

SIMAP KONTRAKTBØRS

– SIMPEL, EFFEKTIV OG SIKKER

HANDEL MED KONTRAKTER

Peter Bogetoft, Økonomisk Institut, Copenhagen Business School

Ivan Damgaard, Datalogisk Institut, Århus Universitet

Kurt Nielsen, Fødevarøkonomisk Institut, Københavns Universitet

Dan Lund Christensen, Jakob Pagter og Thomas Jakobsen, Alexandra Instituttet A/S

Danmarks første børs for sukkerroekontakter blev afholdt i januar 2008. Det var samtidigt verdens første større anvendelse af en ny teknologi, SMC (Secure Multiparty Computation), som muliggør simpel, billig og effektiv afvikling af sådanne børser. Teknologien og børsen, er i vid udstrækning udviklet af et dansk team af dataloger og økonomer i forskningsprojektet SIMAP (Secure Information Management and Processing) med støtte fra Det Strategiske Forskningsråd. Teknologien kan også bruges i en række andre forbindelser, fx afstemninger, forhandlinger, og benchmarking. SIMAP/SMC tilgangen gør det muligt at kombinere den viden, som mange aktører har, uden at den enkeltes aktørs viden nogensinde bliver kendt af andre end ham selv. Dette giver unikke muligheder for at handle i fællesskab på trods af modstridende interesser og decentraliseret viden, hvilket i mange sammenhænge er kerneproblemet ved skabelsen af økonomiske gevinster. I denne artikel beskrives dels baggrunden for og afviklingen af sukkerroe-børsen, og dels skitseres de videre perspektiver i SIMAP/SMC tilgangen, som vurderes at kunne tilføre landbrugssektoren betydelig værdi.

Indledning

Producenter af landbrugsprodukter og de direkte aftagere i den tilhørende forarbejdningsindustri har både fælles og modstriden-

de interesser. På den ene side er der en fælles interesse i at skabe en stor samlet (integreret) profit ved at minimere omkostningerne til produktion og forarbejdning af produkterne

og ved at maksimere salgsrevenue af de forarbejdede produkter. På den anden side er der typisk modstridende interesser når det drejer sig om fordelingen af den integrerede profit. Det gælder naturligvis når forarbejdningssleddet er investorejet, men det gælder også i nogen grad når forarbejdningssleddet er landmandsejet idet forskellige producentgrupper hver især kan ønske en så stor del af kagen som mulig, jf. fx Bogetoft and Olesen (2004, 2007).

Kombinationen af fælles og modstridende interesser er særlig problematisk fordi parternes forsøg på at skaffe sig en større del af den integrerede profit kan få denne til at falde. Det sker fx hvis en af producenterne overdriver omkostningerne ved en særlig justering og hvis forarbejdningsevirsomheden underdriver de markedsræssige potentialer i en sådan. Det kan resultere i at attraktive tilpasninger i producerede mængder og kvaliteter forbigås alene fordi de to grupper forsøger at forbedre deres forhandlingsposition, hvis justeringen skulle gennemføres. Fænomenet er velkendt fra simple handler. En køber kan fristes til at underdrive sin værdi og en sælger til at overdrive sin værdi af godet. Hermed kan det ende med, at en handel ikke gennemføres selvom godet reelt er mere værd for køber end sælger.

I denne artikel viser vi, hvorledes et veltilrettelagt centralt kontraktmarked kan være et nyttigt middel til at forfølge fælles interesser på trods af, at der samtidigt findes modstridende interesser. Samtidig viser vi hvorledes anvendelse af den nyeste forskning og udvikling indenfor kryptografi gør det nemt og billigt at etablere sådanne markeder. Vi illustrerer betydningen af dette med henvisning til den netop afviklede første dobbeltauktion for

sukkerroekontrakter, og vi skitserer hvorledes de nye metoder kan tænkes anvendt til etablering af andre mekanismer og institutioner, som kan fremme indtjeningen i landbruget.

Koordination og motivation og kontrakter

Maksimering af den integrerede profit kræver, hvad man i moderne økonomisk terminologi kalder koordination og motivation.

Koordination handler om at få de rigtige producenter til at producere de rigtige kvaliteter i de rigtige mængder på de rigtige tidspunkter. Det handler også om at optimere forarbejdningen og afsætningen, så de rigtige mængder ender på de rigtige fabrikker og at disse forarbejder produkterne rigtigt og afsætter dem på de rigtige markeder. »Rigtige« betyder i ovenstående sammenhænge henholdsvis omkostningsminimerende og omsætningsmaksimering. Koordinationen er i sig selv en vanskelig planlægningsopgave da det er helheden som skal optimeres og ikke de enkelte dele (sub-optimering).

Motivation handler om at sikre sig, at en plan implementeres, dvs. at de parter som indgår i systemet har private incitamenter til at påtage sig deres del af de koordinerede opgaver. Motivationsproblemet tager mange former. Dels skal man sikre sig at de relevante aktører har incitamenter til at deltage. De skal ikke kunne vinde ved at gå solo – evt. i fællesskab med andre. Dels skal man sikre, at de har private incitamenter til at dele deres private viden med fællesskabet og at de har private interesser i at arbejde målrettet mod den koordinerede »plan«.

Landbruget bruger en mangfoldighed af koordinations- og motivationsmekanismer. Nogle gange findes der naturligt eller histo-

risk et marked for et produkt. Det gælder typisk hvor der er mange sælgere og købere af produktet og når dette er veldefineret og homogent på tværs af købere og sælgere. I stigende grad er der dog en vis markeds-koncentration enten på sælger- eller købersiden, og de udvekslede produkter er komplicerede idet de skal have bestemte egenskaber og leveres i bestemte mængder og kvaliteter og på bestemte tidspunkter. I sådanne tilfælde sker koordinationen og motivationen typisk via produktionskontrakter.

Produktionskontrakter er den konkrete beskrivelse af de tiltag der skal sikre den ønskede koordinering og motivering. Dette gøres ved at tildele særlige rettigheder og pligter og særlige tillæg og fradrag til de involverede parter. Bogetoft og Olesen (2002, 2004) giver en indgående beskrivelse af design af produktionskontrakter ud fra et ønske om at sikre den ønskede koordinering og motivering – og at gøre det billigst muligt – dvs. at minimere de involverede transaktionsomkostninger. Bogetoft og Olesen (2007) beskriver samtidigt hvorledes dette spiller sammen med fordelingen af den integrerede profit, herunder hvorledes andelsselskabers betalingssystemer kan være mere eller mindre fremmende for branchens udvikling som helhed.

Fordelingen af produktionskontrakter

Hvor den enkelte kontrakt som nævnt ovenfor fokuserer på koordinering og motivering mellem den enkelte producent og aftager-virksomheden, er selve fordelingen af kontrakter mellem producenterne et andet centralt problem. Som udgangspunkt vil det være til fordel for alle, hvis kontrakterne tildeles de producenter, der har størst værdi af

dem. Det betyder alt andet lige at kontrakterne skal tildeles de producenter som har de laveste produktionsomkostninger, herunder alternativ omkostninger ved ikke at producere andre afgrøder.

Der er mange problemer med at sikre og løbende opretholde en optimal allokering af produktionskontrakterne. Det er formodentligt forklaringen på, at der tilsyneladende kan hentes betydelige værdier ved en omfordeling. Sådanne værdier er særligt attraktive fordi de i princippet er frit tilgængelige, dvs. det kræver ingen ekstra indsats men er alene et spørgsmål om at sikre at de rigtige producenter.

Et sæt af problemer er fordelingspolitiske og knytter sig til bl.a. til hvem der skal kapitalisere værdien af kontrakterne og hvem der skal bære risikoen for ændringer i forarbejdningsleddet. Vi skal ikke beskæftige os med dette spørgsmål her men blot konstatere, at sådanne begrænsninger kan indlægges i de SIMAP auktioner vi skal beskrive.

Et andet sæt af problemer knytter sig til, at viden om værdien af en produktionskontrakt typisk er privat information. Det vil med andre ord sige at det kun er den enkelte landmand som med rimelig præcision kender sin værdi af at have retten og pligten til at producere en given mængde og kvalitet på et givet tidspunkt. Den private information kan reduceres via analyser og benchmarking på tværs af producenter, men i sidste ende er der et væsentligt element af privat information, som andre ikke umiddelbart kan verificere eller vurdere. Det rejser et grundlæggende motivationsproblem, idet man ikke kan forvente, at en given producent vil afsløre sin sande værdi medmindre dette maksimerer hans egen profit.

Et tredje sæt af problemer knytter sig til, at værdien af en kontrakt for en given producent typisk udvikler sig over tid – og at denne udvikling ikke er ens for alle. Det betyder, at en fornuftig fordeling bør sikres via en løbende omfordeling og at der derfor må findes nemme og ikke for kostbare måder at sikre den løbende omfordeling på.

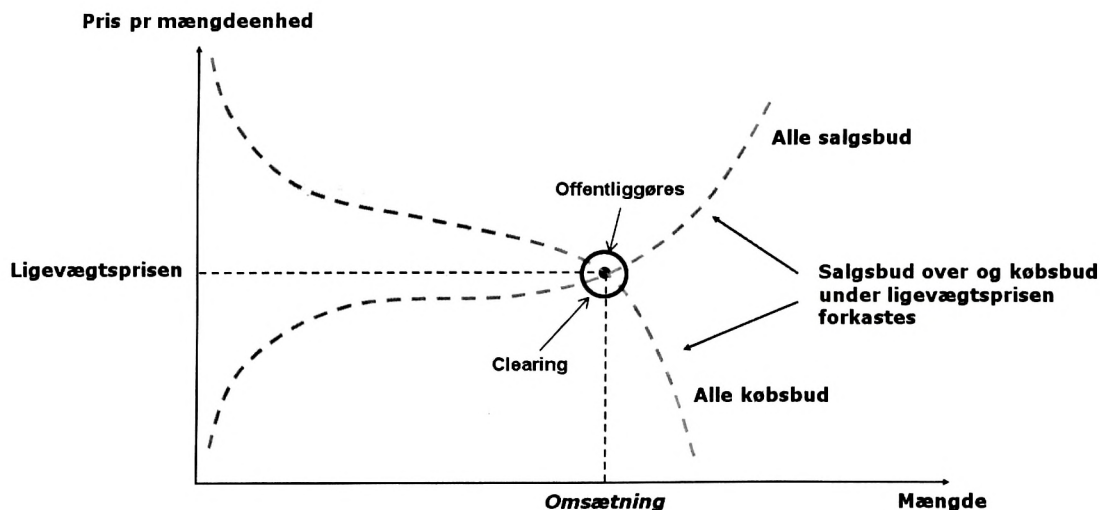
I det følgende skal vi se på, hvorledes kontraktbørser kan være et nyttigt redskab til at løse disse problemer og sikre en løbende omfordeling af produktionen.

Ideen med en kontraktbørs er at etablere et centralt marked. Det optimale marked vil typisk være en dobbeltauktion baseret på lukkede bud. Dette minder meget om den auktionsform der bliver brugt til at handle mælkekvoter bortset fra, at den optimale auktionsform ikke begrænser den enkelte deltager til kun at afgive et bud. Tværtimod giver den optimale auktionsform hver deltager mulighed for at afgive flere købs- og salgs-

bud. Det kan jo meget vel være at en producent til én pris vil sælge en vis mængde af sine kontrakter, og til en højere pris flere af sine kontrakter. Omvendt, kan det være at den samme producent i stedet vil tilkøbe kontrakter til en lavere pris – og flere jo lavere prisen er på disse kontrakter. For en nærmere diskussion af betydningen af flere bud henvises til Bogetoft, Nielsen og Olesen (2003).

Princippet i en dobbeltauktion er meget simpelt: Salgstilbuddene ordnes i voksende orden, dvs. fra laveste til højeste pris, mens købstilbuddene opstilles i aftagende orden, dvs. fra højeste til laveste pristilbud. Ligevægtsprisen kan nu bestemmes som den pris, hvor den efterspurgte mængde er lig den udbudte mængde. For højere priser er der overbud og for lavere priser er der overefterspørgsel. Sælgere som højst har krævet ligevægtsprisen sælger nu til ligevægtsprisen men købere som mindst er villige til at betale ligevægtsprisen køber produktionsrettigheder

Figur 1.
Illustration af en dobbeltauktion



til ligevægtsprisen. Dette er illustreret i *Figur 1* nedenfor.

Det er værd at bemærke at de afgivne bud primært har betydning for, om man ender med at købe, at sælge eller ikke at købe eller sælge. Kun marginalt kan man potentielt påvirke ligevægtsprisen. Det har betydning for den måde man byder på. Selv med få deltagere kan det vises, at den enkelte deltager reelt ikke kan påvirke prisen til egen fordel. Det er derfor optimalt for den enkelte at byde sin sande værdi.

Dette gør det nemt at handle i en dobbeltauktion. Man skal overveje hvilken værdi retten til en vis produktion har for én selv. Man behøver derimod ikke at spekulere på, hvor mange der mon deltager og hvad de har tænkt sig at byde for på denne måde at afgøre, hvor meget man som køber skal underdrive og som sælger skal overdrive sin værdi.

Det forhold, at det er optimalt at byde sin sande værdi, giver samtidigt forklaringen på auktionens optimale egenskaber for branchen som helhed: Produktionen bliver omfordelt, så ingen står tilbage med produktion, som andre reelt ville have større værdi af og ingen går glip af produktion, som andre reelt har mindre værdi af. På denne måde skaber en dobbeltauktion i teorien den størst mulige forøgelse af den profit som deltagerne tilsammen modtager.

Det skal bemærkes, at der naturligvis er enkelte, som kunne have foretrukket en anden handelsform, fx bilaterale handler. En sælger med særlig høj værdi som ikke ender med at sælge kunne måske have været heldig at finde en køber med høj værdi også og så have handlet bilateralt. En sådan sælger kan så ærgre sig over, at der blev omfordelt med en dobbeltauktion. Til gengæld kan køberen i

dette eksempel glæde sig, for han betaler en lavere pris i dobbeltauktionen.

Det er klart at for at en omfordeling via en dobbeltauktion kan forløbe som beskrevet skal man kunne stole på, at de opstillede regler for bestemmelse af ligevægtsprisen og for valg af købere og sælgere følges.

Hertil kommer, at man som køber og sælger kan være interesseret i, at så lidt som muligt af ens bud afsløres overfor de andre deltagere eller overfor forarbejdningsleddet. Det kan fx stille producenterne dårligere i efterfølgende forhandlinger, hvis forarbejdningsleddet får indblik i hvem der ville betale hvad. Det kan forarbejdningsleddet udnytte til at presse producenterne til at afgive en større del af den integrerede profit i forbindelse med fremtidige tilpasninger. Tilsvarende kan den enkelte producent være bekymret for at hans private bud bliver kendt af andre producenter, som måske kan udnytte dette til egen fordel i forbindelse med fremtidige samarbejder eller fremtidige forhandlinger om designet af kontrakterne – fx forhandlinger om hvilke grupper af producenter der skal have tillæg og størrelsen på disse.

Såvel overholdelsen af regler som minimal udslip af information sikres bedst via en såkaldt troværdig tredjepart, dvs. en aktør som indtager en neutral rolle mellem de parter, som har direkte og delvist modstridende interesser. Normalt sker det da også ved, at henlægge auktioner til et auktionshus, en børs eller et revisions- og konsulenthus, som kan tabe værdifuld renommé, hvis reglerne ikke følges eller hvis information lækkes. I SIMAP auktioner sker det på en fundamental anden og typisk billigere måde, nemlig ved at informationen behandles krypteret i et netværk af servere (beregningsnetværket), som

er placeret hos forskellige enkelt personer eller organisationer. De enkelte parter i beregningsnetværket har ingen information om den krypterede information og det er kun når de samarbejder at den krypterede information kan behandles. Det faktum at de enkelte parter i beregningsnetværket ikke har adgang til den fortrolige information, gør administrationen af systemet mere enkel. Systemet designes så beregningerne kun kan kompromitteres og informationerne spredes, hvis en tilstrækkelig stor gruppe af parterne i beregningsnetværket ønsker dette. I princippet kan denne gruppe omfatte alle deltagere i auktionen hvorfor det indirekte er nok at stole på sig selv. Den bagvedliggende teknologi, Secure Multiparty Computation (SMC), er for første gang anvendt i større skala i forbindelse med en dobbeltauktion til handel med sukkerroekontrakter, som blev afviklet tidligere på året. I det følgende beskrives denne case.

Sukkerproduktion, EU reform og den første SIMAP Kontraktbørs

EU's Sukkerreform og Danmark

Den igangværende reform af EU's politik for sukkerproduktion forløber over 4 år fra 2006 til 2009. Når reformen er fuldt gennemført i 2009 vil prisen for hvidt sukker være reduceret med 36 % og prisen for sukkerroer være reduceret med ca. 40 %. I hele EU har denne prisreduktion en afgørende betydning for såvel den primære produktion af sukkerroer som forarbejdningen. De forskellige medlemslande har tilpasset sig reformen på forskellig vis. I Danmark er tilpasningen sket på 3 niveauer: 1) øget produktivitet og omfordeling af kontrakter hos sukkerroeproducenterne, 2) Daniscos lukning af én ud af tre sukkerfabrikker og 3) nettoudnyttelse af EUs omfor-

delingsordning. Dette afsnit omhandler primært den interne omfordeling af sukkerroekontrakter i Danmark.

Der har tidligere været betydelige restriktioner på omfordeling af sukkerroekontrakter, hvilket har ført til en sub-optimal allokering af produktionen. Mindste to problemer har været iøjnefaldende, dels en sub-optimal fordeling på mere eller mindre effektive landbrug og dels en sub-optimal geografisk fordeling i lyset af de tilbageværende sukkerfabrikker.

I en omfattende analyse af et repræsentativt udsnit af danske sukkerroeproducenter kvantificerede vi disse sub-optimaliteter. Vi fandt bl.a., at en effektiv omfordeling under EUs hidtidige sukkerregime kunne have mere end fordoblet landmændenes samlede profit, jf. Bogetoft, Boye, Neergaard-Petersen, and Nielsen (2007). Dette potentiale er interessant fordi det kan motivere en fortsat betydelig produktion af sukkerroer efter EU-reformen.

Studierne har vist, at der er et stort potentiale ved at omfordele sukkerroekontrakter fra producenter med høje omkostninger til producenter med lave omkostninger, inkl. transportudgifter. Den beregnede gevinst er specielt interessant fordi omfordelingen ikke kræver, at producenterne bliver mere effektive, men blot at producenter med høj indtjeningsevne producerer mere. Gevinster kan derfor realiseres meget billigt ved at skabe et effektivt marked. På den anden side viser analyserne også, at en effektiv omfordeling af sukkerroekontrakterne er en forudsætning for at opretholde det nuværende produktionsniveau i Danmark.

Etablering af et marked for sukkerroekontrakter

Det må på denne baggrund vurderes at være fornuftigt, når Danisco og Danske Sukkerroedyrkere (DKS) i indeværende brancheaftale for 2006-2010 har tilladt mere fri handel med kontrakter.

Det er dog ikke nok at tillade handel. Det er også vigtigt at sikre let og effektiv handel. Markedet for sukkerroekontrakter er et nyt marked med mange sælgere og købere, men så længe det alene baseres på bilaterale handler mellem to landmænd, er søgeomkostningerne store og det strategiske spil betydeligt. Der er ingen steder, hvor man kan gå hen og få et overblik over, hvor meget man kan købe eller sælge til en given pris. På et sådant marked findes prisen ved at købere opsøger en eller flere sælgere for at forhandle pris og mængde, og det samme gør sælgere. Kontakt og forhandling er tidskrævende, og hvornår ved man, om man skal slå til? Med omkring 3.000 potentielle købere og sælgere er antallet af forskellige handler uendelig stort. Al erfaring siger, at der vil blive foretaget handler til for høje og for lave priser og såvel købere og sælgere vil fortryde deres handel, når de hører om andre handler. Andre vil slet ikke handle selvom der kunne være gensidige interesser heri, simpelthen fordi de forventer at kunne tjene mere ved at finde andre handelspartnere. Ydermere vil det være meget svært for en køber at sikre sig den ønskede mængde. Den manglende gennemsækelighed og koordinering vil hæmme handlen og efterlade et stort uudnyttet indtjeningspotentiale for hele branchen.

Etableringen af en egentlig kontraktbørs var på denne baggrund et naturligt skridt.

Kontraktbørsen er i princippet en simpel mekanisme som forklaret ovenfor, men i praksis er der naturligvis en række administrative rutiner, som skal spille sammen. Man skal fx sikre sig, at de landmænd, som vælger at sælge en given mængde rent faktisk har tilsvarende kontrakter.

Den etablerede kontraktbørs var imidlertid ikke alene en nyskabelse fordi en central børs ikke tidligere havde været anvendt til handel med sukkerroekontrakter. Danisco og DKS valgte også at gennemføre den med en helt ny teknologi, nemlig såkaldt Secure Multi-party Computation, SMC. Dette skete som led i forskningsprojektet SIMAP som vi deltager i. SIMAP er støttet af det Det Strategiske Forskningsråd. Dermed blev kontraktbørsen også verdens første implementering af de underliggende kryptografiske og teknologiske ideer i en større målestok.

SIMAP Kontraktbørsen

SIMAP Kontraktbørsen er som nævnt i princippet en almindelig dobbeltauktion a la mælkekvotebørsen med den væsentlige udvidelse, at den enkelte producent kunne være både køber og sælger og indsende flere købs- og salgsbud.

SIMAP Kontraktbørsen adskiller sig desuden ved ikke at involvere én betroet tredjepart, men derimod at basere sig på en virtuel tredjepart bestående af Danisco, DKS og SIMAP (forskningsprojektet). De enkelte medlemmer af den virtuelle tredjepart får på intet tidspunkt adgang til den indsendte information. Kontraktbørsen er baseret på distribueret kryptografi. Hver af de 3 parter har én af 3 nøgledele, som skal bruges til at beregne ligevægtsprisen og finde købere og sælgere til denne pris, som er den eneste information

der offentliggøres (se *Figur 1*). De enkelte nøgledele kan ikke bruges til noget. Kun i samarbejde med de andre kan systemet virke og beregningerne foretages.

Kontraktbørsen kan ses som den ideelle mellemmand, som kan sikre et effektivt og gennemsommeligt marked for sukkerroekontrakter. Kontraktbørsen sammenligner alle producenters ønsker til køb og salg og finder én pris (ligevægtsprisen), som alle handler til. Til en given ligevægtspris vil der ikke være nogen, der vil fortryde deres handel. Alle, der på forhånd har sagt, at de vil købe til denne pris (eller en højere) køber, og alle der har sagt at de ønsker at sælge til denne pris (eller lavere) sælger. Da man ikke kender prisen på forhånd, kan man som producent afgive både købs- og salgsbud.

På købsiden kan man afgive op til 5 købsbud. Hvert bud udtrykker, hvor meget man samlet vil købe til en maksimal købspris. Med flere bud giver det producenterne mulighed for at udtrykke forskellige værdier af forskellige kontraktmængder. Behovet herfor kan fx opstå ved ledig maskinkapacitet, ændringer i maskinkapaciteten, sædskiftet eller lign. Som eksempel kan Hansen på forhånd fortælle, at han ønsker kontrakt på 100 tons pølsukker, hvis prisen er 700 eller mindre, men 300 tons, hvis prisen er 400 eller mindre.

På salgssiden kan man afgive ét prisbud per kontrakt. Hvert bud udgør en laveste pris, som denne kontrakt vil blive solgt til. Som eksempel kan Hansen, der har 2 kontrakter, vælge at sælge den første kontrakt, hvis prisen er 1.200 eller derover, og den anden kontrakt hvis prisen er 1.500 eller derover.

De enkelte bud indeholder fortrolig og privat information om, hvad den enkelte produ-

cent maksimalt vil betale for mere kontraktmængde eller, hvad han minimalt vil have for at sælge kontrakter. Udover almindelig tilbageholdenhed med at afsløre den form for information er der også rationelle grunde til ikke at afsløre den. Som beskrevet ovenfor kan den form for information potentielt misbruges af andre i fremtidige relationer. SIMAP Kontraktbørsen tager som nævnt dette forhold meget alvorligt og tilbyder høj fortrolighed. De indsendte bud bliver krypteret og *forbliver* krypterede for altid. Det kan lyde umuligt at de påkrævede beregninger foretages på krypterede data, men det kan lade sig gøre ved hjælp af den nyeste forskning indenfor distribueret kryptografi.

Udover den særlige håndtering af de fortrolige informationer er SIMAP Kontraktbørsen kendetegnet ved at være IT-baseret fra start til slut. Det betød i praksis, at de fleste producenter direkte indsendte deres købs- og salgsbud fra deres hjemmecomputer og at alle efterfølgende beregninger var forprogrammerede. Det betyder også at en gentagelse af en sådan auktion, hvilket er hensigtsmæssig for at sikre en løbende omfordeling af produktionen, bliver særdeles omkostningseffektiv.

I forbindelse med afviklingen af auktionen blev brugerne samtidigt bedt om at evaluere Kontraktbørsen. Evalueringen understregede producenternes fortrolighed med internetbaseret handel, idet 94 % bruger Internetbank og 59 % handler over nettet. Evalueringen understregede samtidigt vigtigheden af den fortrolige håndtering af de indsendte private købs- og salgsbud. 78 % var således enig eller meget enig i at det er vigtigt at de private bud holdes hemmelige og 86 % var tilfreds med det tilbudte fortrolighed. Disse og

andre vurderinger fremgår af *Tabel 1* nedenfor.

Konklusion

For at sikre en fornuftig produktion i et moderne landbrug som det danske er det nødvendigt med optimale kontrakter, som sikrer den nødvendige koordination og motivation af de enkelte landmænd. Erfaringerne viser, at dansk landbrug i den forbindelse er langt fremme, og danske kontrakttyper som fx beskrevet i Bogetoft og Olesen (2004) studeres med interesse i udlandet og i andre brancher.

Det er imidlertid ikke nok, at relationen mellem den enkelte producent og forarbejdningsleddet er optimeret. Det er også vigtigt at produktionen er fordelt hensigtsmæssig på alternative producenter. Analyser af sukkerroeproduktionen har vist, at her var et stort uudnyttet potentiale, og man kan forvente, at tilsvarende gør sig gældende i andre produktionsgrene, hvor den løbende omfordeling af kontrakter har været hæmmet af fordelingspolitiske eller markeds-mæssige forhindringer.

En dobbeltauktion kan være et nyttigt,

ofte optimalt redskab, til at sikre den nødvendige løbende omfordeling af produktionen. Ved inddragelse af den nyeste teknologi, som det skete i forbindelse Kontraktbørsen, kan dette samtidigt gøres med opretholdelse af den maksimale fortrolighed og ved afholdelse af relativt begrænsede omkostninger. Ved afholdelse direkte over internettet er det både administrativt enkelt og let at afgive/ændre sine bud for den enkelte deltager. Det vurderes på denne baggrund at den slags auktioner også har et stort potentiale i andre produktionsgrene.

Det skal afslutningsvis nævnes, at det ikke kun er auktioner, som kan afvikles ved brug af den nye teknologi. Secure Multiparty Computation kan også være nyttig i forbindelse med bilaterale handler, benchmarking, samkøring af fortrolige databaser osv. Ideen er i alle tilfælde, at kombinationen af privat information fra de involverede aktører kan skabe store værdier, men at dette samtidigt forudsætter at den enkelte kan stole på, hvad informationen bliver anvendt til.

Ideerne der er udviklet før og under forskningsprojektet SIMAP videreføres på forskellig vis i andre projekter. På grundforskningsni-

Tabel 1.
Evaluering af SIMAP Kontraktbørsen

Spørgsmål	% »meget enig« eller »enig«
Kontraktbørsen gør det let at handle sukkerroekontrakter	81 %
Det er vigtigt at mine bud holdes hemmeligt	78 %
Jeg er generelt tilfreds med den fortrolighed Kontraktbørsen tilbyder	86 %
Det er enkelt at afgive købs- og salgsbud	81 %
Det er vigtigt at kunne afgive flere købsbud	62 %
Det er vigtigt at kunne afgive både købs- og salgsbud	65 %
Kontraktbørsen er generelt brugervenlig	86 %

veau arbejdes der indenfor 3 områder 1) videreudvikling af den underliggende kryptografiske kerne, 2) analyse af teknologiens informationsøkonomiske implikationer og 3) udvikling af et programmeringssprog til sikker og effektiv implementering. Indenfor anvendt forskning arbejdes med at effektivisere imple-

menteringen og tilpasning til konkrete anvendelser. Endelig arbejdes der i regi af Alexandra Instituttet med konkret implementering, hvor der er ved at blive etableret en kommerciel platform for teknologien i konkrete anvendelser.

Referencer

- 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*.
- Bogetoft, 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. og H.B.Olsen, *Afregningssystemer for Andelsselskaber*, *Landøkonomisk Tidsskrift*, 2000.
- 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
- Milgrom, P., and J.Robert, *Economics, Organization and Management*, Prentice Hall, New Jersey, 1992.
- SIMAPs hjemmeside, www.sikkerhed.alexandra.dk/uk/projects/simap/index.htm