Secure Multi-attribute Procurement Auction

Koutarou Suzuki[1] and Makoto Yokoo[2]

[1] NTT Information Sharing Platform Laboratories, NTT Corporation,
1-1 Hikari-no-oka, Yokosuka, Kanagawa, 239-0847 Japan
suzuki.koutarou@lab.ntt.co.jp
[2] Faculty of Information Science and Electrical Engineering, Kyushu University,
6-10-1 Hakozaki, Higashi-ku, Fukuoka, 812-8581 Japan
lang.is.kyushu-u.ac.jp/~yokoo/
yokoo@is.kyushu-u.ac.jp

Abstract. In this paper, we develop a secure multi-attribute procurement auction, in which a sales item is defined by several attributes called qualities, the buyer is the auctioneer (e.g., a government), and the sellers are the bidders. We first present a Vickrey-type protocol that can be used for multi-attribute procurement auctions. Next, we show how this protocol can be executed securely.

Keywords: Procurement auction, Vickrey auction, security, privacy.

1 Introduction

Internet auctions have become an integral part of Electronic Commerce and a promising field for applying game-theory and information security technologies. Also, electronic bidding over the public network has become popular for procurement auctions. Since these auction procedures can be efficiently carried out, they have been introduced very rapidly and will be used more widely in the future.

Current research on auctions is focusing mostly on models in which price is the unique strategic dimension, with some notable exceptions [2]. However, in many situations, it is necessary to conduct negotiations on multiple attributes of a deal. For example, in the case of allocating a task, the attributes of a deal may include starting time, ending deadline, accuracy level, etc. A service can be characterized by its quality, supply time, and risk involved, in case the service is not supplied on time. Also, a product can be characterized by several attributes, such as size, weight, and supply date.

In this paper, we develop a secure multi-attribute procurement auction, in which a sales item is defined by several attributes called quality, the buyer is the auctioneer (e.g., a government), and the sellers are the bidders. Our goal is to develop a protocol in which acting honestly is a dominant strategy for sellers and that does not leak the true cost of the winner, which is highly classified information that the winner wants to keep private.

We first present a Vickrey-type protocol that can be used for multi-attribute procurement auctions. In this protocol, acting honestly is a dominant strategy

A.S. Patrick and M. Yung (Eds.): FC 2005, LNCS 3570, pp. 333–335, 2005.

for sellers and the resulting allocation is Pareto efficient as shown in Section 2. Next, we show how this protocol can be executed securely, i.e., the protocol does not leak the true cost of the winner, which is highly classified information that the winner wants to keep private in Section 3.

2 Proposed Vickrey-Type Protocol

First, we describe the model of a multi-attribute procurement auction. This model is a special case of [4], in which multiple tasks are assigned.

- There exists a single buyer 0, a set of sellers/bidders $N = \{1, 2, \ldots, n\}$, and a task to be assigned to a seller/bidder.
- For the task, quality $q \in Q$ is defined. We assume there is a special quality $q_0 \in Q$, which represents the fact that the task is not performed at all.
- Each bidder i privately observes his type θ_i, which is drawn from set Θ. The cost of bidder i for performing the task when the achieved quality is q is represented as $c(\theta_i, q)$. We assume c is normalized by $c(\theta_i, q_0) = 0$.
- The gross utility of buyer 0 when the obtained quality is q is represented as $V(q)$. We assume V is normalized by $V(q_0) = 0$.
- The payment from the buyer to a winning seller/bidder i is represented as p_i. We assume each participant's utility is quasi-linear, i.e., for winning seller i, his utility is represented as $p_i - c(\theta_i, q)$. Also, for the buyer, her (net) utility is $V(q) - p_i$.

Please note that although only one parameter q is used to represent the quality of the task, it does not mean our model can handle only one-dimensional quality. We don't assume q is one-dimensional. For example, q can be a vector of multiple attributes.

The proposed Vickrey-type protocol is described as follows.

- Each bidder i submits a pair (q_i, b_i), which means that if he performs a task with quality q_i, the resulting social surplus is b_i. If the bidder acts honestly, he should choose $q_i = \arg\max_q V(q) - c(\theta_i, q)$ and $b_i = V(q_i) - c(\theta_i, q_i)$.
- The buyer 0 chooses i^* so that b_i is maximized, i.e., $i^* = \arg\max_i b_i$. The buyer 0 allocates the task to bidder i^* with quality q_{i^*}.
- The payment p_{i^*} to bidder i^* is defined as: $p_{i^*} = V(q_{i^*}) - b_{2nd}$, where $b_{2nd} = \max_{j \neq i^*} b_j$.

We can consider this protocol to be a special case of the Vickrey-Clarke-Groves-based protocol presented in [4]. However, in the protocol described in [4], a bidder needs to fully expose his private information θ_i. In this protocol, we can avoid the full exposure of types. By this modification, the protocol becomes easier to implement securely.

Please note that if all bidders act honestly, payment p_{i^*} is equal to $V(q^*) - [V(q^*_{\sim i}) - c(\theta_{j^*}, q^*_{\sim i})]$, where $(q^*_{\sim i}, j^*) = \arg\max_{j \neq i^*, q} V(q) - c(\theta'_j, q)$, i.e., $(q^*_{\sim i}, j^*)$ is the second-best choice when the task is not allocated to bidder i^*. We can

assume that the payment to bidder i^* is equal to the increased amount of the social surplus except for i^* caused by the participation of i^*.

For the proposed Vickrey-type protocol, the following theorems hold.

Theorem 1. *In the multi-attribute procurement auction protocol, for each bidder i, acting honestly, i.e., reporting $q_i = \arg\max_q V(q) - c(\theta_i, q)$ and $b_i = V(q_i) - c(\theta_i, q_i)$, is a dominant strategy.*

Theorem 2. *The multi-attribute procurement auction protocol is individually rational both for the sellers and the buyer.*

Theorem 3. *The multi-attribute procurement auction protocol is Pareto efficient in the dominant strategy equilibrium where each agent acts honestly.*

3 Secure Protocol

We propose two cryptographic protocols based on [1] and [3] that realize our procurement auction.

We can securely realize our procurement auction based on the M+1-st price auction in [1] using homomorphic encryption. In the bidding phase, bidder i bids the encryption of his price b_i and encryption $E(q_i)$ of his quality q_i. In the opening phase, winning bidder $i^* = \arg\max_i b_i$ and second highest price $b_{2nd} = \max_{j \neq i^*} b_j$ are computed by using the technique of [1]. Next, quality q_{i^*} of the winning bidder i^* is obtained by decrypting $E(q_i)$, and payment $p_{i^*} = V(q_{i^*}) - b_{2nd}$ is computed. The scheme is easy to make robust. However, the scheme is not efficient, i.e., its complexity is $O(np)$ where n and p are the number of bidders and prices, respectively.

We can also securely realize our procurement auction based on the secure auction in [3], where the auctioneer securely computes the circuit of auction using Yao's garbled circuit. We apply the secure auction circuit evaluation of [3] to the circuit of our procurement auction. The scheme is efficient, i.e., its complexity is $O(n \log(p))$. However, the scheme is difficult to make robust.

This suggests that, we can use the first protocol if strong security is needed, and the second protocol if p is large.

References

1. Masayuki Abe and Koutarou Suzuki. M+1-st price auction using homomorphic encryption. *Proceedings of Public Key Cryptography 2002*, 2002.
2. Yeon-Koo Che. Design cometition through multidimensional auctions. *RAND Journal of Economics*, 24(4):668–680, 1993.
3. Moni Naor, Benny Pinkas, and Reuben Sumner. Privacy preserving auctions and mechanism design. In *Proceedings of the First ACM Conference on Electronic Commerce (EC-99)*, pages 129–139, 1999.
4. Takayuki Suyama and Makoto Yokoo. Strategy/false-name proof protocols for combinatorial multi-attribute procurement auction. In *Third International Joint Conference on Autonomous Agents and Multi-Agent Systems (AAMAS2004)*, 2004.