Journal of Southeast University (English Edition) Vol. 25, No. 1, pp. 132 – 137 Mar. 2009 ISSN 1003—7985

Privacy preserving supply chain quantity discount contract design

Xie Cuihua Zhong Weijun Zhang Yulin

(School of Economics and Management, Southeast University, Nanjing 211189, China)

Abstract: The development and deployment of privary preserving supply chain quantity discount contract design can allow supply chain collaborations to take place without revealing any participant's data to others, reaping the benefits of collaborations while avoiding the drawbacks of privacy information disclosure. First, secure multi-party computation protocols are applied in the joint-ordering policy between a single supplier and a single retailer, the joint-ordering policy can be conducted without disclosing private cost information of any of the other supply chain partners. Secondly, secure multi-party computation protocols are applied in the privacy preserving supply chain quantity discount contract design between a single supplier and a single retailer. The information disclosure analyses of the algorithm show that: the optimal quantity discount of the joint-ordering policy can be conducted without disclosing private cost information of any of the other supply chain partners; the above protocol can be implemented without mediators; the privacy preserving quantity discount algorithm can be mutually verifiable and has solved the problem of asymmetric information.

Key words: supply chain; quantity discount; privacy preserving

A number of researchers have proposed models in which quantity discounts are used for achieving efficient transactions between a seller and a homogeneous group of buyers with constant demand[1-4].

But most of the solutions either assume the existence of a central planner who has all the information about the system, or assume that each participant of the computation shares all of his information with the other participants. These solutions are problematic when the data are sensitive and the participants are reluctant to share their private information[5].

Secure multi-party computation (SMC)[6-8] provides a framework that enables supply-chain partners to make decisions achieve systematic goals without revealing the private information of any of the parties, and without the aid of a "trusted third party", even though the jointly-computed decisions require the information of all the parties.

In this paper, secure multi-party computation protocols are applied in the privacy preserving supply chain quantity discount contract design between a single supplier and a single retailer. The novel parts of this work are as follows: 1) The optimal quantity discount of the joint-ordering policy can be conducted without disclosing private cost information of any of the other supply chain partners; 2) The above protocol can be implemented without mediators; 3) The privacy preserving quantity discount algorithm can be mutually verifiable and has solved the problem of asymmetric information; 4) A group of secure two-party protocols are constructed, such as a secure two-party real add-product protocol, a secure two-party division protocol, and a secure two-party exponential function computation protocol.

Received 2008-09-08.

Biographies: Xie Cuihua (1979—), male, graduate; Zhang Yulin (corresponding author), male, doctor, professor, zhangyl@seu.edu.cn.

Foundation item: The National Natural Science Foundation of China (No. 70771026).

Citation: Xie Cuihua, Zhong Weijun, Zhang Yulin. Privacy preserving supply chain quantity discount contract design[J]. Journal of Southeast University (English Edition), 2009, 25(1): 132 – 137.

1 Problem Description

First, we make the usual assumptions that the seller's inventory policies can be described by the widely used economic order quantity (EOQ) model based on the assumptions of deterministic demand and zero lead time, and no stock outs. Secondly, the retailer's selling price and demand will not change when the supplier offers the quantity discount. Thirdly, we assume that the supplier offers an all-unit quantity discount with a single price break point. The supplier is assumed to purchase the item from another supplier.

1.1 Individual optimal policy

We begin our analysis with a review of the situation from the retailer's point of view. Then the retailer's total annual inventory related cost is

$$T_b(Q) = PD + \frac{DA_b}{Q} + \frac{HPQ}{2} \tag{1}$$

where T_b is the retailer's cost function; P is the current delivered unit price paid by the buyer; D is the total yearly number of units demanded by the retailer (equal to that demanded by his customers); A_b is the retailer's ordering cost per order; Q is the retailer's ordering size per order; H is the retailer's yearly unit inventory holding cost, expressed as a percentage of the value of the item.

With no price breaks offered, only the last two terms in Eq. (1) fluctuate with the buyer's choice of Q. Application of the well-known Wilson lot sizing formula[9] will therefore minimize the buyer's overall total cost specifically, we can assume that with no price discounts available, the retailer initially orders.

$$Q^* = \sqrt{\frac{2DA_b}{HP}} \tag{2}$$

where Q^* is the retailer's optimal ordering size per order.

Substituting Eq. (2) into Eq. (1), we can also infer the retailer's total inventory related expenses as

$$T_b^* = PD + \sqrt{2DA_bHP}$$

Under the current no-discount policy, the supplier's yearly net accounting profits are given by

$$\pi_s = (P - c)D - \frac{A_sD}{Q} + \frac{iPQ}{2} \tag{3}$$

$$\frac{\partial \pi_s}{\partial p} = D + \frac{iQ}{2} > 0,\ \frac{\partial \pi_s}{\partial Q} = \frac{iP}{2} + \frac{A_s D}{Q^2} > 0 \tag{4}$$

where π_s is the retailer's profit function; c is the unit cost to the supplier of purchasing the item; A_s is the supplier's ordering cost per order; i is the supplier's annual inventory carrying charge, expressed as a fraction of the dollar value.

The supplier's profit increases with the increase in its price and retailer's order quantity, so the supplier has the incentive to raise its price and encourage the retailer to increase orders.

1.2 Jointly optimal policy

The systematic profits with joint orders for any order size Q is produced as follows:

$$\pi_j = \pi_s + \pi_b = (P_s - c)D - \frac{(A_s + A_b)D}{Q} - \frac{(H - i)PQ}{2} \tag{5}$$

where π_b is the retailer's profit function, and P_s is the retailer's selling price per unit.

By setting the first derivative of this profit function with respect to Q equal to zero, we obtain

$$Q^{**} = \sqrt{\frac{2D(A_s + A_b)}{P(H - i)}} \tag{6}$$

For $A_s + A_b \geqslant A_b$, $H - i \leqslant H$,

$$Q^{**} = \sqrt{\frac{2D(A_s + A_b)}{P(H - i)}} \geqslant Q^* = \sqrt{\frac{2DA_b}{HP}} \tag{7}$$

where Q^{**} is the jointly optimal ordering size per order without quantity discounts.

With the systematic point, Q^{**} is the jointly optimal order quantity for the same price P. The largest systematic profit is
obtained at this time, therefore, $\pi_j(Q^{**}) > \pi_j(Q^*)$. For retailers, Q^* is the optimal order quantity, so $T_b(Q^{**}) > T_b(Q^*)$, which means that the systematic profits can increase by increasing orders, but the retailer has increased the cost of these orders. This requires the supplier to design a mechanism in order to encourage the retailer to increase independent decision-making order quantity Q^* to joint order quantity Q^{**}, while ensuring $T_b(Q^{**}) \leqslant T_b(Q^*)$. The supplier achieves this goal by quantity discounts.

1.3 Quantity discount design

By setting the first derivative of this profit function (5) with respect to Q equal to zero,

$$\frac{\partial \pi_j}{\partial Q} = \frac{i - H}{2}\left(\frac{dP}{dQ}Q + P\right) + \frac{(A_s + A_b)D}{Q^2} = 0 \tag{8}$$

We obtain

$$\frac{dP}{dQ} = \frac{2(A_s + A_b)D}{Q^3(H - i)} - \frac{P}{Q} \tag{9}$$

Solving differential Eq. (9), we obtain

$$P = \frac{a}{Q} - \frac{M}{Q^2} \tag{10}$$

where a is constant.

$$M = \frac{2(A_s + A_b)D}{H - i}(= PQ^{**2}) \tag{11}$$

When $P = P_0$, $Q = Q^{**}$, where P_0 is the price per unit charged by the supplier before using quantity discounts, $a = P_0 Q^{**} + M/Q^{**}$; then we obtain a quantity discount formula,

$$P = \begin{cases} P_0 & Q < Q^{**} \\ P_0 \dfrac{Q^{**}}{Q} + \dfrac{M}{QQ^{**}} - \dfrac{M}{Q^2} & Q \geqslant Q^{**} \end{cases}$$
$$M = \frac{2(A_s + A_b)D}{H - i}(= P_0 Q^{**2}) \tag{12}$$

1.4 Profit distribution

In this section, we use the methods of profit distribution used in Ref. [10].

The retailer will choose a greater order quantity than Q^* when the cost is not higher than that of adopting the quantity discount, so part of the increased profits must be given to the retailer. The profit distribution of the newly created value is not asymmetrical, which is decided by the forces of both sides in contract.

To set up $\bar{Q}$ as a discount starting point of the quantity discount, r is the profit delivered from the supplier to the retailer. The designed quantity discount should guarantee that the retailer's profit increases r after making a discount (equivalent to reducing r in the cost), then

$$r = T_b(Q^*) - T_b(\bar{Q}) = T(Q^*) - \left[P(\bar{Q})D + \frac{DA_b}{\bar{Q}} + \frac{H\bar{Q}P(\bar{Q})}{2}\right] \tag{13}$$

From Eq. (13), we obtain

$$P(\bar{Q}) = \frac{T_b(Q^*) - r - DA_b/\bar{Q}}{D + H\bar{Q}/2} \tag{14}$$

From Eqs. (12), (13) and (14), we obtain

$$P(\bar{Q}) = \frac{T_b(Q^*) - r - DA_b/\bar{Q}}{D + H\bar{Q}/2} = P_0\left(\frac{Q^{**}}{\bar{Q}} + \frac{M}{Q^{**}\bar{Q}} - \frac{M}{\bar{Q}^2}\right) \tag{15}$$

Simplification of Eq. (15) leads to a new equation:

$$\left[T_b(Q^*) - r - \frac{1}{2}\left[P_0 Q^{**} + \frac{M}{Q^{**}}\right]H\right]\bar{Q}^2 - \left[DA_b + \left(P_0 Q^{**} + \frac{M}{Q^{**}}\right)D - \frac{HM}{2}\right]\bar{Q} + MD = 0 \tag{16}$$

Let

$$\left.\begin{aligned} m &= T_b(Q^*) - r - \frac{1}{2}\left[P_0 Q^{**} + \frac{M}{Q^{**}}\right]H \\ n &= \left[DA_b + \left(P_0 Q^{**} + \frac{M}{Q^{**}}\right)D - \frac{HM}{2}\right] \end{aligned}\right\} \tag{17}$$

Simplification of Eq. (16) leads to a new equation:

$$m\bar{Q}^2 - n\bar{Q} + MD = 0 \tag{18}$$

Solving Eq. (18),

$$\overline{Q}_{1,2} = \frac{-n \pm \sqrt{n^2 - 4mMD}}{2m} \tag{19}$$

When $n^2 - 4mMD \geqslant 0$, Eq. (18) has solutions. The minimums of r can be solved by $n^2 - 4mMD \geqslant 0$. Q_1, Q_2 are the left and the right sides, respectively, in Q^{**}, which guarantees the retailer to share the increased profits and make the supplier's profits increase because of increasing the order quantity. Quantity discount turns into

$$P = \begin{cases} P_0 & Q < Q^{**} \\ P_0 \dfrac{Q^{**}}{Q} + \dfrac{M}{QQ^{**}} - \dfrac{M}{Q^2} & Q \geqslant Q^{**} \end{cases} \tag{20}$$

r is the profit delivered from the supplier to the retailer, and it is realized through the quantity discount. We can find out that r is an internal profit distribution mechanism, and quantity discount is a systematic optimization mechanism. The joint use of the two mechanisms can achieve systematic optimization profit, and ensure that the retailer's and the supplier's profits increase.

Above solutions either assume the existence of a central planner who has all the information about the system, or assume that each participant of the computation shares all of his information with the other participants. These solutions, however, are problematic when the data are sensitive and the participants are reluctant to share their private information.

In the following section, we apply SMC protocols to the quantity discounts for the joint-ordering policy between a single supplier and a single retailer. Our primary goal is to demonstrate that the joint-ordering policy can be conducted without disclosing the private cost information of any supply chain partners.

Before providing our final algorithms, we give some definitions as follows:

Definition 1 Privacy preserving optimal joint-ordering quantity algorithm

Inputs: The retailer supplies $\pi_b = (P_s - P)D - DA_b/Q - HQP/2$, where H, A_b are the retailer's private cost information.

The supplier supplies $\pi_s = (P - c)D - A_sD/Q + iPQ/2$, where i, A_s are the supplier's private cost information.

Outputs: The retailer and the supplier learn the optimal joint-ordering quantity Q^* and nothing else.

Definition 2 Privacy preserving quantity discount design algorithm

Inputs: The retailer supplies $\pi_b = (P_s - P)D - DA_b/Q - HQP/2$, where H, A_b are the retailer's private cost information.

The supplier supplies $\pi_s = (P - c)D - A_sD/Q + iPQ/2$, where i, A_s are the supplier's private cost information.

Outputs: The retailer and the supplier learn $\overline{Q}$ and discount price P_d and nothing else, where $\overline{Q}$ is a price break point of the quantity discount, and P_d is the unit cost whenever the ordering size is larger than or equal to $\overline{Q}$.

2 Building Blocks

In this paper, we assume that all the parties are semi-honest; informally speaking, a semi-honest party is one who follows the protocol properly with the exception that it keeps records of all its intermediate computations and might send the records to an adversary.

Before providing our final protocols we give sub-protocols in order to make the presentation of the final protocols easy to understand.

A group of secure two-party protocols are constructed as follows:

Protocol 1 Secure two-party real product protocol

The secure two-party scalar product protocol as an important building block in solving the secure multi-party scalar product problems will be dealt with later in this paper. This protocol is first presented in Ref. [11], and the application in Refs. [12 – 14].

Let the dimensionality of a vector $n = 1$, we have a secure multi-party real product protocol.

Inputs: A_1 has a private real x_1, and A_2 has a private real x_2.

Outputs: A_1 gets r_1, and A_2 gets r_2, where $r_1 + r_2 = x_1x_2$.

Privacy: Neither party is willing to disclose its own input to anybody else.

Protocol 2 Secure two-party add-product protocol

A_1 has two real (x_1, y_1), A_2 has two real (x_2, y_2). A_1 wants to get real r_1 and A_2 wants to get real r_2, such that $r_l + r_2 = (x_1x_2)(y_1 + y_2)$. If A_j is honest, then only A_j knows r_j.

Inputs: A_1 has two real (x_1, y_1); A_2 has two real (x_2, y_2).

Outputs: A_1 gets r_1 and A_2 gets r_2, such that $r_1 + r_2 = (x_1x_2)(y_1 + y_2)$.

Privacy: Neither party is willing to disclose its own input to an adversary.

Step 1 A_1, A_2 use a two-party real product protocol, A_1 gets R_1 and A_2 gets R_2, such that $R_1 + R_2 = x_1x_2$.

Step 2 A_1 has two real (R_1, y_1); A_2 has two real (R_2, y_2).

① For $j = 1, 2$, A_j conducts the following sub-step:

For $j = 1, 2$, A_j and $A_s (s = 1, 2;\ s \neq j)$ use a two-party real product protocol. A_j gets r_{js} and A_s gets u_{sj}, $r_{js,}$ u_{sj} such that $r_{js} + u_{sj} = R_j y_s$.

② A_1 independently computes $r_1 = r_{12} + r_{21} + R_1y_1$, A_2 independently computes $r_2 = u_{12} + u_{21} + R_2y_2$.

Step 3 A_1 gets r_1 and A_2 gets r_2, such that $r_1 + r_2 = (R_1 + R_2)(y_l + y_2) = (x_1x_2)(y_1 + y_2)$.

Analysis of the protocol: This protocol only uses two-party product protocols, and the privacy is to all appearance.

Protocol 3 Secure two-party division protocol

A_1 has two real (A, H) and A_2 has two real (a, h). A_1 wants to get real r_1 and A_2 wants to get real r_2, such that $r_1 + r_2 = (A + a)/(H + h)$, If A_j is honest, then only A_1 knows r_1, only A_2 knows r_2.

Inputs: A_1 has two real (A, H); A_2 has two real (a, h).

Outputs: A_1 gets r_1 and A_2 gets r_2, such that $r_1 + r_2 = (A + a)/(H + h)$.

A_1 holds two cost values (A, H) and A_2 holds two cost values (a, h).

Step 1 A_1 generates a random number u_1, and A_2 generates a random number u_2;

Step 2 A_1 and A_2 use a secure two-party real add-prod-

uct protocol. A_1 gets r_1 and A_2 gets r_2, where $r_1 + r_2 = (U_1 U_2)(A_b + A_s)$.

Step 3 A_1 and A_2 use a secure two-party real add-product protocol, A_1 gets m_1, A_2 gets m_2, where $m_1 + m_2 = (U_1 U_2)(H + h)$.

Step 4 A_1 sends m_1 to A_2, A_2 computes $m = m_1 + m_2$, and A_2 sends m to A_1.

Step 5 A_1 and A_2 independently compute $s_1 = r_1/m$, $s_2 = r_2/m$, such that $s_1 + s_2 = r_1/m + r_2/m = (r_1 + r_2)/m = (r_1 + r_2)/(m_1 + m_2) = (U_1 U_2)(A_b + A_s)/(U_1 U_2)(H + h) = (A_b + A_s)/(H + h)$.

Analysis of the protocol:

1) Information disclosure The security in step 2 and step 3 depends on protocol 2. In step 5, the computation is independent. So, the computation is private. Now, we discuss the security in step 4.

Any one or two participant parties can know the following equations:

$$r_1 + r_2 = (U_1 U_2)(A_b + A_s) \tag{21}$$

$$m = m_1 + m_2 = (U_1 U_2)(H + h) \tag{22}$$

For A_1(supplier), there are five unknown real: r_2, U_2, A_s, m_2 and h(r_1, U_1, A_b, m_1, and H). One cannot learn the secret input of other participant. This protocol avoids the threat of collusion since there is no mediator.

2) Computational complexity The protocol uses a doubly secure two-party real add-product protocol.

Protocol 4 Secure two-party exponential function computation protocol

The exponential function is $y = x^a$, where a is a real, x is variable, and y is the exponential function of x.

A_1 has a real x_l and A_2 has a real x_2. A_1 wants to get r_l and A_2 wants to get r_2, such that $r_l + r_2 = (x_l + x_2)^a$. If A_j is honest, then only A_j knows r_j.

Inputs: A_1 has one private real x_1, and A_2 has one private real x_2.

Outputs: A_1 gets r_1 and A_2 gets r_2, where $r_l + r_2 = (x_t + x_2)^a$.

Privacy: Neither party is willing to disclose its own input to an adversary.

Step 1 A_1 and A_2 generate a random real p_1 and p_2, respectively.

Step 2 A_1 and A_2 use a secure two-party add-product protocol. Let A_1 get u_1 and A_2 get u_2, such that $u_1 + u_2 = p_l p_2 (x_1 + x_2)$.

Step 3 A_1 sends u_1 to A_2 and A_2 sends u_2 to A_1.

Step 4 A_1 computes $w_1 = (u_1 + u_2)^{\frac{a}{2}}/p_1^a = p_1^{-\frac{a}{2}} p_2^{\frac{a}{2}} (x_1 + x_2)^{\frac{a}{2}}$ and A_2 computes $w_2 = (u_1 + u_2)^{\frac{a}{2}}/p_2^a = p_1^{\frac{a}{2}} p_2^{-\frac{a}{2}} (x_1 + x_2)^{\frac{a}{2}}$.

Step 5 A_1 and A_2 use a secure two-party real product protocol. Let A_1 get r_1 and A_2 get r_2, such that $r_1 + r_2 = w_1 w_2 = (x_1 + x_2)^a$.

Analysis of the protocol:

1) Information disclosure In step 1 and step 4, the computation is independent. So, the computation is private. The security in step 2 depends on protocol 2. In step 5, the security depends on protocol 1.

Any one or two participant parties can know the following equations:

$$u_1 + u_2 = (p_1 p_2)(x_1 + x_2)$$

$$r_1 + r_2 = w_1 w_2 = (x_1 + x_2)^a$$

For A_1(or A_2), there are three unknown real: p_2, x_2, r_2(p_l, x_l, r_1). One cannot learn the secret input of other participants.

2) Computational complexity: The protocol uses a once secure two-party real add-product protocol and a once secure two-party product protocol.

More discussion about secure multi-party elementary function computation protocols can be found in Ref. [15].

3 Privacy Preserving Supply Chain Quantity Discount Contract Design

The existence of a semi-honest mediator suffers from the threat of collusion. In the following section, we present algorithms without mediators. The algorithms only require communication between the retailer and the supplier.

Algorithm 1 Privacy preserving optimal joint-ordering quantity algorithm

Inputs: The retailer supplies $\pi_b = (P_s - P)D - DA_b/Q - HQP/2$, where H, A_b are the retailer's private cost information. The supplier supplies $\pi_s = (P - c)D - A_s D/Q + iPQ/2$, where i, A_s are the supplier's private cost information.

Outputs: The retailer and the supplier learn the optimal joint ordering quantity Q^* and nothing else.

It is assumed that $\pi(\pi_b, \pi_s)$ is only a function which requires inputs π_b from the buyer and π_s from the seller. It is possible to compute $\pi(\pi_b, \pi_s)$ independent of the variables of π_b, π_s; i. e. the variables' values do not impact the form of the solution function $\pi(\pi_b, \pi_s)$. So the formula of the optimal joint-ordering quantity Q^* can be achieved without the values of the variables.

So, the formula of the optimal joint-ordering quantity Q^* is public to the seller and the buyer. Where

$$\pi(\pi_b, \pi_s) = \pi = \pi_b + \pi_s = (P_s - c)D - \frac{(A_s + A_b)D}{Q} - \frac{H - i}{2}PQ$$

$$\pi_b = (P_s - P)D - \frac{DA_b}{Q} - \frac{H}{2}QP$$

$$\pi_s = (P - c)D - \frac{A_s D}{Q} + \frac{i}{2}PQ$$

We obtain $Q^* = \sqrt{2D(A_s + A_b)/P(H - i)}$. So the retailer and the supplier's goals are to compute the formula of the optimal joint-ordering quantity Q^* without disclosing their private cost information.

The buyer and the seller's goals are just to compute $(A_s + A_b)/(H - i)$ for $2D/P$ which is public information.

The retailer holds two cost values(H, A_b) and the supplier holds two cost values (i, A_s).

Step 1 When the retailer and the supplier use the secure

two-party division protocol 3, the retailer gets r_1 and the supplier gets r_2, where $r_1 + r_2 = (A_b + A_s)/(H + (-i))$.

Step 2 The retailer independently computes $u_1 = r_1 2D/P$, and the supplier independently computes $u_2 = r_2 2D/P$.

Step 3 The retailer and the supplier use the secure two-party exponential function protocol.

The retailer gets v_1 and the supplier gets v_2, where $v_1 + v_2 = \sqrt{u_1 + u_2} = \sqrt{(2D/P)(r_1 + r_2)} = \sqrt{(2D/P)(A_s + A_b)/(H - i)} = \sqrt{2D(A_s + A_b)/P(H - i)}$.

Analysis of the algorithm: The security in step 1 depends on protocol 3. In step 2, the computation is independent. So, the computation is private. The security in step 3 depends on protocol 4.

Any one or two of the participant parties can know the following equations:

$$r_1 + r_2 = \frac{A_b + A_s}{H + (-i)}, \quad v_1 + v_2 = \sqrt{\frac{2D(A_s + A_b)}{P(H - i)}}$$

For the retailer(or the supplier), there are four unknown real: $r_2, A_s, (-i), v_2(r_1, A_b, H, v_l)$. One cannot learn the secret input of other participants.

In this algorithm, Alice knows the value of Q^* and so does Bob. This scheme can be mutually verifiable and has solved the problem of asymmetry of information.

Algorithm 2 Privacy preserving quantity discount design algorithm

Inputs: The retailer supplies $\pi_b = (P_s - P)D - DA_b/Q - HQP/2$, where H and A_b are the retailer's private cost information.

The supplier supplies $\pi_s = (P - c)D - A_s D/Q + iPQ/2$, where i and A_s are the supplier's private cost information.

Outputs: The retailer and the supplier learn $\bar{Q}$ (a discount starting point of the quantity discount) and the discount price and nothing else.

The retailer holds two cost values (H, A_b) and the supplier holds two cost values (i, A_s).

Step 1 The retailer and the supplier use the privacy preserving optimal joint-ordering quantity algorithm, the retailer and the supplier get Q^{**} and $M(= P_0 Q^{**2})$.

Step 2 The retailer sends $\Delta TC = TC_b(Q^{**}) - TC_b(Q^*)$ to the supplier.

Step 3 The retailer and the supplier privacy preserving jointly decide r, the profit distribution of newly created profit, which is determined by the force of both the sides in the contract.

Step 4 The retailer and the supplier independently compute $\bar{Q}_{1,2}$(a discount starting point of the quantity discount) and the discount price.

Analysis of the algorithm: The security in step 1 depends on algorithm 1. In step 3, the retailer and the supplier can use an efficient solution[16] to decide r without disclosing their private information. In step 4, the computation is independent; so, the computation is private. Now, we discuss the security in step 2.

Any one or two participant parties can know the following equations:

$$v_1 + v_2 = \sqrt{2D(A_s + A_b)/P(H - i)}$$

$$\bar{Q}_{1,2} = \frac{-n \pm \sqrt{n^2 - 4mMD}}{2m}$$

where

$$m = PD + \frac{DA_b}{Q^*} + \frac{H}{2}PQ^* - r - P_0 Q^{**} H$$

$$n = DA_b + (P_0 Q^{**} + P_0 Q^{**})D - \frac{H}{2}P_0 Q^{**2}$$

$$M = \frac{2(A_s + A_b)D}{H - i} (= P_0 Q^{**2})$$

$$\Delta TC(= TC_b(Q^{**}) - TC_b(Q^*))$$

For the retailer, there are two unknown real: $A_s, (-i)$. One cannot learn the secret input of the supplier.

Proof 1) The retailer only knows $v_1 + v_2 = \sqrt{2D(A_s + A_b)/P(H - i)}$ from the supplier, and there are two unknown real: $A_s, (-i)$, one cannot learn the secret input of the supplier.

For the supplier, there are three unknown real: A_b, H, Q^*. One cannot learn the secret input of the retailer.

2) The supplier knows $v_1 + v_2 = \sqrt{2D(A_s + A_b)/P(H - i)}$ and $\Delta TC(= TC_b(Q^{**}) - TC_b(Q^*))$ from the retailer, and there are three unknown real: A_b, H, Q^*. One cannot learn the secret input of the retailer.

The algorithm only requires communication between the retailer and the supplier. In this algorithm, the retailer independently computes $\bar{Q}_{1,2}$ at the same time that the supplier does it. This scheme can be mutually verifiable and has solved the problem of asymmetry of information.

4 Conclusion

An efficient joint-ordering policy can require a trade-off between the decrease in the ordering and order-processing costs against a potential increase in the retailer's and the seller's holding costs. Most of the solutions either assume the existence of a central planner who has all the information about the system, or assume that each participant of the computation shares all of his information with the other participants. These solutions, however, are problematic when the data are sensitive and the participants are reluctant to share their private proprietary information.

In this paper, we develop and apply secure SMC protocols to the privacy preserving supply chain quantity discount contract design between a single supplier and a single retailer.

The development and deployment of supply chain quantity discount contract designs can allow supply chain collaborations to take place without revealing any participant's data to the others, thus, reaping the benefits of collaboration while avoiding the drawbacks.

References

[1] Kohli R, Park H A. Cooperative game theory model and quantity discounts [J]. *Management Sci*, 1989, **35**(6): 693 – 707.

[2] Dolan R J. A normative model of industrial buyer response to quantity discounts [C]//*Research Frontiers in Marketing: Dialogues and Directions*. Chicago: American Marketing Association, 1978: 121 – 125.

[3] Lal R, Staelin R. An approach for developing an optimal discounts pricing policy [J]. *Management Sci*, 1984, **30**(12): 1524 - 1539.
[4] Dada M, Srkanth K N. Pricing policies for quantity discounts [J]. *Management Sci*, 1987, **33**(10): 1247 - 1252.
[5] Lee H L, Whang S. Information sharing in a supply chain [J]. *Int J Tech Management*, 2000, **20**(3): 373 - 387.
[6] Yao A. Protocols for secure computations [C]//*The* 23*rd Annual Symp on the Foundations of Computer Science*. Chicago, 1982: 160 - 164.
[7] Goldreich O. Secure multi-party computation [EB/OL]. (2006-08-06) [2008-04-30]. http://www.wisdom.weizmann.ac.il/~oded/pp.html.
[8] Atallah M J. Elmongui H G, Deshpande V, et al. Secure supply chain protocols [C]//*IEEE International Conference on Electronic Commerce*. Newport Beach, California, USA, 2003: 293 - 302.
[9] Harris F W. How many parts to make at once [J]. *Factory, the Magazine of Management*, 1913, **10**(2): 135 - 136; 152.
[10] Peng Zuohe, Tian Peng. Supply chain quantity discount contract design under perfect information [J]. *Journal of Industrial Engineering and Engineering Management*, 2006, **20**(2): 114 - 116. (in Chinese)
[11] Atallah M J, Du W L. Secure multiparty computational geometry [C]//*WADS*2001: *Seventh International Workshop on Algorithm and Data Structures*. Providence, Rhode Island, USA, 2001: 165 - 179.
[12] Du W L. A study of several specific secure two party computation problems [D]. West Lafayette: Purdue University, 2001.
[13] Du W L, Atallah M J. Privacy preserving cooperative statistical analysis [C]//*Annual Computer Security Applications Conference*. New Orleans, Louisiana, USA, 2001: 102 - 110.
[14] Luo Wenjun, Li Xiang. A study of secure multi-party statistical analysis [C]//*Proceedings of the* 2003 *International Conference on Computer Networks and Mobile Computing*. Shanghai, China, 2003: 377 - 383.
[15] Luo Wenjun, Li Xiang. A study of secure multi-patty elementary function computation protocols [C]//*Proceedings of the Third International Conference on Information Security* (*Infosecu*'04). Shanghai, China, 2004: 5 - 12.
[16] Li Shundong, Dai Yiqi, You Qiyou. An efficient solution to Yao's millionaires' problem [J]. *Acta Electronica Sinica*, 2005, **33**(5): 769 - 773. (in Chinese)

私有信息保护的供应链数量折扣契约设计

谢翠华　仲伟俊　张玉林

(东南大学经济管理学院,南京 211189)

摘要:私有信息保护的供应链数量折扣契约设计,实现了供应链伙伴之间的协作,同时避免了各自私有信息泄漏的风险. 首先,将安全多方计算技术应用于一个供应商一个销售商供应链成本最小的联合经济订货批量计算;其次,将安全多方计算技术应用于一个供应商一个销售商供应链系统成本最小的数量折扣契约设计. 算法的信息泄漏分析表明:供应链成本最小的联合经济订货批量计算,在没有泄漏计算各参与方私有信息的情况下能够实现;上述计算过程由于没有协议第三方,所以不存在合伙腐败风险;所给出的私有信息保护的供应链数量折扣契约设计算法,计算各参与方能够相互证明,解决了信息不对称的问题.

关键词:供应链;数量折扣;私有信息保护

中图分类号:C931