cryptosystem in Section 5. Finally, we demonstrate that the resulting protocol is incentive compatible in Section 6. All proofs are provided in Appendix A.

[2] The *minmax* punishment approach forces the outcome yielding the minimum utility to the deviator, while maximizing the utility of the other participants.

[3] Our protocol can also be implemented using frameworks for the GMW protocol [14], such as FairPlayMP [2], VIFF [9] or SEPIA [4].

3 The Market Problem

Our SMPC protocol computes the equilibrium for a single seller offering a single good to a set of buyers, which we extend to the general definition of the problem following the notation from Cole and Fleischer [7]. The market under consideration contains a set of infinitely divisible goods G, where $|G| = n$, and a set of agents A, where $|A| = m$. Agent l has quantity w_{il} of good i at the start of the protocol and has a corresponding utility function $\mu_l(x_{1l}, \ldots, x_{nl})$ that gives their preferences for all goods $i \in G$. Note that the initial allocation w_{il} may consist solely of currency; it is a measure of the agent's wealth. We make the simplifying assumption that $\mu_l(x_{1l}, \ldots, x_{nl}) = \Sigma_{i=1}^{n} \mu(x_{il})$; the utility of a basket of goods is the sum of the utility of each individual good. Each good i has a collection of prices $p_i, 1 \leq i \leq n$. Each agent l selects a basket with x_{il} units of good i so that u_l is a maximum and is affordable given their initial allocation. That is: $\sum_{i=1}^{n} x_{il} p_i \leq \sum_{i=1}^{m} w_{il} p_i$. The prices $p = (p_1, p_2, \ldots, p_n)$ are in equilibrium if the demand for all goods $i \in G$ is bounded by the supply for good i: $\sum_{l=1}^{m} x_{il} \leq \sum_{l=1}^{m} w_{il}$.

We define $w_i = \sum_l w_{il}$ to be the supply of good i, and $x_i = \sum_l x_{il}$ to be the corresponding demand. We define $z_i = x_i - w_i$ to be the excess demand of good i. At a given set of prices p, the wealth of agent l is $v_l(p) = \sum_i w_{il} p_i$. By definition, w is from the market specification while v, x and z are computed with respect to the vector of prices. The wealth of an agent l is computed directly from a given price vector p, whereas x and z are computed by agents maximizing their utility functions under the constraints imposed by v.

The model put forth by Cole and Fleischer is based upon a series of iterative price and demand updates. We omit discussion of the proofs of bounded convergence time and refer the reader to their original work [7]. In each iteration r, the price of a good $i \in G^r$ is updated by its price setter using knowledge of only p_i, z_i, and their history. Here, a price setter is a virtual entity that governs the price adjustments. However, the price adjustments are governed by changes in demand in the algorithms. After the price setters have released the new prices p^r, the buying agents compute the set of goods that maximizes their utility under the constraint of their wealth given the current prices, $v_l(p)$. We consider only the oblivious One-Time Market price update rule, which is as follows:

$$p_i \leftarrow p_i \cdot (1 + \frac{1}{2^{\lceil \log_4 r_i \rceil}} \cdot min\{1, \frac{z_i}{w_i}\}) \tag{1}$$

The current round r is bounded prior to the start of the protocol by fixing the terminal round r^*. At the conclusion of the protocol, we will have computed the equilibrium price and demand, p^* and x^*, respectively.

To construct a privacy preserving protocol, we show how buyers compute their demand based on the current price p_i, and how sellers compute the price update given the demand x_i from the buyers. In our privacy preserving protocol, the buyers compute the update for each round locally to prevent the seller from learning intermediate prices. Symmetrically, neither the price nor the demand is known to either the buyers or seller until the conclusion of the protocol. Finally,

we must account for the fact that $\frac{z_i}{w_i}$ may be less than 1, which cannot be represented properly in the field $\mathbb{Z}_n$. To handle this, prices are represented in integer units corresponding to the minimum increment (e.g., cents). We use the division protocol δ of Dahl et al. [8] to compute $\frac{z_i}{w_i}$, which we discuss further in Section 4.1. As the degree of Walrasian auction utility functions is 1 with overwhelming probability [27], all buyers are modeled as having Cobb-Doublas utility functions. As noted by Cole and Fleischer, under these conditions the price update rule converges in a single round [7], so $r^* \leftarrow 1$.

Our work is certainly not the first to apply SMPC principles to economic and game theory. Previous work has shown that SMPC removes potential disincentives from bartering to auctions [12, 23]. Additionally, recent work has shown the potential of combining cryptography with game theoretic principles [1, 16–18, 20–22]. However, no attempt has been made to remedy the paradox of the Walrasian Auction model using SMPC techniques. In this way, we not only remove disincentives from engaging in the protocol, we allow the model to exist in reality. That is, our protocol allows the participants to evaluate the iterative price update function on the basis of the buyers' demand without actually revealing the demand through trade or invoking a trusted third party. Additionally, we show that our construction constitutes an incentive compatible market with respect to both buyers and sellers.

We review the One-Time Market Oblivious tâtonnement algorithm proposed by Cole and Fleischer [7]. The original algorithm is a protocol between a set of buyers $b_l \in B$ and a set of sellers $s_l \in S$. We assume that for each buyer $b_l \in B$ they have an associated utility function $\mu_{b_l}(i)$, where i is the good offered for sale from S. Recall that the seller S has knowledge of their supply of i, given by w_i. The task of the set of buyers B is to compute the excess demand for good i, given by $z_i = x_i - w_i$, where $x_i = \Sigma_l x_{il}$ is the sum of the demand of all buyers $b_l \in B$. The original protocol by Cole and Fleischer is given formally by Algorithm 1.

Algorithm 1 Model by Cole and Fleischer

for $r_i = 0; r_i < r; ++n_i$ **do**
  for $s_l \in S$ **do**
    $p_i \leftarrow p_i + \frac{1}{2^{\lceil \log_4 r_i \rceil}} p_i \cdot min\{1, \frac{z_i}{w_i}\}$
  end for
  for all $b_l \in B$ **do**
    $x_i \leftarrow x_i + \mu_{b_l}(p_i)$
  end for
  $z_i \leftarrow x_i - w_i$
end for
$p^* = p_i$
$x^* = x_i$
return (p^*, x^*)

The algorithm fixes a price p_i for the good, uses the utility functions of the buyers to determine the excess demand x_i at that price, and sets the price for the next round. The key contribution of Cole and Fleischer is to prove that the given update rule gives a guaranteed convergence rate. Beyond simply bounding the number of required rounds, as Walrasian markets typically have Cobb-Douglas utility functions, the algorithm converges in one round [7].

4 Building Blocks

To build the privacy preserving protocol, we build on a collection of cryptographic primitives.

We require an additively homomorphic public-key encryption scheme $\mathcal{E}$, with the additional property of semantic security [15]. Such a scheme was proposed by Paillier [25]. We denote the encryption of some plaintext x with Bob's public key as $E_b(x)$, and the decryption of some ciphertext $c = E_b(x)$ as $D_b(c)$. We require that our cryptosystem's *homomorphic property* is additive, which means that the following operations are supported:

$$E_b(x) \cdot E_b(y) = E_b(x + y), \qquad (E_b(x))^c \equiv E_b(x)^c = E_b(x \cdot c) \tag{2}$$

Here, c is an unencrypted plaintext constant. Note that we omit the enclosing parentheses and treat $E_b(x)$ as a distinct term. The construction of the additively homomorphic encryption scheme allows mathematical operations over encrypted data to be performed, and provides the foundation for our protocol.

4.1 Division Protocol δ

The price update rule requires computing the quotient of the excess demand and the supply, $\frac{x_i - w_i}{w_i}$. Dahl et al. give a protocol for securely computing integer division under the Paillier cryptosystem *without* requiring a bit-decomposition [8]. For l-bit values, the constant round protocol requires $O(l)$ arithmetic operations in $O(1)$ rounds.

5 Protocol Construction

We consider a set of k buyers $b_l \in B$ interacting with a single seller S of a good i. The protocol π securely implements the functionality $f(\mu_1, \cdots, \mu_k, p_S) \mapsto \langle p^*, x^* \rangle$. Here, μ_l is the utility function of buyer $b_l \in B$. The full Walrasian Market (composed of more than a single seller and good) is modeled by instantiating an instance of Protocol 5.1 for each pair of seller and good (S, i), and the associated set of buyers. Note that our protocol centers around specific utility functions known as Marshallian or Walrasian demand functions. That is, the participant's utility function is modeled as a polynomial, and defines the quantity demanded for a single good over all possible prices. Overwhelmingly, the degree of a Walrasian demand function will be one [27]. Thus, a buyer's utility

function μ_{b_i} has the form $\mu_{b_i}(p_i) = cp_i$ where the coefficient c is a constant, satisfying the definition of a Cobb-Douglas utility function. The final argument to the functionality is the initial price p_i specified by the seller. A Paillier-based algorithm for computing the Walrasian equilibrium is given by Protocol 5.1. To increase scalability, this simple ring-based protocol could be replaced with an implementation using a state-of-the-art framework for the GMW protocol [14], such as FairPlayMP [2], VIFF [9] or SEPIA [4]. We defer the proof of security to Appendix A.

Buyers $1 \leq l \leq k$**:**	All buyers issue commitments (e.g. Pedersen [26]) to their private utility function coefficients. This is necessary for the verification stage of the AC-Framework [19].
Seller S**:**	Set p_i as the Seller's initial price for good i. Set w_i as the supply of good i. Send $E_S(p_i)$ to all buyers.
Buyer 1 :	The first buyer computes the initial demand as $E_S(x_i) \leftarrow \mu_{b_1}(E_S(p_i))^{\dagger}$, where μ_{b_1} is the initial buyer's utility function. The first buyer forwards $E_S(x_i)$ to the next buyer, so that they can update the demand x_i based on their utility function.
Buyers $1 < l \leq k$**:**	Each buyer updates the demand at the current price p_i based on their utility function μ_{b_l} by computing $E_S(x_i) \leftarrow \mu_{b_l}(E_S(p_i))^{\dagger}$.
Buyer k**:**	The final buyer b_k must perform additional updates before sending the results of the current round to either buyer 1 (if $r < r^*$) or the seller (if the terminal round r^* has been reached). The final buyer updates the excess demand z_i by computing $E_S(z_i) \leftarrow E_S(x_i) \cdot E_S(w_i)^{-1}$. The final buyer computes the price update coefficient $y_i := \frac{z_i}{w_i}$, the fraction of excess demand to supply, using the division protocol of Dahl et al. [8]: $y_i \leftarrow \delta(E_S(z_i), E_S(w_i))$. The final buyer updates the current round price p_i^r to p_i^{r+1} by computing $E_S(p_i^{r+1}) \leftarrow E_S(p_i^r) \cdot E_S(y_i)$. If $r = r^*$, where r^* is the final round, buyer b_k sends $\langle E_S(p_i), E_S(x_i) \rangle$ to the seller. Otherwise, this tuple is forwarded to buyer 1 and the next round begins.
Seller S**:**	After receiving $\langle E_S(p_i), E_S(x_i) \rangle$ in the final round, the seller computes the equilibrium price $p^* \leftarrow D_S(E_S(p_i))$ and the final demand $x^* \leftarrow D_S(E_S(x_i))$. The seller forwards p^* to all of the buyers.

Protocol 5.1. Additively Homomorphic Encryption Algorithm for Tâtonnement

In the next section, we prove that if a player is unable to deviate from the protocol without being caught (e.g., a protocol secure in the AC-Framework), then the dominant strategy is for parties to provide their true utility functions.

[†] Here, we evaluate $\mu_{b_l}(E_S(p_i))$ as $E_S(p_i) \cdot E_S(c)$, where c is the buyer's coefficient term in μ_{b_l}.

6 Incentive Compatibility

We claim that Protocol 5.1 is inherently *incentive compatible* with respect to protocol inputs from the perspectives of both buyers and sellers. That is, each player has no incentive to maliciously modify their actual input (utility function). We assume that malicious buyers have the option to either inflate or deflate their demand for a given price relative to their actual utility function. We show that while this can influence the price, it works to their detriment. We demonstrate that a seller only sets the initial price, and that their choice does not affect the final equilibrium price, so deviating provides no utility gain.

6.1 Utility Function Assumptions

In order to simplify the game theoretic analysis of the protocol, we write μ^+ to denote positive utility, μ^- to denote negative utility, and μ^0 to denote neutral utility gain. We assume that the magnitude of preference for all μ_i are equal (i.e., $\mu^+ + \mu^- = \mu^0$). Similarly, we assume that μ^ϵ represents only a marginal utility gain. That is, $\mu^+ > \mu^\epsilon > \mu^0$.

Additionally, we assume that $(p_i - p_i^*) \in \{\mu^+, \mu^-, \mu^\epsilon\}$, although this value depends on how much the reported utility function μ_l^* differs from an agent b_l's actual utility function μ_l. Clearly there is an inverse relationship between how much an agent can under-inflate μ_l^* (which subsequently reduces the equilibrium price p_i^*), and the likelihood of a trade occurring between the agent and the seller. As the agent is involved in the protocol, we assume that they prefer a trade occur. If not, they would have abstained from the protocol entirely. Thus, it is natural to assume the agent's utility function assigns the same range to both of these preferences. This assumption does not affect our analysis, and is solely to ease the exposition.

Definition 1. *Let r_l be the **reward** that a buyer b_l gains by reporting μ_l^* in lieu of their actual utility function μ_l. Where p_i^* (resp. p_i) is the resulting equilibrium price when μ_l^* (resp. μ_l) is reported, b_l's reward is given by:*

$$r_l = \begin{cases} (p_i - p_i^*) < 0 : \mu_l^* > \mu_l \\ 0 \qquad\qquad\quad : \mu_l^* = \mu_l \\ (p_i - p_i^*) > 0 : \mu_l^* < \mu_l \end{cases} \tag{3}$$

We make the natural assumption that each buyer prefers some (possibly large) quantity of the seller's good to their initial allocation, otherwise they would not engage in the protocol.

Definition 2. *Define the utility gained through trade as μ_τ:*

$$\mu_\tau = \begin{cases} \mu_\tau^+ \qquad\quad : \textit{trade occurs} \\ \mu_\tau^- : \textit{trade does not occur} \end{cases} \tag{4}$$

Similarly, a buyer offering a higher price has increased control over the *quantity* of the good they can demand, subject to the seller's supply w_i. That is, the seller prefers to sell to the set of buyers $\{b_l | p_i^l \geq p_i^m, l \neq m\}$ offering the highest price. Thus, a highest price buyer b_m can command $min(w_i, w_m)$ units of good i, where w_i is the seller's supply and w_m is the initial allocation of resources for buyer b_m.

Definition 3. *Define buyer b_l's utility gained from control over quantity received, $\mu_{q,l}$, as follows:*

$$\mu_{q,l} = \begin{cases} \mu_{q,l}^+ : \forall m, p_i^l > p_i^m, l \neq m \\ \mu_{q,l}^- : \forall m, p_i^l \leq p_i^m, l \neq m \end{cases} \tag{5}$$

That is, b_l receives μ_q^+ if b_l is offering the highest price p_i, and μ_q^- otherwise.

Definition 4. *Let r_l be the reward for buyer b_l, let $\mu_{\tau,l}$ be b_l's trade utility, and let $\mu_{q,l}$ be b_l's quantity control utility. We define b_l's **total reward** ρ_l as follows:*

$$\rho_l = r_l + \mu_{\tau,l} + \mu_{q,l} \tag{6}$$

Without loss of generality, consider a coalition of buyers with utility functions satisfying the above constraints. Let $a_l = \{a_u, a_t, a_o\}$ denote b_l's action set, where a_u denotes under-inflating, a_o denotes over-inflating, and a_t denotes reporting the buyer's true utility function u_l rather than a modified utility function u_l^*.

We assume that a rational seller will agree to sell their entire allocation of goods to the buyer whose utility function u_b gives the highest valuation for the good, thus maximizing their profit. Thus, for all buyers $b_k \notin \{b_l | p_i^l \geq p_i^m, l \neq m\}$, we have that $\mu_{\tau,k} = \mu_{q,k} = \mu^-$. Note the following:

- A buyer playing a_u in the presence of a buyer playing $\{a_t, a_o\}$ does not have quantity control
- A buyer playing a_u in the presence of a buyer playing $\{a_t, a_o\}$ does not receive any goods
- A unique buyer playing $\{a_t, a_o\}$ in the presence of buyers playing only a_u has quantity control

We begin by reviewing the formal definition for *weakly dominated* strategies as given by Katz [20], where a player can never increase their utility by playing a weakly dominated strategy.

Definition 5. *Given a game $\Gamma = (\{A_l\}_{l=1}^k, \{\mu_l\}_{l=1}^k)$, where $A = A_1 \times \cdots \times A_k$ is a set of actions, with $a = (a_1, \ldots, a_k) \in A$ being a strategy and $\{\mu_l\}$ is a set of utility functions, we say that action $a_l' \in A_l$ is **weakly dominated** by $a_l \in A_l$ if $\mu_l(a_l) \geq \mu_l(a_l')$. That is, player P_l never improves their payoff by playing a_l', but can sometimes improve their payoff by playing a_l.*

To show that our construction is *incentive compatible*, we iteratively delete weakly dominated strategies to arrive at the stable Nash equilibrium [24]. The process of iteratively deleting weakly dominated strategies is criticized because, in some cases, the *order* of deletion affects the final result [21]. In this analysis, weakly dominated strategies can be removed in an arbitrary order without affecting the result.

We present a simplified payoff matrix in Table 1. The strategy a_o of over-inflating the utility function is removed for clarity, as a_u, the strategy of under-inflating, is a much more intuitive deviation for maximizing utility. However, we formally demonstrate that a_o is weakly dominated in lemma 1.

Table 1. Total Payoff Matrix

	a'_u	a'_t
a_u	(μ^+,μ^+)	$(\mu^-,2\mu^+)$
a_t	$(2\mu^+,\mu^-)$	(μ^+,μ^+)

Lemma 1. *The strategy a_o of reporting an over-inflated utility function u_i^* is weakly dominated by a_t.*

Proof. We show that the action of over-inflating the buyer's true utility function is weakly dominated by truthfully reporting the utility function, demonstrating that a_o is weakly dominated by a_t. Recall that buyer b_l's total reward is defined as $\rho_l = r_l + \mu_{\tau,l} + \mu_{q,l}$. For convenience, we will parameterize $\rho_l(\cdot)$ with the action being played. This notation is convenient for comparing the total payoff yielded from different actions.

We begin by deriving the maximum utility that could be gained by playing a_o, the action of over-inflating the true utility function. As buyer b_l is playing a_o, we have that $\mu_l^* > \mu_l$. From Equation 3, we have $\rho_l(a_o) = (p_i - p_i^*) + \mu_{\tau,l} + \mu_{q,l}$. As $(p_i - p_i^*) < 0$, we write μ^- for concreteness. Given that b_l is over-inflating their true utility function μ_l, they are more likely to effect a trade. Clearly the seller S prefers the higher price p_i^* to b_l's true valuation, p_i. By Equation 2, we have that $\rho_l(a_o) = \mu^- + \mu^+_{\tau,l} + \mu_{q,l}$. Similarly, by over-inflating their true utility function, b_l is more likely to have control over the quantity of the good they receive, as they are offering a higher price. By Equation 3, we have that: $\rho_l(a_o) = \mu^- + \mu^+_{\tau,l} + \mu^+_{q,l} = \mu^+$. Thus, we have that $max(\mu_l(a_o)) = \mu^+$. We now derive the maximum utility that could be gained by playing a_t, where buyer b_l reports the true utility function μ_l. By Equation 3, we have that $\rho_l(a_t) = \mu^0 + \mu_{\tau,l} + \mu_{q,l}$ as $p_i = p_i^*$ so $(p_i - p_i^*) = \mu^0$. Buyer b_l maximizes their utility when a trade occurs, and they can control the quantity of the good they receive. Following the same derivation that was used for a_o, we have from Equation 2 that $\rho_l(a_t) = \mu^0 + \mu^+_{\tau,l} + \mu_{q,l}$. Similarly, by Equation 3 we have that $\rho_l(a_t) = \mu^0 + \mu^+_{\tau,l} + \mu^+_{q,l} = 2\mu^+$. We have

that $max(\mu_l(a_t)) = 2\mu^+$, and it follows that $max(\mu_l(a_t)) > max(\mu_l(a_o))$. Thus, a buyer always does *at least as well or better* by playing a_t, and we say that a_t weakly dominates strategy a_o.

Lemma 2. *The strategy a_u of reporting an under-inflated utility function u_l^* is weakly dominated by a_t.*

Proof. We demonstrate that the action a_u is weakly dominated by a_t when considering both individual buyers and members of a buyer coalition that collude to lower the equilibrium price p^*.

Consider an individual buyer b_l that is not a member of a coalition. As b_l reports $\mu_l^*, \mu_l^* < \mu_l$, by Equation 3 we have that $\rho_l(a_u) = (p_i - p_i^*) + \mu_{\tau,l} + \mu_{q,l}$. Again, as $(p_i - p_i^*) > 0$, we assume $(p_i - p_i^*) = \mu^+$ for concreteness. Similarly, we assume that under-inflating μ_l reduces the chances of b_l effecting a trade with S, as b_l is offering a lower price. By Equation 2, we have that $\rho_l(a_u) = \mu^+\mu_{\tau,l}^- + \mu_{q,l}$. Playing action a_u also reduces the chances of b_l having control over the quantity of the good received, if any is received at all. By Equation 3, we have that $\rho_l(a_u) = \mu^+\mu_{\tau,l}^- + \mu_{q,l}^- = \mu^-$. Thus, $max(\mu_l(a_u)) = \mu^-$, and it follows that $max(\mu_l(a_t)) > max(\mu_l(a_u))$. Thus, a (non-coalition) buyer always does *at least as well or better* by playing a_t, and we say that a_t weakly dominates strategy a_u.

We now consider a coalition of *unique* buyers under-reporting μ_l as $\mu_l^* < \mu_l$, colluding to decrease the resulting equilibrium price p^* of the good. That is, the coalition is *not* controlled by a monolithic adversary as is common in the standard security model: they are independent buyers in competition, modeled under the *local adversary* framework of Canetti [5]. In the game theoretic literature, this is referred to as the cartel problem. Note that the best response of any member of the coalition is to report $\mu_l^* + \epsilon$ for any positive ϵ. In doing so, they receive the goods at a price $p' < p^*$ while the other coalition members receive no goods. Applying backward induction, we demonstrate that the best response of all buyers in a coalition is to report μ_l, as $\mu_l^* + \epsilon$ converges to their true utility function μ_l.

Suppose all coalition members agree to collude by reporting $\mu_l^* < \mu_l$, and all members play this strategy. For any buyer b_l in the coalition, we have that $\mu_l^* < \mu_l$ and by Equation 3 we have that $\rho_l(a_u) = (p_i - p_i^*) + \mu_{\tau,l} + \mu_{q,l}$. As $(p_i - p_i^*) > 0$, we set $(p_i - p_i^*) = \mu^+$ to denote a positive utility gain. As the coalition consists of more than a single buyer, all members of the coalition are more likely to effect a trade. From Equation 2, we have that $\rho_l(a_u) = \mu^+ + \mu_{\tau,l}^+ + \mu_{q,l}$. However, as all members of the coalition are offering the same price for the good, they have no control over the quantity of the good they receive. By Equation 3, we have that $\rho_l(a_u) = \mu^+ + \mu_{\tau,l}^+ + \mu_{q,l}^- = \mu^+$. Thus, $max(\mu_l(a_u)) = \mu^+$ for all coalition members. However, consider the case where a coalition member reports a utility function $\mu_l' = \mu_l^* + \epsilon, \epsilon > 0$. That is, some b_l in the coalition increases the price they are willing to pay for the good by any positive amount ϵ. From Equation 3, we have that

$$\rho_l(a_u + \epsilon) = ((p_i - (p_i^* + \epsilon)) + \mu_{\tau,l} + \mu_{q,l} = \mu^{(+)-\epsilon} + \mu_{\tau,l} + \mu_{q,l}$$

However, now b_l is more likely to effect a trade, as $p_i^* + \epsilon > p_i^*$. By Equation 2, we have that $\rho_l(a_u + \epsilon) = \mu^{(+)-\epsilon} + \mu_{\tau,l}^+ + \mu_{q,l}$. Similarly, b_l has control over the quantity of the good received as b_l is offering ϵ more than the coalition members. From Equation 3, we have

$$\rho_l(a_u + \epsilon) = \mu^{(+)-\epsilon} + \mu_{\tau,l}^+ + \mu_{q,l}^+ > 2\mu^+ > max(\mu_l(a_u))$$

Thus, $max(\mu_l(a_u + \epsilon)) > max(\mu_l(a_u))$, as $\mu^{(+)-\epsilon} = \mu^+ + \mu^{-\epsilon} > \mu^0$. However, all coalition members are aware of this fact. Applying backward induction, it is not difficult to see that action a_u converges to a_t by increasing ϵ until $\mu_l^* = \mu_l$, and that a_t weakly dominates a_u.

Corollary 1. *The strategy a_t of reporting the true utility function u_l weakly dominates $\{a_u, a_o\}$ for all buyers.*

Proof. A buyer's action set is defined as $a_l \in \{a_u, a_t, a_o\}$. By lemma 1, we have that a_o is a weakly dominated strategy, and can be eliminated. By lemma 2, we have that a_u is a weakly dominated strategy, and can be eliminated. Thus, reporting the true utility function μ_l as denoted by action a_t is a stable Nash equilibrium.

Theorem 1. *The strategy a_t of reporting the true utility function u_l weakly dominates $\{a_u, a_o\}$ for the seller.*

Proof. As noted in the original paper, the update protocol converges on the equilibrium price p^* from any *arbitrary* initial price p_i [7]. Given that the seller's only influence on the equilibrium price is through setting the initial price p_i, there is no incentive to report some $p_i' \neq p_i$, as p^* is unaffected in doing so.

7 Conclusion

We have presented a privacy preserving, incentive compatible market construction that is secure against malicious parties, going beyond the standard security model to protect against malicious input to the protocol. To do this, we demonstrated that by securely computing the Oblivious One-Time Market protocol given by Cole and Fleischer [7], no agent has an incentive to report false valuations of the goods in the market. Thus, SMPC solves a long-standing problem in economic theory, as it allows Léon Walras' tâtonnement process for arriving at equilibrium to be computed while conforming to the constraints of the Walrasian Auction model. In this way, trade does not occur outside of equilibrium, and yet the final equilibrium price is computed and made available to all agents in the market.

References

1. Asharov, G., Canetti, R., Hazay, C.: Towards a game theoretic view of secure computation. In: Proceedings of the 30th Annual international conference on Theory and applications of cryptographic techniques: advances in cryptology. pp. 426–445. EUROCRYPT'11, Springer-Verlag, Berlin, Heidelberg (2011)

2. Ben-David, A., Nisan, N., Pinkas, B.: Fairplaymp: a system for secure multi-party computation. In: Proceedings of the 15th ACM conference on Computer and communications security. pp. 257–266. CCS '08, ACM, New York, NY, USA (2008)
3. Bogetoft, P., Christensen, D., Damgärd, I., Geisler, M., Jakobsen, T., Krigaard, M., Nielsen, J., Nielsen, J., Nielsen, K., Pagter, J., Schwartzbach, M., Toft, T.: Secure multiparty computation goes live. In: Dingledine, R., Golle, P. (eds.) Financial Cryptography and Data Security, Lecture Notes in Computer Science, vol. 5628, pp. 325–343. Springer Berlin Heidelberg (2009)
4. Burkhart, M., Strasser, M., Many, D., Dimitropoulos, X.: Sepia: privacy-preserving aggregation of multi-domain network events and statistics. In: Proceedings of the 19th USENIX conference on Security. pp. 15–15. USENIX Security'10, USENIX Association, Berkeley, CA, USA (2010)
5. Canetti, R., Vald, M.: Universally composable security with local adversaries. In: Visconti, I., Prisco, R. (eds.) Security and Cryptography for Networks, Lecture Notes in Computer Science, vol. 7485, pp. 281–301. Springer Berlin Heidelberg (2012)
6. Clifton, C., Iyer, A., Cho, R., Jiang, W., Kantarcıoğlu, M., Vaidya, J.: An approach to identifying beneficial collaboration securely in decentralized logistics systems. Management & Service Operations Management 10(1), 108–125 (Winter 2008), http://dx.doi.org/10.1287/msom.1070.0167
7. Cole, R., Fleischer, L.: Fast-converging tatonnement algorithms for one-time and ongoing market problems. In: STOC '08: Proceedings of the 40th annual ACM symposium on Theory of computing. pp. 315–324. ACM, New York, NY, USA (2008)
8. Dahl, M., Ning, C., Toft, T.: On secure two-party integer division. In: Keromytis, A. (ed.) Financial Cryptography and Data Security, Lecture Notes in Computer Science, vol. 7397, pp. 164–178. Springer Berlin Heidelberg (2012)
9. Damgård, I., Geisler, M., Krøigaard, M., Nielsen, J.B.: Asynchronous multiparty computation: Theory and implementation. In: Jarecki, S., Tsudik, G. (eds.) Public Key Cryptography. Lecture Notes in Computer Science, vol. 5443, pp. 160–179. Springer (2009)
10. Dodis, Y., Halevi, S., Rabin, T.: A cryptographic solution to a game theoretic problem. In: Bellare, M. (ed.) Advances in Cryptology CRYPTO 2000, Lecture Notes in Computer Science, vol. 1880, pp. 112–130. Springer Berlin Heidelberg (2000)
11. Eaves, J., Williams, J.C.: Walrasian ttonnement auctions on the tokyo grain exchange. Review of Financial Studies 20(4), 1183–1218 (2007), http://EconPapers.repec.org/RePEc:oup:rfinst:v:20:y:2007:i:4:p:1183-1218
12. Frikken, K., Opyrchal, L.: Pbs: Private bartering systems. In: Financial Cryptography and Data Security: 12th International Conference, FC 2008, Cozumel, Mexico, January 28-31, 2008. Revised Selected Papers. pp. 113–127. Springer-Verlag, Berlin, Heidelberg (2008)
13. Goldreich, O.: Foundations of Cryptography, vol. 2. Cambridge University Press (2004)
14. Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game. In: STOC '87: Proceedings of the nineteenth annual ACM symposium on Theory of computing. pp. 218–229. ACM, New York, NY, USA (1987)
15. Goldwasser, S., Micali, S.: Probabilistic encryption. Journal of Computer and System Sciences 28(2), 270 – 299 (1984), http://www.sciencedirect.com/science/article/B6WJ0-4B4RWB9-17/2/3926c7a6afdab2e2dda0b6fdead72b4e

16. Gradwohl, R., Livne, N., Rosen, A.: Sequential rationality in cryptographic protocols. In: Proceedings of the 2010 IEEE 51st Annual Symposium on Foundations of Computer Science. pp. 623–632. FOCS '10, IEEE Computer Society, Washington, DC, USA (2010)
17. Halpern, J.Y., Pass, R.: Game theory with costly computation. Proceedings of the Behavioral and Quantitative Game Theory on Conference on Future Directions BQGT 10 pp. 1–1 (2008)
18. Izmalkov, S., Micali, S., Lepinski, M.: Rational secure computation and ideal mechanism design. In: Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science. pp. 585–595. FOCS '05, IEEE Computer Society, Washington, DC, USA (2005)
19. Jiang, W., Clifton, C.: Ac-framework for privacy-preserving collaboration. In: Proceedings of the Seventh SIAM International Conference on Data Mining, April 26-28, 2007, Minneapolis, Minnesota, USA. SIAM (2007)
20. Katz, J.: Bridging game theory and cryptography: Recent results and future directions. In: Canetti, R. (ed.) TCC. Lecture Notes in Computer Science, vol. 4948, pp. 251–272. Springer (2008)
21. Kol, G., Naor, M.: Games for exchanging information. In: Proceedings of the 40th annual ACM symposium on Theory of computing. pp. 423–432. STOC '08, ACM, New York, NY, USA (2008), http://doi.acm.org/10.1145/1374376.1374437
22. Lysyanskaya, A., Triandopoulos, N.: Rationality and adversarial behavior in multiparty computation. In: Dwork, C. (ed.) CRYPTO. Lecture Notes in Computer Science, vol. 4117, pp. 180–197. Springer (2006)
23. Naor, M., Pinkas, B., Sumner, R.: Privacy preserving auctions and mechanism design. In: EC '99: Proceedings of the 1st ACM conference on Electronic commerce. pp. 129–139. ACM, New York, NY, USA (1999)
24. Nash, J.: Non-Cooperative Games. The Annals of Mathematics 54(2), 286–295 (Sep 1951)
25. Paillier, P.: Public-key cryptosystems based on composite degree residuosity classes. In: EUROCRYPT'99: Proceedings of the 17th international conference on Theory and application of cryptographic techniques. pp. 223–238. Springer-Verlag, Berlin, Heidelberg (1999)
26. Pedersen, T.: Non-interactive and information-theoretic secure verifiable secret sharing. In: Feigenbaum, J. (ed.) Advances in Cryptology CRYPTO 91, Lecture Notes in Computer Science, vol. 576, pp. 129–140. Springer Berlin Heidelberg (1992)
27. Walras, L.: Élements d'Economie Politique or Elements of Pure Economics; translated by William Jaffe (1874)
28. Yao, A.C.: How to generate and exchange secrets. In: SFCS '86: Proceedings of the 27th Annual Symposium on Foundations of Computer Science. pp. 162–167. IEEE Computer Society, Washington, DC, USA (1986)

A Security under the AC-Framework

The Accountable Computing (AC) -framework [19] considers adversaries in the gap between the semi-honest and malicious models. The AC-framework guarantees that an honest party *can* catch malicious behavior (unlike Aumann's covert model, which requires that such behavior be caught); honest parties can choose not to verify that behavior is correct (thus saving computation), verify if they

do not trust the results, or probabilistically verify sufficiently often to ensure incentives for correct behavior. We now show that our protocol satisfies the conditions necessary under the AC-framework. As part of this, we formally prove that the protocol is secure under the semi-honest model (Theorem 2), as security under the standard semi-honest model is a requirement for satisfying security under the AC-Framework.

The definition as given by Jiang and Clifton [19] is as follows:

Definition 6. *(AC-protocol) An AC-protocol Φ must satisfy the following three requirements:*

1. ***Basic Security:*** *Without consideration of the verification process, Φ satisfies the security requirements of a SSMC-protocol (a SMC-protocol secure under the semi-honest model).*
2. ***Basic Structure:*** *The execution of Φ consists of two phases:*
   - ***Computation phase:*** *Compute the prescribed functionality and store information needed for the verification process.*
   - ***Verification phase:*** *An honest party (we name such a party as a prover hereafter) can succeed in verifying an accountable behavior.*
3. ***Sound Verification:*** *Φ is sound providing that the verification phase cannot be fabricated by a malicious party.*

We now demonstrate that Φ satisfies all requirements of the AC-framework.

Theorem 2. ***Basic Security*** *Given an adversary $\mathcal{A}$'s private inputs $I_{\mathcal{A}}$ and output $O_{\mathcal{A}}$, $\mathcal{A}$'s view of the protocol can be efficiently simulated.*

Proof. We follow the simulation proof of semi-honest security characterized by Goldreich [13]. Consider the case where $\mathcal{A}$ is a buyer. With the exception of $\mathcal{A}$'s private input and the result of Φ, all messages are encrypted with the seller's public key of an additively homomorphic encryption scheme $\mathcal{E}$. It follows naturally that a simulator could generate and send a series of random elements in $\mathbb{Z}^*_{n^2}$ to $\mathcal{A}$. The encryption scheme $\mathcal{E}$ is semantically secure, which implies that $\mathcal{A}$ is unable to distinguish the random elements of $\mathbb{Z}^*_{n^2}$ from true encryptions. Thus, $\mathcal{A}$'s view of Φ is efficiently simulatable. Consider next the case where $\mathcal{A}$ is the seller. $\mathcal{A}$ sees only the final message $E_S(p_i)$, which is the output of the protocol. Thus, $O_{\mathcal{A}} = E_S(p_i)$ can be efficiently simulated by encrypting the final result p_i with the seller's public key (known to the seller/simulator) to get $E_S(p_i)$. Thus, Φ does not reveal any additional information to $\mathcal{A}$ through the intermediary messages.

Lemma 3. *(Basic Structure: Computation) Φ stores sufficient information to support the verification phase.*

Proof. In the case of the seller S, the initial price $p_{initial}$ as well as all internal coin tosses used for encryption are stored. In the case of a buyer, the committed (e.g. Pedersen's scheme [26]) coefficients, all encrypted price updates, as well as all internal coin tosses are stored.

Lemma 4. *(Basic Structure: Verification) An honest party in Φ can succeed in verifying an accountable behavior while revealing only that information in β.*

Proof. Let T_Φ represent the entire protocol transcript. Consider the case where an honest buyer b_l wishes to demonstrate accountable behavior. In this case, all intermediate prices p_i are revealed. A verifier uses the internal coin tosses of b_l to reconstruct $E_S(\mu_{b_l}(p_i))$. For each committed coefficient c_l, we reconstruct $E_S(\mu b_l(p_i)) \in T_\Phi$ by computing $\Pi_{j=1}^{t} E_S(c_l)^{p_i}$ using the internal coin tosses of b_l. The encryptions of $E_S(\mu_{b_l}(p_i))$ will have *identical representations* in $\mathbb{Z}^*_{n^2}$, as they were generated with the same randomness. Thus, the encrypted elements can be compared bitwise for equality. If the price updates of $b_l \in T_\Phi$ match the reconstructed values, b_l demonstrates accountable behavior. Consider the case of the seller S. A seller needs to demonstrate that the final decrypted price $p^r = D_S(E_S(p^r))$ in the final round is equal to the *reported* final price p_r^*. Any verifier can compute a seller verification value $V_S = E_S(R_2 \cdot (R_1 - p_r)) = (E_S(p_r) \cdot E_S(-R_1))^{R_2}$, where R_1, R_2 are chosen uniformly at random from $\mathbb{Z}_n$, and ask S to decrypt the value. If $R_2 \cdot (R_1 - p_r) = R_2 \cdot (R_1 - p_r^*)$, the seller demonstrates accountable behavior. Each buyer signs $E_S(p_r)$ to prevent a dishonest buyer from recanting in order to falsely implicate an honest seller.

Theorem 3. *Φ satisfies the sound verification phase.*

Proof. Consider the case of a malicious buyer b_m. If any of b_m's price updates were not computed using the committed coefficients of b_m's utility function, the reconstructed encrypted update will not match the update in T_Φ. Further, there does not exist a series of coin tosses that allow b_m to represent an altered update $E_S(\mu^*_{b_m}(p_i))$ as the actual update $E_S(\mu_{b_m}(p_i)) \in T_\Phi$, as this would prevent deterministic decryption.Thus, no malicious buyer b_m can forge a legitimate verification. In the case of a malicious seller S_m, the blinded value of p_r prevents S_m from constructing a response $V'_S \neq V_S$ such that some p_r^* can be reported in lieu of the actual equilibrium price p_r.

Theorem 4. ***Basic Structure (buyer)*** *Let Φ represent Protocol 5.1 for the Walrasian Auction problem. Assuming an honest majority, an honest buyer can be verified by any honest party (including an independent verifier) other than the seller.*

Proof. The verifier is provided with the commitment of coefficients by all buyers (with the majority agreeing). The buyer b_l being verified provides their input and output values of each round; the following buyer b_{l+1} also provides their input for each round. b_l also provides the random value used in encryption during each round. The verifier can then duplicate the calculations of b_l, ensuring that the output of each round is consistent with the committed coefficients. If not, b_l is dishonest.

If the output reported by b_l does not match the input reported by b_{l+1}, then either b_l is dishonest, or b_{l+1} is reporting an incorrect value to the verifier. In the latter case, b_{l+1} can be required to verify, if it succeeds, then b_l is dishonest.

Theorem 5. ***Sound Verification (buyer)*** *A rational malicious buyer b_l cannot fabricate verification provided b_{l+1} is honest.*

Proof. If b_{l+1} correctly reports the value received from b_l, then b_l must provide the same value to the verifier, and this must be the value generated from b_l's input. Generating this input from the output violates the assumption that the encryption is semantically secure. If b_l uses an incorrect input in the protocol (thus generating a matching output, but not following the protocol), the actual value and thus the impact on the outcome is completely unpredictable due to the security of the encryption, violating the assumption of a rational party.

Lemma 5. *Φ computes the equilibrium value of the Walrasian Auction model and stores sufficient information for verification to occur.*

Proof. Note that given the set $V = \{E_S(p_{initial}), E_S(w_{initial})\}$ and the seller S's private decryption key D_S, the entire protocol can be executed by a participating-party. By revealing D_S, the seller only exposes the verification set V and no other private data. Given this, the participating-party can verify the correctness of the output of Φ by retrieving the demand $x_i - x_p$ from the remaining buyers through a trivial protocol (where x_p is the demand of the participating-party performing the verification). The participating-party is thus able to execute Φ to verify the correctness of the equilibrium price p^*.

Theorem 6. ***Accountability (seller)*** *A rational seller S will not behave dishonestly in Φ.*

Proof. This follows from the proof of Theorem 1, as the seller's input has no effect on the final equilibrium price.

Given the previous two lemma's, we can conclude that Φ satisfies the *Basic Structure* condition.

Theorem 7. ***Sound Verification*** *The verification phase of Φ cannot be fabricated by a malicious party.*

Proof. At the beginning of Φ, the seller S distributes the set V, where $V = \{E_S(p_{initial}), E_S(w_{initial})\}$ to all buyers $b \in B$. It follows naturally that once this commitment is made, the seller is unable to alter the commitments. Should the seller provide an erroneous decryption key $D_S^* \neq D_S$, the commitments will decrypt to values $p^*_{initial} \neq p_{initial}$ and $w^*_{initial} \neq w_{initial}$ which defeats the seller's intention to fabricate the verification. Thus, we can conclude that the seller cannot succeed in fabricating the result of the verification process.

With this, we can conclude that our protocol is secure under the AC-framework, thus enabling malicious behaviour to be caught and contractual incentives put into place to ensure that semi-honest behavior is incentive compatible.