Πλήρης ιδιωτικότητα σε δημοπρασίες

How to obtain full privacy in auctions by **Felix Brandt**

Ηλίας-Δημήτρης Βραχνής
Α.Μ.: 3899
vrachnis@ceid.upatras.gr

Ιωάννης Καλαντζής
Α.Μ.: 3928
ikalantzis@ceid.upatras.gr

Μιχαήλ-Άγγελος Σίμος
Α.Μ.: 4015
asimos@ceid.upatras.gr

Περίληψη

Το θέμα με το οποίο καταπιάνεται το paper που καλούμαστε να σχολιάσουμε είναι η ασφάλεια δημοπρασιών. Αναγνωρίζοντας την αυξανόμενη σημασία της ιδιωτικότητας των συναλλαγών στο σχεδιασμό δημοπρασιών, προτείνονται τεχνικές και πρωτόκολλα δημοπρασιών πρώτης τιμής καθώς και (ν+1)-ιοστής τιμής που αποκαλύπτουν μόνο την ταυτότητα των "νικητών" και την τιμή πώλησης. Επιπλέον, αν είναι επιθυμητό, δεν παρέχεται καμία επιπλέον πληροφορία στους "χαμένους" πλειοδότες πέραν της ήττας τους. Το προτεινόμενο μοντέλο ασφαλείας βασίζεται στην υπολογιστική δυσκολία εντοπισμού (computational intractability) και δεν επικαλείται την αξιοπιστία άλλων συμβαλλόμενων προσώπων (π.χ. ο δημοπράτης).

Παρουσιάζεται επίσης και μια υλοποίηση των προτεινόμενων τεχνικών βασιζόμενη στο σύστημα κρυπτογράφησης El Gamal. Τα απορρέοντα πρωτόκολλα απαιτούν μονάχα τρείς γύρους μετάδοσης μεταξύ των πλειοδοτών. Η πολυπλοκότητα επικοινωνίας είναι γραμμική στον αριθμό των πιθανών προσφορών.

1 Εισαγωγή

Τα τελευταία χρόνια, οι δημοπρασίες έχουν εξελιχθεί σε βασικό άξονα του ηλεκτρονικού εμπορίου. Δεν αποτελούν μόνο μηχανισμούς για την πώληση αγαθών αλλά έχουν εφαρμογή και σε φαινομενικά άσχετους τομείς όπως η ανάθεση έργων, ο προγραμματισμός δραστηριοτήτων ή ακόμα και η εύρεση του συντομότερου μονοπατιού σε ένα δίκτυο. Ταυτόχρονα όμως, η ανάγκη για ύπαρξη ιδιωτικότητας στις δημοπρασίες έχει εξελιχθεί σε παράγοντα μείζονος σημασίας. Τα κρυπτογραφικά πρωτόκολλα που παρουσιάζονται στο paper τους Brandt διαφέρουν από προηγούμενες έρευνες που

έχουν γίνει πάνω στο θέμα στο γεγονός ότι δεν απαιτούν αξιόπιστους τρίτους (trusted third-parties). Βασίζονται μονάχα σε υπολογιστική δυσκολία εντοπισμού (computational intractability). Η ιδιωτικότητα εξασφαλίζεται στο μέγιστο βαθμό χωρίς να γίνεται συμβιβασμός στην αποδοτικότητα των γύρων.

Το σκηνικό μας αποτελείται από έναν πωλητή και ν πλειοδότες με σκοπό να καταλήξουν σε κάποια συμφωνία για την πώληση ενός αγαθού. Μιλάμε πάντα για κλειστές δημοπρασίες (sealed-bid auctions) που σημαίνει ότι ο κάθε πλειοδότης γνωρίζει μόνο τη δική του προσφορά και καμία άλλη. Οι δύο βασικοί μηχανισμοί που οδηγούν σε συμφωνία είναι οι ***δημοπρασίες πρώτης τιμής*** και οι δημοπρασίες ***δεύτερης τιμής (Vickrey auctions[12])***.

Και στους δύο παραπάνω μηχανισμούς ο κάθε πλειοδότης υποβάλει μια κρυφή προσφορά στον δημοπράτη δηλώνοντας το ποσό που είναι διατεθειμένος να πληρώσει. Ο δημοπράτης ορίζει ως νικητή τον πλειοδότη με την υψηλότερη προσφορά. Στις δημοπρασίες πρώτης τιμής, ο νικητής πληρώνει το ποσό που προσέφερε ο ίδιος ενώ στις δημοπρασίες Vickrey καλείται να πληρώσει το ποσό της δεύτερης μεγαλύτερης προσφοράς.

Και οι δύο μηχανισμοί έχουν δυνατά και αδύνατα σημεία. Για παράδειγμα, οι δημοπρασίες πρώτης τιμής έχουν καλύτερα έσοδα όταν οι πλειοδότες είναι περισσότερο συντηρητικοί ενώ οι δημοπρασίες Vickrey είναι strategyproof (όρος από τη θεωρία παιγνίων) που σημαίνει ότι είναι πάντα προτιμότερο για τους πλειοδότες να προσφέρουν με βάση την πραγματική τους εκτίμηση για την αξία του προς πώλησην αγαθού. Οι ανεπιθύμητες ενέργειες του πλεονεκτήματος αυτού συνεισφέρουν στο γεγονόε οτι οι δημοπρασίες Vickrey έχουν μικρή πρακτική εφαρμογή για τους εξής λόγους [9, 10, 11]:

- Οι πλειοδότες είναι απρόθυμοι να αποκαλύψουν την πραγματική τους εκτίμηση στον δημοπράτη.
- Οι πλειοδότες αμφισβητούν την ακρίβεια της δημοπρασίας αφού δεν πληρώνουν το ποσό που προσέφεραν.

΄Ενα κλασσικό παράδειγμα που υποδεικνύει τα παραπάνω είναι όταν ο δημοπράτης κατασκευάζει μια πλαστή δεύτερη μεγαλύτερη προσφορά με σκοπό να αυξήσει τα έσοδα του (για παράδειγμα [8]). Και τα δύο παραπάνω ζητήματα βασίζονται στην έλλειψη εμπιστοσύνης στον δημοπράτη. Για αυτό το λόγο, θα ήταν επιθυμητό με κάποιο τρόπο να "εξαναγκάσουμε" τον δημοπράτη να επιλέγει πάντα την σωστή έκβαση και να "απαγορεύσουμε" τη διάδοση πληροφοριών των ιδιωτικών προσφορών. Τα τελευταία χρόνια, έχουν προταθεί διάφορα σχέδια για την επίτευξη αυτού του σκοπού. Πρακτικά όμως όλα βασίζονται σε αξιόπιστα συμβαλλόμενα μέρη. Στόχος του paper του Brandt είναι η κατασκευή αποδοτικών πολυκομματικών πρωτοκόλλων που επιτρέπουν στους *πλειοδότες* να λογαριάσουν απο κοινού την έκβαση της δημοπρασίας χωρίς να αποκαλύψουν περαιτέρω πληροφορίες.

Τα πρωτόκολλα που εισάγει το paper αφορούν δημοπρασίες πρώτης τιμής και (M+1)-ιοστής τιμής. Οι τελευταίες είναι γενίκευση των δημοπρασιών δεύτερης τιμής. Σε μια δημοπρασία (M+1)-ιοστής τιμής, ο πωλητής προσφέρει M ξεχωριστές μονάδες του ίδιου αντικειμένου ($1 \leq M \leq n$) και κάθε πλειοδότης επιθυμεί να αποκτήσει *ένα* απο αυτά (unit demand).

1.1 Δομή του paper

Η δομή του paper έχει ως εξής. Αρχικά, περιγράφει το υποκείμενο γενικό μοντέλο ασφαλείας. Ακολουθεί μια αναφορά σε σχετικές προηγούμενες έρευνες πάνω σε πρωτόκολλα δημοπρασιών και σύγκριση με την προτεινόμενη προσέγγιση. Το επόμενο κομμάτι περιέχει μια αναλυτική περιγραφή των εννοιών που χρησιμοποιούνται στην υλοποίηση που ακολουθεί. Έπεται μια ανάλυση πάνω στην ασφάλεια και την αποδοτικότητα των προτεινόμενων πρωτοκόλλων. Στο τέλος, ο συντάκτης του paper κάνει μια σύντομη ανασκόπηση των αποτελεσμάτων.

2 Μοντέλο Ασφαλείας

Πρωταρχικός στόχος του ερευνητή είναι ιδιωτικότητα στις δημοπρασίες που δεν μπορεί να παραβιαστεί από κανένα συνασπισμό τρίτων προσώπων ή πλειοδοτών. Για το λόγο αυτό, συνηγορεί σε ένα μοντέλο ασφαλείας στο οποίο οι πλειοδότες λογαριάζουν από κοινού την έκβαση της δημοπρασίας με τέτοιο τρόπο ώστε κανένα υποσύνολο τους να μην μπορεί να αποκαλύψει ιδιωτικές πληροφορίες. Παρά το γεγονός ότι είναι ανεπιθύμητη η εκτεταμένη αλληλεπίδραση με τους πλειοδότες, ο ερευνητής δεν μπορεί να το αποφύγει και προσπαθεί να ελαχιστοποιήσει την επίδρασή του κρατώντας την πολυπλοκότητα των γύρων στο ελάχιστο, γεγονός που απαιτεί την ύπαρξη ενός καναλιού εκπομπής. Τα μειονεκτήματα που παρουσιάζονται λόγω της συγκεκριμένης προσέγγισης, είναι η μικρή ανοχή της καθώς και σχετικά υψηλή υπολογιστική και επικοινωνιακή πολυπλοκότητα. Είναι γεγονός ότι σε πλειστηριασμούς που απαιτούν τόσο μεγάλο βαθμό ιδιωτικότητας συνήθως γίνονται με λίγους (και γνωστούς) πλειοδότες.

Ο ερευνητής χρησιμοποιεί κρυπτογραφικά πρωτόκολλα για n πλειοδότες και έναν πωλητή (στη συνέχεια θα λέγονται συντελεστές). Κάθε πλειοδότης i κατέχει μια προσωπική είσοδο, την προσφορά του bid[i] E B. Οι συντελεστές συμπλέκονται σε ένα πρωτόκολλο πολλών ατόμων ώστε κοινά και με ασφάλεια να αποφασίσουν το αποτέλεσμα της συνάρτησης f. Στη δική μας σκοπιά, η ασφάλεια αποτελείται από ορθότητα και ιδιωτικότητα. Τα συνήθη αποτελέσματα από ασφαλείς υπολογισμούς πολλών προσώπων υποδεικνύουν ότι κάθε συνάρτηση f μπορεί να υπολογιστεί με ασφάλεια όταν

- το πολύ $\lfloor \frac{n-1}{2} \rfloor$ συντελεστές μοιράζονται τις πληροφορίες τους και υπάρχουν παραλαγές κατωφλιού [5], ή
- το πολύ $\lfloor \frac{n-1}{3} \rfloor$ συντελεστές μοιράζονται τις πληροφορίες τους και υπάρχει πλήρες δίκτυο από ιδιωτικά κανάλια [1, 2].

Η πρώτη υπόθεση είναι γνωστή ως υπολογιστικό μοντέλο ενώ η δεύτερη είναι γνωστή ως το άνευ όρων μοντέλο. Ωστόσο, καμία υπόθεση από τις δυο δεν μπορεί να γίνει στην δική μας περίπτωση γιατί θα επέτρεπε σε υποσύνολα πλειοδοτών να προκαθορίσουν το αποτέλεσμα του πλειστηριασμού και να ανακαλύψουν τις προσφορές των άλλων συντελεστών. Παρ' όλα αυτά, υπάρχουν επιπλέον υποθέσεις που επιτρέπουν τον ασφαλή υπολογισμό αυθαίρετων συναρτήσεων στο υπολογιστικό μοντέλο, και ένα περιορισμένο σύνολο συναρτήσεων στο άνευ όρων μοντέλο, χωρίς έμπιστα κατώφλια στους συντελεστές (για παράδειγμα [4, 6, 7]. Ιδιωτικότητα που στηρίζεται στο γεγονός ότι δεν είναι όλοι οι συντελεστές συνεννοημένοι θα αναφέρεται ως πλήρης ιδιωτικότητα. Στο υπολογιστικό μοντέλο, κάθε συνάρτηση f μπορεί να υπολογιστεί πλήρως κατ'ιδίαν όταν

- υπάρχουν παραλαγές κατωφλιού, και
- ένας καθορισμένος συντελεστής δεν παραιτείται ή αποκαλύπτει πληροφορίες πρόωρα.

Στα πρωτόκολλα πλειστηριασμών που παρουσιάζονται σε αυτό το paper, ο πωλητής θα πάρει το ρόλο του καθορισμένου συντελεστή. Είναι σημαντικό να σημειώσουμε ότι ακόμα και στην περίπτωση που ο πωλητής παραιτείται ή αποκαλύπτει πληροφορίες πρόωρα, το χειρότερο που θα μπορούσε να συμβεί είναι ότι ένας πλειοδότης μαθαίνει το αποτέλεσμα και παραιτείται πριν οι υπόλοιποι συντελεστές μάθουν το αποτέλεσμα. Η ιδιωτικότητα των προσφορών δεν επηρεάζεται από πρόωρες παραιτήσεις. Ένας άλλος κοινός τρόπος για να επιτύχουμε δικαιοσύνη χωρίς έμπιστη πλειοψηφία είναι η αυξανόμενη αποκάλυψη μυστικών (για παράδειγμα [3, 6, 13]).

Κάθε φορά που ένας κακόβουλος πλειοδότης παρεμποδίζει το πρωτόκολλο στέλνοντας εσφαλμένα μηνύματα ή αδυνατώντας να αποδείξει την ορθότητα της συμπεριφοράς του στη μηδαμινή γνώση, αυτός ο πλειοδότης αφαιρείται και το πρωτόκολλο επανεκκινείται. Θεωρούμε ότι το "κοινό" παρατηρεί το πρωτόκολλο και γι' αυτό ένας κακόβουλος χρήστης μπορεί αδιαμφισβήτητα να ταυτοποιηθεί, ανεξάρτητα από το πόσοι από τους υπόλοιπους συντελεστές είναι αξιόπιστοι. Επειδή στους κακόβουλους χρήστες μπορεί εύκολα να κοπεί πρόστιμο και δεν κερδίζουν καθόλου πληροφορίες, δε θα έπρεπε να υπάρχει κίνητρο για παρεμπόδιση του πλειστηριασμού και γι' αυτό από εδώ και στο εξής θεωρούμε ότι μία εκτέλεση του πρωτοκόλλου αρκεί.

Εξαιτίας της ανεπάρκειας των υπαρχόντων MPC schemes, είναι αναπόφευκτο να σχεδιάσουμε πρωτόκολλα ειδικού σκοπού για τον υπολογισμό συγκεκριμένων συναρτήσεων. Αν $b = (bid_1, bid_2, ..., bid_n)$ είναι το διάνυσμα με όλες τις προσφορές και $f : B^n \rightarrow O^{n+1}$ η συνάρτηση εξόδου όπου $f(b) = (f_1(b), f_2(b), ..., f_n(b), (f_1(b), f_2(b), ..., f_n(b)))$ ώστε ο πλειοδότης i μαθαίνει $f_i(b)$ και ο πωλητής μαθαίνει $(f_1(b), f_2(b), ..., f_n(b))$. Αν ο πλειοδότης i κερδίσει τον πλειστηριασμό, το $f_i(b)$ παράγει τη τιμή πώλησης. Αλλιώς "άχρηστες" πληροφορίες επιστρέφονται. Αυτό θα λέγεται σκηνικό ιδιωτικού αποτελέσματος αφού το αποτέλεσμα ανακοινώνεται μόνο στα ενδιαφερόμενα μέρη. Για λόγους διαφάνειας και αποτελεσματικότητας, θα θεωρήσουμε επίσης τον υπολογισμό μιας συνάρτησης δημοσίου αποτελέσματος όπου όλα τα $f_i(b)$ είναι πανομοιότυπα και παράγουν την ταυτότητα του νικητή του πλειστηριασμού και τη τιμή πώλησης.

3 Σχετικές Έρευνες

Το ενδιαφέρον σε κρυπτογραφικά πρωτόκολλα για δημοπρασίες έχει αυξηθεί δραματικά. Έχουν προταθεί διάφορα ασφαλή μοντέλα για διεξαγωγή δημοπρασιών κλειστής προσφοράς (sealed-bid auctions). Ένα κοινό στοιχείο που μοιράζονται όλα τα υπάρχοντα πρωτόκολλα είναι ότι η ιδιωτικότητα λαμβάνεται κατανέμοντας τον υπολογισμό της έκβασης της δημοπρασίας σε μια ομάδα τρίτων.

Υπάρχουν *συμμετρικά* πρωτόκολλα, όπου υπάρχουν πολλοί δημοπράτες που αποφασίζουν από κοινού την έκβαση χρησιμοποιώντας threshold MPC, και *ασύμμετρα* πρωτόκολλα, τα οποία εισάγουν μια επιπλέον αρχή στη δημοπρασία (όπως για παράδειγμα έναν "εκδότη" της δημοπρασίας ή κάτι ανάλογο).

3.1 Κρυπτογραφικά πρωτόκολλα δημοπρασιών

Σε αυτό το section, ο Brandt παρουσιάζει μια περίληψη των διάφορων υπάρχοντων πρωτοκόλλως που πραγματεύονται το θέμα της ασφάλειας δημοπρασιών. Συγκεκριμένα, γίνεται αναφορά στα πρωτόκολλα των Yao, Baudron και Stern, Lipmaa et al., Abe και Suzuki. Η περιγραφή/ανάλυση αυτών των πρωτοκόλλων ξεφεύγει από τα πλαίσια αυτής της περίληψης.

3.2 Bidder-resolved auctions

Γενικά, η ασφάλεια των πρωτοκόλλων που αναφέρθηκαν στο προηγούμενο τμήμα βασίζονται στην παραδοχή ότι δεν υπάρχει περίπτωση συμπαιγνίας μεταξύ των εμπλεκόμενων μερών. Στο paper αυτό, ο Brandt πραγματεύεται αυτό που ονομάζει "bidder-resolved" πρωτόκολλα, πρωτόκολλα δηλ.

στα οποία εξομοιώνεται η ύπαρξη του δημοπράτη και η έκβαση της δημοπρασίας είναι ανεξάρτητη των συμβαλλόμενων μερών.

Συνεχίζοντας τη σύγκριση με άλλα υπάρχοντα πρωτόκολλα, ο Brandt αναφέρει ότι τα πρωτόκολλα που προτείνει είναι τα μοναδικά που προσφέρουν επαληθευσιμότητα, μη-αποκύρηξη και πολυπλοκότητα σταθερού αριθμού γύρων. Παρουσιάζει επίσης πρωτόκολλα ιδιωτικής έκβασης (private outcome protocols) στα οποία οι χαμένοι πλειοδότες δεν μαθαίνουν επιπλέον πληροφορίες πέραν της ήττας τους.

4 Περιγραφή του Πρωτοκόλλου

Στην ενότητα αυτή, προτείνεται μια αφηρημένη περιγραφή για τα πρωτόκολλα πλειστηριασμού. Δεν έχει σημασία αν ενα αριθμητικό σύστημα MPC βασίζεται σε επαληθεύσιμα μυστικό διαμοιρασμό, ομόμορφικής κρυπτογράφησης, ή άλλες τεχνικές, η προσθήκη των μυστικών τιμών μπορεί συνήθως να γίνεται πολύ αποτελεσματικά ενώ ο πολλαπλασιασμός των "μυστικών" απαιτεί υψηλό ποσόστό επικοινωνιακών πόρων. Για το λόγο αυτό, τα πρωτόκολλα που προτείνονται απαιτούν: τον υπολογισμό των γραμμικών συνδυασμών των εισόδων (που μπορεί να βασίζεται αποκλειστικά στην προσθήκη) και πολλαπλασιασμούς με από κοινού δημιουργημένες τυχαίες τιμές (προτείνεται μια αποτελεσματικό υπο-πρωτόκολλο στο 5.1). Κατά τον υπολογισμό στα διανυσμάτα "μυστικών", ο υπολογισμός των γραμμικών συνδυασμών ενεργοποιεί την προσθεση και την αφαίρεση των διανυσμάτων "μυστικών", καθώς και τον πολλαπλασιασμό των διανυσμάτων με προκαθορισμένους γνωστούς πίνακες.

΄Εστω **p** ένα διάνυσμα με k δυνατές τιμές, $\mathbf{p} = (p1, p2, ..., PK)$, και $bid_i \in 1, 2, ..., K$ η προσφορά του πλειοδότη i. Το διάνυσμα b_i του υποψηφίου i ορίζεται έτσι ώστε $b_{i,bidi} = 1$ (πλειοδότης i πλειοδοτεί p_{bid_i}), καθώς και όλα τα άλλα στοιχεία είναι 0, δηλαδή

$$b_i = \begin{pmatrix} b_{ik} \\ \vdots \\ b_{i,bid_i+1} \\ b_{i,bid_i} \\ b_{i,bid_i-1} \\ \vdots \\ b_{i1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Η αναπαράσταση αυτή επιτρέπει αποτελεσματική απόδειξη για την ορθότητα του διανύσματος. Ωστόσο το κύριο πλεονέκτημα της αναπαράστασης με διανύσματα είναι η δυνατότητα αποδοτικών υπολογισμών.

Για παράδειγμα το ενσωματωμένο διάνυσμα προσφοράς (Abe and Suzuki)

$$b'_i = \begin{pmatrix} b'_{ik} \\ \vdots \\ b'_{i,bid_i+1} \\ b'_{i,bid_i} \\ b'_{i,bid_i-1} \\ \vdots \\ b'_{i1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$$

μπορεί να προκύψει πολλαπλασιάζοντας το διάνυσμα προσφοράς με τον k×k κάτω τριγωνικό πίνακα L_k, που είναι $b'_i = L_k b_i$ όπου Ll κάτω τριγωνικός μοναδιαίος πίνακας και $l \in \{k, n\}$.

Επιπλέον l×l πίνακες που θα χρησιμοποιηθούν στα επόμενα τμήματα είναι ένας άνω τριγωνικός (U_l), ένας πίνακας ταυτοτήτων (I_l) και ένας πίνακας τυχαίου πολλαπλασιασμού (R_l^*).

Τα στοιχεία του διαγωνίου R_l^* είναι τυχαίοι αριθμοί, άγνωστοι στους παράγοντες της δημοπρασίας. Δημιουργούνται σύμφωνα με ένα ειδικό υποπροτόκολο που προτείνεται παρακάτω. Ο πολλαπλασιασμός με R_l^* μετατρέπει όλες τις τιμές που δεν είναι μηδέν σε ασήμαντους τυχαίους αριθμούς. Για το λόγο αυτό, είναι το τελευταίο βήμα κλειδί στα πρωτόκολα που παρουσιάζονται στην εργασία. Η ειδική δομή όλων των χρησιμοποιηθέντων μητρώων επιτρέπει πολλαπλασιασμό μητρώου-διανύσματος χησιμοποιώντας μόνο k πολλαπλασιασμούς.

Μοναδικό κόστος της αναπαράστασης αυτής είναι η πολυπλοκότητα υπολογισμων και επικοινωνία που είναι γραμμική ανάλογη με το k. Από την άλλη η αναπαράσταση αυτή δίνει δυνατότητα προσαρμογής και εξομοίωσης άλλων πρωτοκόλων επαναληπτικών δημοπρασιών.

Στην πραγματικότητα, υπάρχουν κοινές επαναληπτικές αντιστοιχίες για τα δύο είδη δημοπρασιών που εξετάζονται Η δημοπρασία πρώτης τιμής (first-price auction) είναι στρατηγικά ισοδύναμη με την ολλανδική (ή φθίνουσα-τιμή) δημοπρασία, και η δημοπρασία δεύτερης τιμής (second-price auction) αντιστοιχεί στο γνωστό αγγλικό (ή αύξουσα τιμή) μοντέλο πλειστηριασμού, όπως χρησιμοποιείται στο eBay ή Sotheby's. Μερικές φορές, επαναληπτικές δημοπρασίες είναι προτιμότερες από τις δημοπρασίες κλειστής προσφοράς.

4.1 Δημοπρασίες πρώτης τιμής

Σε αυτό το κομμάτι, ο Brandt προτείνει ένα πολυτμηματικό σύστημα υπολογισμού για first-price δημοπρασίες. Με σεβασμό στο πλαίσιο που παρουσιάζεται στο τμήμα 2, ορίζουμε συνάρτηση $f_a^1(b)$ η οποία κατοχυρώνει την

τιμή πώλησης, αν και μόνο αν ο πλειοδότης a είναι ο νικητής της δημοπρασίας. Μπορούμε να έχουμε ένα διάνυσμα στο οποίο όλα τα στοιχεία που αναφέρονται σε τιμές μεγαλύτερες ή ίσες με αυτήν της μέγαλύτερης μέχρι στιγμής πλειοδοσίας είναι μηδέν, αθροίζοντας όλα τα ενσωματωμένα διανύσματα πλειοδοσιών, και μετακινώντας το αποτέλεσμα κάτω μία θέση:

$$(L_k - I_k) \sum_{i=1}^{n} b_i$$

Προσθέτοντας τα διανύσματα $(U_k – I_k)\mathbf{b}_a$, μία τιμή πραραμένει 0 αν και μόνο αν ο πλειοδότης a, πλειοδοτεί περισσότερο απο την τρέχουσα πλειοδοσία, πράγμα που τον καθιστά νικητή της δημοπρασίας. Αυτό το στοιχείο προσδιορίζει την τιμή πώλησης. Αφού πολλαπλασιάσουμε με τον μυστικό τυχαίο πίνακα πολλαπλασιασμού το διάνυσμά αποτελείται απο τυχαίες τιμές, αν ο πλειοδότης δέν έχει υποβάλει τη μεγαλύτερη πλειοδοσία.

$$\left((L_k - I_k) \sum_{i=1}^{n} b_i + (U_k - I_k) b_a \right) R_k^*$$

Αλλιώς η τοποθέτηση του μονού μηδενικού υποδεικνύει την τιμή πώλησης (στον πωλητή, καθώς ο πλειοδότης a γνωρίζει ήδη προσφορά του). Όλα τα υπόλοιπα στοιχεία έχουν τυχαίες τιμές.

4.1.1 Περιπτώσεις ισοπαλίας

Μέχρι στιγμής, αν υπάρχουν περισσότερες από μία προσφορές που κερδίζουν, το πρωτόκολλο αποκαλύπτει την ταυτότητα όλων των νικητών (αφήνοντας στον πωλητή τις επιλογές για τη συνέχεια).

Ωστόσο, είναι δυνατόν να τροποποιήσει το πρωτόκολλο δίνοντας το νικητή με το χαμηλότερο δείκτη. Αυτό μπορεί να χρησιμοποιηθεί σε συνδυασμό με μια ρύθμιση κατά την οποία σε υποψήφιους που εισέρχονται για τη δημοπρασία ανατίθενται διαδοχικούς αριθμοι ως δείκτες, δημιουργώντας ένα κίνητρο εισόδου απο νωρίς. Ακόμα και τυχαία θα μπορούσε να επιλέγεται δίκαια ένας απο τους νικητές. Σε κάθε περίπτωση, ένα ακόμα διάνυσμα που έχει 0 σε όλους τους άλλους παράγοντεσ εκτός απο το νικητή πλειοδότη με το μικρότερο δείκτη προστίθεται, έστω:

$$u_j = \begin{pmatrix} b_{1_j} \\ b_{2_j} \\ \vdots \\ b_{n_j} \end{pmatrix}$$

$$X = (x_1, x_2, ..., x_n) = \begin{pmatrix} ((L_n - I_n)u_k)^T \\ ((L_n - I_n)u_{k-1})^T \\ \vdots \\ ((L_n - I_n)u_1)^T \end{pmatrix}$$

X είναι ένα $k \times n$ μητρώο που αποτελείται απο τα n διανύσματα x_i. Τελικά το πλήρες αποτέλεσμα της δημοπρασίας first-price ορίζεται ως:

$$f_a^1(b) = \left((L_k - I_k) \sum_{i=1}^{n} b_i + (U_k - I_k) b_a + x_a \right) R_k^*$$

4.1.2 Public outcome

Για λόγους αποτελεσματικότητας και διαφάνειας μπορεί να χρειάζεται να υπολογιστεί το αποτελεσμα της δημοπρασίας ωστε όλοι οι πλειοδότες να μάθουν την τελική τιμή. Τότε, υπάρχει μονο μία συνάρτηση υπολογισμού:

$$f^1(b) = \left((L_k - I_k) \sum_{i=1}^{n} b_i \right) R_k^* + \sum_{i=1}^{n} 2^{i-1} b_i$$

Το πρώτο μη μηδενικό στοιχείο του $f^1(b)$ ορίζει την τιμή πώλησης. Ο πλειοδότης i κερδίζει την δημοπρασία αν το

$$(i\text{–}1)$$

bit αυτού του στοιχείου έχει οριστεί.

4.2 (M+1)st-price auctions

Αναλύονται οι τεχνικές έυρεσης αποτελεσμάτων (M + 1)st-price δημοπρασιών. Κατασκευάζεται ένα διανύσμα (χρησιμοποιώντας γραμμικούς συνδιασμούς των b_i) στο οποίο η (M + 1)η υψηλότερη πλειοδοσία σημαδεύεται με 0. Έστω

$$e = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$$

το k-διάστατο διάνυσμα μονάδας.

$$(2L_k - I_k) \sum_{i=1}^{n} b_i - (2M + 1)e$$

δίνει ένα διάνυσμα στο οποίο όλα τα στοιχεία εκτός απο αυτό που αναφέρεται στην (M + 1) μεγαλύτερη πλειοδοσία δεν είναι 0.

Ο υπολογισμός του $(2L_k – I_k) \sum_{i=1}^{n} b_i$ ισοδυναμεί με την πρόσθεση όλων των ενσωματωμένων διανυσμάτων πλειοδοσίας με τα μετατοπισμένα προς τα κάτω διανυσμάτα πλειοδοσίας.

Αυτό έχει αποτέλεσμα μια αυστηρά αυξανόμενη ακολουθία οπου το 1 σημειώνει την υψηλότερη πλειοδοσία το 3 την δεύτερη υψηλότερη το 5 την τρίτη κ.λπ. Αφαιρώντας $(2M + 1)$ δίνει ένα διάνυσμα στο οποίο το συστατικό που δηλώνει τη $(M+1)$ υψηλότερη πλειοδοσία είναι μηδέν. Όταν καλύψουμε τις πληροφορίες αυτές το διάνυσμα αποτελεσμάτων καθε πλειοδότη γίνεται:

$$price_a^{M+1}(b) = \left((2L_k - I_k) \sum_{i=1}^{n} b_i - (2M + 1)e + (2M + 2)U_k b_a \right) R_k^*$$

Ο παράγοντας $(2M + 2)$ διαβεβαιώνει οτι επιπρόσθετα μηδενικά δεν εμφανίζονται "κατά λάθος". Άν το διάνυσμα $price_a^{M+1}(b)$ περιέχει ένα μηδενικό, ο πλειοδότης a είναι ο νικητής της δημοπρασίας. Η θέση του 0 υποδεικνύει την τιμή πώλησης. Όλα τα άλλα στοιχεία είναι τυχαίες τιμες.

Όταν δύο ή περισσότεροι πλειοδότες έχουν κοινή την $(M + 1)$ υψηλότερη πλειοδοσία η παραπάνω τεχνική δε δουλεύει, αφού το διάνυσμα του αποτελέσματος δεν περιέχει 0. Για το λόγο αυτό, οι παράγοντες (agents) υπολογίζουν συμπληρωματικά διανύσματα για κάθε πλειοδότη, που δίνουν το σωστό αποτέλεσμα στις περιπτώσεις αυτές. Η παρακάτω μέθοδος σημειώνει τις $(M + 1)$ υψηλότερες πλειοδοσίες, ενώ δεν αποκαλύπτει άλλες πληροφορίες. Το $\sum_{i=1}^{n} b_i - te$ είναι ένα διάνυσμα που περιέχει μηδενικά αν υπάρχει "ισοψηφία".

Μας αφορούν μόνο οι ισοδυναμίες που αφορούν τις $(M + 1)$ υψηλότερες πλειοδοσίες αφού αυτές προκαλούν την αποτυχία του υπολογισμού $price_a^{M+1}(b)$. Άλλες ισοδυναμίες εξαλείφονται προσθέτοντας
$(n+1)\,(L_k \sum_{i=1}^{n} b_i - (t + u)e)$ όπου $u \in \{max(0, M+1–t), ..., min(M, n–t)\}$ για κάθε t.

Το διάνυσμα των αποτελεσμάτων περιέχει ένα 0, όπου t πλειοδοσίες είναι ίσες και υπάρχουν u πλειοδοσίες με μεγαλύτερη τιμή απο αυτήν της ισοψηφίας. Ο παράγοντας $(n + 1)$ είναι αρκετά μεγάλος για να διαβεβαιώσει οτι οι δύο προσθετέοι δεν έχουν άθροισμα 0. Τελικά οι θέσεις της ισοψηφίας γίνονται αόρατες για να κρυφτούν οι πλειοδότες. Αυτό μπορεί να γίνει προσθέτοντας $(n + 1)^2 U_k b_a$ ή $(n + 1)^2 (U_k - I_k) b_a$ ανάλογα με το u.

4.2.1 Περιπτώσεις ισοπαλίας

Αν και ισοψηφίες που αφορούν τις $(M+1)$ υψηλότερες πλειοδοσίες δεν μπορούν να εμποδίσουν τον μηχανισμο στον υπολογισμό του αποτελέσματος, θα υπάρχουν πολλοί νικητές, όταν υπάρχουν ισοψηφίες που αφορούν την υψηλότερη πλειοδοσία. Έτσι δημιουργείται το επιπλέον διάνυσμα αποτελέσματος $pricetie^2_{at0}$ που μπορεί να τροποποιηθεί ωστε να δίνει το νικητή με το μικρότερο δείκτη προσθέτοντας το διάνυσμα x_a. Έτσι,

$$pricetie^2_{at0}(b) = \left(((n+1)L_k + I_k) \sum_{i=1}^{n} b_i - ((n+2)t)\, e + (n+1)^2((U_k - I_k)b_a + x_a) \right) R^*_k$$

Τα διανύσματα αποτελεσμάτων ($price^2_a(b)$ και $pricetie^2_{at1}(b)$) δε χρειάζεται να κρυφτούν.

5 Ανάλυση

Σε αυτό το κομμάτι, ο συντάκτης του αρχικού paper αναλύει περαιτέρω την ασφάλεια και αποδοτικότητα των πρωτοκόλλων δημοπρασιών. Υποθέτει ότι το υποκείμενο κανάλι επικοινωνίας είναι πάντα αξιόπιστο. Παραθέτει αποδείξεις για τις ακόλουθες προτάσεις.

Πρόταση 1 *Τα προτεινόμενα πρωτόκολλα είναι*

- *ορθά* με αμελητέα πιθανότητα σφάλματος,
- *απόλυτα ιδιωτικά* με προϋπόθεση την δυσκολία του προβλήματος Diffie-Helman (Diffie–Hellman assumption)
- *δίκαια* με την έννοια ότι ή όλοι οι πλειοδότες ή κανένας μαθαίνουν την έκβαση, αν ο πωλητής δεν εγκαταλήψει ή αποκαλύψει πληροφορίες πρόωρα.

Δεν έχει μεγάλο νόημα να παραθέσουμε αυτούσια την απόδειξη των παραπάνων, αλλά εν συντομία αναφέρουμε ότι η ιδιωτικότητα εξασφαλίζεται μέσω του El-Gamal cipher καθώς και του προαναφερθέντος προβλήματος Diffie-Hellman.

5.1 Το πρόβλημα Diffie-Hellman

Το πρόβλημα Diffie-Hellman (DHP) είναι ένα μαθηματικό πρόβλημα που προτάθηκε από τους Whitfield Diffie και Martin Hellman στα πλαίσια της κρυπτογραφίας. Κίνητρο για τη διατύπωση του προβλήματος είναι το γεγονός

ότι πολλά συστήματα ασφαλείας χρησιμοποιούν μαθηματικές πράξεις, γρήγορες στον υπολογισμό αλλά δύσκολες στην αντιστροφή. Χαρακτηριστικό παράδειγμα είναι η κρυπτογράφηση ενός μηνύματος όπου η αντιστροφή του αλγορίθμου για την επιστροφή στο αρχικό μήνυμα είναι ιδιαίτερα δύσκολη. Αν το πρόβλημα Diffie-Hellman ήταν εύκολο, αυτά τα συστήματα θα ”έσπαγαν” πολύ εύκολα.

Το πρόβλημα Diffie-Hellman διατυπώνεται ανεπίσημα ως εξής:

> Δοθέντος ενός στοιχείου g και των τιμών g^x και g^y, ποιά είναι η τιμή του $g^(xy)$;

Στην κρυπτογραφία, υποθέτουμε ότι το Diffie-Hellman είναι ιδιαίτερα δύσκολο και συχνά ονομάζεται και *παραδοχή Diffie-Hellman*. Το πρόβλημα έχει ”επιβιώσει” από λεπτομερείς έρευνες τις τελευταίες δεκαετίες και δεν έχει δημοσιευτεί μέχρι σήμερα κάποια ”εύκολη” λύση.

5.2 Ανάλυση αποδοτικότητας

Ο συντάκτης αναλύει επίσης την υπολογιστική πολυπλοκότητα (αριθμός πράξεων ύψωσης σε δύναμη και πολλαπλασιασμών) και πολυπλοκότητα επικοινωνίας. Θεωρεί το υπολογιστικό κόστος των πολλαπλασιασμών αμελητέο. Η ύψωση σε δύναμη και επικοινωνιακή πολυπλοκότητα είναι ίδιες σε όλα τα προτεινόμενα πρωτόκολλα. Στο αρχικό paper, ακολουθεί ο υπολογισμός της πολυπλοκότητας σε κάθε γύρο. Τα αποτελέσματα φαίνονται στον ακόλουθο πίνακα.

	Body	Zero-knowledge proofs
Prologue	P	$P + Q$
Round 1	$2kP$	$4k(P + Q) + 2P + Q$
Round 2	$2nkP$	$nk(2P + Q)$
Round 3	nkP	$(nk + 1)P + Q$
Σ	$(k(3n + 2) + 1)P$	$(k(3n + 4) + 4)P + (2k(n + 2) + 3)Q$

6 Συμπεράσματα

Ο συντάκτης του paper παρουσίασε κρυπτογραφικά πρωτόκολλα σταθερού αριθμού γύρων για διάφορους τύπους δημοπρασιών κλειστής προσφοράς (sealed-bid auctions). Η ασφάλεια των προτεινόμενων προτοκόλλων βασίζεται στην υπολογιστική δυσκολία εντοπισμού και όχι στην ύπαρξη τρίτων μερών. Στον παρακάτω πίνακα φαίνονται οι διάφορες ιδιότητες του πρωτκόλλου ανά περίπτωση. Εξετάστηκαν δημοπρασίες με *ιδιωτική έκβαση*

(private outcome), όπου μόνο ο νικητής και ο πωλητής μαθαίνουν το αποτέλεσμα, και δημοπρασίες με *δημόσια έκβαση* (public outcome), όπου όλοι οι συντελεστές μαθαίνουν το αποτέλεσμα. Τα πρωτόκολλα δημοπρασιών ιδιωτικής έκβασης πρώτης και δεύτερης τιμής έχουν "αυτόματα" την ικανότητα επίλυσης των ισοπαλιών ενώ τα υπόλοιπα πρωτόκολλα αποδίδουν τις ταυτότητες όλων των νικητών. Σε αυτή την περίπτωση, οι ισοπαλίες μπορούν να επιλυθούν με την διαδοχική εφαρμογή ενός πρωτοκόλλου για ρίψη νομίσματος.

Auction Type	Outcome	Automatic tie-breaking	Rounds	Communication
First-price	Private	Yes	$O(1)$	$O(nk)$
First-price	Public	No	$O(1)$	$O(k)$
Second-price	Private	Yes	$O(1)$	$O(n^2k)$
Second-price	Public	No	$O(1)$	$O(nk)$
(M+1)-price	Private	No	$O(1)$	$O(n(n-M)kM)$
(M+1)-price	Public	No	$O(1)$	$O((n-M)kM)$

Αναφορές

[1] Ben-Or, M., Goldwasser, S., Wigderson, A.: Completeness theorems for non-cryptographic fault-tolerant distributed computation. In: Proceedings of the 20th Annual ACM Symposium on the Theory of Computing (STOC), pp. 1–10. ACM, New York (1988)

[2] Chaum, D., Crépeau, C., Damgård, I.: Multi-party unconditionally secure protocols. In: Proceedings of the 20th Annual ACM Symposium on the Theory of Computing (STOC), pp. 11–19. ACM, New York (1988)

[3] Garay, J., MacKenzie, P., Yang, K.: Efficient and secure multiparty computation with faulty majority and complete fairness. Cryptology ePrint Archive, Report 2004/009 (2004)

[4] Goldreich, O.: Foundations of Cryptography, vol. 2. Basic Applications. Cambridge University Press, Cambridge (2004)

[5] Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game or a completeness theorem for protocols with honest majority. In: Proceedings of the 19th Annual ACM Symposium on the Theory of Computing (STOC), pp. 218–229. ACM, New York (1987)

[6] Goldwasser, S., Levin, L.: Fair computation of general functions in presence of immoral majority. In: Advances in Cryptology— Proceedings of the 10th Annual International Cryptology Conference (CRYPTO). Lecture Notes in

Computer Science (LNCS), vol. 537, pp. 77–93. Springer, Berlin Heidelberg New York (1990)

[7] Pass, R.: Bounded-concurrent secure multiparty computation with a dishonest majority. In: Proceedings of the 36th Annual ACM Symposium on the Theory of Computing (STOC), pp. 232–241. ACM, New York (2004)

[8] Porter, R., Shoham, Y.: On cheating in sealed-bid auctions. In: Proceedings of the 4th ACM Conference on Electronic Commerce (ACM-EC), pp. 76–84. ACM, New York (2003)

[9] Rothkopf, M.H., Harstad, R.M.: Two models of bid-taker cheating in Vickrey auctions. J. Business 68(2), 257–267 (1995)

[10] Rothkopf, M.H., Teisberg, T.J., Kahn, E.P.: Why are Vickrey auctions rare? J. Pol. Econ. 98(1), 94–109 (1990)

[11] Sandholm, T.: Issues in computational Vickrey auctions. International Journal of Electronic Commerce, Special Issue Intell. Agents Electron. Commer. 4(3), 107–129 (2000)

[12] Vickrey, W.: Counter speculation, auctions, and competitive sealed tenders. J. Finance 16(1), 8–37 (1961)

[13] Yao, A.C.: How to generate and exchange secrets. In: Proceedings of the 27th Symposium on Foundations of Computer Science (FOCS), pp. 162–167. IEEE Comput. Soc. Press (1986)