Πρακτική διατήρηση εχεμύθειας, επαληθεύσιμα ορθές και αξιόπιστες δημοπρασίες

David C. Parkes, Michael O. Rabin, Stuart M. Shieber, Christopher Thorpe
Harvard University SEAS
33 Oxford Street,
Cambridge MA 02138, USA

Περίληψη

Στην παρούσα εργασία παρουσιάζεται ένα πρακτικό πρωτόκολλο βασισμένο σε ομοιομορφικές μεθόδους κρυπτογραφίας για την διεξαγωγή αποδείξιμα δίκαιων δημοπρασιών σφραγισμένης προσφοράς. Το σύστημα διατηρεί την εχεμύθεια των προσφορών ακόμα και μετά την ανακοίνωση των αποτελεσμάτων της δημοπρασίας, ενώ παράλληλα παρέχει δυνατότητες δημόσιας επαλήθευσης της ορθότητας και της εμπιστευτικότητας. Καμία πλευρά, συμπεριλαμβανομένου και του δημοπράτη, δεν λαμβάνει πληροφορίες για τις προσφορές πριν κλείσει η δημοπρασία. Επίσης, κανένας πλειοδότης δεν έχει την δυνατότητα να αλλάξει ή να αποσύρει την προσφορά του. Το προτεινόμενο σύστημα παρουσιάζεται για εφαρμογές πρώτης προσφοράς, ομοιόμορφης προσφοράς καθώς και δεύτερης προσφοράς δημοπρασίες, συμπεριλαμβανομένων και δημοπρασιών πολλών αντικειμένων. Τέλος, παρατίθενται εμπειρικά αποτελέσματα στην ανάλυση ενός πρωτοτύπου που παρουσιάζουν την πρακτικότητα του πρωτοκόλλου σε εφαρμογές του πραγματικού κόσμου.

I. Εισαγωγη

Α΄. Σημασία

Τα τελευταία χρόνια πολλές συνιστώσες (ανταγωνιστικότητα τιμών, οικονομική αποδοτικότητα κτλ) έχουν συμβάλλει στην ραγδαία αύξηση του αριθμού των δημοπρασιών παγκοσμίως, όπως επιβεβαιώνεται και από το ύψος των συναλλαγών που πραγματοποιούνται διεθνώς. Το διαδίκτυο διαδραματίζει σημαντικό ρόλο γιατί μειώνει το κόστος της συμμετοχής ενώ παράλληλα ενισχύει τον παγκόσμιο ανταγωνισμό, επιταχύνοντας πολλές διαδικασίες που μια δημοπρασία απαιτεί. Ένας παράγοντας που επιδρά θετικά στην δημοφιλία των δημοπρασιών είναι η παροχή κινήτρων στους πλειοδότες[1] ώστε αυτοί να λειτουργήσουν ως 'έμπιστοι μεσάζοντες' πληροφορίας έτσι ώστε στο πλαίσιο της προμήθειας, ο νικητής να είναι αυτός με την τεχνικά πιο συμφέρουσα προσφορά.

Β΄. Προβλήματα

Οι δημοπρασίες αντιμετωπίζουν προβλήματα που κληρονομούν από τον πραγματικό κόσμο στον οποίο διεξάγονται. Τυπικά προβλήματα που πρέπει να αντιμετωπιστούν αφορούν την διαφθορά και την ορθή διεκπεραίωση της διαδικασίας. Αυτά μπορούν να χωριστούν σε δυο κατηγορίες ανάλογα με τον χρόνο στον οποίο γίνεται η αλλοίωση του αποτελέσματος (κατά την διάρκεια της δημοπρασίας ή μετά). Όσον αφορά τα προβλήματα πριν το κλείσιμο της δημοπρασίας, ελοχεύει ο κίνδυνος να αποκαλύπτονται πληροφορίες για τις υποβαλλόμενες προσφορές ή και να εισάγονται, ή τροποποιούνται, προσφορές έπειτα από την κατάθεση μιας προσφοράς από έναν πλειοδότη. Προβλήματα μετά το κλείσιμο της δημοπρασίας περιλαμβάνουν την τροποποίηση, ή ακύρωση, κάποιας προσφοράς από τον δημοπράτη, συνήθως έπειτα από μια δωροδοκία. Παράδειγμα αποτελεί η πρόσκληση κάποιου μετέχοντα στην δημοπρασία, ύστερα από το τέλος αυτής, με σκοπό την τροποποίηση της προσφοράς του ώστε να κερδίσει την δημοπρασία με τους καλύτερους δυνατούς όρους για αυτόν.

Οι δημοπρασίες δεύτερης προσφοράς είναι ανθεκτικές στα προαναφερθέντα προβλήματα καθώς κανένας πλειοδότης δεν αποκτά πλεονέκτημα αφού όλοι έχουν την ίδια δυνατότητα να συνδυάσουν

[1] Λόγω έλλειψης αντίστοιχου όρου με το bidder στα ελληνικά ώστε να το μεταφράσουμε, θα κάνουμε κατάχρηση από εδώ και στο εξής του όρου 'πλειοδότης', εννοώντας πάντα κάποιον που κάνει προσφορά στη δημοπρασία και όχι απαραίτητα αυτόν που τελικά κερδίζει.

τις διάφορες προσφορές μέσω των κανόνων της δημοπρασίας. Ωστόσο παρουσιάζουν τις δικές τους ιδιοσυγκρασίες που δημιουργούν καινούργια προβλήματα. Ένα παράδειγμα αποτελεί ο δημοπράτης να έχει συνεργαστεί με τους πλειοδότες με τις δυο μεγαλύτερες προσφορές προτρέποντας τον πλειοδότη με την δεύτερη υψηλότερη προσφορά να αποσυρθεί με αποτέλεσμα ο νικητής να πληρώσει την τρίτη μεγαλύτερη προσφορά. Επίσης, παρέχεται η δυνατότητα στον δημοπράτη να τοποθετήσει μια πλαστή προσφορά λίγο μικρότερη από την προσφορά του νικητή ώστε να τον αναγκάσει να πληρώσει μεγαλύτερο χρηματικό ποσό.

Ως γενικό συμπέρασμα, σύμφωνα με την έρευνα που έχει γίνει στο συγκεκριμένο πεδίο, προκύπτει η ανάγκη για αποδεδειγμένα αξιόπιστες και εχέμυθες δημοπρασίες σφραγισμένης πρώτης προσφοράς, με έμφαση στην ανάγκη ανοικτής και διαφανούς διαδικασίας. Από τα παραπάνω παραδείγματα προκύπτει ότι η χρήση κανόνων και ποινών συχνά είναι ανεπαρκής για τις συνήθεις λύσεις. Όπως επιβεβαιώνει και ο Andvig [1], δεν αποτελεί λύση ο περιορισμός της πρόσβασης σε πληροφορίες καθώς όσο μειώνονται τα εμπλεκόμενα άτομα που είναι υπεύθυνα για την διασφάλιση της διαδικασίας, τόσο αυξάνεται η πιθανότητα για διαφθορά.

Γ΄. Λύση

Η ορθότητα της προτεινόμενης λύσης εξασφαλίζεται από την μυστικότητα των προσφορών (ακόμα και από τον δημοπράτη) μέχρι το πέρας της δημοπρασίας. Η επαλήθευση του αποτελέσματος γίνεται με την χρήση κρυπτογραφικών μεθόδων.

Όλες οι πλευρές κατέχουν ένα ζευγάρι δημόσιου/ιδιωτικού κλειδιού και χρησιμοποιούν την ομομορφική μέθοδο κρυπτογραφίας του Pascal Paillier [5]. Ο δημοπράτης δίνει το εναρκτήριο λάκτισμα της δημοπρασίας, τοποθετώντας τις απαραίτητες πληροφορίες για αυτήν σε έναν πίνακα ανακοινώσεων. Οι πλειοδότες μέσα σε συγκεκριμένο χρονικό διάστημα υποβάλλουν κρυπτογραφημένες φόρμες με τις προσφορές τους μαζί με κάποια τυχαία δεδομένα που χρησιμοποιούνται για την διασφάλιση της διαδικασίας. Ύστερα από το πέρας της δημοπρασίας, ο δημοπράτης αποκρυπτογραφεί τις προσφορές και εξάγει το αποτέλεσμα της δημοπρασίας σύμφωνα με τους ανακοινωθέντες κανόνες. Έπειτα, αναρτάται το αποτέλεσμα στον πίνακα ανακοινώσεων και οι απαραίτητες πληροφορίες έτσι ώστε κάθε πλειοδότης να μπορεί να επαληθεύσει την εγκυρότητα του. Αν ο πλειοδότης για κάποιον λόγο δεν μείνει ικανοποιημένος από τα μέσα που του παρέχονται για την επαληθευσιμότητα της εγκυρότητας, μπορεί ιδιωτικά να λάβει επιπλέον αποδεικτικά στοιχεία για αυτήν (πχ σε περίπτωση κίνησης δικαστικών μέσων).

Η συγκεκριμένη λύση δεν προσπαθεί να διασφαλίσει την ανωνυμία των πλειοδοτών καθώς θεωρείται ότι υπάρχουν επαρκείς μέθοδοι (πχ μέσω κάποιου νόμιμου ενδιάμεσου εξυπηρετητή (proxy server)) στις οποίες μπορεί να καταφύγει ο πλειοδότης. Όλα τα παραπάνω προϋποθέτουν μια έμπιστη υπολογιστική δομή βασισμένη σε ασφαλές υλικό και έμπιστο (ψηφιακά υπογεγραμμένο) λογισμικό εγκατεστημένη σε μια φυσικά ασφαλή τοποθεσία.

Ιδιαίτερη προσοχή δίνεται σε δυο επιπρόσθετες πλευρές από άποψη πρακτικότητας. Η δημοπρασία πρέπει να τερματίζει σε λογικό χρόνο και έχοντας λογικές απαιτήσεις σε κόστος επικοινωνίας, χρησιμοποιώντας κοινό υλικό ακόμα και για μεγάλου μεγέθους, ως προς τον αριθμό πλειοδοτών, δημοπρασίες. Για τον λόγο αυτό, η προτεινόμενη μέθοδος παραλληλοποιείται εύκολα. Επιπρόσθετα, η υπολογιστική αρχιτεκτονική οφείλει να συνάδει με πρακτικά επιχειρηματικά μοντέλα. Θεωρήθηκε πως ένα μοντέλο στο οποίο συμμετέχει ένας μόνο δημοπράτης ο οποίος είναι αποκλειστικά υπεύθυνος για την διεξαγωγή της δημοπρασίας και ανεξάρτητη επαλήθευση από τρίτους, αποτελεί ρεαλιστικότερη λύση από επιχειρηματικής πλευράς.

Για την διασφάλιση της ορθότητας της διαδικασίας χρησιμοποιούνται δύο επιπλέον οντότητες. Οι συμβολαιογράφοι που λειτουργούν ως μάρτυρες για την υποβολή των προσφορών και για την ορθή αποδοχή τους από τον δημοπράτη, και η υπηρεσία κρυπτογράφησης περιορισμένου χρόνου (TLC –

time-lapse cryptography service) που αποτρέπει την αποκάλυψη, ή απόσυρση, των προσφορών πριν το τέλος της δημοπρασίας.

Μέριμνα έχει ληφθεί για την αποτροπή της σύστασης των δακτυλίων προσφοράς (bidding rings). Ένα χαρακτηριστικό το οποίο υποβοηθάει τη σύσταση τέτοιων δακτυλίων είναι η πληροφόρηση για το ποια προσφορά αντιστοιχεί σε κάποιον. Μη καθιστώντας δυνατή επομένως την πρόσβαση σε αυτού του είδους την πληροφορία δυσκολεύεται η δημιουργία τους καθώς δεν προσφέρονται επαρκή στοιχεία ώστε να πιεστεί κάποιος πλειοδότης από τους υπόλοιπους λόγω της προσφοράς του. Τα παραπάνω διασφαλίζονται από την εχεμύθεια των υποβαλλόμενων δεδομένων.

Στο τέλος του paper, επίσης, παρατίθενται τα αποτελέσματα της πειραματικής αξιολόγησης της λύσης, όπως αυτή υλοποιήθηκε σε Python και σε C++.

II. Βασικες Εννοιες

Α΄. Ορισμός δημοπρασίας

Ορίζουμε ως προς τα εμπρός δημοπρασία, εκείνη στην οποία στόχος είναι η δέσμευση ενός ή περισσοτέρων αντικειμένων από ένα σύνολο από πλειοδότες. Οι αντίστροφες δημοπρασίες, με αγοραστή αντί για πωλητή, που είναι κατάλληλες για δημοπρασίες προμήθειας, μπορούν να μοντελοποιηθούν παρομοίως και για αυτό τον λόγο θα επικεντρωθούμε στις πρώτες.

Η προσφορά Bid_i από τον πλειοδότη B_i γίνεται χωρίς κάποια πληροφόρηση για την αξία της προσφοράς των υπολοίπων, και ένα αντικείμενο πωλείται στο μεγαλύτερο πλειοδότη, ο οποίος πληρώνει και την τιμή που ορίζεται σύμφωνα με τους κανόνες της δημοπρασίας[2].

Β΄. Επιθυμητές ιδιότητες δημοπρασίας

Για να χαρακτηριστεί ως αποδεκτός ο αλγόριθμος που προτείνεται, είναι επιθυμητό αυτός να παρέχει ορισμένες συγκεκριμένες δυνατότητες.

- *Μη απόσυρση προσφοράς από πλειοδότη:* Όταν ένας πλειοδότης υποβάλλει την προσφορά του, αυτή αποδείξιμα δεν μπορεί να αλλαχθεί.
- *Μη απόσυρση προσφοράς από δημοπράτη:* Ο αποκλεισμός από τον δημοπράτη μιας έγκυρα υποβεβλημένης προσφοράς μπορεί να αποδειχθεί και έτσι να επιφέρει νομική δράση.
- *Εμπιστευτικότητα:* Ο δημοπράτης δεν μπορεί να λάβει γνώση των προσφορών πριν το πέρας του χρονικού διαστήματος υποβολής προσφορών.
- *Εχεμύθεια:* Οι προσφορές είναι κρυφές από όλους μέχρι την υποβολή τους. Στο κλείσιμο της δημοπρασίας μόνο ο δημοπράτης γνωρίζει όποια κρυφή πληροφορία και εναπόκειται στην κρίση του η αποκάλυψη της.
- *Επαληθεύσιμη ορθότητα:* Οποιαδήποτε αποκαλυπτόμενη πληροφορία, είτε ιδιωτικά είτε δημόσια, είναι επαληθεύσιμη.

Επειδή η ασφάλεια της κρυπτογράφησης σχετίζεται με την υπολογιστική αδυναμία της επίλυσης ‘δύσκολων’ κρυπτογραφικών προβλημάτων, μεγαλύτερα κλειδιά μπορούν να χρησιμοποιούνται με το πέρας του χρόνου, όπως το υλικό των υπολογιστικών συστημάτων γίνεται όλο και πιο ισχυρό.

Γ΄. Είδη δημοπρασίας

1) Vickrey δημοπρασία: Η Vickrey δημοπρασία είναι μια δημοπρασία σφραγισμένης προσφοράς, όπου οι πλειοδότες δεν γνωρίζουν τις προσφορές των άλλων. Η μεγαλύτερη προσφορά κερδίζει, αλλά πληρώνεται από τον νικητή το ποσό που αντιστοιχεί στην αμέσως μικρότερη προσφορά. Όταν αναφερόμαστε σε δημοπρασίες ενός αντικειμένου, ο όρος είναι ταυτόσημος με τον όρο δημοπρασία σφραγισμένης δεύτερης προσφοράς.

[2]Ανάλογα με το αν είναι μια δημοπρασία πρώτης προσφοράς ή δεύτερης

Μια πρώτη, προφανή γενίκευση της Vickrey δημοπρασίας, αποτελεί η δημοπρασία ομοιόμορφης τιμής. Αυτή αφορά δημοπρασίες πολλών αντικειμένων και εκεί οι νικητές πληρώνουν την τιμή που αντιστοιχεί στην μεγαλύτερη προσφορά που έγινε από παίκτη που δεν πήρε κάποιο αντικείμενο. Ωστόσο, η δημοπρασία ομοιόμορφης τιμής δεν αναγκάζει τους μετέχοντες να δηλώσουν την πραγματική αξία που πιστεύουν ότι αντιστοιχεί στα αντικείμενα που επιθυμούν να αγοράσουν. Αυτό το πρόβλημα έρχεται να αντιμετωπίσει η GVA. Η κεντρική ιδέα στη GVA είναι ότι κάθε πλειοδότης πληρώνει το κόστος ευκαιρίας που προκαλεί η παρουσία του στους υπόλοιπους μετέχοντες. [4]

Η GVA πληρωμή δίνεται από τον τύπο (1).

$$p_{(VCG,i)} = QTY_i^* \cdot Bid_i - [V(B) - V(B_{-i})] \tag{1}$$

όπου $p_{(VCG,i)}$ είναι η πληρωμή του i-οστού πλειοδότη για να πάρει ποσότητα αντικειμένων ίση με QTY_i^* και να πληρώσει για καθένα Bid_i. Το $V(B)$ πρόκειται για το συνολικό κέρδος της δημοπρασίας από όλους τους πλειοδότες ενώ το $V(B_{-i})$ το συνολικό κέρδος από όλους τους πλειοδότες χωρίς τον B_i.

Δ΄. Στοιχεία πραγματικού κόσμου

Υποθέτουμε ένα παγκόσμια προσβάσιμο και αξιόπιστο ρολόι, όπως για παράδειγμα αυτό προσφέρεται από τον NIST server στις ΗΠΑ και τα παρακάτω στοιχεία.

1) Επικυρωμένος πίνακας ανακοινώσεων: Ο δημοπράτης διατηρεί ένα επικυρωμένο πίνακα ανακοινώσεων. Αυτός μπορεί να είναι δημοσιευμένος σε μια ιστοσελίδα και να διαχειρίζεται από τον ίδιο. Χρησιμοποιείται από αυτόν για να δημοσιεύει όλες τις δημόσιες πληροφορίες σχετικά με την δημοπρασία, περιλαμβάνοντας αρχικές ανακοινώσεις, (κρυπτογραφημένες) πληροφορίες προσφορών και αποδείξεις που μπορούν να υποβοηθήσουν στην επαλήθευση των προσφορών. Κάθε ανάρτηση στον πίνακα ανακοινώσεων περιλαμβάνει μια ψηφιακή υπογραφή που ταυτοποιεί το πρόσωπο που προβαίνει σε αυτή.

2) Διαφθορά: Με τον όρο διαφθορά εννοούμε την παραβίαση των κανόνων της δημοπρασίας από τον δημοπράτη με σκοπό να ευνοήσει κάποιους πλειοδότες έπειτα από δωροδοκία. Το ενδεχόμενο διαφθοράς υπάρχει σε δημοπρασίες όπου ο κάτοχος των αγαθών προς πώληση δεν είναι ο δημοπράτης. Ένα τυπικό παράδειγμα αποτελεί η δημοπρασία δημοσίων αγαθών.

3) Συμβολαιογράφοι: Οι συμβολαιογράφοι είναι ευυπόληπτοι πράκτορες, όπως δικηγορικά γραφεία ή λογιστές, οι οποίοι δρουν ως *μάρτυρες* για τους πλειοδότες. Πριν τη συμμετοχή του σε μία δημοπρασία ο πλειοδότης καλείτε να διαλέξει ένα σύνολο συμβολαιογράφων από το επιτρεπόμενο σύνολο το οποίο μπορεί να έχει επιλεχθεί από τον δημοπράτη. Στη συνέχεια κάθε υποβαλλόμενη πληροφορία από τον πλειοδότη προς τον δημοπράτη κοινοποιείται κρυπτογραφημένα και στον συμβολαιογράφο. Έτσι αυτός αναλαμβάνει το ρόλο της επίλυσης οποιασδήποτε διαφωνίας για την εγκυρότητα των υποβληθέντων προσφορών. Απαιτείται η πλειοψηφία των συμβολαιογράφων να μη μπορούν να χρηματιστούν.

4) Κρυπτογραφική υπηρεσία περιορισμένου χρόνου: Ένας πλειοδότης B_i πιθανώς σε συνεργασία με τον δημοπράτη, μπορεί να αρνηθεί να αποκαλύψει τη κρυπτογραφημένη προσφορά $E(Bid_i)$. Ένας τρόπος να αποτρέψουμε αυτή τη πρακτική είναι η χρήση μιας κρυπτογραφικής υπηρεσίας περιορισμένου χρόνου.

Η υπηρεσία σε κανονικά διαστήματα θα δημοσιεύει ένα καινούργιο δημόσιο κρυπτογραφικό κλειδί TPK (Time-lapse Public Key), και μετά από μία σταθερή χρονική περίοδο το αντίστοιχο ιδιωτικό κλειδί αποκρυπτογράφησης TSK (Time-lapse Secret Key). Για τους σκοπούς της παρούσας εργασίας αρκεί το δημόσιο κλειδί να είναι διαθέσιμο πριν την υποβολή των προσφορών και το αντίστοιχο ιδιωτικό κλειδί σύντομα μετά το πέρας της δημοπρασίας.

Πιο αναλυτικά κάθε πλειοδότης B_i υποβάλει την κρυπτογραφημένη προσφορά $Z = E_{TPK}(E(Bid_i))$. Το $E(Bid_i)$ συνιστά την κρυπτογραφημένη προσφορά του B_i με το δημόσιο κλειδί του δημοπράτη AU.

Ο πλειοδότης έπειτα αναρτά το $Sign_i(Z)$ στο πίνακα ανακοινώσεων. Μετά το χρονικό διάστημα $T+1$,[3] το κλειδί αποκρυπτογράφησης TSK θα αναρτηθεί από την TLC υπηρεσία με αποτέλεσμα ο δημοπράτης να ανακτήσει τις κρυπτογραφημένες προσφορές των πλειοδοτών.

Ε'. Ομοιομορφική κρυπτογράφηση

Ορισμός 2.1: Ο αλγόριθμος κρυπτογράφησης $E()$ είναι ομοιομορφικός αν δοθέντος $E(x)$ και $E(y)$, κάποιος μπορεί να αποκτήσει το $E(x \circ y)$ για κάποια $\circ$ λειτουργία. [8]

Η ομοιομορφική κρυπτογράφηση είναι μια μορφή κρυπτογράφησης όπου κάποιος μπορεί να εφαρμόσει ένα συγκεκριμένο σύνολο από αλγεβρικές πράξεις σε ένα μη κρυπτογραφημένο κείμενο, εφαρμόζοντας αντίστοιχες (όχι απαραίτητα ίδιες) στο αντίστοιχο κρυπτογραφημένο. Αυτή η ιδιότητα, από κρυπτογραφικής απόψεως, έχει θετικά και αρνητικά. Στα ομοιομορφικά συστήματα κρυπτογράφησης, λόγω της παραπάνω ιδιότητας μπορεί κάποιος να μεταβάλλει τις τιμές σε ένα κρυπτογραφημένο κείμενο, και να παράξει κάποιο άλλο, στο οποίο να μπορεί να καθορίσει τον τρόπο με τον οποίο θα διαφέρει από το αρχικό. Αυτό καθιστά τα ομοιομορφικά συστήματα, που έχουν την παραπάνω ιδιότητα από σχεδιασμού, ακατάλληλα για ασφαλή μεταφορά δεδομένων. Γι αυτό για παράδειγμα το RSA[4] χρησιμοποιεί τεχνικές μετακίνησης padding του κρυπτογραφημένου μηνύματος με βάση μια ψευδοτυχαία σταθερά. Από την άλλη, η ιδιότητα αυτή (ομοιομορφισμός), τα καθιστά ιδιαίτερα χρήσιμα για την δημιουργία ασφαλών συστημάτων ψηφοφορίας, ιδιωτικής ανάκτησης πληροφορίας αλλά και on-line δημοπρασιών.

ϝ'. Paillier

1) Δημιουργία κλειδιού: Όπως στο RSA, διαλέγουμε δυο πρώτους αριθμούς p, q και έστω $N = p \cdot q$ αλλά εδώ θα δουλέψουμε $mod\, N^2$. Ισχύει: $\phi(N^2) = N \cdot \phi(N) = N \cdot \phi(p) \cdot \phi(q)$ και ότι όλα τα στοιχεία έχουν διάταξη διαιρώντας το $\phi(N^2)$. Δημιουργούμε το $PK = (N, g)$, το οποίο είναι τάξης πολλαπλάσιο του N και $SK = (\lambda(n) = lcm(p-1, q-1))$, όπου το lcm είναι το ελάχιστο κοινό πολλαπλάσιο lowest common multiple. [8]

Θυμίζουμε πως $\phi(n) = (p-1)(q-1)$, είναι η συνάρτηση του Euler και επιστρέφει το πλήθος των ακεραίων που είναι σχετικά πρώτοι στο n.

2) Κωδικοποίηση μηνύματος: Για την κωδικοποίηση ενός μηνύματος $m \in Z_n$:

- Διαλέγουμε ένα $x \in_R Z_N^*$.
- Έχουμε $E(m) = g^m x^N \, mod\, N^2$.

Αν χρησιμοποιήσουμε και μια τυχαία μεταβλητή r τότε η κρυπτογράφηση δίνεται από την (2).

$$E(x, r) = (1 + xn) \cdot r^n \, (mod\, n^2) \tag{2}$$

Ο Pallier έχει την προσθετική ομοιομορφική ιδιότητα. Ο πολλαπλασιασμός ή η διαίρεση είναι δυνατές μόνο αν ο αριθμός k με τον οποίο θέλουμε να πολλαπλασιάσουμε ή να διαιρέσουμε αντίστοιχα είναι αντιστρέψιμος $mod\, n^2$.

3) Αποκωδικοποίηση μηνύματος: Ορίζουμε για $u \equiv 1 mod\, N$:

$$L(u) = \frac{u-1}{N} \tag{3}$$

- Εάν $c = E(m)$, τότε:

[3] όπου T ο χρόνος λήξης της δημοπρασίας

[4] Το RSA έχει την πολλαπλασιαστική ομοιομορφική ιδιότητα. $E(m_1) \cdot E(m_2) = E(m_1 m_2)$

$$m = \frac{L(c^{\lambda(n)} \, mod \, N^2)}{L(c^{\lambda(n)} \, mod \, N^2)} \, mod \, N \quad [2] \tag{4}$$

- Εάν $c = E(m, r)$, τότε:

$$x = \frac{\frac{C^{\phi(n)}-1}{\phi(n)} \, mod \, n^2}{n} \tag{5}$$

αφού $r^{n \cdot \phi(n)} \equiv 1 \, (mod \, n^2)$

4) Λόγοι χρήσης Paillier:

- Έχει την ομοιομορφική ιδιότητα που χρειαζόμαστε για την επαλήθευση της δημοπρασίας. Το επιφορτισμένο μέλος για την απόδειξη της ορθότητας P, το οποίο γνωρίζει το μυστικό κλειδί ϕ, μπορεί να αποδείξει ένα πλήρες σύνολο με ισότητες και ανισότητες για δύο κρυπτογραφημένες τιμές $E(x_1)$ και $E(x_2)$, χωρίς να αποκαλύψει τίποτα για τις τιμές x_1 ή x_2.
- Είναι *σημασιολογικά 'ασφαλής'*. Σημασιολογικά ασφαλής σημαίνει ότι δεν μπορούμε να ξεχωρίσουμε το $E(0)$ από το $E(1)$ καλύτερα από 50% όπως το $N \to \infty$.
- Είναι δυνατό κάποιος που γνωρίζει την τιμή r που έχει χρησιμοποιηθεί για την κρυπτογράφηση $c = E(x, r)$, να αποδείξει ότι η αποκρυπτογράφηση x είναι η μοναδική αποκρυπτογράφηση του C, αποκαλύπτοντας το r.

Ζ'. Ασφαλή τυχαία δεδομένα

Υποθέτουμε ότι τουλάχιστον ένα συμμετέχοντας στη δημοπρασία έχει μια πραγματικά τυχαία ακολουθία δεδομένων. Θεωρώντας ως δεδομένη τη παραπάνω υπόθεση, και με τη χρήση της συνάρτησης *Αποκλειστικό - 'Η* (Exclusive - OR) διασφαλίζουμε ότι ο συνδυασμός των τυχαίων ακολουθιών όλων των μετεχόντων είναι πράγματι τυχαίος. Χρησιμοποιώντας το αποτέλεσμα X της παραπάνω λειτουργίας αναγκάζουμε τον δημοπράτη όταν αποδεικνύει την ορθότητα της δημοπρασίας να αποκαλύπτει και δεδομένα όπως αυτά καθορίζονται από τα ψηφία του X.

Η'. Επανακρυπτογράφηση κρυπτογραφημένων κειμένων

Για να επανακρυπτογραφήσουμε μία ήδη κρυπτογραφημένη τιμή μέσω Paillier, έστω $E(Bid_i, r)$, το επιφορτισμένο μέλος για την απόδειξη της ορθότητας υπολογίζει μία τυχαία τιμή $S \in \mathbb{Z}_n^*$ και υπολογίζει το $s^n \cdot E(Bid_i, r) \equiv E(Bid_i, r \cdot s)(mod \, n^2)$. Αυτό παραμένει μία έγκυρη κρυπτογράφηση του Bid_i, αλλά μόνο κάποιος που γνωρίζει το s ή το μυστικό κλειδί αποκωδικοποίησης ϕ μπορεί να το αποδείξει.

Η επανακρυπτογράφηση είναι *καλά συμπληρωμένη* μέσω ενός πρωτοκόλλου 'τομής και επιλογής' έτσι ώστε αυτός που κάνει την απόδειξη P να κατασκευάζει 2ν τυχαία επανακρυπτογραφημένα σύνολα τιμών, και ο επαληθευτής V ζητάει για ν από τα σύνολα να εμφανιστούν, αποκαλύπτοντας τους τυχαίους παράγοντες που χρησιμοποιήθηκαν για την κατασκευή τους. Τότε ο V ελέγχει κάθε επανακρυπτογραφημένο σύνολο αν περιέχει ακριβώς τα αρχικά στοιχεία.

III. Βασικα θεωρηματα

Παρακάτω παρατίθενται κάποια βασικά θεωρήματα που χρειάζονται για την απόδειξη των απαραίτητων ιδιοτήτων που προαναφέρθηκαν ότι είναι επιθυμητό να έχει μοντέλο. Οι αποδείξεις παραλείπονται και όποιος ενδιαφέρεται μπορεί να ανατρέξει στο [6].

Α΄. Διατηρησιμότητας εχεμύθειας για ισότητες και ανισότητες

Θεώρημα 3.1: Συγκρίσεις Ισότητας: Δοθέντων δύο κρυπτογραφημένων κειμένων $C_1 = E(x_1, r_1)$ και $C_2 = E(x_2, r_2)$, ο P μπορεί να αποδείξει ότι $x_1 = x_2$ χωρίς να αποκαλύψει επιπλέον πληροφορίες για την τιμή του x_1 ή του x_2.

Θεώρημα 3.2: Συγκρίσεις Ανισότητας: Δοθέντων δύο κρυπτογραφημένων κειμένων $C_x = E(x)$ και $C_y = E(y)$, ο P μπορεί να δείξει ότι $x > y$ και $x \geq y$. Επειδή οι τιμές x, y είναι ακέραιοι $mod\, n^2$, μπορεί να αποδειχθεί ότι $x > y$ δείχνοντας ότι $x \geq y + 1$, θεωρώντας ότι $y \neq n - 1$.

Β΄. Διατηρησιμότητας εχεμύθειας για κρυπτογραφημένα γινόμενα

Επειδή η κρυπτογράφηση Paillier δεν υποστηρίζει διατηρησιμότητα εχεμύθειας κατά τον πολλαπλασιασμό δυο κρυπτογραφημένων τιμών, όπως γίνεται στην πρόσθεση, απαιτείται μια μέθοδος που επιτρέπει στον P με 3 κείμενα u, v, w, έτσι ώστε $uv = w\,(mod\, n)$, να αποδείξει το γεγονός σε έναν επαληθευτή V που έχει τις κρυπτογραφήσεις Paillier $E(u)$, $E(v)$, $E(w)$ αντίστοιχα.

Ορισμός 3.3: Ένα σύνολο δοκιμών πολλαπλασιασμού (Multiplication test set (MTS)) για $E(u, r)$, $E(v, s)$, $E(w, t)$ είναι ένα σύνολο από 8 στοιχεία:

$\{E(u_1, r_1), E(u_2, r_2), E(v_1, s_1), E(v_2, s_2), E(w_{i,j}) = E(u_i v_j, p_{i,j}) | i, j \in \{1, 2\}\}$.

Όπου $u = u_1 + u_2 (mod\, n)$ και $v = v_1 + v_2 (mod\, n)$.

Σε κάθε MTS, τα u_1 και v_1 επιλέγονται τυχαία με βάση την ομοιόμορφη κατανομή από το $\mathbb{Z}_n$· u_2 και v_2 είναι αντίστοιχα ορισμένα, όπως παραπάνω, έτσι ώστε $u = u_1 + u_2 (mod\, n)$. Ομοίως και για το v.

Είναι εμφανές ότι δοθέντων κρυπτογραφήσεων όπως σε ένα MTS και $w_{1,1} + w_{1,2} + w_{2,1} + w_{2,2} = w\,(mod\, n)$, τότε πράγματι $uv = w\,(mod\, n)$. Για να αποδείξει ο P και να επαληθεύσει ο V όλες τις σχέσεις που περιλαμβάνονται σε ένα MTS ο P πρέπει να αποκαλύψει τα u_1, u_2, v_1, v_2, τα οποία τελικά θα αποκαλύψουν τα u, v.

Γ΄. Επαληθεύσιμες δοκιμές εύρους τιμών, διατηρώντας την μυστικότητα

Για να αποδείξουμε για δυο τιμές a, b ότι $a \geq b$ μπορούμε να δείξουμε ότι $a, b < \frac{n}{2}$ και ακολούθως ότι $(a - b)\,(mod\, n) < \frac{n}{2}$. Δοθέντων δύο κρυπτογραφημένων κειμένων $C = E(x, r)$ θέλουμε να αποδείξουμε ότι $x < 2^t$ για t τέτοιο ώστε $2^t < \frac{n}{2}$ ώστε να μπορούμε να δείξουμε ότι μια προσφορά είναι μικρότερη από ένα άνω όριο (2^t).

Ορισμός 3.4: Ένα έγκυρο σύνολο τιμών TS για τον ισχυρισμό ότι '$C = E(x, r)$ είναι μια κρυπτογράφηση ενός αριθμού $x < 2^t < \frac{N}{2}$ ', είναι ένα σύνολο από $2t$ κρυπτογραφήσεις: $TS = \{G_1 = E(u_1, s_1) ..., G_{2t} = E(u_{2t}, s_{2t})$, όπου κάθε μια από τις δυνάμεις του 2 μέχρι το 2^{t-1} εμφανίζεται στο u_i ακριβώς μία φορά και οι εναπομείναντες t τιμές u_j είναι όλες 0. Κάθε στοιχείο του συνόλου δοκιμών είναι σε τυχαία σειρά.

Με την χρήση ενός συνόλου δοκιμών ο P μπορεί να αποδείξει ότι $x < 2^t < \frac{n}{2}$ όπως παρουσιάζεται παρακάτω.

Δ΄. Πρωτόκολλο εύρους και επαλήθευσης

Έστω $x = 2^{t_1} + ... + 2^{t_l}$ η αναπαράσταση του x σαν άθροισμα διακριτών δυνάμεων του 2. Ο δημοπράτης διαλέγει από ένα TS τις κρυπτογραφήσεις $G_{j_1}, ..., G_{j_l}$ των $2^{t_1}, ..., 2^{t_l}$ και επιπλέον $t - l$ κρυπτογραφήσεις $G_{j_{l+1}}, ..., G_{j_t}$ του 0. Σημειώνεται ότι:

$(E(x, r)^{-1} \cdot G_{j_1} \cdot ... \cdot G_{j_t})(mod\, n^2) = E(0, s)$ είναι μια κρυπτογράφηση του 0 με βοηθητική τιμή $s = (r^{-1} \cdot s_{j_1} \cdot ... \cdot s_{j_t})(mod\, n)$ αν και μόνο αν $x = 2^{t_1} + ... + 2^{t_l}$ και G_{j_h} έχει επιλεγεί όπως αναφέρθηκε. Από την στιγμή που ο P έχει το κλειδί αποκρυπτογράφησης ϕ και ξέρει την προαναφερθείσα βοηθητική τιμή r, τότε μπορεί να παραδώσει στον V το σύνολο $\{G_{j_1}, ..., G_{j_t}\}$ και την προαναφερθείσα τιμή s. Ο V

μπορεί να επαληθεύσει ότι πράγματι ισχύει $x < 2^t < \frac{n}{2}$. Το παραπάνω πρωτόκολλο δεν αποκαλύπτει τίποτα περισσότερο στο V πέρα από του ότι $x < 2^t < \frac{n}{2}$ αφού το TS είναι ένα σύνολο που με βάση τον ορισμό του προκύπτει από μια τυχαία αναδιάταξη ενός πίνακα των παραπάνω στοιχείων.

Συνεπώς, ο V δεν έχει καμία πληροφορία για το ποιες κρυπτογραφήσεις δυνάμεων του 2 συμπεριλαμβάνονται στο $\{G_{j_1}, ..., G_{j_t}\}$. Επιπλέον, με την συμπερίληψη των $t - l$ κρυπτογραφήσεων του 0 κρύβονται ακόμα και οι αριθμοί μη μηδενικών ψηφίων στην δυαδική αναπαράσταση του x. Τελικά, οι τυχαίοι παράγοντες $s_{j_1}, ..., s_{j_t}$ στο δοκιμαστικό σύνολο κρυπτογραφήσεων TS συνιστούν μια ομοιόμορφα τυχαία s, η οποία αποκρύπτει εντελώς οποιαδήποτε πληροφορία σχετικά με την βοηθητική τιμή r, στην $E(x, r)$. Συνεπώς, καμία πληροφορία σχετικά με το x δεν αποκαλύπτεται.

Παρόλα αυτά το πρόβλημα με το παραπάνω πρωτόκολλο είναι ότι ο V δε γνωρίζει ότι ο P του έχει παρουσιάσει ένα αληθινό TS. Για να ξεπεραστεί αυτό το πρόβλημα, γίνεται χρήση της παραλλαγής ενός διαδραστικού πρωτοκόλλου επαλήθευσης. Η ιδέα είναι η χρησιμοποίηση μιας διαδικασίας 'τομής και επιλογής' κατά την οποία ο P δεσμεύεται σε έναν σύνολο από TS και επιτρέπει στον V να διαλέξει και να ελέγξει πολλαπλά σύνολα δοκιμών ώστε να διασφαλίσει την εγκυρότητα κάθε ενός από αυτά. Τελικά, τα εναπομείναντα σύνολα δοκιμών χρησιμοποιούνται για να συμπληρώσουν την απόδειξη. Την ιδέα αυτή πρώτος την παρουσίασε ο Rabin [7].

Ε΄. Μαζική επαλήθευση συνόλου δοκιμών

Σε μία πραγματική δημοπρασία απαιτείται μεγάλο πλήθος από σύνολα δοκιμών. Για την επιτάχυνση της επαλήθευσής τους αυτή θα γίνει μαζικά, απαιτώντας έτσι μικρότερο σύνολο δοκιμών να αποκαλυφθεί.

Αντί ο επαληθευτής P να επιλέξει ποια σύνολα να αποκαλυφθούν, τυχαιοποιούνται αυτά τα σύνολα και γίνεται χρήση της παραγόμενης τυχαιότητας ώστε να οριστούν τα σύνολα που θα αποκαλυφθούν καθώς και η σειρά με την οποία θα γίνει αυτό.

Είναι δυνατή η επίτευξη ενός λογικού ποσού 'τυχαιότητας', χρησιμοποιώντας το αλφαριθμητικό X που έχει προκύψει κάνοντας XOR στις τιμές $S_1, ..., S_k$ από τους πλειοδότες, S_{AU} από τον δημοπράτη και S_S από τον πωλητή. Ορίζουμε ως R κάποιο προκαθορισμένο κομμάτι του αλφαριθμητικού X.

Ένα παράδειγμα της διαδικασίας για προσφορές που έχουν εύρος 4 δισεκατομμυρίων τιμών, με την οποία γίνεται μαζική επαλήθευση του συνόλου δοκιμών είναι:

1) Ο AU δημιουργεί 2500 ιδιωτικά σύνολα δοκιμών $TS_i, i \in [0, 2499]$, καθένα από τα οποία αποτελείται από κρυπτογραφήσεις 64 μικρών τιμών, $\{c_{i0}, ..., c_{i63}\} = \{E(0) \times 32, E(2^0), ..., E(2^{31})\}$. Ο AU δημιουργεί μία μυστική τυχαία αναδιάταξη $\pi_i(0...63) \in \{0...63\}$ για κάθε TS_i, για κάθε κρυπτογραφημένη τιμή στο σύνολο δοκιμών και αποθηκεύει ιδιωτικά τα κείμενα, τις τυχαίες βοηθητικές τιμές r και την ύψωση τους σε δύναμη $r^n (mod\, n^2)$.
2) Ο AU δημιουργεί μία αναδιάταξη $\rho(0...2499) \in \{0...2499\}$ των 2500 συνόλων δοκιμών κάνοντας χρήση του R σύμφωνα με το πρωτόκολλο που αναφέρθηκε στην έναρξη της δημοπρασίας.
3) Ο AU αποκαλύπτει τα πρώτα 500 σύνολα δοκιμών σύμφωνα με τη διάταξη ρ. Έπειτα στα άτομα που είναι επιφορτισμένα με την επαλήθευση των συνόλων δίνεται ένα λογικό χρονικό διάστημα (το λογικό εξαρτάται από το μέγεθος και την πολυπλοκότητα της δημοπρασίας) προκειμένου να πιστοποιήσουν την ορθότητά τους. Μετά το πέρας του χρονικού αυτού διαστήματος και με την προϋπόθεση ότι δεν προκύπτει κάποια ένσταση σε σχέση με τον AU ή τους συμβολαιογράφους τα σύνολα αυτά κρίνονται σωστά. Αν προκύψει ότι κάποιο σύνολο δοκιμών είναι μη-έγκυρο τότε ο AU προβαίνει στη δημιουργία 2500 νέων συνόλων δοκιμών και η διαδικασία ξεκινάει από την αρχή
4) Αν και τα 500 σύνολα δοκιμών είναι σωστά τότε το ρ υποδηλώνει την τυχαία διάταξη των μη-αποκαλυφθέντων συνόλων δοκιμών τα οποία χρησιμοποιούνται για την απόδειξη των προσφορών των πλειοδοτών.

Από τη στιγμή που γίνεται η δημοσίευση στον πίνακα ανακοινώσεων των προσφορών με μια αυστηρή διάταξη από τον AU, μπορεί να γίνει η υπόθεση, χωρίς βλάβη της γενικότητας, ότι για κάθε $i < j$, $Bid_i \geqslant Bid_j$. Τότε κάθε Bid_i, $1 \leqslant i \leqslant B$ αποδεικνύεται σωστό από τα επόμενα 10 αχρησιμοποίητα σύνολα δοκιμών σύμφωνα με τη διάταξη που έχει οριστεί από το ρ. Συνεπώς για κάθε i αποδεικνύεται ότι $Bid_i \geqslant Bid_{i+1}$.

IV. Περιγραφη πρωτοκολλου

Θεωρούμε πως οι πλειοδότες είναι δημοσίως γνωστοί. Με αυτό εννοούμε πως οι ψηφιακές τους υπογραφές είναι διαθέσιμες δημόσια. Το πρωτόκολλο που θα περιγράψουμε μπορεί να εφαρμοστεί σε δημοπρασίες πρώτης καθώς και δεύτερης προσφοράς. Ακολουθεί η περιγραφή του πρωτοκόλλου.

1) Αρχικά ο δημοπράτης αναρτά στον πίνακα ανακοινώσεων όλες τις απαραίτητες πληροφορίες για την δημοπρασία. Σε αυτές περιλαμβάνονται: όροι δημοπρασίας, μηχανισμός εκλογής νικητή, διορία υποβολής προσφορών, το αναγνωριστικό της συγκεκριμένης δημοπρασίας, το κλειδί κρυπτογράφησης Paillier όπου το κλειδί αποκρυπτογράφησης ϕ το γνωρίζει μόνο ο δημοπράτης. Σε περίπτωση δημοπρασίας πολλών αντικειμένων, δημοσιεύεται επιπλέον ο συνολικός αριθμός αντικειμένων και το μεγιστό ποσό αντικειμένων που μπορεί να λάβει κάποιος. Επιπρόσθετα σε αυτά, παρέχονται πληροφορίες για τους συμβολαιογράφους που είναι εγκεκριμένοι να λάβουν μέρος στην δημοπρασία και το κλειδί κρυπτογράφησης TPK. Τέλος, δεσμεύεται για την εξασφάλιση της εγκυρότητας της διαδικασίας σε ένα τυχαίο αλφαριθμητικό ώστε να είναι εφικτή η απόδειξη της εγκυρότητας της διαδικασίας και επίσης ανακοινώνει την διαδικασία από την οποία θα παραχθούν οι τυχαίες επαναδιατάξεις χρησιμοποιώντας το τυχαίο αλφαριθμητικό X. Όλα τα παραπάνω συνοδεύονται από την ψηφιακή υπογραφή του δημοπράτη.
2) Κάθε πλειοδότης B_i επιλέγει το ποσό της προσφοράς του Bid_i και το μέγιστο επιθυμητό πλήθος Qty_i σε περίπτωση δημοπρασίας πολλών αντικειμένων, τα οποία τα κρυπτογραφεί με το δημόσιο κλειδί κρυπτογράφησης Paillier[5] σε C_i και $E(Qty_i)$ χρησιμοποιώντας και μια τυχαία επιλεγμένη βοηθητική τιμή r_i. Ακολούθως, παράγεται ένα τυχαίο αλφαριθμητικό S_i που θα χρησιμοποιηθεί για την απόδειξη της ορθότητας του αποτελέσματος. Τα αποτελέσματα C_i, $E(Qty_i)$ αν υπάρχει, και S_i αποστέλλονται αφού πρώτα κρυπτογραφηθούν με το TPK και ενσωματωθεί η υπογραφή του πλειοδότη. Μετά την αποστολή τους, ο πλειοδότης λαμβάνει από τον δημοπράτη την απόδειξη αποδοχής τους.
3) Με την λήξη του χρόνου υποβολής αιτήσεων (μετά από χρόνο T), ο δημοπράτης αναρτά στον πίνακα ανακοινώσεων όλες τις κρυπτογραφημένες πληροφορίες που έχει δεχθεί από τους πλειοδότες. Επιπρόσθετα, αναρτώνται και διάφορα σύνολα δοκιμών ώστε να μπορεί να εξακριβωθεί η εγκυρότητα της δημοπρασίας. Όλες οι αναρτήσεις είναι υπογεγραμμένες.
4) Κάθε πλειοδότης σε αυτό το στάδιο μπορεί να ελέγξει αν υπάρχουν τα δικά του απεσταλμένα στοιχεία στον πίνακα ανακοινώσεων.
5) Αποκαλύπτεται το κρυφό κλειδί TSK. Ο καθένας, μπορεί να ανακτήσει τόσο τις κρυπτογραφημένες προσφορές C_i, το $E(Qty_i)$ αν πρόκειται για δημοπρασία πολλών αντικειμένων, όσο και τα τυχαία αλφαριθμητικά S_i. Αυτό αποτελεί άλλο ένα σημείο όπου οι μετέχοντες μπορούν να εξακριβώσουν την εγκυρότητα των δεδομένων που έχουν αποσταλεί. Αυτό γίνεται, καθώς το S_i, το $E(Qty_i)$, αν υπάρχει, και το C_i έχουν πλέον αποκαλυφθεί και κάθε πλειοδότης j μπορεί να εξακριβώσει ότι τα S_i, $E(Qty_i)$ και C_i όντως ανήκουν στον πλειοδότη i.
6) Πλέον, ο δημοπράτης μπορεί να αποκρυπτογραφήσει όλες τις προσφορές, και τις ποσότητες αν πρόκειται για δημοπρασία πολλών αντικειμένων, χρησιμοποιώντας το μυστικό κλειδί ϕ και να αποφανθεί τους τελικούς νικητές σύμφωνα με τους κανόνες της δημοπρασίας και την ποσότητα αντικειμένων που θα πάρει ο καθένας. Η ταυτότητα του νικητή ανακοινώνεται μαζί με ένα σύνολο

[5]Είναι το δημόσιο κλειδί, που το αντίστοιχο ιδιωτικό κλειδί για την αποκρυπτογράφηση γνωρίζει μόνο ο δημοπράτης

πληροφοριών οι οποίες επιτρέπουν στους μετέχοντες στην διαδικασία να επαληθεύσουν το τελικό αποτέλεσμα. Για αυτό τον σκοπό χρησιμοποιούνται οι τυχαίες βοηθητικές τιμές $r_1, ..., r_k$.

Α΄. Επαλήθευση εγκυρότητας δημοπρασίας

Όλη η διαδικασία της επαλήθευσης γίνεται με μηδενική αρχική πληροφόρηση. Ο δημοπράτης επιλέγει ποια στοιχεία του αποτελέσματος θα αποκαλυφθούν.

Σύμφωνα με αυτά που αναφέραμε στο ΙΙ-Η΄ και τα θεωρήματα 3.1, 3.2 μπορούν να διαταχθούν οι προσφορές και να εκλεχθεί ο νικητής της δημοπρασίας. Σε περίπτωση που δυο πλειοδότες έχουν υποβάλλει την ίδια μεγαλύτερη προσφορά, σε δημοπρασία ενός αντικειμένου, ο νικητής καθορίζεται είτε με βάση τους κανόνες της δημοπρασίας, είτε με τυχαία επιλογή, είτε μέσα από μια επιπρόσθετη δημοπρασία για αυτό τον λόγο. Σε δημοπρασίες πολλών αντικειμένων, ύστερα από την εξέταση των προσφορών, ορίζεται ένα Bid_a, όπου όσοι έχουν κάνει μεγαλύτερη από αυτό θα πάρουν όσα αντικείμενα έχουν ζητήσει.

Σε περίπτωση που υπάρχουν ίσες προσφορές Bid_a, εφαρμόζεται μια ειδική διαδικασία επίλυσης ισοπαλίας (tiebreaking). Ο αλγόριθμος που χρησιμοποιείται για την επίλυση αυτού του προβλήματος είναι τύπου round-robin. Μοιράζει τα αντικείμενα στους μετέχοντες μέχρι την εξάντληση τους. Ωστόσο, τίθενται θέματα δικαιοσύνης όσον αφορά την σειρά με την οποία θα ανατεθούν τα αντικείμενα στους πλειοδότες. Για την επίλυση τους, καθορίζεται η σειρά με έναν τρόπο, έτσι ώστε αυτή να είναι δημόσια επαληθεύσιμη η τυχαιότητα της. Για τον σκοπό αυτό χρησιμοποιείται το τυχαίο X που κατασκευάζεται συλλογικά από όλους τους συμμετέχοντες. Όλοι οι μετέχοντες, με βάση την σειρά που ορίστηκε, θα πάρουν την μικρότερη από τις δύο ποσότητες: είτε όσα ζητήσανε, είτε κατά ένα λιγότερο από αυτούς που τους ανατέθηκαν τα περισσότερα αντικείμενα.

Β΄. Πληρωμές

Διασφαλίζεται ότι ένας πλειοδότης θα έχει πληρώσει τουλάχιστον ίσα χρήματα με όλους τους άλλους πλειοδότες (που δεν πήραν κάποιο αντικείμενο εξαιτίας αυτού). Η ορθότητα της πληρωμής αυτής, όπως άλλωστε έχουμε προαναφέρει, μπορεί να ελεγθεί από τους μετέχοντες χωρίς να αποκαλυφθούν σε αυτούς πληροφορίες σχετικά με τις προσφορές που κατατέθηκαν. Σε δημοπρασίες πολλών αντικειμένων, η πληρωμή γίνεται με βάση την γενικευμένη Vickrey δημοπρασία (Generalized Vickrey Auction - GVA) [4].

Γ΄. Απόδειξη διατήρησης εχεμύθειας στις πληρωμές

Με τη μέθοδο GVA που αναπτύχθηκε προηγουμένως χρειάζεται να αποκαλυφθούν κάποιες πληροφορίες σχετικά με τις προσφορές των πλειοδοτών. Στην ενότητα αυτή παρουσιάζεται μία λύση που εξαλείφει την ανάγκη για αποκάλυψη αυτών των πληροφοριών, προσθέτοντας όμως ένα επιπλέον κόστος στην πολυπλοκότητα και στους υπολογισμούς. Για την λύση του προβλήματος παρουσιάζεται μία τεχνική που αποδεικνύει την ορθότητα ενός κρυπτογραφημένου όρου $V(B_{-i})$ χωρίς να αποκαλύπτεται ο αριθμός των νικητών.

Έστω k ο πληθάριθμος των προσφορών στην είσοδο. Στον αριθμό αυτό συμπεριλαμβάνεται όποτε χρειάζεται και ένας πλειοδότης με προσφορά μηδέν και ζητούμενη ποσότητα l. Προκειμένου να είναι κρυφή η θέση του πλειοδότη του οποίου η προσφορά είναι ίση με Bid_a (κατώφλι) προσθέτουμε στην είσοδο $k-1$ προσφορές έτσι ώστε η νέα θέση του κατωφλιού α της καινούργιας εισόδου να ορίζεται πάντα ως $\alpha - 1 = k$. Επίσης έστω γ η θέση του κατωφλιού της αρχικής εισόδου των k προσφορών. Οι νέες προσφορές ορίζονται ως εξής: Υπάρχουν $k - \gamma + 1$ προσφορές με $QTY_j^* = 0$ και $Bid_j = V$ για μια μέγιστη τιμή V μεγαλύτερη από κάθε άλλη προσφορά που έχει αναρτηθεί και $\gamma - 2$ προσφορές με $QTY_j^* = 0$ και $Bid_j = 0$. Άρα η θέση του κατωφλίου της καινούργιας εισόδου ισούται με $k+1$ και καμία πληροφορία δεν αποκαλύπτεται για το αρχικό κατώφλι.

Παρόλα αυτά, δεν έχει διασφαλιστεί ότι ο δημοπράτης μπορεί να εισάγει τις επιπλέον προσφορές χωρίς να αποκαλύπτει στα άτομα που είναι επιφορτισμένα για την επαλήθευση, την ανάμειξη προσφορών μηδενικών και μη μηδενικών τιμών που εισάγονται. Η αρχή που είναι επιφορτισμένη για την επαλήθευση των προσφορων πρέπει να μην μπορεί να διαχωρίσει αν μία προσφορά είναι πραγματική ή έχει εισέλθει για την αποφυγή της ταυτοποίησης της προσφοράς κατωφλίου. Για να πετύχουμε αυτό χρησιμοποιούμε την ιδέα της 'τομής και επιλογής' που έχει αναφερθεί και προηγουμένως.

V. Εμπειρικα Αποτελεσματα

Η υλοποίηση της κρυπτογράφησης Paillier καθώς και του συνόλου δοκιμών έγινε σε C++ με τη βοήθεια της βιβλιοθήκης LiDIA[6], σε ένα τυπικό υπολογιστικό σύστημα του εμπορίου, με ένα επεξεργαστή Pentium 4 στα 2.8 GHz και λειτουργικό σύστημα Linux.

Το κομμάτι του πρωτοκόλλου με το μεγαλύτερο υπολογιστικό κόστος, είναι αυτό της κατασκευής και της επαλήθευσης των συνόλων δοκιμών. Όμως, αξίζει να σημειωθεί ότι τόσο η φάση αυτή της προετοιμασίας όσο και της επαλήθευσης, κλιμακώνονται γραμμικά και είναι εύκολο να παραλληλοποιηθούν. Έτσι με μια απλή κατανεμημένη προσέγγιση του πρωτοκόλλου ακόμα και μία δημοπρασία πολλών αντικειμένων με 10000 πλειοδότες μπορεί να προετοιμαστεί μέσα σε λίγες ώρες και να γίνει επαλήθευση της μέσα σε λογικό χρόνο.

Στους παρακάτω πίνακες παρουσιάζονται οι μετρήσεις που λήφθηκαν κατά την πειραματική αξιολόγηση χρησιμοποιώντας κλειδιά των 1024 και 2048 δυαδικών ψηφίων. Τέτοια κλειδιά θεωρούνται ασφαλή, με τα μέχρι τώρα δεδομένα, μέχρι το 2010 και 2030 αντίστοιχα [3].

Πιο συγκεκριμένα τώρα στον πίνακα I φαίνονται οι χρόνοι που απαιτούνται για τις καίριες διαδικασίες κρυπτογράφησης του παρουσιαζόμενου πρωτοκόλλου στην προαναφερθείσα μηχανή. Όπως φαίνεται και από τις μετρήσεις ο χρόνος που απαιτείται για την προετοιμασία και την επαλήθευση του συνόλου δοκιμών είναι ουσιαστικά όσος απαιτείται για την κρυπτογράφηση και την αποκρυπτογράφηση. Όλα τα σύνολα δοκιμών αναπαριστούν 2^34 διακριτές τιμές.

Διαδικασία	Χρόνος (sec)	
	(1024-bit)	(2048-bit)
Υπολογισμός του r^n	0.045	0.287
Κρυπτογράφηση	0.045	0.287
Αποκρυπτογράφηση με χρήση του r	0.045	0.287
Αποκρυπτογράφηση με χρήση του ϕ	0.014	0.089
Αποκρυπτογράφηση με χρήση του r^n	0.000	0.001
Κατασκευή του Συνόλου Δοκιμών	3.01	19.32
Επαλήθευση του Συνόλου Δοκιμών	3.00	19.30
Αποδεικνύοντας $0 \leq x < 2^t$ δοθέντος του Συνόλου Δοκιμών	0.001	0.001
Επαληθεύοντας την απόδειξη $0 \leq x < 2^t$	0.070	0.41

Πίνακας I
Χρονος για την εκτελεση βασικων λειτουργιων

Στον πίνακα II καταγράφονται οι χρόνοι που απαιτούνται για την προετοιμασία και την επαλήθευση των συνόλων δοκιμών για ποικίλους αριθμούς προσφορών σε δημοπρασίες είτε ενός είτε πολλών αντικειμένων με κλειδιά είτε 1024 δυαδικών ψηφίων, είτε 2048.

Ο πίνακας III παρουσιάζει το χρόνο που απαιτείται για την επαλήθευση των πληρωμών Vickrey στη χειρότερη περίπτωση για ποικίλα μεγέθη δημοπρασιών πολλών αντικειμένων. Αυτοί οι υπολογισμοί είναι απαραίτητοι σε αντίθεση με τους πιο πάνω υπολογισμούς που αφορούν την επαλήθευση των τιμών και των ποσοτήτων.

[6]Πρόκειται για μία C++ βιβλιοθήκη για υπολογιστική θεωρία αριθμών η οποία παρέχει μια συλλογή υλοποιήσεων υψηλού βαθμού βελτιστοποίησης από διάφορους τύπους δεδομένων πολλαπλής ακρίβειας και χρονοβόρων αλγορίθμων.

Διαδικασία	Αριθμός προσφορών		
	100	1000	10000
Δημοπρασίες ενός αντικειμένου			
Προετοιμασία (1024-bit)	2.1 ώρες	21 ώρες	8.7 μέρες
Επαλήθευση (1024-bit)	25 λεπτά	4.2 ώρες	42 ώρες
Προετοιμασία (2048-bit)	13.4 ώρες	5.6 μέρες	56 μέρες
Επαλήθευση (2048-bit)	2.7 ώρες	27 ώρες	11 μέρες
Δημοπρασίες πολλών αντικειμένων			
Προετοιμασία (1024-bit)	4.2 ώρες	42 ώρες	17.5 μέρες
Επαλήθευση (1024-bit)	52 λεπτά	8.7 ώρες	3.6 μέρες
Προετοιμασία (2048-bit)	27 ώρες	11.2 μέρες	112 μέρες
Επαλήθευση (2048-bit)	5.4 ώρες	54 ώρες	22 μέρες

Πίνακας II
ΧΡΟΝΟΣ ΓΙΑ ΤΗΝ ΠΡΟΕΤΟΙΜΑΣΙΑ ΚΑΙ ΤΗΝ ΕΠΑΛΗΘΕΥΣΗ ΔΗΜΟΠΡΑΣΙΩΝ

Διαδικασία	Αριθμός προσφορών		
	100	1000	10000
Προετοιμασία (1024-bit)	48 λεπτά	8 ώρες	3.3 μέρες
Επαλήθευση (1024-bit)	72 λεπτά	12 ώρες	5 μέρες
Προετοιμασία (2048-bit)	5.1 ώρες	51 ώρες	21 μέρες
Επαλήθευση (2048-bit)	7.7 ώρες	77 ώρες	32 μέρες

Πίνακας III
ΕΠΑΛΗΘΕΥΣΗ ΤΩΝ VICKREY ΠΛΗΡΩΜΩΝ ΓΙΑ ΔΗΜΟΠΡΑΣΙΕΣ ΠΟΛΛΩΝ ΑΝΤΙΚΕΙΜΕΝΩΝ

VI. Επιλογος & Μελλοντικη Εργασια

Στην αναφορά αυτή παρουσιάστηκε ένα νέο πρωτόκολλο για δημοπρασίες σφραγισμένων προσφορών που εγγυώνται την εμπιστοσύνη και την υψηλού επιπέδου εχεμύθεια, ενώ παράλληλα το πρωτόκολλο αυτό μπορεί να τρέξει σε μηχανές που βρίσκονται στην αγορά και είναι δυνατό να αποκτηθούν από τις διάφορες επιχειρήσεις.

Παρά το γεγονός ότι το πρωτόκολλο αυτό στηρίζεται σε αποδείξεις ορθότητας και εχεμύθειας κατά τη διαδικασία της δημοπρασίας, ο δημοπράτης μπορεί να υπολογίσει τα αποτελέσματα και τις αποδείξεις αυτών αποδοτικά. Το πρωτόκολλο αυτό έχει σαν βάση του την κρυπτογραφία και αποτελεί μία ενδιαφέρουσα προέκταση και για άλλου τύπου δημοπρασίες με τις οποίες έχουν σκοπό οι δημιουργοί του να ασχοληθούν μελλοντικά. Επίσης, μπορεί να επεκταθεί και σε άλλες περιοχές που στηρίζονται στη ιδιωτικότητα των δεδομένων. Τέτοιες θα μπορούσε να είναι συστήματα ηλεκτρονικών συναλλαγών, ανοιχτές αγορές που βάζουν σαν στόχο τη διατήρηση της ιδιωτικότητας και συστήματα για την δημόσια επαλήθευση ιδιωτικών δεδομένων χωρίς την αποκάλυψη κάποια πληροφορίας για αυτά.

Να σημειωθεί στο σημείο αυτό ότι το πρωτόκολλο αυτό υλοποιήθηκε και σε Python από τον David Austin. Το πρότυπο αυτό αποτελείται από έναν εξυπηρέτη διαδικτύου και έναν αυτόνομο πελάτη για την διεξαγωγή δημοπρασιών σφραγισμένων προσφορών. Παρά το γεγονός ότι σε Python η εκτέλεση του διήρκησε διπλάσιο χρόνο από ότι η υλοποίηση του με βελτιστοποιημένη C++, ο χρόνος παραμένει ικανοποιητικός για την πρακτική εφαρμογή του.

Επίσης, σαν μελλοντική εργασία θα μπορούσε να είναι η βελτίωση του χρόνου εκτέλεσης, τόσο από τη μεριά τον υπολογισμών όσο και από τη μεριά της χρήσης πιο εξειδικευμένου, σε σχέση με την κρυπτογραφία, υλικού. Για τη μείωση του χρόνου θα μπορούσαν να χρησιμοποιηθούν και μικρότερα κλειδιά κρυπτογράφησης, καθώς μπορεί να μην θεωρείται απαραίτητο σε κάποιες δημοπρασίες να διασφαλίζεται η εχεμύθεια των δεδομένων για πολλά χρόνια.

Τέλος ένας ακόμα μελλοντικός στόχος είναι η επέκταση του πρωτοκόλλου και σε άλλες παραλλαγές που σαν κριτήριο για την επιλογή κάποιας προσφοράς δε θα είναι μόνο κάποιο χρηματικό ποσό αλλά και μη-οικονομικοί λόγοι, όπως η ποιότητα και οι όροι πληρωμής. Τέτοιες επεκτάσεις μπορούν να θέσουν νέες βάσεις για άλλου τύπου διαφθοράς της όλης διαδικασίας. Επίσης θεωρείται ενδιαφέρουσα και η ανάπτυξη ενός παρόμοιου πρωτοκόλλου και σε δημοπρασίες ανοιχτής προσφοράς.

References

[1] J.C. Andvig. *Corruption in the North Sea oil industry: issues and assessments, Crime, Law & Social Change 23*, chapter 4, pages 289 – 314. 1995.

[2] O. Baudron, P.-A. Fouque, D. Pointcheval, G. Poupard, and J. Stern. Practical multi-candidate election system. In *In PODC*, pages 274–283. ACM Press, 2001.

[3] P. Bulens D. Giry. Cryptographic key length recommendation. http://www.keylength.com, April 2008.

[4] V. Krishna. *Auction Theory*. Academic Press, 2002.

[5] P. Paillier. *Public-key cryptosystems based on composite residuosity classes, in: Proceedings of EUROCRYPT '99*, pages 223 – 239. 1999.

[6] D. C. Parkes, M. O. Rabin, S. M. Shieber, and C. A. Thorpe. Practical secrecy-preserving, verifiably correct and trustworthy auctions. In *ICEC '06: Proceedings of the 8th international conference on Electronic commerce*, pages 70–81, New York, NY, USA, 2006. ACM.

[7] M.O. Rabin. *Digitalized Signatures in: Foundations of Secure Computing*, pages 155 – 166. Academic Press, New York, 1978.

[8] Ron Rivest. Voting, homomorphic encryption. Computer and Network Security: Lecture Notes, October 2002.