University of Patras

Computer Engineering and Informatics Department

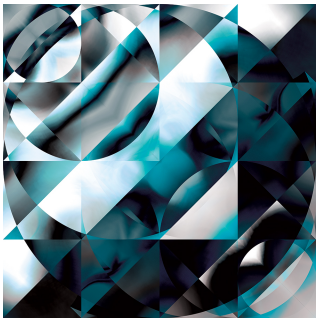
Cryptography

Towards a Practical Cryptographic Voting Scheme Based on Malleable Proofs

Authors:
Ioannis Douratsos
Ioanna Tzanetou
Nikolas Pavlou

Supervisor:
Panagiotis Kanellopoulos

July, 2014



Contents

1 Εισαγωγή

Τα τελευταία χρόνια έχει αρχίσει να γίνεται σημαντική έρευνα για την ανάπτυξη ενός κρυπτοσυστήματος ψηφοφοριών. Συγκεκριμένα, θα θέλαμε οι συμμετέχοντες να μπορούν να ψηφίσουν κάποιον υποψήφιο χωρίς να χρειάζεται να φανερωθεί η ταυτότητα τους. Σημαντικός παράγοντας σε αυτό είναι το γεγονός ότι χρειαζόμαστε οι εκλογές να είναι επιβεβαιώσιμα σωστές, δηλαδή να μη μπορεί κάποιος κακόβουλος συμμετέχων να πειράξει τα αποτελέσματα κατά τη διαδικασία απόφασης των αποτελεσμάτων. Για αυτό το λόγο, γίνεται η προσπάθει ανάπτυξης πρωτοκόλλων ψηφοφορίας όπως αυτό που θα περιγραφεί παρακάτω. Σε αυτά, οι συμμετέχοντες-ψηφοφόροι αρχικά κρυπτογραφούν τις ψήφους τους με ένα κατάλληλο δημόσιο κλειδί και ύστερα τις "πετούν" σε ένα online χώρο ψηφοφορίας. Οι ψήφοι αυτοί ανακατεύονται από κατάλληλα εργαλεία αρκετές φορές ώστε να γίνει αδύνατη η εύρεση του αρχικού δημιουργού. Τέλος, γίνεται η αποκρυπτογράφηση των ψήφων ώστε να βρεθεί ο νικητής της ψηφοφορίας. Τα μεγαλύτερα προβλήματα της διαδικασίας αυτής βρίσκονται στο γεγονός ότι μπορεί κάποιος κακόβουλος συμμετέχον να προσπαθήσει να αλλάξει τα αποτελέσματα της αποκρυπτογράφησης, για αυτό και πρέπει να βρούμε κάποιο τρόπο να μην έχει ποτέ κάποιος δυνατότητα πλήρης αποκρυπτογράφησης των ψήφων καθώς και στο γεγονός ότι οι διαδικασίες που χρησιμοποιούνται για την επίλυση του προβλήματος αυτού έχουν ως αποτέλεσμα η διαδικασία επιβεβαίωσης της ψηφοφορίας να διαρκεί πάρα πολύ χρόνο, κάνοντας δύσκολη την εφαρμογή της σε πραγματικές συνθήκες.

Παρακάτω θα δούμε μία νέα μέθοδο που προτείνεται η οποία ενισχύει τις μέχρι τώρα ανεπτυγμένες, ενώ θα προσπαθήσουμε να δούμε και κατά πόσον μπορεί η μέθοδος αυτή να εφαρμοστεί σε πραγματικά δεδομένα.

2 Τα θεμέλια του αλγορίθμου

Στο συνέδριο Eurocrypt 2012 η ομάδα επιστημόνων με επικεφαλή τη Melissa Chase παρουσίασε την έννοια των “mallable proof systems”. Στο paper αυτό οι ερευνητές έδειξαν πως μπορεί να χρησιμοποιηθεί η ιδιότητα του malleability ως ένα χρήσιμο χαρακτηριστικό ώστε να παραχθούν αποδείξεις μηδενικής γνώσης.

Πριν προχωρήσουμε παρακάτω δίνεται ο ορισμός του **malleability**:

Η ιδιότητα που έχουν κάποιοι κρυπτογραφικοί αλγόριθμοι που επιτρέπει σε κάποιον αν έχει τη κρυπτογράφηση c ενός μηνύματος m, να παράξει την κρυπτογράφηση της f(m), όπου f μια γνωστή συνάρτηση, χωρίς απαραίτητα να μάθει το m. Αυτό επιτρέπει σε κάποιον που ακούει το κανάλι επικοινωνίας να εκτελέσει μια επίθεση χωρίς αναγκαστικά να μάθει το αρχικό μήνυμα m.

Σαν εφαρμογή χρησιμοποίησαν ένα ψηφιακό σύστημα ψηφοφορίας στο οποίο κάθε οντότητα παίρνει ένα σύνολο κρυπτογραφημένων ψήφων και κάποιο αποδεικτικό στοιχείο μηδενικής γνώσης ότι αυτό το σύνολο αποτελεί το ανακάτεμα της αρχικής ακολουθίας κρυπτογραφημένων ψήφων, το

ανακατεύει ξανά και ανανεώνει το αποδεικτικό στοιχείο εκμεταλλευόμενη την ιδιότητα του malleability.

Σε δεύτερο paper προσαρμόζουν τα malleable proofs σε ένα σύστημα κατανεμημένης κρυπτογράφησης με δυνατότητα επιβεβαίωσης το οποίο έχει ως αποτέλεσμα ένα πρωτόκολο κρυπτοψηφοφορίας, με ταυτόχρονο αποτέλεσμα την γραμμική αύξηση των δεδομένων που πρέπει να επεξεργαστούν μόνο σε σχέση με τους ψηφοφόρους.

Στο paper αυτό που μελετήσαμε εμείς εξετάζονται κάποια ερωτήματα τα οποία δεν απαντήθηκαν από την Chase. Συγκεκριμένα, προσαρμόζεται κατάλληλα ένα πρωτόκολλο υπολογισμού από πολλαπλές οντότητες ώστε να φτιαχθεί ένα πρωτόκολλο κατανεμημένης παραγωγής των κλειδιών που θα χρησιμοποιηθούν για τη κρυπτογραφία με σκοπό να αφαιρεθεί η ανάγκη για κάποια έμπειστη πηγή παραγωγής του κλειδιού αυτού. Επίσης προσφέρουν περαιτέρω ανάλυση των εντολών που εκτελούνται κατά τη διάρκεια του πρωτοκόλλου ψηφοφορίας μετρώντας των αριθμό αυτών που χρειάζεται για το ανακάτεμα και για την απόδειξη*ποια είναι η σωστή λέξη; verification* των ψήφων , κάνοντας ταυτόχρονα μια μελέτη για την πιθανή εφαρμογή των πρωτοκόλλων αυτών σε πραγματικά δεδομένα κοιτώντας τις πρόσφατες Γερμανικές εκλογές.

Από τη στιγμή που η Chase έθεσε τα θεμέλια με την αρχική της εργασία επάνω στα malleable proofs, έχουν προταθεί πολλοί τρόποι για την διεξαγωγή μυστικών εκλογών των οποίων η ορθότητα μπορεί να επιβεβαιωθεί . Σημαντικό ενδιαφέρον έχει δωθεί από την ακαδημαική κοινότητα στη χρήση των mixnets για τους σκοπούς αυτούς.

Εδώ κρίνεται σκόπιμο να δοθεί ο ορισμός των **mixnets**:

Τα mixnets χρησιμοποιούνται για να δημιουργήσουν επικοινωνίες στις οποίες είναι πολύ δύσκολο σε κάποιον να βρεί τον αρχικό αποστολέα ενός μηνύματος. Για να το κάνουν αυτό, χρησιμοποιούν αλυσίδες από proxies οι οποίοι παίρνουν μηνύματα από πολλούς αποστολείς, τα ανακατεύουν και ύστερα τα στέλνουν με τυχαία σειρά στον επόμενο προορισμό. Οι proxies αυτοί δεν γνωρίζουν τον αρχικό αποστολέα, παρά μόνον τον προηγούμενο και επόμενο από αυτούς κόμβο, κάνοντας έτσι ακόμη δυσκολότερη την εύρεση του αρχικού αποστολέα κάποιου μηνύματος.

3 Επισκόπηση Αλγορίθμου

Σε μια τέτοια προσέγγιση του προβλήματος, οι εκλογές συνήθως γίνονται με τον παρακάτω τρόπο:

Αρχικά οι ψηφοφόροι κρυπτογραφούν κάθε ένας την ψήφο του βάση του δημόσιου κλειδιού που παρέχεται από τον φορέα τον εκλογών και ύστερα δημοσιεύουν τα κρυπτοκείμενα σε ένα ψηφιακό πίνακα ανακοινώσεων. Ύστερα, χρησιμοποιείται ένα mixnet ώστε να αποσυσχετίσει τα κρυπτοκείμενα από τους αντίστοιχους ψηφοφόρους με τέτοιο τρόπο ώστε ύστερα από τη διαδικασία αυτή ο κάθε ψήφος να μπορεί να αποκρυπτογραφηθεί από τον εκλογικό φορέα. Τα mixnets αυτά αποτελούνται από επιμέρους mix nodes, κάθε ένας από τους οποίους επιβεβαιώνει τα στοιχεία των προηγούμενων mix nodes, ξανα-ανακατεύει τους κρυπτογραφημένους ψήφους και προσθέτει ένα αποδεικτήριο μηδενικής γνώσης στην έξοδο του ώστε να ενημερώσει ότι η διαδικασία ανακατέματος λειτούργησε σωστά.

Ύστερα από αυτή τη διαδικασία, κάθε αποκρυπτογράφος εκτελεί μερική αποκρυπτογράφηση της λίστας των κρυπτοκειμένων και κατασκευάζει μια κατάλληλη απόδειξη ότι η διαδικασία αποκρυπτογράφησης λειτούργησε σωστά. Οι αρχικοί ψήφοι μπορούν τότε να ανακατασκευαστούν ύστερα από τον συνδιασμό κατάλληλου αριθμού από μερικές αποκρυπτογραφήσεις. Η ορθότητα των εκλογών επιβεβαιώνεται από τους παρατηρητές, οι οποίοι αναλαμβάνουν τον έλεγχο όλων των αποδείξεων που παρήχθησαν από τους mix nodes και από τους αποκρυπτογράφους. Για αυτό το λόγο, το πλήθος των δεδομένων που χρειάζεται να επεξεργαστούν αυξάνει γραμμικά σε συνάρτηση με τον αριθμό των mix nodes, των αποκρυπτογράφων και τον αριθμό των ψηφοφόρων. Με την εφεύρεση των malleable proof systems από την Chase το 2012 επέτρεψαν στο πλήθος αυτό των δεδομένων να γίνει ανεξάρτητο του αριθμού των mix nodes. Αυτό επιτράπηκε επειδή τα malleable proofs επιτρέπουν σε ένα mix node i+1 να ανανεώσει το αποδεικτήριο μηδενικής γνώσης Π(i) που παρήχθει από τον mix node i και να προσθέσει ένα ακόμη επίπεδο ανακατέματος ώστε να παράξει το αποδεικτήριο Π(i+1). Το ανανεωμένο αποδεικτήριο είναι στην ίδια μορφή με το προηγούμενο με μόνη αλλαγή στις σταθερές, οι οποίες έχουν αλλάξει τιμή.

Σε μια πρόσφατη εργασία τους (CKLM13), η ίδια ομάδα προσαρμόζει τα malleable proofs στη κατανεμημένη κρυπτογράφηση φτιάχνοντας έτσι ένα σύστημα κρυπτοψηφοφοριών η οποία και αποτελεί τη βάση του paper αυτού. Στο σύστημα αυτό, το πλήθος των δεδομένων που πρέπει να επεξεργαστεί κάθε παρατηρητής αυξάνεται μόνο γραμμικά σε σχέση με τον αριθμό των ψηφοφόρων.

4 Συνεισφορά των Συγγραφέων

Στο paper που μελετάμε, οι ερευνητές ασχολούνται με την πρακτική αξία των κρυπτογραφικών πρωτοκόλλων ψηφοφορίας.

Συγκεκριμένα, κανένα από τα μέχρι τώρα προταθέντα πρωτόκολλα ψηφοφορίας δεν προτείνει κάποιο τρόπο για κατανεμημένο υπολογισμό του δημόσιου κλειδιού και συνεπώς όλα βασίζονται στην ύπαρξη ενός έμπειστου φορέα ο οποίος θα διανέμει το κλειδί αυτό. Για να αντιμετωπίσουν το πρόβλημα αυτό, προτείνεται ένα πρωτόκολλο κατανεμημένου υπολογισμού του κλειδιού. Αυτό έχει ως αποτέλεσμα την μετατροπή του CKLM13 σε ένα πλήρως κατανεμημένο κρυπτογραφικό πρωτόκολλο ψηφοφορίας. Αυτό το πετυχαίνουν προσαρμόζοντας κατάλληλα το πρωτόκολλο συνδυαστικού υπολογισμού που φτιάχθηκε από τους Smart και Geisler ώστε να ταιριάζει στο πρωτόκολλο κρυπτογράφησης που μελετούν. Ο μόνος περιορισμός για την σωστή εφαρμογή του πρωτοκόλλου αυτού είναι πως η ορθότητα του παραμένει όταν μέχρι και το πολύ n/3 των διαχειριστών της ψηφοφορίας προσπαθούν να κλέψουν. Αν και το σωστό θα ήταν να μπορεί η ψηφοφορία να διεξαχθεί ορθά ακόμη και με όλους τους διαχειριστές να κλέβουν, το πρωτόκολλο αυτό είναι το πρώτο που είναι ανθεκτικό απέναντι ακόμη και σε έναν κακόβουλο συμμετέχοντα, κάτι που θεωρείται μεγάλο βήμα.

Το δεύτερο πράγμα με το οποίο ασχολήθηκαν οι ερευνητές είναι η εκτίμηση του κατά πόσον κάποιο πρωτόκολλο ψηφοφορίας μπορεί να χρησιμοποιηθεί σε πραγματικές συνθήκες. Για αυτό το λόγο κάνουν ανάλυση των ενεργειών που εκτελούνται κατά την διάρκεια του πρωτοκόλλου ώστε να μπορέσουν να έχουν μια εκτίμηση στο χρόνο που θα χρειαζόταν για διάφορα μεγέθη του πλήθους των ψηφοφόρων, καταλήγοντας ότι το προτεινόμενο πρωτόκολλο θα μπορούσε να αντικαταστήσει τη διαδικασία ψηφοφορίας μέσω αλληλογραφίας στη Γερμανία, ενώ σε επίπεδο μιας ολόκληρης πόλης το πρωτόκολλο είναι ακόμη εκτός πρακτικής εφαρμογής.

5 Κρυπτογράφηση βασισμένη σε threshold

Ένα σχήμα κρυπτογράφησης δημοσίου κλειδιού αποτελείται από μια τριάδα αλγορίθμων: (Keygen, Encrypt, Decrypt). Ο Keygen παίρνει ως είσοδο μια παράμετρο και παράγει ένα δημόσιο και ένα ιδιωτικό κλειδί. Ο Encrypt παίρνει ως είσοδο το αρχικό μήνυμα και το δημόσιο κλειδί και επιστρέφει το κρυπτοκείμενο που προκύπτει, ενώ ο Decrypt είναι ντετερμινιστικός και παίρνει ως είσοδο το κρυπτοκείμενο και ένα ιδιωτικό κλειδί και δίνει στην έξοδο του το αποκρυπτογραφημένο μήνυμα. Η διαφορά του threshold encryption σχήματος από τα συνηθισμένα είναι ότι χαρακτηρίζεται από δύο παραμέτρους: τον αριθμό των αποκρυπτογράφων n και από ένα όριο t < n.

Οι ιδιότητες που θέλουμε από ένα τέτοιο σχήμα κρυπτογράφησης είναι ότι δεδομένου αυτών των παραμέτρων, μια οποιαδήποτε ομάδα από τουλάχιστον t+1 αποκρυπτογράφους μπορεί να αποκρυπτογραφήσει τα κρυπτοκείμενα , αλλά καμιά ομάδα αποτελούμενη από το πολύ t δεν μπορεί να πάρει καμία πληροφορία από αυτά. Συγκεκριμένα, σε καμία περίπτωση δεν θα έχει μια ομάδα των πολύ t ατόμων στην κατοχή της το πλήρες κλειδί που χρειάζεται για την αποκρυπτογράφηση των κρυπτοκειμένων.

Πιο αυστηρά, ένα σχήμα κρυπτογράφησης που βασίζεται σε ένα threshold κλειδιών ορίζεται από τέσσερις αλγορίθμους. Ο Keygen παίρνει ως είσοδο μια παράμετρο και παράγει ένα δημόσιο n μερίδια του ιδιωτικού κλειδιού για τους αποκρυπτογράφους. Ο Encrypt παίρνει ως είσοδο το αρχικό μήνυμα και το δημόσιο κλειδί και επιστρέφει το κρυπτοκείμενο που προκύπτει, ο Decrypt παίρνει ως είσοδο το κρυπτοκείμενο και ένα μέρος του ιδιωτικού κλειδιού και δίνει στην έξοδο του ένα μερίδιο του αποκρυπτογραφημένου μηνύματος. Τέλος, ο αλγόριθμος Combine παίρνει ένα κρυπτοκείμενο και μια ομάδα από τουλάχιστον t+1 μερίδια από το μήνυμα και δίνει ως έξοδο είτε το αρχικό, αποκρυπτογραφημένο μήνυμα είτε ένα ειδικό σύμβολο για να δείξει ότι η αποκρυπτογράφηση απέτυχε.

Για να είναι σωστό το σχήμα κρυπτογράφησης, πρέπει να ισχύει ότι για κάθε δημόσιο κλειδί και κάθε ομάδα από μερίδια του δημόσιου κλειδιού που έχουν παραχθεί από τον Keygen και για κάθε μήνυμα m και κάθε κρυπτοκείμενο c που έχει προκύψει από τον Encrypt με είσοδο το m και το pk και για κάθε ομάδα από τα μερίδια του δημόσιου κλειδιού με μέγεθος t+1 πρέπει να ισχύει ότι αν υπολογίσουμε τα μερίδια του αποκρυπτογραφημένου μηνύματος μέσω του Decrypt και χρησιμοποιήσουμε τον Combine με είσοδο αυτά και το κρυπτοκείμενο c τότε πρέπει να πάρουμε το αρχικό μήνυμα m.

Ο αλγόριθμος κρυπτογράφησης στον οποίο βασίζεται το προτεινόμενο σχήμα του paper είναι ο DLIN. Σε αυτόν, το ιδιωτικό κλειδί είναι ένα ζευγάρι (x,y) διαλεγμένο τυχαία από το Zq x Zq και το αντίστοιχο δημόσιο κλειδί είναι το $(X, Y) = (G^x, G^y)$. Για να κρυπτογραφήσει κάποιος ένα μήνυμα M διαλέγει ένα ζευγάρι (r,s) τυχαία από το Zq x Zq και υπολογίζει την τριπλέτα $(A, B, C) = (X^r, Y^s, M * G^{r+s})$ ενώ για να αποκρυπτογραφήσει το κρυπτοκείμενο C,υπολογίζει το $C/(A^{1/x} * B^{1/y})$.

Ένα σύνολο ζευγαρόματος είναι μια τριπλέτα από σύνολα (G_1, G_2, G_T) κάποιου μεγέθους q με μια αποδοτικώς υπολογιζόμενη διγραμμική μη εκφυλισμένη αντιστοίχιση $e : G_1 \times G_2 \longrightarrow G_T$. Για παράδειγμα, αν Γ_1, Γ_2 οι generators των G_1, G_2,και α,β ακέραιοι, τότε $e(\alpha\Gamma_1, \beta\Gamma_2) = e(\Gamma_1, \Gamma_2)^{\alpha\beta}$ και το $e(\Gamma_1, \Gamma_2)$ είναι ένας generator του G_T.

Ο τρόπος που χρησιμοποιείται για να μοιραστεί το κατανεμημένο ιδιωτικό κλειδί είναι το σχήμα μοιράσματος του Shamir. Σύμφωνα με αυτό, μπορούμε να μοιράσουμε ένα μυστικό σε n άτομα με τέτοιο τρόπο ώστε κάθε υποσύνολο από t<=n από αυτούς να μπορεί να ανακατασκευάσει το μυστικό, αλλά κάθε υποσύνολο αποτελούμενο από λιγότερα άτομα δεν μαθαίνει καμία πληροφορία για το μυστικό αυτό. Για να επιτευχθεί αυτό, σε κάθε άτομο δίνεται ως μερίδιο η τιμή ενός πολυωνύμου βαθμού t σε μια συγκεκριμένο σημείο ενός διακριτού χώρου τέτοιου ώστε το μυστικό να είναι η τιμή του πολυωνύμου σε κάποιο άλλο σημείο του χώρου αυτού, συνήθως το 0. Δεδομένων οποιοδήποτε t μεριδίων, το μυστικό μπορεί εύκολα να ανακατασκευαστεί χρησιμοποιώντας τη μέθοδο παρεμβολής του Lagrange.

Παρακάτω θα περιγράψουμε τη διαδικασία που θα χρησιμοποιηθεί για τη δημιουργία των κλειδιών. Για να το κάνουμε αυτό, θα χρειαστεί πρώτα να παρουσιάσουμε τις διαφορές ενός αλγορίθμου παραγωγής κλειδιών και ενός πρωτοκόλλου ώστε να μπορέσουμε να δείξουμε τους λόγους για τους οποίους έχουμε ανάγκη την ύπαρξη ενός πρωτοκόλλου.

6 Ένα πρωτόκολλο κατασκευής κλειδιών

Στις μέχρι τώρα εργασίες, έχει οριστεί μόνο η ύπαρξη ενός αλγορίθμου υπολογισμού των κλειδιών, ο οποίος όμως μπορεί να εγγυηθεί ασφάλεια μόνον όταν υπάρχει ένας έμπιστος φορέας. Στη πραγματικότητα υπάρχει ανάγκη για ένα πρωτόκολλο παραγωγής των κλειδιών, το οποίο θα τρέξουν συμμετοχικά οι αποκρυπτογράφοι και δεν δίνει ποτέ σε κανένα άτομο τη δυνατότητα να μπορέσει να αποκρυπτογραφήσει ένα μήνυμα μόνος του. Στο σχήμα κρυπτογράφησης DLIN που χρησιμοποιείται, η κρυπτογράφηση βασίζεται σε δύο δημόσιο κλειδιά X και Y. Εφόσον η λειτουργία τους είναι απολύτως συμμετρική, θα εξετάσουμε μόνο το κλειδί $= \Gamma^x$ για κάποιο μυστικό x. Κατά τη διάρκεια της αποκρυπτογράφησης, αναφέραμε ήδη ότι υψώνουμε τη παράμετρο A στο 1/x . Συνεπώς ο αλγόριθμος αυτό που κάνει είναι διαλέγει ένα x, δημιουργείο το δημόσιο κλειδί G^x , υπολογίζει το $\bar{x}$–$1/x$ και δημιουργεί τα μερίδια $\bar{x_i}$ από το $\bar{x}$, αφού οι αποκρυπτογράφοι χρειάζονται τα μερίδια από το αντίστροφο του αριθμού x.

Εδώ αρχίζει και η δυσκολία μετατροπής του αλγορίθμου αυτού σε διαμοιραζόμενο πρωτόκολλο. Αν υποθέσουμε ότι αρχικά κάθε άτομο φτιάχνει μερίδια του x και παρεμβάλει το G^x, υπάρχει το πρόβλημα ότι τα μερίδια του αντιστρόφου του 1/x δεν είναι τα ίδια με τους αντιστρόφους των μεριδίων του x και δεν υπάρχει κανένας εύκολος τρόπος να πάρει κάποιος το ένα δεδομένου του άλλου! Αν αντίθετα απλά ξεκινούσαμε με τα μερίδια του $\bar{x} = 1/x$, πάλι δεν έχουμε δυνατότητα να βρούμε το δημόσιο κλειδί, το οποίο

είναι τώρα το $G^{1/\bar{x}}$

Για να κατασκευάσουμε ένα κατάλληλο σχήμα κρυπτογράφησης για το DLIN, θα βασιστούμε στο σχήμα διαμοιρασμού του Shamir, το οποίο λόγο των ομομορφικών του ιδιοτήτων επιτρέπει σε μερίδια να χρησιμοποιηθούν για την αποκρυπτογράφηση χωρίς ποτέ να κάνουμε πλήρη ανακατασκευή του κλειδιού.

7 Ένας αλγόριθμος βασισμένος σε threshold

Για δεδομένα t και n, διάλεξε τυχαία τα μυστικά κλειδιά x,y από το F_q και υπολόγισε τα $\bar{x} = 1/x$ και $\bar{y} = 1/y$. Χρησιμοποιήσε το σχήμα του Shamir για να φτιάξεις ένα (t,n) διαμοιρασμό του $\bar{x}$ και μοίρασε σε κάθε αποκρυπτογράφο το μερίδιου του $\bar{x}_i$ και ύστερα επανέλαβε για το y. Δώσε ως έξοδο το δημόσιο κλειδί $(X, Y) = (G^x, G^y)$

Encrypt : ίδιος όπως σε κάθε κλασσικό σχήμα κρυπτογράφησης DLIN.

Decrypt(A,B,C) : Υπολόγισε το μερίδιο αποκρυπτογράφησης ως $D_i = A^{\bar{x}_i} * B^{\bar{x}_i}$ από τα μερίδια $\bar{x}_i, \bar{y}_i$.

Combine: Δεδομένου ενός set από τουλάχιστον t+1 μερίδια αποκρυπτογράφησης, υπολόγισε το κλειδί απόκρυπτογράφησης D ως τη τιμή στη θέση 0 του πολυωνύμου p χρησιμοποιώντας τη μέθοδο παρεμβολής. Το τελικό μήνυμα δίνεται ως M = C/D.

Δεδομένου αυτού του αλγορίθμου για την λειτουργία του σχήματος κρυπτογράφησης, αρκεί να δείξουμε πως να τον μετατρέψουμε σε ένα πρωτόκολλο και να αφαιρέσουμε τελείως την ανάγκη ύπαρξης ενός έμπιστου φορέα για την παραγωγή των κλειδιών. Για να το δείξουμε όμως αυτό, πρέπει πρώτα να γνωρίζουμε τη χρήση του συμμετοχικού υπολογισμού, ο οποίος επιτρέπει σε ένα σύνολο ατόμων, κάθε ένα από τα οποία έχει κάποια μυστική είσοδο x_i να υπολογίσει συμμετοχικά μια συνάρτηση $(y_i)i = f((x_i)_i)$ των εισόδων αυτών με ένα τρόπο τόσο ασφαλή όσο αν κάθε ένας έστελνε την είσοδο του xi σε κάποια έμπιστη οντότητα και αυτή υπολόγιζε τη συνάρτηση f και επέστρεφε σε κάθε έναν τη κατάλληλη τιμή y_i.

Το πρωτόκολλο που αναπτύσσεται έχει ανθεκτικότητα για t < n/3. Για να το επιτύχει αυτό, υποθέτουμε ότι είναι δυνατό να ανακοινώσουμε μια τιμή σε όλους τους συμμετέχοντες και πως μπορεί κάποιος να στείλει σε οποιονδήποτε άλλο μια τιμή χωρίς οι υπόλοιποι να τον ακούσουν. Για την ανάπτυξη του, θα γίνουν δύο μικρές αλλαγές στο πρωτόκολλο Smart-Geisler: αρχικά χρειαστεί η προσαρμογή του στο σχήμα κρυπτογράφησης DLIN και ύστερα θα πειραχθεί έτσι ώστε να χρησιμοποιεί συμμετοχικό υπολογισμό για την παραγωγή των κλειδιών και μια πιο γρήγορη διαδικασία για την αποκρυπτογράφηση, σε αντίθεση με το αρχικό πρωτόκολλο το οποίο είχε πιο γρήγορη παραγωγή κλειδιών και πιο αργή αποκρυπτογράφηση.

8 Το πρωτόκολλο

Αρχικά, ως x(j) θα αναφερόμαστε σε μία τιμή που προήλθε από το άτομο j, είτε ως ανακοίνωση είτε ως προσωπικό μήνυμα. Αντίθετα, μια τιμή που είναι κοινή για όλους τους συμμετέχοντες, θα συμβολίζεται με ένα άστρο ως u* . Αρχικά αρχικοποιούμε ένα Pseudo-Random Secret Sharing (PRSS), το οποίο επιτρέπει στους συμμετέχοντες να «τραβήξουν» τιμές x_l για κάθε l το οποίο ορίζει ένα μοίρασμα κάποιας τυχαίας μυστικής τιμής x_l*

Άπαξ και έχουμε το PRSS, κάθε συμμετέχον τραβά μια τιμή x' η οποία θα αποτελεί το μερίδιο του για το κλειδί αποκρυπτογράφησης και μία άλλη τιμή r. Ύστερα υπολογίζει το $u = \bar{x} * r$ το οποίο, εφόσον τα $\bar{x}$ και r ήταν βαθμού t μερίδια των αντιστοίχων μυστικών τιμών, τώρα αποτελεί μερίδιο 2t μιας άλλης τιμής u*. Από αυτό το σημείο και πέρα, κάθε συμμετέχον, περνά από τις παρακάτω 4 φάσεις.

Φάση 1η – Μοίρασμα του u : Δημιούργησε τοπικά ένα μοίρασμα βαθμού t για το u και στείλε σε κάθε συμμετέχον j το μοίρασμα u_j που του αντιστοιχεί. Για να γίνει αυτό αρκεί να θέσει $c_0 \leftarrow u$ και να διαλέξει τυχαίους συντελεστές $c_1, c_2, ...c_t$ από το Zq ώστε να ορίσει ένα κατάλληλο πολυώνυμο p(x) και να θέσει $u_j \leftarrow p(j)$ για κάθε j.

Φάση 2η – Παρεμβολή του u' : Κάθε συμμετέχον μαζεύει τα μερίδια $u^{(j)}$ από όλους τους υπόλοιπους και υπολογίζουν το u' ως τη τιμή του πολυωνύμου που προκύπτει όταν χρησιμοποιηθεί η μέθοδος παρεμβολής για τα u(j) και ύστερα ανακοινώνουν τη τιμή u' σε όλους.

Φάση 3 – Ανακατασκευή του u* Κάθε συμμετέχων λαμβάνει τις τιμές $u'^{(j)}$ από τους υπόλοιπους και ανακατασκευάζει το u* από τις τιμές αυτές. Όλοι οι συμμετέχοντες τώρα έχουν στη κατοχή τους μια τιμή u* η οποία είναι το γινόμενο των μυστικών r* και $x'*$ τα οποία έχουν οριστεί από τα μερίδια r και $\bar{x}$ αντίστοιχα. Σε αυτό το σημείο κάθε συμμετέχων υπολογίζει το μερίδιο του δημόσιου κλειδιού $X = G^{r/u*}$ και ανακοινώνει την τιμή του σε όλους τους υπολοίπους.

Φάση 4 – Δημόσιο κλειδί Σε αυτή τη φάση κάθε ένας λαμβάνει τα μερίδια X(j) του δημοσίου κλειδιού από όλους τους υπόλοιπους και τα χρησιμοποιεί για να ανακατασκευάσει το δημόσιο κλειδί X* από αυτά.

9 Αποδοτικότητα και Ασφάλεια

Αν και η μέθοδος συμμετοχικού υπολογισμού μπορεί θεωρητικά να χρησιμοποιηθεί για τον υπολογισμό οποιασδήποτε λειτουργίας, στην πράξη πολλές φορές τα πρωτόκολλα που χτίζονται επάνω σε αυτή είναι πολύ αργά ώστε να φανούν χρήσιμα, λόγω του υπερβολικά μεγάλου κόστους επικοινωνίας ανάμεσα στους συμμετέχοντες. Το πρωτόκολλο που αναπτύχθηκε παραπάνω για τα κλειδιά είναι αρκετά αποδοτικό ώστε να χρησιμοποιηθεί και στην πράξη, αφού το κόστος του είναι μηδαμινό μπροστά στο κόστος των malleable proofs κάτι που σημαίνει ότι η δημιουργία των κλειδιών θα καταλαμβάνει μόνο ένα μικρό μέρος του συνολικού χρόνου που θα απαιτεί το πρωτόκολλο.

Το πρωτόκολλο που αναπτύχθηκε έχει ασφάλεια ενάντια σε t < n/3 κακόβουλους συμμετέχοντες κατά τη διάρκεια της ανταλλαγής δεδομένων. Επειδή οι μόνοι υπολογισμοί που εκτελεί κάποιος σε δεδομένα που έλαβε από τους υπόλοιπους συμμετέχοντες είναι παρεμβολές πολυωνύμων βαθμού το πολύ 2t, οι κακόβουλοι συμμετέχοντες δεν μπορούν να μεταδώσουν σωστές τιμές χωρίς να οδηγήσουν το πρωτόκολλο στην αναστολή του.

10 Ανάλυση της πολυπλοκότητας των proofs

Για μια ακόμη φορά οι δημιουργοί του πρωτοκόλλου καλούνται να διαλέξουν ανάμεσα στις διαφορετικές υλοποιήσεις που υπάρχουν, αυτή τη φορά όσον αφορά τους αλγορίθμους για κρυπτογράφησης με βάση ζεύγη. Με γνώμονα τη μέγιστη αποδοτικότητα για ένα επίπεδο ασφάλειας, κρίνεται καταλληλότερη η χρήση ελλειπτικών καμπυλών και συγκεκριμένα μιας καμπύλης Barreto-Naehrig.

Το πρόβλημα με την συγκεκριμένη επιλογή έγκειται στο ότι το ζευγάρωμα των συνόλων που προκύπτει από τις ελλειπτικές καμπύλες είναι ασύμμετρο, ενώ το σχήμα κρυπτογράφησης στο οποίο θέλουν να το χρησιμοποιήσουν είναι συμμετρικό. Για το λόγο αυτό χρειάζεται να γίνουν δύο αλλαγές στο σχήμα: 1) Το σχήμα κρυπτογράφησης πρέπει τώρα πια να κρατάει και τα δύο σύνολα της G_1, G_2 που θα χρησιμοποιηθούν και 2) Κάθε στοιχείο των συνόλων το οποίο εμφανίζεται τόσο στο σύνολο G1 και στο σύνολο G_2 στο συμμετρικό πρωτόκολλο πρέπει να αντικατασταθεί από ένα ζευγάρι από στοιχεία του συμμετρικού πρωτοκόλλου και να φυλαχτεί από μια επιπλέον εξίσωση.

Τα αποδεικτήρια Groth-Sahai βασίζονται στα ζεύγη ανάμεσα σε σύνολα και μπορούν να δημιουργηθούν κάνοντας κάποιες υποθέσεις για αρκετούς τύπους εξισώσεων. Έστω ένα αρχικό σετ από παραμέτρους το οποίο περιγράφει τα σύνολα (G_1, G_2, G_T) κάποιου βαθμού p, ο οποίος είναι πρώτος ή δύναμη κάποιου πρώτου με τους αντίστοιχους generators $(\Gamma_1, \Gamma_2, \Gamma_T)$ και μια διγραμμική αντιστοίχηση $e : G_1 x G_2 \rightarrow G_T$, ένα μοντέλο το οποίο καλύπτεται από τις BN καμπύλες. Τότε, μας ενδιαφέρουν οι εξισώσεις Pairing

Product Equations (PPE) οι οποίες περιγράφονται στο DLIN. Μια PPE είναι μια συνάρτηση με τα διανύσματα μεταβλητών a που ανήκουν στο G1 και b που ανήκουν στο G2 με τη μορφή $v \bullet \underline{b} \cdot \underline{a} \bullet w \cdot \underline{a} \bullet \Gamma \bullet \underline{b} = t$ όπου $\cdot$ η πράξη στο σύνολο G_T και $\bullet$ ο απλός πολλαπλασιασμός.

Ένα GS proof τότε αποδεικνύει ότι ο κάτοχος του γνωρίζει μια ανάθεση τιμών σε ένα σύνολο μεταβλητών η οποία ικανοποιεί ένα σύνολο εξισώσεων. Οι τιμές αυτές συχνά αναφέρονται και ως μάρτυρας. Αυτός που θέλει να αποδείξει κάτι ξεκινάει κάνοντας μια δέσμευση σε κάθε τιμή και ύστερα υπολογίζει ένα proof pair για κάθε εξίσωση. Το συνολικό αποδεικτήριο αποτελείται από μια δέσμευση για κάθε μεταβλητή που εμφανίζεται στις εξισώσεις και από ένα proof pair για κάθε εξίσωση. Για να επιβεβαιωθεί ένα GS proof, πρέπει να υπολογιστεί μια εξίσωση επιβεβαίωσης για κάθε εξίσωση που περιλαμβάνει τις δεσμεύσεις σε μεταβλητές, τις σταθερές στην αρχική εξίσωση και τα proof pairs.

11 Αποτελεσμάτα

Έστω L ο αριθμός των ψήφων που ανακατεύτηκαν κατά τη διάρκεια λειτουργίας του mixnet. Από τις 4L μεταβλητές και τις 11 εξισώσεις που χρησιμοποιούνται στο πρωτόκολλο, οι εξισώσεις 1-4 είναι απλές PPE οι 5 και 6 χρειάζονται (μαζί) L βοηθητικές μεταβλητές και εξισώσεις ώστε να γίνουν πλήρης PPE, οι 7 και 8 είναι γραμμικές PPE και οι 9 έως και 11 είναι ποσοτικοποιημένες (γιακαθε I : 1 <= I <=L) και συνεπώς είναι στη πραγματικότητα L PPE η κάθε μια. Για να τις μεταφέρουμε σε ένα ασύμμετρο σχήμα χρειαζόμαστε ακόμη 2L βοηθητικές μεταβλητές και 4L βοηθητικές εξισώσεις. Συνολικά καταλήγουμε με 4L μεταβλητές στο G_1 και 7L μεταβλητές στο G_2.

Για τις μετρήσεις χρησιμοποιήθηκε η υλοποίηση των BN καμπύλων που προσφέρεται από τη βιβλιοθήκη ανοιχτού κώδικα MIRACL. Για να μπορέσουν να ληφθούν κάποια κατάλληλα συμπεράσματα, γίνεται εξέταση του κατά πόσο θα μπορούσε να χρησιμοποιηθεί η τεχνική που αναπτύχθηκε για τις εκλογές στο Darmstadt της Γερμανίας, για τη διαδικασία της ψηφοφορίας δια αλληλογραφίας, όπου υπάρχουν περίπου 824 ψηφοφόροι δια αλληλογραφίας σε κάθε περιοχή. Το αποτέλεσμα των μετρήσεων δείχνει ότι η μέθοδος είναι κατάλληλη για πραγματική χρήση σε ένα μικρό αριθμό ατόμων, όπως στο παραπάνω σενάριο στο οποίο η επιβεβαίωση των ψήφων χρειαζόταν περίπου 20 λεπτά.

12 Συμπεράσματα

Με βάση όσα αναφέρθηκαν παραπάνω, μπορούμε να δούμε ότι η αντικατάσταση της ψηφοφορίας δια αλληλογραφίας είναι δυνατή σε επίπεδο κάποιας περιφέρειας αλλά η χρήση του ως κύριο σύστημα ψηφοφορίας, ακόμη και σε επίπεδο πόλης είναι ακόμη ακατόρθωτη, αφού θα απαιτούσε συνολικό χρόνο περίπου δύο εβδομάδων.

Στην εργασία αφήνονται αρκετά ανοιχτά προβλήματα για όσους θέλουν να ασχοληθούν με τη περαιτέρω επέκταση του πρωτοκόλλου, αφού παραμένει η ανάγκη για ενίσχυση του ώστε να αντέχει σε επιθέσεις από παραπάνω από n/3 κακόβουλους συμμετέχοντες, ενώ υπάρχει και η δυνατότητα για αντοχή σε επίθεση από έως και n-1 επιτιθέμενους, αν γίνει χρήση του πρωτοκόλλου SPDZ.

Τέλος, για να υπάρχει μεγαλύτερες ελπίδες για εφαρμογή του πρωτοκόλλου σε πραγματικές συνθήκες, θα ήταν καλή η προσαρμογή του στην υλοποίηση των BN καμπυλών όπως παρουσιάζονται από την ομάδα του Beuchat καθώς αυτό θα επιτάχυνε το πρωτόκολλο έως και 5 φορές, κάνοντας ευκολότερη τη χρήση του σε συνθήκες όπου το πλήθος των ψηφοφόρων είναι πολύ μεγάλο.

13 Βιβλιογραφία

1. Towards a Practical Cryptographic Voting Scheme Based on Malleable Proofs, Bernard, Neumann, Volkamer
2. Verifiable Elections that Scale for Free, Chase, Kohlweiss, Meiklejohn, Lysyanskaya
3. Share Conversion, Pseudorandom Secret-Sharing and Applications to Secure Computation, Cramer, Ishai
4. Multiparty Computation an Introduction, Cramer, Nielsen