CERIAS

The Center for Education and Research in Information Assurance and Security

PURDUE UNIVERSITY

Privacy Preserving Tâtonnement

A Cryptographic Construction of an Incentive Compatible Market

John Ross Wallrabenstein and Chris Clifton

Department of Computer Science, Purdue University

Walrasian Auction Market

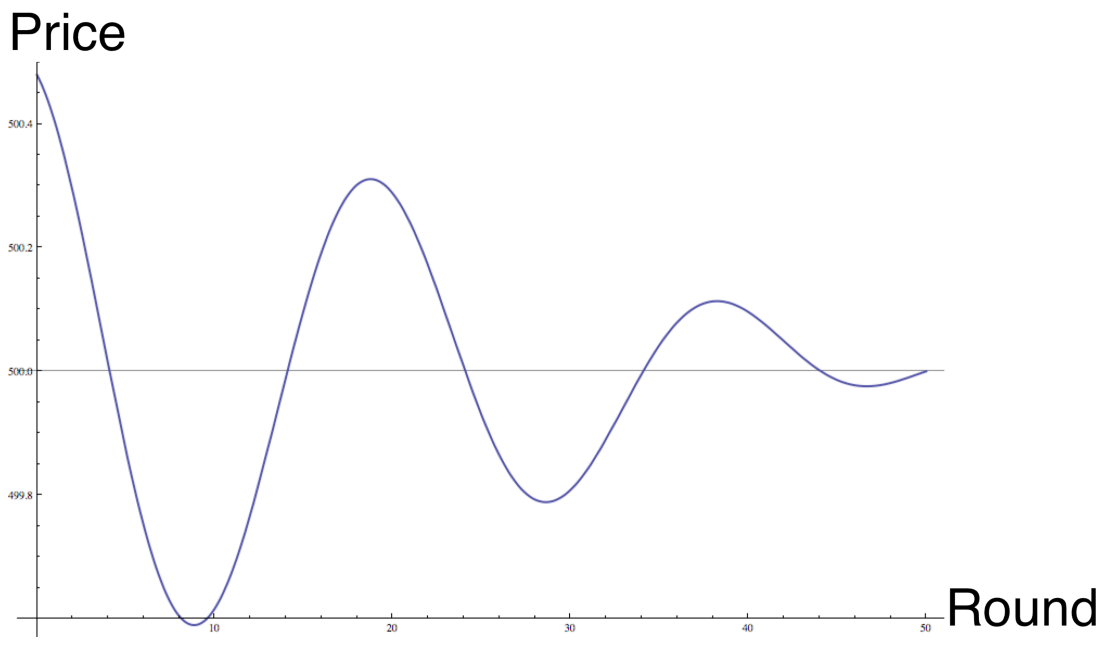
Theory of General Equilibrium

Goal: Reach Equilibrium Price

- Sellers distribute goods
- Buyers purchase some quantity

Tâtonnement mechanism

•A "Hill Climbing" approach



Utility Functions

- Describe a player's preferences
- Specify a *quantity* for all *prices*

$$\mu(price) \mapsto quantity\ demanded$$

Protocol

- Sellers set the initial price
- Buyers *pledge* quantity at price
- Equilibrium sets the final price

Real World Market Applications

- Tokyo Grain Exchange (*itayose*)

Debate on Applicability

- Walker, *J. Political Economy* 1987
- Are dynamic markets modeled?
- Are static markets modeled?

Obstacles

Real World Paradox

- Disallows trade outside of equilibrium
- Demand is revealed through trade

Convergence Bounds

- When is equilibrium reached?

Privacy Concerns

- Utility functions are private
- Evaluation reveals information

Solution

Provable Convergence Bounds

- Cole and Fleischer, *STOC* 2008
- Price Update Rule for each round

$$p_i \leftarrow p_i + \frac{1}{2^{\lceil \log_4 r_i \rceil}} p_i \cdot min\{1, \frac{x_i - w_i}{w_i}\}$$

$$x_i = quantity\ demanded(p_i)$$

$$w_i = supply(p_i)$$

Secure Multiparty Computation

- Evaluate Price Update Rule using SFE
- Current price remains private
- Utility functions remain private

Solves Real World Paradox

- Trade *only* occurs after completion
- Evaluating utility *simulates* trade
- Price adjusted obliviously
- All model restrictions satisfied

Collusion

- SMC Protocol is collusion resilient
- Market is now *incentive compatible*

Incentive Compatibility

Definition

- No party gains by deviating
- Players report *true* utility function
- Usually only possible in limited models

Reward from Deviating

$$r_i = \begin{cases} p_i - p_i^* & : u_i^* > u_i \\ 0 & : u_i^* = u_i \\ p_i^* - p_i & : u_i^* < u_i \end{cases}$$

Other Utility Factors

$$\mu_{\tau,i} \in \{1,-1\} = reward\ from\ trade$$

$$\mu_q \in \{1,-1\} = quantity\ control\ benefit$$

$$\rho_i = r_i + \mu_{tau} + \mu_q$$

Total Payoff Matrix

	a'_u	a'_t
a_u	(1,1)	(-1,2)
a_t	(2,-1)	(1,1)

Theorem: The strategy of truthfully reporting an agent's utility function, for all buyers and sellers, weakly dominates the strategies of under-inflating or over-inflating the utility function.

Key Insight: Any coalition member gains by reporting a slightly higher demand than other coalition members.

CERIAS

Discovery Park e-Enterprise Center