INSTITUTE OF FOOD AND RESOURCE ECONOMICS
UNIVERSITY OF COPENHAGEN

MSAP Working Paper Series

No. 07/2010

Efficient and Confidential Reallocation of Contracts: How The Danish Sugar Industry Adapted to The New Sugar Regime

Peter Bogetoft

Department of Economics

Copenhagen Business School

Kurt Nielsen

Institute of Food and Resource Economics

University of Copenhagen

Efficient and Confidential Reallocation of Contracts:

How The Danish Sugar Industry Adapted to The New Sugar Regime

Peter Bogetoft [1] and Kurt Nielsen[2]

Abstract: *The first Danish exchange for sugar beet contracts was established in January 2008. It was also the world's first major application of a particular new technology, secure multiparty computation (SMC), which ensures the security and cost-effectiveness of such exchanges. The technology can also be used in a number of other applications, including voting, negotiations, and benchmarking. The SMC approach makes it possible to combine private knowledge from a large number of players without ever revealing their individual knowledge. This provides unique opportunities for individual players to act together despite conflicting interests and decentralized knowledge, which, in many contexts, constitute the primary obstacle to the creation of economic gains. This exchange was the culmination of a novel and successful collaboration between economists and cryptologists, and it constitutes a successful operations research project using novel scientific methods to solve a real, large-scale problem. This article describes the background for and the implementation of the exchange and discusses some other potential applications.*

Keywords: double auction, secure multiparty computation, sugar beets, data envelopment analysis (DEA)

JEL Classification: C61 - D51 - L23 - Q13

Acknowledgements: This work builds in part on a research project called SIMAP that was sponsored by the Danish Council for Strategic Research. The Center for the Foundation of Electronic Markets (CFEM) is an extension of this research.

1. Introduction

Farmers and the processing industry have both common and conflicting interests. On the one hand, there is a common interest in creating large-scale, integrated profits by minimizing the cost of production and product processing and by maximizing revenues from the sale of the processed products. On the other hand, conflicts of interest arise in the distribution of integrated profits. This is obvious when the processing occurs via external investors, but it is also true to some extent when the producers themselves handle the processing. The reason for this is that different groups of producers may each

[1] Department of Economics, Copenhagen Business School CBS, Porcelaenshaven 16 A, 2000 Frederiksberg, Denmark. E-mail pb.eco@cbs.dk.

[2]Institute of Food and Resource Economics, Faculty of Life Sciences, University of Copenhagen, Rolighedsvej 25, 1958 Frederiksberg C, Denmark. E-mail kun@foi.dk.

want a large portion of the integrated profit at the expense of other groups; see for example Bogetoft and Olesen (2004, 2007).

The combination of common and conflicting interests is especially problematic when the parties' attempts to gain a greater share of the integrated profit causes this to fall. This problem is well known in economic theory; the best possible outcome under asymmetric information is often ex-post inefficient. This phenomenon is clearly demonstrated in simple buyer-seller models. A buyer may be tempted to understate a product's value to a seller so as to exaggerate its value. This may cause certain trades to fail even if the item in question is actually worth more to the buyer than to the seller.

In this article, we show how a well-coordinated central market for contracts may help various actors pursue common interests despite the simultaneous existence of conflicting interests. At the same time, we show how the use of the latest research and developments in cryptography makes it easy and inexpensive to set up such markets. We illustrate the importance of this latter consideration by using the case of sugar beet production in Denmark and describing the establishment of an exchange for trading sugar beet contracts.

2. Coordination, Motivation, and Contracts

In order to maximize integrated profits, we must solve two basic problems: coordination and motivation.

Coordination has to do with getting the right producers to produce products with the right qualities in the right quantities at the right time. Coordination is also about optimizing processing and marketing such that the right quantities are processed at the right factories and made into the right products to be sold in the right markets. The "right" quantities, products, or markets in the above contexts are those that minimize costs and maximize revenue. Coordination is a difficult task in itself because the full system must be optimized and not just the individual parts (sub-optimizing).

Motivation is about ensuring that a plan is implemented: i.e., that the parties in the system have private incentives to undertake their respective tasks. The problem of motivation can be addressed in many ways. First, one should ensure that the relevant players have an incentive to participate. An individual or subgroup of individuals should not be able to find better positions by going solo. Second, we must ensure that each participant has personal incentives to share its private information with the other participants and that their private interests encourage them to jointly work towards the "coordinated plan."

A variety of coordination and motivation mechanisms are used in any economic system and, particularly, in the agricultural sector. Sometimes, there are natural or historic markets for a product. This is often the case when there are many sellers and many buyers of a product and when the product is well defined and homogeneous across the buyers and sellers; however, there is typically some market concentration either on the sellers' or the buyers' side. Furthermore, the products exchanged are typically

complicated because they are supplied in certain quantities and with certain qualities at certain times. In such cases, coordination and motivation are typically regulated by contracts.

Production contracts grant special rights, obligations, allowances, and deductions to the parties involved. Bogetoft and Olesen (2002, 2004) give a detailed description of contract design as intended to ensure coordination and motivation while minimizing the involved transaction costs. In addition, Bogetoft and Olesen (2007) describe how these efforts interact with the distribution of the integrated profit.

3. The Distribution of Production Contracts

The individual contract, as discussed above, focuses on the coordination and motivation of the individual producer and the processing firm. The distribution of contracts across producers (farmers) is another major concern.

The distribution will be to the benefit of all if the contracts are allocated to the producers who value them the most. This means, all other things being equal, that the contracts should be awarded to the producers who have the lowest production costs, including the alternative cost of foregoing other crops.

It is essential and potentially challenging to ensure and continuously maintain an optimal allocation of production contracts. This is probably why there seems to be significant potential value in the redistribution of production in several sectors, including the sugar sector. Such gains are particularly attractive because, in principle, they are freely available, i.e., they require no extra effort but ensure that the right producers receive the contracts.

One of the challenges that is associated with ensuring optimal contract allocation is the political problem of deciding who should capitalize on the value of the contracts and who should bear the risk of processing changes. We will not discuss such issues in any detail; however, we note that restrictions on distribution can be incorporated into the auction mechanism.

Another set of problems relates to asymmetric information. The value of a production contract to a given farmer is private information. That is, only the individual farmer can estimate the value of having the right and obligation to produce a given quantity and quality of goods at a given time with reasonable accuracy. The privacy of information can be reduced through analyses and benchmarking across producers, but, ultimately, there is a significant amount of private information that others cannot immediately verify or estimate. This raises a fundamental motivation problem because one cannot expect that any producer will reveal the true value of a contract unless it maximizes his own profits.

An additional challenge is that contract value typically evolves over time and that these changes differ from one farmer to another. This means that reasonable allocation should be ensured through ongoing reallocation, which, itself, must be conducted in an easy and

cost efficient way.

In what follows, we look at how contract exchanges can be a useful tool for addressing these problems and ensuring the ongoing reallocation of production.

The premise of a contract exchange is to establish a central market. An optimal market would typically involve a double auction that is based on sealed bids and asks. In the optimal double auction, each participant has the opportunity to submit multiple bids for buying and multiple asks for selling, i.e., they can submit full demand and supply curves. It might be that a producer will sell a certain amount of his contracts at a given price but will buy up more contracts at a lower price. For a detailed discussion of the importance of allowing multiple bids and asks, see Bogetoft, Nielsen, and Olesen (2003).

With given supply and demand curves, a double auction is simple to undertake: asks for selling are sorted in an increasing order (i.e., from the lowest to the highest price), whereas bids for buying are sorted in a decreasing order (i.e., from the highest to the lowest price offer). The market-clearing price is now the price at which the demanded quantity equals the supplied quantity. At higher prices, there is excess supply, whereas at lower prices, there is excess demand. All trade occurs at the market-clearing price. Sellers must sell the quantity stated in the asks that are below the market-clearing price, whereas buyers must buy the quantity stated in the bids that are above the market-clearing price. Figure 1 illustrates this phenomenon below.

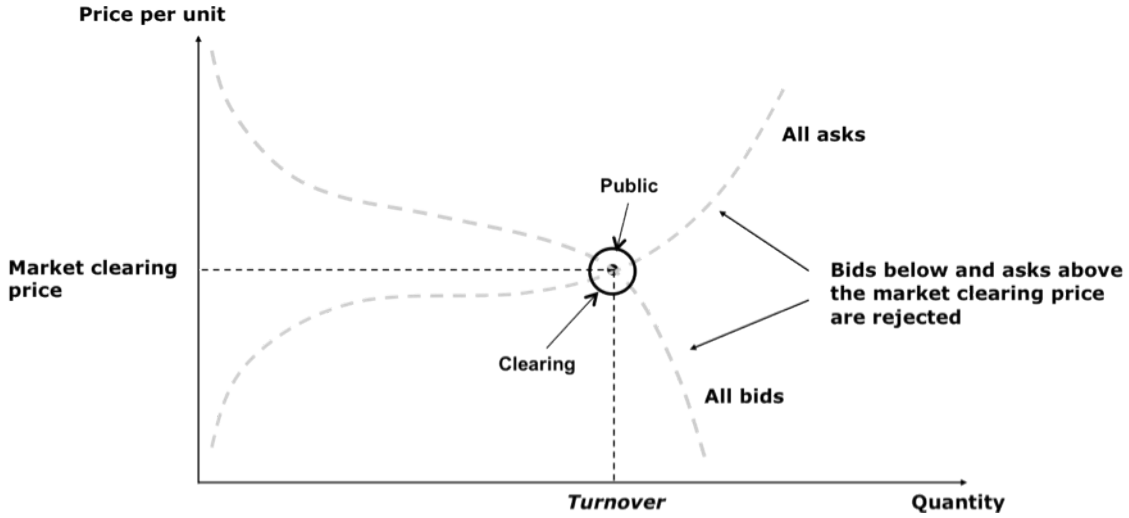

Figure 1: Illustration of the double auction.

It is worth noting that the bids and asks primarily determine whether a participant ends up buying, selling, or not trading at all. Each participant has only a very small impact on the market-clearing price, which influences the optimal way of forming bids and asks. Even when there are only a few participants, it appears in theory as well as practice that each participant typically cannot influence the price to his or her own benefit. It is, therefore,

optimal to let the bids and asks reflect the true value of getting and losing contracts.

This makes it easy to trade on a double auction. Each participant should consider his own situation and determine the value of having the right to a certain kind of production. One does not have to speculate on the number of other participants or what they intend to bid.

The fact that it is best to state the true value explains why the auction is optimal for the industry as a whole: production will be reallocated such that no producer is left with higher-value production and no producer will miss production that has a lower value to others. In this way, the double auction creates the greatest increase in aggregate profit for the industry as a whole.

It is clear that for the redistribution to proceed as described in a double auction, we must be confident that the established rules for determining the market-clearing price are followed.

Moreover, it may be important to ensure that supply and demand curve information is exclusively used to determine the auction outcome. It might, for example, weaken the producers' position in subsequent negotiations regarding contract issues if the processing firm had a sense of who would pay what. The processors could use such information to push producers to give up a greater part of the overall profit in future adjustment processes. Similarly, individual producers might worry that their private bids or asks would be familiar to other producers that might use this to their advantage in future negotiations regarding contract design: for example, negotiations regarding which groups of producers should have certain bonuses and the sizes of these bonuses.

Both compliance with the exchange rules and the minimal release of information are best achieved through a so-called trusted third party (TTP), i.e., an agent that takes on the role of a neutral mediator between parties with conflicting interests. Normally, the exchange is handled by an auction house, a stock exchange, or an audit and consultancy house that may see its reputation damaged if the rules are not followed or if information is leaked. In this paper, we describe a new approach that is fundamentally different and typically less expensive.

4. The Design of The Trusted Third Party

The focus of our research project, SIMAP, combines economics and basic cryptography research in order to design an ideal trusted third party. In this section, we provide a brief introduction to applied cryptography, which is referred to as secure multiparty computation (SMC). Bogetoft et al. (2009) present the technical characteristics of the exchange that is used to reallocate sugar beet contracts in Denmark.

SMC allows us to construct a TTP that confidentially coordinates private information according to a comprehensive protocol. The notion of a TTP has been a common construct in information economics since the original work on *The Revelation Principle*: see, e.g., Gibbard (1973) or Myerson (1979). Based on the revelation principle, any

equilibrium outcome that is based on any mechanism can also be arranged as the outcome of a direct revelation game in which the participants have an incentive to honestly reveal their private information; however, while economic theory has little to say about the design of such a TTP, it has been a central research question in computer science for decades. Unlike traditional cryptography, which focuses on preserving privacy within a group of individuals with full access to information, recent contributions break with the idea of placing all trust in a single entity at any time. This field is known as *distributed cryptography*, and *SMC is a theoretical solution that allows a number of parties to jointly perform computation on private inputs without releasing other information than what has been agreed upon a priori.* The seminal aspects of this concept can be traced back to Shamir (1979), and the theory was founded in the 1980s: see, e.g., Goldreich (1988), Ben (1988), and Chaum (1988); however, the involved ideas have only recently been refined and made applicable in practice: see, e.g., Bogetoft et al. (2005), Bogetoft et al. (2009), and Malkhi (2004).

In order to explore how secure multiparty computation works, consider the following simplified problem of adding the two privately held numbers *a* and *b*.

Under so-called public-key cryptography, the sender and receiver have separate keys, one to lock, which is called the public key, and one to unlock, which is called the secret key. The system works much like a padlock; everyone can lock (encrypt) but only the holder of the secret key can open (decrypt). Assuming that the secret key is *c* and the encryption function is effectively $E(x) = c^x$, a TTP can, therefore, receive the encrypted information c^a and c^b from the holders of *a* and *b*. If we multiply the encrypted numbers, we get c^{a+b}. Therefore, we can calculate on encrypted numbers. Now, in order to understand the final results, we must know *c* in order to convert c^{a+b} into *a*+*b*; however, if we know *c*, we can also calculate the private information *a* and *b* based on the encrypted information, and this will not protect the private information. The key *c* should, therefore, be kept secret or should be split into pieces such that we need several pieces to actually construct *c*. This is done in SMC by making it necessary for the partial key-holders to collaborate in the calculations.

In order to see how a secret key *c* can be shared, we can consider it as the solution to a linear function $f(0) = c$. Let $f(x_1) = y_1$ and $f(x_2) = y_2$ be two random function values. Now, by knowing only one of the two numbers (x_1, y_1) or (x_2, y_2), we have no information about *c*; however, if we know both, we can determine *c*. Had $f(.)$ been a second-degree polynomial, any two points would not reveal anything about *c* whereas three points would. This approach is known as (n,t) secret-sharing, wherein *n* is the number of distributed points and *t* is the largest number of points that does not reveal any information about the private inputs. With *n* TTPs, *t+1* is the number of TTPs it takes to use (or misuse) the system. In other words, it requires collaboration between at least t+1 of the selected TTPs. Figure 1 depicts an illustration that estimates a third-degree polynomial below.

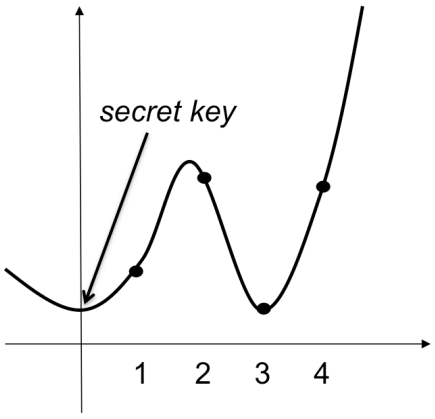

Figure 1 Sharing a secret.

Figure 2 illustrates an SMC system with $n = 5$ and $t = 2$. The participants (to the left) submit encrypted inputs (bids), and the required computations are done in the network of servers that is constituted by the five TTPs (to the right). The administrator in the middle coordinates the predesigned protocol. The only information that is revealed is the results that are prescribed by the protocol. On the contract exchange, the result is a market-clearing price and a list of buyers and sellers and the quantities they are willing to trade at the market-clearing price.

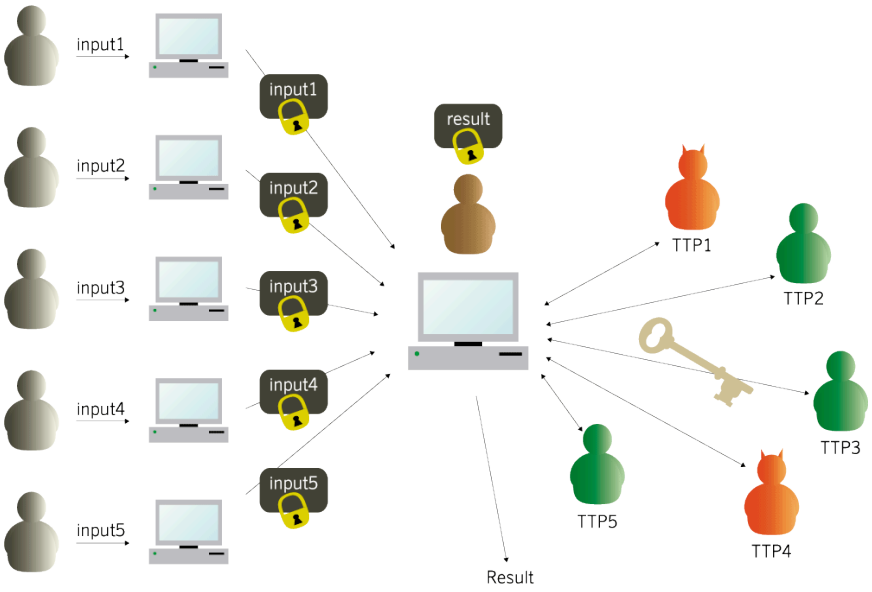

Figure 2 An illustration of an SMC system.

A fully functional SMC system can be used for basic operations, such as addition, subtraction, multiplication, division, and comparisons. While adding numbers is

relatively simple, as illustrated above, multiplication and particularly division and comparisons are more complicated. In order to better clarify this point, consider the slightly more difficult problem of multiplying two encrypted numbers *a* and *b*. As in the example with addition, let the encryption function be $E(x) = c^x$, where *c* is the distributed secret key, and let each of the five TTPs generate a random number $d_i, i \in (1,2,3,4,5)$. The d_is are encrypted and broadcast such that all TTPs can compute $E(d)$ via simple addition. Also, let all TTPs compute the encrypted value of $E(a) + E(d)$, and let the results $a + d$ be decrypted. These results reveal nothing because no one knows either *a* or *d*. Using the number (*a*+*d*), TTP_1 computes the private number $a_1 = (a + d) - d_1$, and the remaining TTPs set their private numbers as $a_i = -d_i, i \in (2,3,4,5)$. Finally, each TTP computes $E(a_i \cdot b)$ by simply adding $E(b)$ a_i times. Now, adding these five encrypted numbers yields the number we are looking for, ab:

$$\sum_{i=1}^{5} E(a_i b) = \prod_{i=1}^{5} c^{a_i b} = c^{a_1 b + a_2 b + a_3 b + a_4 b + a_5 b} = c^{((a+d)-d_1)b - d_2 b - d_3 b - d_4 b - d_5 b} = c^{ab}$$

Based on this example, multiplying requires more coordination between the TTPs; however, the most complicated operations are comparisons, which require significantly more coordination between the TTPs. When we compare two numbers, the complexity depends on the size of the numbers to be compared (understood as the number of bits required to represent the numbers). For example, comparing two 32-bit integers in an SMC setting with n=3 and t=1 and takes approximately one second; see e.g. Bogetoft (2006). This is a fairly long period of time in some problems, and this lack of efficiency makes it difficult to solve some problems using SMC; however, when the goal is to solve a sealed bid auction, there is sufficient time for the computations. Also, R&D in SMC algorithms and hardware such as processors and communication techniques continuously improve the applicability of SMC.

Let us now return to the overall properties of the SMC system, i.e., the choice of the *n* TTPs and the threshold of *t*. The number of TTPs that are required to reveal the confidential inputs can be arbitrarily chosen. It may in fact be possible to set the threshold such that all TTPs are required to run the SMC system. Furthermore, if we let each of the participants be a TTP, no one can collude the system without controlling all of the participants. This might be the ideal level of confidentiality; however, this setup does require that all of the participants participate so as to avoid system failure. Therefore, the choices for *n* and *t* require a tradeoff between availability (the SMC system must be operational) and confidentiality.

The SMC approach is analogous to paying a consultancy house to act as a single TTP; however, there are some fundamental differences between the two ways of coordinating confidential information:

1) With the SMC approach, no single person or institution gains access to confidential information, unlike when a consultancy house is used, wherein confidential information is revealed to some trusted person, which opens up room for human errors and bribes.

2) With SMC, trust is based on the intentions of the TTPs. Because collusion requires coordination between more TTPs, selecting TTPs with opposing interests strengthens trust. In contrast, when a consultancy house is used, opposing interests may lead to higher stakes and therefore more payoffs due to possible bribes.
3) With SMC, coordination is represented by a piece of software. Therefore, the marginal cost of repeating trusted coordination is lower than that achieved in a traditional scenario.

Because SMC limits the dissemination of private information to an absolute minimum, political questions regarding whom to trust are greatly simplified. This issue was acknowledged by the parties who were involved in developing and implementing the contract exchange: "The secure approach contributed positively to our decision to deploy Partisia contract exchange. Afterwards, it was of a greater importance for the growers than I initially thought it would be" (Private citation from the head negotiator of the farmers, Klaus Sørensen, Danish Sugar Beet Growers' Organization).

5. Sugar Production, EU Sugar Reform, and The SIMAP Contract Exchange: a Case Outline

The EU Sugar Reform and Denmark

The ongoing reform of the EU policy regarding sugar production was implemented from 2006 to 2009. When the reform was fully implemented in 2009, the price of white sugar had been reduced by 36% and the price of sugar beets by approximately 40%. Throughout the EU, this price reduction was crucial for both primary production and the processing of sugar beets. The different associated countries have adapted to the reform in different ways. In Denmark, three tactics have been used: 1) increasing productivity and redistributing contracts among sugar beet producers, 2) closing one of three processing plants, and 3) net utilization of the EU-organized reallocation process that involves the different EU member countries. This section primarily deals with the internal redistribution of sugar beet contracts in Denmark.

Previously, there were significant restrictions on the redistribution of sugar beet contracts, which led to the sub-optimal allocation of production. A minimum of two problems have been prominent: sub-optimal allocation among more or less efficient producers and sub-optimal geographical allocation in light of the remaining processing plants.

Before the introduction of a sugar beet contract exchange, we undertook a comprehensive empirical analysis of Danish sugar beet production. Among other things, we found that effective redistribution under the previous EU sugar regime could have more than doubled the farmers' aggregate profit: see Bogetoft, Boye, Neergaard-Petersen, and Nielsen (2007). These results are interesting because they suggest that even after the EU

reform, it remains possible to maintain a significant production of sugar beets if production is reallocated.

The analyses show that significant possible gains could be achieved by shifting sugar beet contracts from producers with high costs to producers with low costs, including transportation costs. The calculated gains were particularly interesting because the redistribution process did not require that the individual producers become more efficient, only that producers with high profitability produce more. Consequently, the gains can be realized very cheaply by creating an efficient market. On the other hand, the analysis also showed that the efficient redistribution of sugar beet contracts is a prerequisite for maintaining current production levels in Denmark.

Establishing a central market for sugar beet contracts

Based on the previously described reallocation study, it seems reasonable that Danisco and the Danish Sugar Beet Growers Association, in their trade agreement for 2006-2010, allowed more free trade of sugar beet contracts.

Interestingly, it was not sufficient to permit trade. It was also important to ensure easy and efficient trade. The market for sugar beet contracts is a new market with many sellers and buyers; however, as long as it is exclusively based on bilateral trade between farmers, searching and matching costs are high and the associated strategic behavior is considerable. It is not possible to obtain an overview of how much one can buy or sell at a given price. In such a market, prices are identified by buyers who are seeking one or more sellers with which to negotiate price and quantity. Sellers also do the same. The contacting and negotiation processes are time consuming, and it is hard to know when one has achieved a good deal. Given that there were approximately 3,000 potential buyers and sellers before opening the SIMAP Contract Exchange, the number of possible trades is infinitely large. Experience indicates that in a market that is based on bilateral trading, there will be trades at prices that are too high and too low, and both buyers and sellers will regret their trades when they hear about other trades. Others will not trade, even when doing so could be to the benefit of both parties, simply because they expect to earn more by finding other trading partners. Furthermore, it will be very difficult for a buyer to ensure the exact amount that is necessary to match his capacity constraints. In summary, the lack of transparency and coordination in a market that is exclusively based on bilateral trades will hamper trade and leave the industry unable to reap the benefits of reallocation.

Based on the above study and such information regarding the inefficiency of bilateral trades, the processor Danisco and the producers agreed to establish a genuine contract exchange. The contract exchange is, in principle, a simple mechanism, as explained above; however, in practice, there are, of course, a number of administrative routines that must be integrated. For example, it must be ensured that the farmers who choose to sell a given amount actually have this amount available based on their contracts.

The established contract exchange was not merely an innovation in the sense that an exchange had not previously been used to trade sugar beet contracts. Danisco and the

Danish Sugar Beet Growers Association also decided to implement the exchange using the new SMC technology. This was done as part of the SIMAP research project. Effectively, the Danish sugar beet contract exchange became the world's first platform for the use of the underlying cryptographic technology and concepts on a larger scale.

The SIMAP Contract Exchange

In the SIMAP contract exchange, confidentiality is based on a virtual third party that consists of Danisco, the Danish Sugar Beet Growers Association, and SIMAP (the research project). No member of the virtual third party has access to the submitted information at any time. Each of the three parties have one of three parts of a secret key that is used to calculate the market-clearing price and determine the buyers and sellers that trade at that price. The individual parts of the key cannot be used for anything. The system only works when the members of the virtual third party cooperate.

A buyer can submit up to five bids. Each bid expresses how much he wants to buy at the submitted price or less. More bids provide the producers with the opportunity to express different values for different contracted amounts based on vacant machine capacity, crop rotation, etc. For example, a producer can tell in advance that he wants a contract of 100 tons of sugar if the price is 700 or less and 300 tons if the price is 400 or less.

On the other side of the market, a seller was initially allowed to only submit one tender (ask) per contract. Each tender was the lowest price at which the contract would be sold. For example, a producer who has two contracts may choose to sell the first contract if the price is 1,200 or more and the second contract if the price is 1,500 or more. Today, the producers have only a single contract and may sell parts of the contracts. Therefore, a seller can now submit up to five bids where each bid expresses how much he wants to sell at the submitted price or more.

Each submission (bids and asks) contains confidential and private information regarding a producer's maximum willingness to pay for different contracted amounts or a producer's minimum selling requirements for different contracts. In addition to producers' general reluctance to reveal such information, there are also rational reasons for not revealing it. As described above, this kind of information may potentially be abused by others in future relationships. As previously mentioned, the SIMAP contract exchange takes these issues very seriously and offers a high level of confidentiality. The submitted bids are encrypted and remain encrypted forever.

In addition to specially handling the confidential information, the SIMAP contract exchange is based on IT from start to finish. In practice, this means that most producers directly submit their bids and asks from home and that all subsequent calculations are pre-programmed. This scenario also means that the repeated use of such auctions, which is appropriate to ensure the ongoing reallocation of production, are particularly cost-effective. Contract exchanges have occurred once or twice every year since the first iteration in 2008; they have, in recent years, been called the Partisia Contract Exchange, cf. www.partisia.com.

After the SIMAP contract exchange, the users were also asked to evaluate the exchange. The evaluation indicated that the farmers are experienced Internet users: 94% used online banking services and 59% used the Internet for purchases. The evaluation also stressed the importance of confidentiality. Approximately 78% "agreed" or "totally agreed" regarding the importance of safeguarding private bids and asks, whereas 86% were satisfied with the provided level of confidentiality. Table 1 summarizes these and other assessments below.

Table 1: An evaluation of the SIMAP contract exchange.

Questions:	**% "totally agree" or "agree"**
The SIMAP contract exchange makes it easy to trade sugar contracts	81%
It is important that my bids and asks are kept confidential	78%
In general, I am satisfied with the level of confidentiality that is supported by the SIMAP contract exchange	86%
It is simple to present bids and asks for buying and selling	81%
It is important to allow for multiple bids	62%
It is important to allow for both bids and asks	65%

Table 2 provides a few key figures from the four iterations of the exchange below. Therein, we see that the initial market-clearing price (MCP) was very low and considerably below the price that had been used in bilateral trades before the opening of the exchange. In later runs, the market-clearing price returned to somewhat higher levels. The turnover was considerably larger in the initial runs than in subsequent runs. A series of institutional details and specific events can be used to explain the developments that occurred over time; however, the single most important factor is that the market was essentially locked prior to the introduction of the exchange. The exchange managed to unlock the market and facilitate major reallocation efforts from the area in Denmark in which a processing plant was closed to other parts of Denmark that were closer to the remaining plants. "The contract exchange was an important element to ensure a fast adjustment to the new market situation that was a result of the EU sugar reform" (Private citation from the head negotiator of Danisco Sugar, Lars M. Petersen).

Table 2: Market-clearing price, turnovers, and the number of participants.

Exchange	**MCP (DDK)**	**Turnover (tons)**	**Bidders**	**Traders**
2008 (January)	1	52.000	1.200+	NA
2008 (August)	3	3.860	178	116
2009 (August)	501	481	117	17
2010 (August)	800	405	64	14

In the long run, changes in productivity may be two-fold and stem from actual productivity changes for individual producers and the continuous reallocation of existing contracts so as to exploit differences in individual productivity levels.

6. Conclusion

In order to ensure reasonable production in a modern agricultural sector as is the case in Denmark, optimal contracts are very important; they ensure the necessary coordination and motivation of individual farmers. Experience shows that Danish agriculture is well advanced in this regard, and Danish agricultural contracts, like those described in Bogetoft and Olesen (2004), are studied with interest abroad and in other industries.

It is not sufficient to optimize the relationship between individual producers and processors. It is also important to appropriately spread production among various different producers. An analysis of Danish sugar beet production has demonstrated significant untapped potential. We can expect similar potentials in other sectors in which the current redistributions of contracts have been hampered by political concerns or market obstacles.

Double auctions are useful to ensure the necessary ongoing reallocation of production. Using the latest SMC technology, this reallocation can be implemented with maximum confidentiality and at minimal cost. Auctions that are directly conducted over the internet are administratively simple, and it is easy for the participants to submit (or modify and resubmit) bids and asks. With this in mind, we suggest that such auctions may be valuable in many other sectors as well.

Secure multiparty computation (SMC) technology may ultimately emerge as useful not just in auctions but also in the context of mediation, bilateral trade, benchmarking, the matching of confidential databases, etc. The idea in all cases is that correctly combined private information from independent players can create value; however, this simultaneously requires that the individuals have reliable knowledge of what the information is used for.

The ideas developed before and during the SIMAP research project have been extended in different ways in other projects. In the area of basic research, the work continues in three areas: 1) further developments of the underlying concepts of cryptography, 2) an analysis of the technological implications of these ideas in relation to information economics, and 3) the development of a programming language for safe and effective implementation. Within the field of applied research, future work will focus on improving implementation efficiency and adapting the concept to specific applications. Finally, a commercial platform, Partisia Market Design, has been established in cooperation with The Alexandra Institute in Denmark to offer products like the SIMAP contract exchange.

References

Bogetoft, P., K. Boye, H. Neergaard-Petersen and K. Nielsen (2007), *Reallocating Sugar Beet Contracts: Can Sugar Production Survive in Denmark?*, European Review of Agricultural Economics, vol 34 (1) 1-20.

Bogetoft, P., D.L. Christensen, I.B. Damgaard, M. Geisler, T.Jacobsen, M. Krøigaard, J.D. Nielsen, J.B. Nielsen, K. Nielsen, J. Pagter, M Schwartzbach and T.Toft (2008), Multiparty Computation Goes Live, Cryptology ePrint Archive, Report 2008/068.

Bogetoft,P., I.B. Damgaard, T. Jacobsen, K. Nielsen, J. Pagter and T.Toft (2005), Secure Computation, Economy, and Trust - A Generic Solution for Secure Auctions with Real-world Applications, Basic Research in Computer Science report RS-05-18.

Bogetott, P., K. Nielsen, and H.B. Olesen, Single Bid Restriction in Milk Quota Exchanges, *European Review of Agricultural Economics*, 30, pp. 193-215, 2003.

Bogetoft, P. and H.B. Olsen, Ten Rule of Thumb in Contract Design: Lessons from Danish Agriculture, *European Review of Agricultural Economics*, 29, pp. 185-204, 2002

Bogetoft, P. and H.B. Olsen, Design of Production Contracts: Lessons from Theory and Agriculture, pp. 1-207, CBS-Press, 2004

Bogetoft, P. and H.B.Olsen, Cooperatives and payment schemes, pp. 1-245, CBS Press, 2007

CFEM homepage, www.cfem.dk

Milgrom, P., and J. Robert, Economics, Organization and Management, Prentice Hall, New Jersey, 1992.

SIMAP homepage, http://www.alexandra.dk/dk/projekter/Sider/SIMAP.aspx