Ατομική Διπλωματική Εργασία

ΥΛΟΠΟΙΗΣΗ ΣΥΣΤΗΜΑΤΟΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΨΗΦΟΦΟΡΙΑΣ

Νεκταρία Σταύρου

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μάιος 2013

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΥΛΟΠΟΙΗΣΗ ΣΥΣΤΗΜΑΤΟΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΨΗΦΟΦΟΡΙΑΣ

Νεκταρία Σταύρου

Επιβλέπουσα Καθηγήτρια

Δρ. Άννα Φιλίππου

Η Ατομική Διπλωματική Εργασία υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων απόκτησης του πτυχίου Πληροφορικής του Τμήματος Πληροφορικής του Πανεπιστημίου Κύπρου

Μάιος 2013

Ευχαριστίες

Θα ήθελα να εκφράσω τις ειλικρινές μου ευχαριστίες στην επιβλέπουσα καθηγήτρια μου, κυρία Άννα Φιλίππου που με πίστεψε, στήριξε και μου έδωσε την ευκαιρία να εργαστώ σε ένα τόσο ενδιαφέρον θέμα. Η καθοδήγηση και η καλή διάθεση που εκπνέει ήταν σημαντικοί παράγοντες για την μελέτη και την διεκπεραίωση της παρούσας διπλωματικής. Σας ευχαριστώ!

Περίληψη

Η Ατομική Διπλωματική Εργασία, πραγματεύεται τη μελέτη της ηλεκτρονικής ψηφοφορίας και την υλοποίηση ενός συστήματος ηλεκτρονικής ψηφοφορίας μέσω Διαδικτύου.

Στο Κεφάλαιο 1, αναφέρονται οι λόγοι οι οποίοι μας κίνησαν τον ενδιαφέρον για να ασχοληθούμε με το θέμα της ηλεκτρονικής ψηφοφορίας, καθώς και τους στόχους οι οποίοι αναμένονται να επιτευχθούν από τη Διπλωματική Εργασία.

Στην συνέχεια παρέχουμε μία μελέτη για την ηλεκτρονική ψηφοφορία, για τα στάδια τα οποία απαιτούνται σε μία ηλεκτρονική ψηφοφορία. Επίσης αναλύονται οι απαιτήσεις ασφάλειας και πρακτικότητας οι οποίες αναμένεται να υπάρχουν σε ένα πρωτόκολλο ηλεκτρονικής ψηφοφορίας. Έπειτα αξιολογούμε και μελετούμε συστήματα ηλεκτρονικής ψηφοφορίας, τα οποία έχουν ήδη εφαρμοστεί με επιτυχία στην Εσθονία και στη Γενεύη, καθώς και το σύστημα Sensus. Ακολούθως μελετούμε κρυπτογραφικές τεχνικές και μοντέλα τα οποία εφαρμόζονται στην ηλεκτρονική ψηφοφορία.

Το Κεφάλαιο 3 ασχολείται με τη μελέτη έξι διαφορετικών πρωτοκόλλων ηλεκτρονικής ψηφοφορίας, τα οποία αξιολογούνται ως προς τις απαιτήσεις τις οποίες πληρούν.

Στη διπλωματική αυτή εργασία, έχουμε υλοποιήσει ένα σύστημα ηλεκτρονικής ψηφοφορίας βασισμένο στο πρωτόκολλο IIS. Το πρωτόκολλο, έχει επιλεγεί λόγω σημαντικών πλεονεκτημάτων του έναντι των υπόλοιπων, τα οποία ήταν ίσως σημαντικότερα από πλεονεκτήματα άλλων πρωτοκόλλων. Στο Κεφάλαιο 4 περιγράφονται οι φάσεις του πρωτοκόλλου που έχουμε υλοποιήσει, αξιολογούμε το πρωτόκολλο αυτό, καθώς επίσης περιγράφονται οι περιγραφές υλοποίησής του, και παρουσιάζονται διαγράμματα τα οποία μπορούμε να μελετήσουμε για να κατανοήσουμε καλύτερα το πρωτόκολλο το οποίο έχουμε υλοποιήσει.

Το σύστημα το οποίο έχει υλοποιήσει τρέχει σε κάθε φυλλομετρητή, είναι βασισμένο στο πρωτόκολλο IIS. Για την υλοποίηση του συστήματος έχουν χρησιμοποιηθεί οι πιο σύγχρονες τεχνολογίες διαδικτύου, όπως η HTML5, η τεχνολογία FancyBox, καθώς επίσης και η γλώσσα προγραμματισμού PHP.

Περιεχόμενα

Κεφάλαιο 1 ..... **1**

Εισαγωγή **1**

1.1 Υποκίνηση Διπλωματικής Εργασίας 1

1.2 Στόχοι Διπλωματικής Εργασίας 3

1.3 Δομή Εργασίας 4

Κεφάλαιο 2 ..... **6**

Ηλεκτρονική Ψηφοφορία **6**

2.1 Ηλεκτρονική Ψηφοφορία 6

2.2 Στάδια Ηλεκτρονικής Ψηφοφορίας 7

2.3 Απαιτήσεις 8

2.4 Αξιολόγηση Συστημάτων Ηλεκτρονικής Ψηφοφορίας 10

2.5 Ηλεκτρονική Ψηφοφορία και Κρυπτογραφία 13

2.6 Παράδειγμα Εφαρμογής της Ηλεκτρονικής Ψηφοφορίας 19

Κεφάλαιο 3 ..... **24**

Πρωτόκολλα Ηλεκτρονικής Ψηφοφορίας **24**

3.1 A six-authority protocol 24

3.2 Foo Protocol (Fujioka,Okamoto και Ohta) 29

3.3 An Anonymous Electronic Voting Protocol for Voting Over The Internet 30

3.4 REVS- A Robust Electronic Voting System 34

3.5 Wu And Sankaranarayana Protocol 36

3.6 A Novel Simple Secure Internet Voting Protocol 37

Κεφάλαιο 4 ..... **39**

Πρωτόκολλο Ψηφοφορίας βασισμένο στο IIS **39**

4.1 Πρωτόκολλο IIS 39

4.1.1 Φάση Εγγραφής 41

4.1.2 Φάση Ψηφοφορίας 43

4.1.3 Φάση Καταμέτρησης 45

4.2 Αξιολόγηση Πρωτοκόλλου 49

4.3 Βασικές Τεχνικές που χρησιμοποιούνται στο Πρωτόκολλο 51

Κεφάλαιο 5 ..... **61**

Προδιαγραφές **61**

5.1 Απαιτήσεις Χρήστη 61

5.2 Προοπτική Συστήματος (Product Perspective) 62

5.3 Διαγράμματα Ροής Δεδομένων 64

5.4 Περιπτώσεις Χρήσεις 71

5.5 Αποθήκευση Δεδομένων 76

5.6 Διαγράμματα Ακολουθίας 79

5.7 Υλοποίηση 82

Κεφάλαιο 6 ..... **89**

Συμπεράσματα και Μελλοντικές Επεκτάσεις **89**

Παράρτημα Α **1**

Παράρτημα Β **15**

Κεφάλαιο 1

Εισαγωγή

1.1 Υποκίνηση Διπλωματικής Εργασίας 1

1.2 Στόχοι Διπλωματικής Εργασίας 3

1.3 Δομή Εργασίας 4

1.1 Υποκίνηση Διπλωματικής Εργασίας

Ο μαγευτικός κόσμος της ασφάλειας και της κρυπτογραφίας, με συνέπαιρνε αρκετό καιρό τώρα, και μου έλκυσε το ενδιαφέρον. Η ασφάλεια είναι τόσο σωματική όσο και πνευματική.

Το σπίτι μας αποτελεί προσωπική μας ιδιοκτησία, και φροντίζουμε να το κρατούμε ασφαλές, οχυρωμένο από οποιεσδήποτε επιθέσεις. Ένα κράτος επίσης, οφείλει να διατηρεί την δική του ασφάλεια. Έτσι ξοδεύονται τρισεκατομμύρια δολάρια κάθε χρόνο στον στρατό, για να είναι σε θέση κάθε κράτος να προστατεύεται από επιθέσεις. Συνεπώς ο καθένας μας αντιλαμβάνεται ότι η ασφάλειά μας αποτελεί ένα μείζον σημασίας θέμα.

Η ασφάλεια μας όμως δεν είναι μόνο σωματική, αλλά και πνευματική. Επιζητούμε, τα δεδομένα και οι πληροφορίες μας, να παραμένουν ασφαλισμένα και καμία κακόβουλη επίθεση να μην μπορεί να τα διαγράψει ή να τα αλλοιώσει. Αρκετά συχνά, λαμβάνουμε μηνύματα από φορείς του πανεπιστήμιου, για να προστατέψουμε τους εαυτούς μας από επιθέσεις τύπου fishing. Η ασφάλειά μας είναι και μέρος της ελευθερίας μας.

Ίσως μία από τις μεγαλύτερες ελευθερίες που έχει ένας ελεύθερος άνθρωπος, είναι η ελευθερία της Δημοκρατίας. Να είναι σε θέση δηλαδή, ως πολίτης ενός κράτους, να ασκεί τον δικό του ρόλο στην διακυβέρνηση μίας χώρας. Και το μεγαλύτερο εργαλείο για να το πράξει αυτό είναι το δικαίωμά του να ψηφίσει μέσα από τη διαδικασία της ψηφοφορίας. Το

δικαίωμά δηλαδή της ψήφου του. Μέσω αυτού μπορεί να εκφράζει την άποψή του σε σημαντικά θέματα, όπως την επιλογή του ως προς την εκλογή προέδρου, πρωθυπουργού ή δημάρχου, αλλά και για πιο απλές θέσεις, όπως την εκλογή φοιτητικών εκπροσώπων στο σώμα του Πανεπιστημίου Κύπρου. Η ψήφος πρέπει πάντοτε να είναι μυστική, και ασφαλισμένη κάτω από οποιεσδήποτε προϋποθέσεις

Οι ψηφοφορίες, στην Κύπρο και σε πολλές άλλες χώρες, διεξάγονται με τον παραδοσιακό τρόπο, ένα τρόπο που λειτουργεί για εκατοντάδες χρόνια. Την ψήφο σε χαρτί με όλα τα μειονεκτήματα ή πλεονεκτήματα τα οποία γνωρίζουμε. Άλλες πάλι χώρες όπως η Εσθονία ή η Ελβετία, είχαν μετακινηθεί ένα βήμα παραπέρα, καθιστώντας την τεχνολογία ως μεγάλο παράγοντα στην εκλογική διαδικασία, καθώς έχουν υιοθετήσει την ηλεκτρονική ψηφοφορία ως ένα εναλλακτικό τρόπο ψηφοφορίας.

Η ηλεκτρονική ψηφοφορία, προσφέρει πολλά πλεονεκτήματα. Για παράδειγμα, δίνει τη δυνατότητα να ψηφίσουν άτομα που βρίσκονται στο εξωτερικό όπως φοιτητές και οι οποίοι δεν έχουν πρόσβαση σε κάλπη. Ακόμη μπορούν να ψηφίσουν άτομα τα οποία δεν έχουν κάποιο μεταφορικό μέσο, ή άτομα τα οποία πρέπει να μεταβούν σε άλλη πόλη για να ψηφίσουν. Επίσης μειώνεται η σπατάλη χρημάτων για χαρτί και μελάνι, καθώς επίσης η καταμέτρηση γίνεται σε ελάχιστο διάστημα από τα συστήματα. Έτσι κυβερνήσεις και οργανισμοί μειώνουν τις εκλογικές τους δαπάνες κατά πολύ. Επίσης τα συστήματα ηλεκτρονικής ψηφοφορίας μπορούν να προσφέρουν πολλές περισσότερες πληροφορίες από ότι ένα παραδοσιακό ψηφοδέλτιο όπως για παράδειγμα το βιογραφικό του υποψηφίου και δίνουν τη δυνατότητα στους ανθρώπους να ψηφίσουν όποτε θέλουν και από την άνεση του σπιτιού τους. Έτσι μπορούμε να δούμε ότι η συγκεκριμένη τεχνολογία έχει τεράστιες προοπτικές και θα ήταν καλό να μελετηθεί περαιτέρω. Τα παραπάνω γεγονότα, με ώθησαν αρχικά στο να ασχοληθώ με την ηλεκτρονική ψηφοφορία.

Η ηλεκτρονική ψηφοφορία πρέπει να διασφαλίζει ότι η ψήφος ενός ψηφοφόρου παραμένει μυστική και δεν αλλοιώνεται το περιεχόμενο της. Επίσης, καμία ψήφος δεν είναι δυνατόν να καταμετρηθεί περισσότερο από μια φορές ή να διαγραφεί. Αυτές, είναι μερικές από τις απαιτήσεις που ένα σύστημα ηλεκτρονικής ψηφοφορίας πρέπει να ικανοποιεί.

Πως θα μπορούσαν αυτές οι απαιτήσεις να αξιοποιηθούν στα πλαίσια ενός ηλεκτρονικού συστήματος ψηφοφορίας; Πως έχουν εφαρμοστεί τα ηλεκτρονικά συστήματα σε άλλες χώρες, και πως αυτά είχαν πετύχει τον σκοπό τους; Τι πρωτόκολλα ηλεκτρονικής ψηφοφορίας ήδη υπάρχουν;

Αυτά ήταν κάποια ερωτήματα τα οποία με υποκίνησαν να ασχοληθώ με το θέμα της ηλεκτρονικής ψηφοφορίας. Μέσα από την μελέτη μου, το συγκεκριμένο θέμα με ενδιέφερε ακόμη περισσότερο. Έτσι, εν το μέσω της Ατομικής μου Διπλωματικής Εργασίας, και αφού είχα δει επαρκείς τεχνικές κρυπτογραφίας, πρωτόκολλα αλλά και συστήματα ηλεκτρονικής ψηφοφορίας, είχα βρει ακόμη πιο ενδιαφέρον με την σειρά μου, να εφαρμόσω όλα όσα είχα μάθει στην πράξη και να υλοποιήσω και εγώ ένα πρωτόκολλο ηλεκτρονικής ψηφοφορίας, κατασκευάζοντας ένα σύστημα, το οποίο θα μπορούσε να χρησιμοποιηθεί σε πραγματικές εκλογές για το κοινό καλό.

1.2 Στόχοι Διπλωματικής Εργασίας

Η Διπλωματική αυτή εργασία, έχει ως ένα από τους στόχους της να μελετήσει τις διάφορες απαιτήσεις που υπάρχουν σε πρωτόκολλα ηλεκτρονικής ψηφοφορίας όπως τα πιο κάτω:

Απουσία απόδειξης: Κάποιοι ψηφοφόροι, για χάρη χρημάτων ή άλλου είδους υπηρεσιών, ίσως να ήθελαν να πουλήσουν την ψήφο τους. Έτσι υφίσταται η αγορά ψήφων. Αυτό πλήττει το δημοκρατικό δικαίωμα της ψήφου, και θα πρέπει οι ψηφοφόροι να μην είναι σε θέση να αποδείξουν έναντι τρίτου, εκ των υστέρων την ψήφο του, για να αποφεύγεται η αγορά ψήφων.

Δυνατότητα επαλήθευσης: Η εμπιστοσύνη σε ένα σύστημα ηλεκτρονικής ψηφοφορίας, είναι μείζων παράγοντας για την χρήση του. Ο ψηφοφόρος, πρέπει να είναι σίγουρος ότι η ψήφος του πράγματι καταχωρήθηκε και λήφθηκε υπόψη, και ισότιμα με οποιοδήποτε άλλο ψηφοφόρο, στη διαμόρφωση του εκλογικού αποτελέσματος.

Δικαιοσύνη: Πολλές φορές επηρεαζόμαστε από το πως έχουν πράξει, ή ψηφίσει στην δική μας περίπτωση άλλα άτομα. Έτσι, το σύστημα, δεν θα πρέπει να εμφανίζει τα μέχρι στιγμής αποτελέσματα, πριν δηλαδή από το τέλος της ψηφοφορίας, ώστε να μην επηρεάζονται τα άτομα τα οποία δεν έχουν ψηφίσει ακόμη.

Κάποιες από τις απαιτήσεις αυτές είναι δυνατόν να αντιφάσκουν μεταξύ τους. Για παράδειγμα, αν δοθεί σε κάθε χρήστη η δυνατότητα να εντοπίσει ότι η ψήφος του έχει μετρήσει όπως αυτή έχει καταρριφθεί, ικανοποιείται η δεύτερη απαίτηση, αλλά ταυτόχρονα παραβιάζεται η πρώτη.

Η εργασία αυτή έχει ως στόχο να μελετήσει τις βασικότερες απαιτήσεις, όπως και τις πιο πάνω, στα πλαίσια πρωτοκόλλων που έχουν προταθεί, και υπάρχουν σήμερα για ηλεκτρονική ψηφοφορία και να τα αξιολογήσει ως προς τον βαθμό στον οποίο ικανοποιούν ιδιότητες πιο πάνω.

Επίσης ακόμη ένας στόχος της Διπλωματικής μου Εργασίας, στον οποίο είχα αφιερώσει και το μεγαλύτερο μέρος της εργασίας μου, είναι να υλοποιήσω ένα πραγματικό σύστημα ηλεκτρονικής ψηφοφορίας βασισμένο σε ένα ήδη υπάρχον πρωτόκολλο ηλεκτρονικής ψηφοφορίας, το οποίο επιλέχθηκε ανάμεσα σε διάφορα άλλα που υπάρχουν στη βιβλιογραφία με ένα από τα κριτήρια τη λειτουργία του, που προσφέρει δυνατότητα αλλαγής ψήφους από το ψηφοφόρο και το διαμοιρασμό της ψήφους σε διαφορετικούς διακομιστές. Το σύστημα αυτό πρέπει να ακολουθεί πιστά το πρωτόκολλο, να παρέχει την απαραίτητη ασφάλεια, να είναι πρακτικό, και να μπορεί να τρέχει σε οποιοδήποτε φυλλομετρητή.

1.3 Δομή Εργασίας

Η παρούσα μελέτη σκοπό έχει να παρουσιάσει τις βασικές έννοιες της ηλεκτρονικής ψηφοφορίας, κάποια πρωτόκολλα ηλεκτρονικής ψηφοφορίας που προτάθηκαν και να αναλύσει περαιτέρω το πρωτόκολλο IIS, το οποίο επιλέχθηκε ανάμεσα σε αυτά τα πρωτόκολλα.

Στο δεύτερο κεφάλαιο παρουσιάζεται μία μελέτη για την ηλεκτρονική ψηφοφορία, τα στάδια τα οποία έχει, αλλά επίσης και τις απαιτήσεις που χρειάζονται τόσο στο φάσμα της ασφάλειας όσο και στο φάσμα της πρακτικότητας. Στη συνέχεια παρουσιάζονται ήδη υπάρχοντα συστήματα όπως της Ελβετίας και της Εσθονίας καθώς επίσης κάποιες τεχνικές κρυπτογραφίας που χρησιμοποιούνται στην ηλεκτρονική ψηφοφορία. Αυτή η μελέτη, μου είχε δώσει σημαντικά εφόδια για μετέπειτα, στην κατανόηση των προτεινόμενων πρωτοκόλλων.

Στο τρίτο κεφάλαιο παρουσιάζονται συνοπτικά κάποια πρωτόκολλα ηλεκτρονικής ψηφοφορίας όπως το A six Authority Protocol και το πρωτόκολλο An Anonymous Electronic Voting Protocol for Voting Over The Internet.

Το τέταρτο κεφάλαιο της μελέτης παρουσιάζεται το πρωτόκολλο που έχω επιλέξει, το οποίο είχε εξαιρετικά μεγάλο ενδιαφέρον. Το πρωτόκολλο αυτό ονομάζεται “Πρωτόκολλο Ψηφοφορίας Βασισμένο στο Improved Implicit Security”. Περιγράφω και αναλύω το

πρωτόκολλο, τα τρία στάδια από τα οποία αποτελείται (εγγραφή, ψηφοφορία, καταμέτρηση και επαλήθευση) δίνοντας τα απαραίτητα παραδείγματα και επεξηγήσεις. Περιγράφω τις βασικές τεχνικές που χρησιμοποιούνται στο πρωτόκολλο το οποίο έχω υλοποιήσει. Περιγράφω δηλαδή τις συναρτήσεις κατατεμαχισμού, οι οποίες και χρησιμοποιούνται σε μεγάλο βαθμό, καθώς επίσης την συμμετρική, ασύμμετρη και μη κρυπτογραφημένη αυθεντικοποίηση. Περιγράφω ακόμη το πρωτόκολλο επικοινωνίας SSL το οποίο εγγυάται την ασφαλή επικοινωνία μεταξύ των μελών τα οποία αλληλεπιδρούν με το συστήμά μου. Επίσης περιγράφεται η αριθμητική των υπολοίπων, η οποία είναι η αριθμητική του πρωτόκολλου, καθώς επίσης και η απόδειξη με μηδενική γνώση challenge/responce protocol.

Στο πέμπτο κεφάλαιο περιγράφονται οι προδιαγραφές απαιτήσεων λογισμικού, όπως τις διεπαφές συστήματος, υλικού, λογισμικού και επικοινωνίας του συστήματος, τις λειτουργίες του, τα χαρακτηριστικά των χρηστών του και τους περιορισμούς οι οποίοι υπάρχουν και πρέπει να ληφθούν υπόψη.

Στο κεφάλαιο αυτό, δίνονται τα απαραίτητα σχεδιαγράμματα, για να κατανοήσουμε την λειτουργία του πρωτοκόλλου αυτού. Πιο συγκεκριμένα για τις διάφορες φάσεις δίνονται τα σχεδιαγράμματα περιπτώσεων χρήσεων, διαγράμματα ροής δεδομένων και διαγράμματα ακολουθίας. Επίσης περιγράφεται η αποθήκευση των δεδομένων, και τα χαρακτηριστικά της βάσης δεδομένων το οποίο θα απαιτείται να υπάρχει στο σύστημα.

Στην συνέχεια περιγράφονται οι παράμετροι της υλοποίησης του συστήματός μου. Δηλαδή περιγράφονται τα εργαλεία τα οποία έχω χρησιμοποιήσει, οι γλώσσες προγραμματισμού, οι οντότητες οι οποίες υπάρχουν στις διάφορες βάσεις δεδομένων.

Στο έκτο κεφάλαιο, αναφέρονται τα συμπεράσματα και οι μελοντικές επεκτάσεις της Διπλωματικής Εργασίας.

Στα παραρτήματα που ακολουθούν περιλαμβάνονται ένα εγχειρίδιο χρήσης του συστήματος, καθώς επίσης και ένα ερωτηματολόγιο, το οποίο είχε διαμοιραστεί σχετικά με την ηλεκτρονική ψηφοφορία.

Κεφάλαιο 2

Ηλεκτρονική Ψηφοφορία

2.1 Ηλεκτρονική Ψηφοφορία 6

2.2 Στάδια Ηλεκτρονικής Ψηφοφορίας 7

2.3 Απαιτήσεις 8

2.4 Αξιολόγηση Συστημάτων Ηλεκτρονικής Ψηφοφορίας 10

2.5 Ηλεκτρονική Ψηφοφορία και Κρυπτογραφία 13

2.6 Παράδειγμα Εφαρμογής της Ηλεκτρονικής Ψηφοφορίας 19

2.1 Ηλεκτρονική Ψηφοφορία

Σε αυτό το κεφάλαιο θα εξετάσουμε το θεωρητικό πλαίσιο των βασικών θεμάτων που αφορούν την ηλεκτρονική ψηφοφορία. Ορίζεται η έννοια της ηλεκτρονικής ψηφοφορίας και γίνεται εκτενής αναφορά στα στάδια και στις απαιτήσεις που πρέπει να πληρεί ένα σύστημα ηλεκτρονικής ψηφοφορίας καθώς επίσης επιχειρείται μια αποτίμηση της ηλεκτρονικής ψηφοφορίας. Επίσης παρουσιάζονται κάποια χαρακτηριστικά παραδείγματα εφαρμογών της ηλεκτρονικής ψηφοφορίας. Το κεφάλαιο αυτό κλείνει με την σύνδεση της κρυπτογραφίας στην ηλεκτρονική ψηφοφορία.

Η ηλεκτρονική ψηφοφορία είναι ένας όρος που περικλείει πολλούς διαφορετικούς τύπους ψηφοφορίας, και περιλαμβάνει τόσο τα ηλεκτρονικά μέσα για να δηλώνεται μία ψήφος όσο και τα ηλεκτρονικά μέσα καταμέτρησης των ψήφων [21]. Με απλά λόγια θα λέγαμε πως η ηλεκτρονική ψηφοφορία σχετίζεται με την χρήση ηλεκτρονικών μέσων για να διεκπεραιωθεί η ψηφοφορία κατά τη διάρκεια της εκλογικής αναμέτρησης.

Κρίσιμη είναι η διάκριση των μορφών της ηλεκτρονικής ψηφοφορίας, μεταξύ της απομακρυσμένης Διαδικτυακής ηλεκτρονικής ψηφοφορίας και της ηλεκτρονικής ψηφοφορίας στα εκλογικά κέντρα. Στην πρώτη περίπτωση ο ψηφοφόρος μπορεί να ασκήσει το εκλογικό του δικαίωμα από οποιοδήποτε ηλεκτρονικό υπολογιστή που διαθέτει πρόσβαση στο Διαδίκτυο, ενώ στη δεύτερη περίπτωση ο ψηφοφόρος καλείται να προσέλθει στα εκλογικά κέντρα για να ψηφίσει μέσω συγκεκριμένων υπολογιστών που είναι εγκατεστημένοι στο εκλογικό κέντρο. Η παρούσα μελέτη επικεντρώνεται στην απομακρυσμένη Διαδικτυακή ηλεκτρονική ψηφοφορία.

Η ψηφοφορία μέσω Διαδικτύου είναι ένας νέος τρόπος ηλεκτρονικής ψηφοφορίας που προσφέρει πολλές υπηρεσίες, δυνατότητες και πολλά πλεονεκτήματα από την χρήση της με βασικότερες την προοπτική αύξησης του ποσοστού συμμετοχής, την ταχύτητα καταμέτρησης και τη δυνατότητα πρόσβασης για να ασκήσεις το εκλογικό σου δικαίωμα από οποιοδήποτε σημείο.

Εντούτοις, είναι εύλογο το ερώτημα πώς η ηλεκτρονική ψηφοφορία μέσω Διαδικτύου μπορεί να είναι ασφαλής και να αποπνέει εμπιστοσύνη και δικαιοσύνη. Για αυτό απαιτείται εκτενής μελέτη και έρευνα σε αυτό τον τομέα ώστε να περιορίζονται οι κίνδυνοι και να εξασφαλίζεται η εμπιστοσύνη του κοινού και να επωφελούμαστε από τα πλεονεκτήματα που παρέχει.

2.2 Στάδια Ηλεκτρονικής Ψηφοφορίας

Στο υποκεφάλαιο αυτό παρατίθενται τα τέσσερα διακριτά στάδια που διέπουν την ηλεκτρονική ψηφοφορία και αποσκοπεί στο να κατανοήσουμε τον τρόπο λειτουργία της, εξετάζοντας τα βασικότερα χαρακτηριστικά του κάθε σταδίου της που είναι τα ακόλουθα:

- Εγγραφή ψηφοφόρου στο εκλογικό κατάλογο.
- Επικύρωση της ταυτότητας του ψηφοφόρου.
- Υποβολή Ψήφου από το ψηφοφόρο.
- Καταμέτρηση Ψήφων.

Τα επιμέρους στάδια αναλύονται διεξοδικά παρακάτω.

- **Εγγραφή:** Το στάδιο της εγγραφής πραγματοποιείται πριν την διεξαγωγή των εκλογών. Είναι ένα σημαντικό στάδιο μιας και διερευνάται η νομιμότητα του ατόμου

για να ασκήσει το εκλογικό του δικαίωμα. Για παράδειγμα για εκλογές που σχετίζονται με το κράτος κάποιοι παράγοντες που μπορεί να απαγορεύσουν σε κάποιο άτομο να ψηφίσει είναι το όριο ηλικίας ή η στέρηση των πολιτικών δικαιωμάτων. Στα άτομα που πληρούν τις προϋποθέσεις, παραχωρούνται κατάλληλα πιστοποιητικά, εγγράφονται στο εκλογικό κατάλογο και είναι σε θέση να ψηφίσουν. Υπάρχουν διάφοροι κίνδυνοι σε αυτό το στάδιο όπως ο κίνδυνος να καταχωρηθεί σε κάποιον πολλαπλότητα ψήφου, δηλαδή να του επιτραπεί από λάθος να ψηφίσει περισσότερο από μία φορές σε μια εκλογική αναμέτρηση, που αυτό παραβιάζει την δημοκρατία.

- **Επικύρωση:** Για να ψηφίσει κάποιος πρέπει να γίνει ταυτοποίηση της νομιμότητας του χρήστη. Για θέματα ασφαλείας διερευνάται η ταυτότητα των ψηφοφόρων. Αυτό μπορεί να επιτευχθεί αν το σύστημα ζητά από τους ψηφοφόρους την κάρτα τους ή τον κωδικό που τους έχει δοθεί. Επίσης, στο στάδιο αυτό εξετάζεται ποιοι ψηφοφόροι έχουν ήδη ψηφήσει για να αποφευχθεί ο κίνδυνος κάποιο άτομο να ψηφίσει περισσότερες από μία φορές.
- **Υποβολή Ψήφου:** Έπειτα ο ψηφοφόρος υποβάλλει την ψήφο του. Έχει δικαίωμα υποβολής ψήφου μόνο μία φορά. Σε αυτό το στάδιο συλλέγονται όλες οι ψήφοι που έχουν υποβληθεί. Αν η ασφάλεια των προηγούμενων σταδίων παραβιάστηκε μπορεί να προκύψουν διπλές ψήφοι από κάποιο ψηφοφόρο ή κάποιο μη εγγεγραμμένο μέλος να έχει ψηφήσει .
- **Καταμέτρηση Ψήφου:** Όταν λήξει η προθεσμία κατά την οποία οι ψηφοφόροι μπορούν να ψηφήσουν, καταμετρούνται οι ψήφοι εύκολα και γρήγορα μιας και οι ψήφοι είναι αποθηκευμένοι πλέον σε ηλεκτρονική μορφή και έπειτα ανακοινώνονται τα αποτελέσματα.

Όλα τα στάδια είναι αλληλένδετα και εξίσου σημαντικά. Αν κάποιο στάδιο παραβιαστεί, η εγκυρότητα των αποτελεσμάτων καταρρέει, μιας και εγκυμονούν διάφοροι κίνδυνοι που μπορούν να αλλοιώσουν το τελικό αποτέλεσμα των εκλογών, όπως για παράδειγμα να ψηφίσουν μη εγγεγραμμένοι ψηφοφόροι.

2.3 Απαιτήσεις

Στο προηγούμενο υποκεφάλαιο μελετήσαμε τον γενικό τρόπο λειτουργίας της ηλεκτρονικής ψηφοφορίας. Στον παρόν υποκεφάλαιο θα αναλύσουμε τις κυριότερες απαιτήσεις που πρέπει να ικανοποιούνται από ένα ευρέως αποδεκτό σύστημα ηλεκτρονικής ψηφοφορίας. Η απαίτηση της ασφάλειας καθώς επίσης και της πρακτικότητας είναι οι βασικότερες

απαιτήσεις που πρέπει να διασφαλίζονται και πρέπει να ισχύουν ανεξάρτητα από τα τεχνολογικά μέσα που χρησιμοποιούνται για την ανάπτυξη του συστήματος [33] [34] .

Η απαίτηση της ασφάλειας περιλαμβάνει διάφορες επί μέρους απαιτήσεις που ανάγονται πιο κάτω:

- **Δημοκρατικό (Democratic):** Η υποβολή ψήφων είναι επιτρεπτή μόνο σε εγγεγραμμένα μέλη. Κάθε μέλος έχει την δυνατότητα να υποβάλλει μόνο μία ψήφο. Η ψήφος οποιουδήποτε ψηφοφόρου μετράει ισάξια με την ψήφο οποιουδήποτε άλλου ψηφοφόρου.
- **Ακριβές (Accurate):**Όταν ένας ψηφοφόρος υποβάλει τη ψήφο του είναι επίκτητη ανάγκη το περιεχόμενο της ψήφου να μην αλλοιωθεί και να μην διαγραφεί από τις Εκλογικές Αρχές ή από άλλου είδους κακόβουλη ενέργεια. Επίσης πρέπει να εξασφαλιστεί ότι η ψήφος ενός ψηφοφόρου δεν καταμετρείται περισσότερες από μία φορά.
- **Προστατευμένο από Καταναγκασμό (Uncoercible):** Για να διασφαλίζεται η δημοκρατία πρέπει να εκφράζεται η ελεύθερη βούληση των ψηφοφόρων. Πολλοί υποψήφιοι επιδιώκουν να εξασφαλίσουν ψήφο εξαναγκάζοντας τους ψηφοφόρους. Το φαινόμενο αυτό μπορεί να αντιμετωπιστεί αν το σύστημα δεν επιτρέπει σε κανένα ψηφοφόρο να αποδείξει σε κάποιο τρίτο άτομο τι ψήφησε. Η ύπαρξη των εν λόγω αποδεικτικών ενδείξεων θα επέτρεπαν τον εξαγορασμό της ψήφου από τους υποψήφιους. Ένας τρόπος με τον οποίο το σύστημα θα μπορούσε να ικανοποίηση την απαίτηση για προστασία από καταναγκασμό είναι με το να προσφέρει τη δυνατότητα αναίρεσης της ψήφου του ψηφοφόρου. Με τον τρόπο αυτό ο ψηφοφόρος θα μπορεί οποιαδήποτε στιγμή να ξαναψηφίσει αυτό που πραγματικά επιθυμεί.
- **Μυστικό(Secret):** Για να αποφευχθεί το φαινόμενο του καταναγκασμού και της πούλησης ψήφων πρέπει να εξασφαλισθεί μυστικότητα και να μην είναι εφικτή η σύνδεση της ψήφου με το ψηφοφόρο που την υπόβαλλε.
- **Οικουμενικά Επαληθεύσιμο (Universally Verifiable):** Η όλη διαδικασία και το αποτέλεσμα των εκλογών πρέπει να εμπνέει εμπιστοσύνη. Για να επιτευχθεί αυτό πρέπει οποιοσδήποτε να μπορεί να πείθεται πως καταμετρούνται όλες οι ψήφοι, πως κάθε ψήφος μετρήθηκε ισότιμα και πως η όλη διαδικασία πραγματοποιείται ορθά. Κάποιες λύσεις που προτάθηκαν και χρησιμοποιήθηκαν επιτυχώς ήταν η χρήση Ανοικτού Κώδικα τον οποίο οποιοσδήποτε μπορεί να δει και να μελετήσει.
- **Ανθεκτικό(Robust):** Παρά την ύπαρξη σφαλμάτων ή κακόβουλων ενεργειών το σύστημα πρέπει να παραμένει ασφαλές και διαθέσιμο στους χρήστες .

Επίσης το σύστημα πρέπει να είναι πρακτικό. Αυτό περιλαμβάνει τα πιο κάτω:

- Να είναι εύκολα υλοποιήσιμο και συνάμα να είναι προσαρμοσμένο με τις σημερινές τεχνολογίες και πλατφόρμες.
- Να είναι εύκολη και κατανοητή η χρήση του για όλους τους ψηφοφόρους ανεξαρτήτως ηλικίας ή αναπηρίας και ειδικότερα για ψηφοφόρους που είναι «ψηφιακά αναλφάβητοι», που δεν κατέχουν βασικές δεξιότητες διαδικτύου, ηλεκτρονικού υπολογιστή ή γενικότερα νέων τεχνολογιών.
- Η απόδοση του συστήματος πρέπει να είναι ανεξάρτητη από το πλήθος των ψηφοφόρων.
- Το σύστημα πρέπει να είναι διαθέσιμο στους εξουσιοδοτημένους χρήστες όποτε το επιθυμούν χωρίς να αντιμετωπίζουν προβλήματα άρνησης παροχής υπηρεσιών και αδικαιολόγητη καθυστέρηση .

2.4 Αξιολόγηση Συστημάτων Ηλεκτρονικής Ψηφοφορίας

Μετά τη διατύπωση των απαιτήσεων ενός συστήματος ηλεκτρονικής ψηφοφορίας θα επιχειρήσουμε να παρουσιάσουμε τα πλεονεκτήματα και τα μειονεκτήματα που προκύπτουν από τη χρήση συστημάτων ηλεκτρονικής ψηφοφορίας. Η ψηφοφορία μέσω διαδικτύου είναι ένας νέος τρόπος ψηφοφορίας που προσφέρει πολλές υπηρεσίες και δυνατότητες. Τα βασικότερα πλεονεκτήματα από την χρήση της είναι τα εξής:

- **Ευκολία:** Με καλοσχεδιασμένο λογισμικό και σύστημα, οι ψηφοφόροι μπορούν να χρησιμοποιήσουν τον εξοπλισμό για να ψηφίσουν γρήγορα και από την άνεση του σπιτιού τους.
- **Έλεγχος Εγκυρότητας:** Στις εκλογές με τον παραδοσιακό τρόπο ψηφοφορίας παρατηρείται μεγάλο ποσοστό άκυρων ψήφων. Αυτό προκύπτει από το γεγονός ότι ο ψηφοφόρος μπορεί να μην είναι καλά ενημερωμένος για τον τρόπο ψηφοφορίας και τους κανόνες που διέπουν την ψηφοφορία για παράδειγμα να ψηφίσει μόνο υποψηφίους του ίδιου πολιτικού κόμματος. Η ηλεκτρονική ψηφοφορία δίνει την δυνατότητα ελέγχου της εγκυρότητας των ψήφων την ίδια στιγμή που οι ψηφοφόροι ψηφίζουν και έτσι αντιμετωπίζονται πιθανά λάθη. Αν κάποιος ψηφοφόρος προβεί σε μη έγκυρη ψήφο τότε του εμφανίζεται κατάλληλο μήνυμα που του επεξηγεί το λάθος.
- **Ενημέρωση:** Κατά τη διεξαγωγή της ηλεκτρονικής ψηφοφορίας ο ψηφοφόρος έχει την ευχέρεια να ενημερωθεί για τον τρόπο διεξαγωγής της ψηφοφορίας μέσω βοήθειας που του παρέχει το σύστημα. Καθώς επίσης να ενημερωθεί περεταίρω για

τους υποψήφιους, μέσω εμφάνισης από το σύστημα περισσότερων πληροφοριών για τον τρόπο δράσης και την ζωή τους πράγμα που δεν υπάρχει στα κλασσικά ψηφοδέλτια. Έτσι θα έχει τη δυνατότητα να γνωρίσει περισσότερα στοιχεία για τον κάθε υποψήφιο.

- **Πρόσβαση:** Ένα από τα βασικότερα πλεονεκτήματα της ηλεκτρονικής ψηφοφορίας είναι το γεγονός ότι δεν υπάρχει κανένας περιορισμός αναφορικά με την τοποθεσία που μπορείς να ασκήσεις το εκλογικό σου δικαίωμα αρκεί να έχει πρόσβαση στο διαδίκτυο. Οι ψηφοφόροι μπορούν να ψηφίσουν σε ένα εκλογικό κέντρο, στο σπίτι τους ή από οποιοδήποτε μέρος το οποίο έχει πρόσβαση στο διαδίκτυο. Επίσης είναι εφικτή και η ψηφοφορία με την χρήση κινητής συσκευής. Έτσι, παρέχεται με γρήγορο τρόπο η δυνατότητα ψηφοφορίας σε περισσότερες ομάδες ατόμων όπως οι ηλικιωμένοι και τα άτομα που βρίσκονται στο εξωτερικό, το αρκετά μεγάλο ποσοστό φοιτητών το οποίο σπουδάζει σε εξωτερικά εκπαιδευτικά ιδρύματα ή τα άτομα της διασποράς**.**
- **Αποδοτικότητα της διαδικασίας:** Μετά τη λήξη της προθεσμίας που παραχωρείται στους ψηφοφόρους για να ψηφίσουν, μπορεί αμέσως να υπολογιστεί το αποτέλεσμα των εκλογών μιας και η καταμέτρηση γίνεται με τη χρήση του ηλεκτρονικού υπολογιστή. Συνεπώς ο χρόνος που απαιτείται για τη παράδοση των τελικών αποτελεσμάτων εκλογής είναι πολύ γρηγορότερος εν αντιθέσει με τη παραδοσιακή μέθοδο που απαιτεί η καταμέτρηση από ανθρώπους .
- **Μικρότερο Κόστος:** Συγκριτικά με το παραδοσιακό τρόπο ψηφοφορίας που διεξάγεται με τη χρήση ψηφοδελτίων, η ηλεκτρονική ψηφοφορία αποτελεί φθηνότερο τρόπο για τη διεξαγωγή των εκλογών και την καταμέτρηση των ψήφων**.** Στην αρχή, το κόστος που επενδύεται για τη δημιουργία ηλεκτρονικών συστημάτων ψηφοφορίας είναι πολύ δαπανηρό. Στη συνέχεια όμως τα συνολικά έξοδα είναι μειωμένα και πολύ χαμηλότερα από τον παραδοσιακό τρόπο. Αυτό επειδή απαλείφονται ή μειώνονται τα κόστη που απαιτούνται για εκτυπώσεις ψηφοδελτίων και καταλόγων. Μείωση παρατηρείται επίσης και στα έξοδα του προσωπικού μιας και χρειάζεται λιγότερο προσωπικό για να επιτηρεί και να συντονίζει τον τρόπο διεξαγωγής των εκλογών και να καταμετρά το αποτέλεσμα**.**
- **Ευέλικτο:** Το σύστημα ηλεκτρονικής ψηφοφορίας έχει τη δυνατότητα να σχεδιαστεί για να υποστηρίζει μια ποικιλία μορφών ερωτήσεων. Μπορεί να χρησιμοποιηθεί για τη συλλογή της κοινής γνώμης καθώς επίσης και για εκλογές. Προσαρμόζεται εύκολα και γρήγορα σε νέες απαιτήσεις όπως για παράδειγμα μεγαλύτερο πλήθος υποψηφίων. Επίσης, υπάρχει η δυνατότητα προσαρμογής της ψηφοφορίας σε

διάφορες γλώσσες. Έτσι ο ψηφοφόρος θα επιλέγει την γλώσσα που επιθυμεί και γνωρίζει για να ασκήσει το εκλογικό του δικαίωμα.

Όπως σε κάθε εργαλείο και υπηρεσία που υπάρχει θα ήταν σχεδόν απίθανο αν η ηλεκτρονική ψηφοφορία δεν είχε μειονεκτήματα. Παραθέτω τα σημαντικότερα από αυτά παρακάτω.

- **Απαίτηση εξοπλισμού:** Σε μερικές περιπτώσεις η ηλεκτρονική ψηφοφορία απαιτεί κάποιου είδους ειδικό εξοπλισμό, όπως για παράδειγμα συσκευή που πιστοποιεί τον ψηφοφόρο όπως τον ηλεκτρονικό αναγνώστη έξυπνων καρτών που χρησιμοποιήθηκε στην Εσθονία [4][21]. Οι συσκευές αυτές έχουν κάποια μικρή χρηματική επιβάρυνση για να αγοραστούν. Εντούτοις ένα μεγάλο σύνολο ανθρώπων λόγω της οικονομικής τους δυνατότητα δεν θα μπορούσαν να τα αγοράσουν.
- **Γνώση χρήσης Ηλεκτρονικού υπολογιστή:** Το γεγονός ότι η ηλεκτρονική ψηφοφορία απαιτεί την χρήση ηλεκτρονικού υπολογιστή στις πλείστες των περιπτώσεων μπορεί επίσης να είναι απαγορευτικό για μια μερίδα ατόμων. Αυτό επειδή υπάρχει ένα μεγάλο ποσοστών ανθρώπων που δεν έχουν τις βασικές γνώσεις υπολογιστών και Διαδικτύου, που να τους επιτρέπουν να ψηφίσουν με ευκολία. Σε κάθε περίπτωση για να ψηφίσει κάποιος πρέπει να διαθέτει κάποιο είδος υπολογιστικής μηχανής.
- **Επιρρέπεια σε επιθέσεις:** Ένα σύστημα ηλεκτρονικής ψηφοφορίας πρέπει να διασφαλίζει ότι το αποτέλεσμα των εκλογών είναι ορθό και δεν παραβιάζει κανένα τομέα ασφάλειας διατηρώντας την μυστικότητα της ψήφου. Εντούτοις παρατηρούνται πολλές απόπειρες επιθέσεων και παραβιάσεις σε συστήματα [13] [20]. Υπάρχουν αρκετοί λόγοι για τους οποίους γίνονται τέτοιες είδους επιθέσεις όπως είναι η εξυπηρέτηση κομματικών συμφερόντων, η επίδειξη δύναμης από τους εισβολείς ή ακόμη και η ένδειξη διαμαρτυρίας προς κάποια κυβέρνηση από χακτιβιστές (hacktivists).

  Έτσι πιθανόν να γίνουν επιθέσεις στην σελίδα για διαμόρφωση της εικόνας και της μορφής της, στη βάση δεδομένων για παραποίηση των στοιχείων της και απόσπαση πληροφοριών ή ακόμη επίθεση τύπου "Άρνησης Εξυπηρέτησης". Μέσω της επίθεσης Άρνησης Εξυπηρέτησης, η υπηρεσία τίθεται ανίκανη να εξυπηρετήσει άλλους επισκέπτες και εξαναγκάζει τον εξυπηρετητή στον οποίο τρέχει το σύστημα σε άρνηση για παροχή υπηρεσίας. Ένας εισβολέας μπορεί να επιχειρήσει να υπερφορτώσει το δίκτυο και ως επακόλουθο είναι η μείωση του εύρος ζώνη που παρέχεται σε ένα νόμιμο μέλος ή ακόμη να εμποδίζεται η πρόσβαση στο δίκτυο. Πραγματοποιούνται προσπάθειες αντιμετώπισης αυτού τους είδους επίθεσης μέσω

Δρομολογητές φίλτρου (“FilteringRouters”), Απενεργοποίηση μετάδοσης IP (“Disabling IP Broadcast”), Απενεργοποίηση μη χρησιμοποιημένων υπηρεσιών (“Disabling UnusedServices”) και Εκτέλεση ανίχνευσης [25].

Μία άλλου είδους επίθεση είναι τα κακόβουλα προγράμματα όπως είναι οι «ιοί» και οι «δούρειοι ίπποι». Ο «δούρειος ίππος» για παράδειγμα εισβάλει σε έναν ηλεκτρονικό υπολογιστή για να τον καταστρέψει και συνάμα να τον παρακολουθήσει. Όταν ο δούρειος ίππος ενεργοποιηθεί στέλνει τις πληροφορίες στο δημιουργό του και παίρνει τον έλεγχο του υπολογιστή. Είναι ύπουλοι ιοί γιατί κρύβονται μέσα σε άλλα "Αθώα" προγράμματα όπως τα παιχνίδια και για αυτό άλλωστε έχουν πάρει το όνομα τους από το μυθικό πόλεμο της Τροίας, για την παρόμοια τακτική που υπήρξε στον πόλεμο αυτό. Δρουν αθόρυβα, εν αγνοία του χρήστη. Ο εξυπηρετητής που φιλοξενεί το σύστημα ηλεκτρονικής ψηφοφορίας μπορεί να προστατευτεί από ιούς χρησιμοποιώντας συγκεκριμένα λειτουργικά συστήματα, λογισμικά και τις πρακτικές που είχαμε αναφέρει πιο πάνω. Αν οι προσωπικοί υπολογιστές δεν έχουν την απαραίτητη προστασία μπορεί να μολυνθούν με ιό. Οι ιοί μπορεί να επιτεθούν στον υπολογιστή από το επίπεδο του λειτουργικού συστήματος μέχρι το επίπεδο του προγράμματος περιήγησης του διαδικτύου. Θα μπορούσε να παραβιάσει την ιδιότητα της ψηφοφορίας να παραμένει μυστική ή ακόμη και να τροποποιήσει τα αποτελέσματα χωρίς την έγκριση του ψηφοφόρου, μειώνοντας έτσι την δικαιοσύνη εκλογών. Εάν μεγάλος αριθμός ηλεκτρονικών υπολογιστών μολυνθούν από ιούς, τότε οι εκλογές μπορεί να ακυρωθούν ή να επαναληφθούν σε κάποια άλλη στιγμή.

2.5 Ηλεκτρονική Ψηφοφορία και Κρυπτογραφία

Συνεχίζοντας την περιγραφή των βασικών θεμάτων που αφορούν την ηλεκτρονική ψηφοφορία παρατίθενται εδώ η σύνδεση της κρυπτογραφίας με την ηλεκτρονική ψηφοφορία. Η κρυπτογραφία είναι άκρως απαραίτητη για την ηλεκτρονική ψηφοφορία καθώς είναι πρακτικά αδύνατο να επιτευχθούν χωρίς αυτή οι αυστηρές προδιαγραφές ασφαλείας όπως, η εμπιστευτικότητα, η ακεραιότητα των δεδομένων, η μη απάρνηση πηγής, η μη απάρνηση προορισμού, η πιστοποιήση.

Η κρυπτογραφία είναι ένας επιστημονικός κλάδος που χρησιμοποιεί μαθηματικά για την κρυπτογράφηση και αποκρυπτογράφηση δεδομένων με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων. «Κρυπτογραφία: η τέχνη της γραφής με την βοήθεια ενός μυστικού κλειδιού ή με αινιγματικό τρόπο». Λεξικό της Ισπανικής Βασιλικής Ακαδημίας

2.5.1 Κρυπτογραφικές Τεχνικές

Σε αυτό το υποκεφάλαιο θα εξετάσουμε τις σημαντικότερες κρυπτογραφικές τεχνικές οι οποίες χρησιμοποιούνται σε συστήματα ηλεκτρονικής ψηφοφορίας για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων. Οι βασικές τεχνικές για την κρυπτογράφηση πληροφοριών είναι η συμμετρική και η ασύμμετρη κρυπτογράφηση καθώς επίσης και η κρυπτογράφηση με τη χρήση της ψηφιακής υπογραφής. Είναι σημαντική η γνώση των στοιχειωδών τεχνικών κρυπτογραφίας για τη συνέχεια της παρούσας διπλωματικής μιας και τα πρωτόκολλα που περιγράφονται στο επόμενο κεφάλαιο και το πρωτόκολλο το οποίο έχει υλοποιηθεί χρησιμοποιεί κάποιες από αυτές τις τεχνικές [24] [28].

Συμμετρική Κρυπτογραφία: Η συμμετρική κρυπτογραφία ιδιωτικού κλειδιού είναι μια μορφή κρυπτογραφίας η οποία είναι εξαρτημένη από ένα και μόνο κλειδί που μοιράζεται ο αποστολέας και ο παραλήπτης. Εξυπηρετεί τόσο στη διαδικασία της κρυπτογράφησης όσο και στη διαδικασία της αποκρυπτογράφησης. Η συμμετρική κρυπτογραφία είναι κατά πολύ αρχαιότερη από την ασύμμετρη κρυπτογραφία. Χρονολογείται από την Αρχαία Αίγυπτο και χρησιμοποιούταν μέχρι πρόσφατα σε όλα τα κρυπτογραφικά συστήματα. Η διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης πραγματοποιείται πολύ γρήγορα και έτσι η υπολογιστική ισχύς που καταναλώνεται είναι λίγη. Εντούτοις, ένα τρωτό σημείο που υφίσταται η συμμετρική κρυπτογραφία είναι η αδυναμία της ανταλλαγής του κλειδιού με ασφαλή τρόπο [31].

Από τις πιο γνωστές μεθόδους συμμετρικής κρυπτογράφησης είναι ο κρυπταλγόριθμος DES (Data Encryption Standard) είναι ένας κρυπταλγόριθμος που ακολουθεί τη λογική της κρυπτογράφησης τμημάτων. Σχεδιάστηκε από την IBM και δημοσιεύθηκε το 1977 από το National Institute of Standards and Technology.

Εν συνεχεία, θα μελετήσουμε την ασύμμετρη κρυπτογραφία η οποία επινοήθηκε από τους Whitfield Diffie και Martin Hellman στο τέλος της δεκαετίας του 1970 .

Ασύμμετρη Κρυπτογραφία: Η ασύμμετρη κρυπτογραφία δημόσιου κλειδιού είναι μια μορφή κρυπτογραφίας στην οποία χρησιμοποιείται ένα ζεύγος κλειδιών, το δημόσιο και το ιδιωτικό, κατά τις διαδικασίες της κρυπτογράφησης και της αποκρυπτογράφησης. Τα δύο αυτά κλειδιά έχουν μια μαθηματική σχέση μεταξύ τους, το δημόσιο κλειδί χρησιμοποιείται για την κρυπτογράφηση των δεδομένων ενώ το ιδιωτικό κλειδί τα αποκρυπτογραφεί. Παρόλο

που είναι γνωστό το δημόσιο κλειδί και ο αλγόριθμος που χρησιμοποιείται είναι πρακτικά αδύνατο να υπολογιστεί το ιδιωτικό κλειδί. Με τον τρόπο αυτό διασφαλίζεται ότι τα δεδομένα που κρυπτογραφήθηκαν μπορούν να διαβαστούν μονάχα από το άτομο που κατέχει το αντίστοιχο ιδιωτικό κλειδί [23].

Από τις πιο γνωστές μεθόδους ασύμμετρης κρυπτογράφησης είναι ο κρυπταλγόριθμος RSA που ονομάστηκε έτσι από τους δημιουργούς του, Ron Rivest, Adi Shamir και Len Adleman.

Κρυπτοσύστημα RSA: Η κρυπτογράφηση RSA είναι ο πρώτος κρυπτογραφικός αλγόριθμος δημόσιου-κλειδιού και είναι ευρέως αποδεκτώς ως ο καλύτερος αλγόριθμος μέχρι σήμερα [17] [35]. Για τον σκοπό αυτό υιοθετείται για χρήση του και από την ηλεκτρονική ψηφοφορία αφού απαιτεί υψηλό επίπεδο κρυπτογραφίας και ασφάλειας. Συγκεκριμένα χρησιμοποιείται για την δημιουργία της ψηφιακής υπογραφής στην ηλεκτρονική ψηφοφορία.

Ο RSA είναι μια ασύμμετρη κρυπτογραφία, και για την εκτέλεση της διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης απαιτείται η χρήση δύο διαφορετικών κλειδιών, του δημοσίου και του ιδιωτικού κλειδιού.

Το ένα κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το άλλο για την επαλήθευση της. Συγκεκριμένα, για τη διαδικασία της δημιουργίας της ψηφιακής υπογραφής, ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για τη διαδικασία της επαλήθευσης ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα.

Το ζεύγος κλειδιών δημιουργείται ως ακολούθως:

- Αρχικά παράγονται δύο πρώτοι αριθμοί, οι p και q. Οι αριθμοί αυτοί δηλαδή διαιρούνται ακριβώς μόνο από τον αριθμό 1 και τον εαυτό τους. Στη συνέχεια σχηματίζεται το γινόμενο των p και q και προκύπτει το n. Σε αυτό το σημείο να σημειωθεί ότι είναι αρκετά εύκολο να πολλαπλασιάσουμε δύο αριθμούς και να βρούμε το αποτέλεσμα τους. Αν δοκιμάσουμε το αντίστροφο, δηλαδή, δοθέντος του γινομένου δύο πρώτων αριθμών να βρούμε τους δύο αριθμούς , η διαδικασία αυτή είναι δυσκολότερη. Το περίφημο αυτό πρόβλημα ονομάζεται πρόβλημα παραγοντοποίησης σε πρώτους αριθμούς (factoring problem). Το πρόβλημα της παραγοντοποίησης αριθμών είναι από τα προβλήματα από τα οποία δεν έχει βρεθεί ακόμη κάποιος γρήγορος τρόπος επίλυσης με υπολογιστή.

- Ακολούθως παίρνουμε το Φ(n) ως το γινόμενο των (p-1) και του (q-1) και διαλέγουμε ένα δημόσιο εκθέτη τον οποίο συμβολίζουμε ως e, ως ο μικρότερος σχετικά πρώτος αριθμός με τον Φ(n). Αυτό σημαίνει ότι ο ΜΚΔ των Φ(n) και e είναι το ένα (1).
- Ο αριθμός d είναι ένας οποιοσδήποτε ακέραιος που είναι συν-πρώτος (coprime) προς τον (p-1) (q-1), δηλαδή ο μεγαλύτερος αριθμός που διαιρεί και τους δύο είναι ο αριθμός 1 και ταυτόχρονα είναι ο αντίστροφος του e ως προς υπόλοιπα. Υπολογίζοντας μία λύση για την εξίσωση (d * e) % Φ (n) = 1 παίρνουμε και τον ιδιωτικό εκθέτη d. Οι αριθμοί d και e είναι τέτοιοι ώστε η διαφορά ed-1 διαιρείται ακριβώς από τον αριθμό (p-1) (q-1) .

Με τον τρόπο που μόλις έχουμε περιγράψει δημιουργείται το δημόσιο κλειδί που αποτελείται από το ζεύγος (e,n) και το ιδιωτικό κλειδί που αποτελείται από το ζεύγος (d,n).

Για να πραγματοποιηθεί η διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης πρέπει να υπολογιστούν οι ακόλουθες εξισώσεις:

- Εξίσωση κρυπτογράφησης: $C=m^e \bmod n$, όπου m το μήνυμα που θέλουμε να κρυπτογραφήσουμε και C είναι η κρυπτογραφημένη έκδοση του μηνύματος m.
- Εξίσωση αποκρυπτογράφησης: $M=C^d \bmod n$. Για την αποκρυπτογράφηση απαιτείται η χρήση του αριθμού d, ο οποίος είναι γνωστός μόνο στον νόμιμο παραλήπτη του μηνύματος.

Ένας ωτακουστή θα είχε στα χέρια του μόνο το κωδικοποιημένο μήνυμα C, αλλά δεν γνωρίζει το ιδιωτικό κλειδί d και επιπλέον ενώ γνωρίζει το n δεν είναι καθόλου εύκολο όπως έχουμε προαναφέρει να ανακαλύψει γρήγορα τους παράγοντες p και q, είναι υπολογιστικά αδύνατο για μεγάλους αριθμούς n!, ούτως ώστε να υπολογίσει εύκολα το ιδιωτικό κλειδί d,

Θα εξετάσουμε επίσης, μία άλλη κρυπτογραφική τεχνική η οποία κάνει χρήση της ψηφιακής υπογραφής για την κρυπτογράφηση των δεδομένων.

Ψηφιακές Υπογραφές: Στην καθημερινή μας ζωή πολλές φορές καλούμαστε να πιστοποιήσουμε ότι είμαστε αυτοί που ισχυριζόμαστε ότι είμαστε. Έτσι, στον πραγματικό κόσμο έχουμε εφεύρει την υπογραφή για να δείξουμε αυθεντικότητα. Μία παρόμοια διαδικασία διεξάγεται και στον κόσμο των υπολογιστών με την ψηφιακή υπογραφή. Η ψηφιακή υπογραφή χρησιμοποιείται για να πιστοποιήσει τη γνησιότητα μιας πληροφορίας που λαμβάνεται σε ηλεκτρονική μορφή, ότι δηλαδή, μια πληροφορία έρχεται από ένα συγκεκριμένο αποστολέα. Στην ουσία η ψηφιακή υπογραφή είναι απλά ένα κρυπτογράφημα

που επισυνάπτεται στο αρχικό μήνυμα. Η υπογραφή αυτή εγγυάται τόσο την προέλευση του μηνύματος, όσο και επικυρώνει την ακεραιότητα του [10] [30] [32].

Η διαδικασία της δημιουργίας της ψηφιακής υπογραφής ξεκινά με κατακερματισμό του μηνύματος m ανεξάρτητου μεγέθους, για να παραχθεί η σύνοψη του, την οποία συμβολίζουμε με το γράμμα Η. Το ιδιωτικό κλειδί {n, d} του αποστολέα χρησιμοποιείται για την κρυπτογράφηση του Η όπου το αποτέλεσμα που προκύπτει είναι η υπογραφή S.
$S = H^d \bmod n$

Η ψηφιακή υπογραφή αποστέλλεται μαζί με το αρχικό κείμενο. Στη συνέχεια ο παραλήπτης του μηνύματος αποσπά από το μήνυμα την ψηφιακή υπογραφή του μηνύματος. Το δημόσιο κλειδί του παραλήπτη χρησιμοποιείται για την αποκρυπτογράφηση της υπογραφής S. Η συνάρτηση που χρησιμοποιείται για να παραχθεί η σύνοψη του μηνύματος είναι η ακόλουθη:
$H=S^e \bmod n$

Την ίδια ώρα, χρησιμοποιώντας την ίδια συνάρτηση κατακερματισμού, θα κατατεμαχίσει το μήνυμα m, δημιουργώντας έτσι τη σύνοψη του μηνύματος.

Αν τα αποτελέσματα είναι ίδια, τότε το μήνυμα που έλαβε ο παραλήπτης διατηρήθηκε ακέραιο και πιστοποιείται, διαφορετικά εντοπίζεται αλλοίωση του μηνύματος.

2.5.2 Κρυπτογραφικά Μοντέλα

Συνεχίζοντας την περιγραφή των βασικών θεμάτων κρυπτογραφίας που συνδέονται με την ηλεκτρονική ψηφοφορία θα μελετήσουμε τα βασικότερα κρυπτογραφικά μοντέλα. Συγκεκριμένα θα μελετήσουμε το κρυπτογραφικό μοντέλο των τυφλών υπογραφών καθώς επίσης και το μοντέλο MIX-net.

Τυφλές Υπογραφές: Η έννοια της τυφλής υπογραφής αποδίδεται στον David Chaum και είναι μία μορφή ψηφιακής υπογραφής στην οποία το περιεχόμενο της δεν αποκαλύπτεται πριν υπογραφεί. Λόγω της παραπάνω ιδιότητας, το κύριο χαρακτηριστικό των τυφλών υπογραφών είναι ότι ο υπογράφων δεν έχει γνώση του περιεχομένου του μηνύματος που υπογράφει.
Οι τυφλές υπογραφές συνέβαλλαν καθοριστικά στο πρόβλημα της επικύρωσης των ψήφων καθώς επίσης και στο πρόβλημα της μυστικότητας τους στις ηλεκτρονικές εκλογές. Αυτό

επιλύθηκε από τους Fujioka, Okamoto και Ohta εφαρμόζοντας την κρυπτογραφική μέθοδο των τυφλών υπογραφών.

Ένα σύστημα τυφλών ψηφιακών υπογραφών αποτελείται από τρεις διαδικασίες, την τύφλωση, την υπογραφή και την απομάκρυνση του παράγοντα τύφλωσης.

Ας ορίσουμε ως (n,e) να είναι το δημόσιο κλειδί του επικυρωτή και ως (n,d) το ιδιωτικό του κλειδί καθώς επίσης ως m την ψήφο.

Ο ψηφοφόρος επιλέγει τον υποψήφιο που επιθυμεί και η ψήφος κρυπτογραφείται.

Η διαδικασία της κρυπτογράφησης της ψήφου πραγματοποιείται ως ακολούθως:

Πρωτίστως, επιλέγεται ένας τυχαίος ακέραιος αριθμός k, που ονομάζεται παράγοντας τύφλωσης, τέτοιος ώστε $0<k<n$ και $\gcd(k,n)=1$.

Έπειτα χρησιμοποιείται ο παράγοντας τύφλωσης σε μια μαθηματική σχέση για να τυφλωθεί και συνάμα να κρυπτογραφηθεί η ψήφος.

(Τύφλωση) Υπολογισμός του $m' \equiv mk^e \pmod n$

Όπου m΄είναι η ψήφος που έχει τυφλωθεί και κρυπτογραφηθεί.

Στην συνέχεια αυτό το πακέτο (η τυφλή κρυπτογραφημένη ψήφος) διαδίδεται μέσω ενός δικτύου στον επικυρωτή.

Διερευνάται με βάση των δεδομένων που είναι καταχωρημένα στον σύστημα αν ο ψηφοφόρος είναι υπαρκτό πρόσωπο και ελέγχεται αν έχει ήδη ψηφίσει .

Σε αυτό το σημείο καθορίζεται αν μία ψήφος είναι επιτρεπτή. Στην περίπτωση που ο ψηφοφόρος έχει δικαίωμα ψήφου, υπογράφεται η ψήφος.

Η διαδικασία της υπογραφής της ψήφους έχει ως ακολούθως:

(Υπογραφή) $s \equiv (m')^d \pmod n$

Με τον τρόπο αυτό το μήνυμα υπογράφεται χωρίς να αποκαλύπτεται το περιεχόμενο της ψήφους.

Έπειτα η υπογεγραμμένη τυφλή ψήφος επιστρέφεται στον ψηφοφόρο.

Ο ψηφοφόρος απομακρύνει το παράγοντα τύφλωσης ούτως ώστε να πάρει την υπογραφή.

Η διαδικασία της απομάκρυνσης του παράγοντα τύφλωσης έχει ως ακολούθως:

Υπολογισμός του $sk^{-1} \bmod n$.

Το αποτέλεσμα του υπολογισμού είναι η υπογραφή του μηνύματος.

Στη συνέχεια παρουσιάζουμε συνοπτικά το κρυπτογραφικό μοντέλο MIX-net. Μιας και τα πρωτόκολλα που μελετούμε στη συνέχεια δεν χρησιμοποιούν αυτό το κρυπτογραφικό μοντέλο κάνουμε μία σύντομη περιγραφή του.

Το Μοντέλο MIX-net : Ο David Chaum το 1981 επινόησε τα δίκτυα MIX-net (MIX networks) γνωστά και ως Digital mixes τα οποία αποτελούν έναν κρυπτογραφικό

μηχανισμό για την κατασκευή ανώνυμων καναλιών (anonymous channels) σε εφαρμογές υψηλής ασφάλειας.

Ένα δίκτυο MIX-net αποτελείται από έναν αριθμό εξυπηρετητών, συνδεδεμένων μεταξύ τους, που καλούνται κόμβοι MIX. Σκοπός των κόμβων MIX είναι να λαμβάνουν ένα σύνολο μηνυμάτων για παράδειγμα τις κρυπτογραφημένες ψήφους και εφαρμόζοντας μια ακολουθία από k κρυπτογραφημένους μετασχηματισμούς παράγουν ένα διαφορετικό σύνολο μηνυμάτων. Με τον τρόπο αυτό δεν θα είναι δυνατή η συσχέτιση των μηνυμάτων εισόδων με των μηνυμάτων εξόδων. Δηλαδή, δεν θα μπορεί να καθοριστεί ποια ψήφος αντιστοιχεί σε ποιο ψηφοφόρο. Κατ' αυτόν τον τρόπο, καμία συνεργία οποιουδήποτε αριθμού κόμβων MIX (εκτός από την περίπτωση όπου συνεργούν όλοι οι κόμβοι) δεν μπορεί να καθορίσει ποια ψήφος αντιστοιχεί σε ποιόν ψηφοφόρο.

2.6 Παράδειγμα Εφαρμογής της Ηλεκτρονικής Ψηφοφορίας

Το κεφάλαιο αυτό θα κλείσει με κάποια χαρακτηριστικά παραδείγματα εφαρμογών της ηλεκτρονικής ψηφοφορίας. Η ηλεκτρονική ψηφοφορία έχει εφαρμοστεί με επιτυχία σε πολλές χώρες μέχρι σήμερα. Μερικές από τις χώρες που χρησιμοποιούν ηλεκτρονική ψηφοφορία για την άσκηση του εκλογικού τους δικαιώματος είναι η Βραζιλία, Αυστραλία, Καναδάς, Βέλγιο, Γερμανία, Ρουμανία, Γαλλία, Βενεζουέλα, Φιλιππίνες, Ελβετία, Εσθονία, Νορβηγία, Ρουμανία και το Ηνωμένο Βασίλειο. Σε αυτό το υποκεφάλαιο περιγράφουμε κάποιες από αυτές τις εφαρμογές.

Αρχικά θα μελετήσουμε την εφαρμογή της ηλεκτρονικής ψηφοφορίας στην Εσθονία.

2.6.1 Εφαρμογή στην Εσθονία

Αν και η Εσθονία είναι ένα μικρό κράτος, εντούτοις έχει ενσωματώσει την ηλεκτρονική ψηφοφορία σε πολύ μεγάλο βαθμό από το 2005, τόσο σε επίπεδο δημοτικών και εθνικών εκλογών, όσο και σε επίπεδο ευρωεκλογών [3] [4]. Η συγκεκριμένη μέθοδος αποδείχτηκε πλήρως επιτυχημένη μιας και υπήρξε αύξηση της συμμετοχής των πολιτών [27] .

Οι ψηφοφόροι στην Εσθονία έχουν την ευχέρεια να επιλέξουν τον τρόπο με τον οποίο επιθυμούν να ασκήσουν το εκλογικό τους δικαίωμα. Μπορούν είτε να ψηφίσουν με τον παραδοσιακό τρόπο στα εκλογικά τμήματα, είτε ηλεκτρονικά μέσω διαδικτύου. Όσοι ψηφοφόροι προτιμήσουν να ασκήσουν το εκλογικό τους δικαίωμα ηλεκτρονικά, πρέπει πρωτίστως να αποκτήσουν ταυτότητα με ψηφιακή υπογραφή που εκδίδεται με βάση τα νομοθετικά έγγραφα που αφορούν τις ταυτότητες των ατόμων. Η ηλεκτρονική ψηφοφορία

πραγματοποιείται στο διάστημα δέκα έως τεσσάρων ημερών νωρίτερα από την καθορισμένη ημέρα των εκλογών. Στο διάστημα αυτό, οι ψηφοφόροι μεταβαίνουν διαδικτυακά στην ιστοσελίδα της Εθνικής Εκλογικής Επιτροπής για να ψηφίσουν τον υποψήφιο που επιθυμούν. Φυσικά η διαδικασία της ηλεκτρονικής ψηφοφορίας απαιτεί την επικύρωση της ταυτότητας του ψηφοφόρου πριν την υποβολή της ψήφου του. Αυτό πραγματοποιείται μέσω του προσωπικού κωδικού του ψηφοφόρου και με την αντίστοιχη ψηφιακή του υπογραφή. Έπειτα από το στάδιο της επικύρωσης, εμφανίζεται στην ιστοσελίδα η λίστα που εμπεριέχει τους υποψήφιους της εκλογικής περιφέρειας και ο ψηφοφόρος καλείται να επιλέξει τους εκπροσώπους που επιθυμεί. Το ηλεκτρονικό σύστημα για σκοπούς ασφαλείας χρησιμοποιεί το μοντέλο των τυφλών υπογραφών. Οι ψηφοφόροι πριν την υποβολή των ψήφων τους καλούνται να υπογράψουν ψηφιακά. Η διαδικασία ολοκληρώνεται εμφανίζοντας ένα κατάλληλο μήνυμα αποδοχής της ψήφου στην οθόνη.

Ένας ψηφοφόρος έχει τη δυνατότητα να αλλάξει την ηλεκτρονική του ψήφο είτε ψηφίζοντας ξανά ηλεκτρονικά μεταξύ του διαστήματος των δέκα έως τεσσάρων ημερών νωρίτερα από την Εκλογική Ημέρα είτε ψηφίζοντας με το παραδοσιακό τρόπο στα εκλογικά κέντρα μεταξύ του διαστήματος των έξι έως τεσσάρων ημερών νωρίτερα από την Εκλογική Ημέρα.

Η Εσθονία μέσω της ηλεκτρονικής ψηφοφορίας έχει δώσει επιπρόσθετα κίνητρα προς τους πολίτες και ειδικότερα τους νέους για να συμμετάσχουν στις εκλογές [ ] .

2.6.2 Ηλεκτρονικό Σύστημα της Γενεύης

Θα συνεχίσουμε τη μελέτη μας με θέμα την εφαρμογή συστημάτων ηλεκτρονικής ψηφοφορίας, εξετάζοντας το σύστημα της Γενεύης.

Στις 8 Φεβρουαρίου του 2009 οι κάτοικοι της Γενεύης, έκριναν με πλειοψηφία 70,2% την ηλεκτρονική ψηφοφορία στο Σύνταγμα τους. Μέσω αυτής της ψηφοφορίας έληξε η πειραματική φάση της ηλεκτρονικής ψηφοφορία στο επίπεδο των καντονιών, ενώ στο ομοσπονδιακό επίπεδο έληξε το 2007.

Η ηλεκτρονική ψηφοφορία προτάθηκε μιας και οι περισσότεροι ψηφοφόροι επιθυμούσαν να ασκούν την ψήφο τους ταχυδρομικά παρά να πηγαίνουν στα εκλογικά κέντρα και να ψηφίζουν. Έτσι η ηλεκτρονική ψηφοφορία ως προέκταση της ψηφοφορίας μέσω ταχυδρομείου έρχεται με τις διάφορες σύγχρονες τεχνολογίες να διευκολύνει τον τρόπο ψηφοφορίας.

Στο σύστημα της Γενεύης, η ακεραιότητα των πληροφοριών κατά τη διάρκεια της μεταφοράς στο Διαδίκτυο επιτυγχάνεται με τη δημιουργία μιας ασφαλούς σύνδεσης μεταξύ του υπολογιστή του ψηφοφόρου και των διακομιστών ψήφου. Η σύνδεση αυτή έχει διπλή ασφάλεια, μέσω του πρωτοκόλλου SSL128 και μέσα από μια βοηθητική εφαρμογή Java, η οποία έχει αναπτυχθεί ειδικά για την εφαρμογή ψηφοφορίας και ανήκει στο κράτος της Γενεύης. Η βοηθητική εφαρμογή Java στέλνεται στον υπολογιστή του ψηφοφόρου με την έναρξη της ψηφοφορίας. Μέσω αυτού του προγράμματος ελέγχεται η εκτέλεση της ψηφοφορίας, κρυπτογραφώντας τα δεδομένα και εμποδίζοντας ιούς ή δούρειους ίππους να δράσουν.

Προκειμένου να αποτραπεί το φαινόμενο υποβολής των ψήφων σε παραποιημένες ιστοσελίδες, ο πολίτης μπορεί να ελέγξει τη γνησιότητα του ηλεκτρονικού πιστοποιητικού που πιστοποιεί την ιστοσελίδα ψήφου. Ο πολίτης εντοπίζει από το ηλεκτρονικό πιστοποιητικό το ψηφιακό αποτύπωμα και το συγκρίνει με το αποτύπωμα που αναγράφεται στην κάρτα ψηφοφορίας του.

Ο κάθε ψηφοφόρος έχει μία κάρτα ψηφοφορίας, η οποία του παρέχει την δυνατότητα να ψηφίσει ηλεκτρονικά, μέσω ταχυδρομείου ή στο εκλογικό τμήμα. Πάνω στη κάρτα ψηφοφορίας βρίσκεται κρυμμένος ένας κωδικός PIN. Ο ψηφοφόρος για να εισάγει τον κωδικό πρέπει να ξύσει την ταινία ώστε να αποκαλυφθεί ο κωδικός. Η κάρτα ψηφοφορίας εγγυάται την αρχή «ένας άνθρωπος - μία ψήφος", δηλαδή όταν χρησιμοποιηθεί, δεν μπορεί να χρησιμοποιηθεί και δεύτερη φορά. Έτσι, κάθε ψηφοφόρος έχει μόνο μία ψήφο και μπορεί να ψηφίσει μόνο μία φορά.

Η διαδικασία της ψηφοφορίας ξεκινά με την καταχώρηση της ταυτότητας του ψηφοφόρου, μήκους 16 ψηφίων. Εν συνεχεία εμφανίζεται στον ψηφοφόρο, οι διάφορες επιλογές ψήφου και ο ψηφοφόρος καλείται να επιλέξει την ψήφο που τον εκφράζει. Σε αυτό το σημείο, πραγματοποιείται ένας εκτενέστερος έλεγχος της ταυτότητας του ψηφοφόρου. Ο ψηφοφόρος καλείται να δώσει τον κωδικό PIN, την ημερομηνία γέννησης και τον δήμο προέλευσης του. Με την άσκηση της ψήφου, επιστρέφεται στο χρήστη η ημερομηνία και ώρα καταχώρησης της ψήφους. Ασφαλώς, το σύστημα δε δέχεται ψήφους εκτός της περιόδου ψηφοφορίας.

Το ηλεκτρονικό σύστημα της Γενεύης διασφαλίζει ότι δε θα υπάρχει οποιαδήποτε δυνατή σύνδεση μιας ψήφου με τον ψηφοφόρο. Για να διασφαλιστεί η ανωνυμία των ψήφων, η ηλεκτρονική κάλπη η οποία εμπεριέχει τις κρυπτογραφημένες ψήφους δε συνδέεται με τους εκλογικούς καταλόγους. Επίσης, ο εκλογικός κατάλογος δεν περιέχει ονόματα παρά μόνο

αριθμητικά αναγνωριστικά και πριν πραγματοποιηθεί η διαδικασία της αποκρυπτογράφησης των ψήφων, η ηλεκτρονική κάλπη ταξινομείται με ένα αυθαίρετο τρόπο.Έτσι δεν υπάρχει κανένας τρόπος για να εντοπιστεί πώς ένα συγκεκριμένος πολίτης έχει ψηφίσει.

Για κάθε ζήτημα σε δημοψήφισμα, υπάρχουν μόνο τρεις πιθανές ψήφοι: "ναι", "όχι" ή κενό. Με τόσο λίγες δυνατότητες, ο κώδικας θα μπορούσε εύκολα να ανακαλυφθεί. Ως εκ τούτου, κάθε ψήφος ολοκληρώνεται από ένα αυθαίρετο κείμενο πριν την κωδικοποίηση για να γίνει η κωδικοποίηση απαραβίαστη. Το πρόβλημα είναι παρόμοιο για τις εκλογές. Εκεί επίσης, η μυστικότητα της ψήφου είναι εγγυημένη με την προσθήκη ενός αυθαίρετου κείμενου πριν την κωδικοποίηση.

Η κωδικοποίηση των δεδομένων βασίζεται σε κλειδιά κρυπτογράφησης που παράγονται από καθαρά τυχαίους αριθμούς μέσω μιας κβαντικής μηχανής. Οι διακομιστές εγκαθίστανται στην ασφαλέστερη αίθουσα υπολογιστών του κράτους, στα υπόγεια του αρχηγείου της Αστυνομίας. Η φυσική πρόσβαση στο δωμάτιο είναι καλά ελεγχόμενη και υπάρχει μόνο μία πρόσβαση στους διακομιστές του δικτύου μέσω μίας ειδικής οπτικής ίνας που ενεργοποιείται μόνο κατά τη διάρκεια της ψηφοφορίας.

Ανάλογα με τον αριθμό κάρτας του ψηφοφόρου, δημιουργείται ένα συμμετρικό κλειδί που κρυπτογραφεί όλα τα ευαίσθητα σημεία της συναλλαγής. Επίσης, μέσω του αριθμού κάρτας του ψηφοφόρου ενεργοποιείται μια βοηθητική εφαρμογή Java στο διακομιστή ψηφοφορίας.
Ένας αυτόματος έλεγχος για την ταυτότητα του διακομιστή πραγματοποιείται κατά τη διάρκεια της φάσης του ελέγχου της ταυτότητας του ψηφοφόρου. Όταν το σύστημα ζητά από τον ψηφοφόρο το μοναδικό αριθμό του, εμφανίζεται στην οθόνη ένας μοναδικός αλφαβητικός κωδικός. Στην περίπτωση που ο κωδικός που εμφανίζεται στην οθόνη δεν ταιριάζει με τον κωδικό που είναι εκτυπωμένος στην κάρτα ψηφοφορίας, ο ψηφοφόρος τερματίζει την ψηφοφορία και καλεί την υπηρεσία εξυπηρέτησης.

Χάρη στην αρχιτεκτονική PKI, κάθε ψήφος κωδικοποιείται ξεχωριστά από ένα ασύμμετρο κλειδί κωδικοποίησης που κατέχουν οι ελεγκτές που διορίζονται από την κυβέρνηση του κράτους. Το δημόσιο κλειδί εισάγεται στην εφαρμογή και χρησιμοποιείται από όλους τους πολίτες για να κωδικοποιήσουν την ψήφο τους. Το ιδιωτικό κλειδί χρησιμοποιείται για να διαβαστούν τα ψηφοδέλτια. Προστατεύεται από δύο κωδικούς που ορίζονται από τους ελεγκτές και είναι γνωστοί σε αυτούς μόνο.
Η εμπειρία της Ελβετίας δείχνει πως όλο και περισσότεροι νέοι φαίνεται να ψηφίζουν μέσω του Διαδικτύου.

2.6.3 Το σύστημα Sensus

Συνεχίζοντας την περιγραφή εφαρμογών συστημάτων ηλεκτρονικής ψηφοφορίας θα εξετάσουμε το σύστημα 'Sensus' που είναι ένα ηλεκτρονικό σύστημα ψηφοφορίας μέσω του Διαδίκτυου, που επιτρέπει στους ψηφοφόρους του να ασκήσουν το εκλογικό τους δικαίωμα και τους παρέχει δυνατότητα επαλήθευσης των αποτελεσμάτων της ψηφοφορίας. Το Sensus βασίζεται σε ένα αλγόριθμο που δημοσιεύθηκε από τους Fujioka, Okamoto και Ohta το 1993. Χρησιμοποίησε την κρυπτογραφική μέθοδο των τυφλών υπογραφών ούτως ώστε να διασφαλιστεί μυστικότητα στη ψηφοφορία, ενώ ταυτόχρονα διασφάλιζε ότι κάθε νόμιμος ψηφοφόρος μπορεί να ψηφίσει μόνο μία φορά. Οι προαναφερόμενοι λόγοι έλκυσαν αρκετούς ερευνητές για να το μελετήσουν και είναι ένα σύστημα που επηρέασε μετέπειτα μελέτες [25].

Ουσιαστικά, ο ψηφοφόρος παρασκευάζει την ψήφο του, χρησιμοποιώντας ένα πρόγραμμα που κρυπτογραφεί τις ψήφους και δημιουργεί επίσης ένα μοναδικό ψηφιακό αποτύπωμα για κάθε ψήφο. Το πρόγραμμα εν συνεχεία πολλαπλασιάζει τους αριθμούς στο αποτύπωμα, με ένα τυχαίο αριθμό και αποστέλλει το αποτέλεσμα μαζί με την ψηφιακή υπογραφή του ψηφοφόρου στον επικυρωτή. Ο επικυρωτής είναι ένας υπολογιστής ο οποίος τρέχει από την εκλογική αρχή. Ο επικυρωτής ελέγχει την ψηφιακή υπογραφή του ψηφοφόρου για να διασφαλίσει ότι ο ψηφοφόρος έχει δικαίωμα να ψηφίσει και ότι δεν έχει ξαναψηφίσει. Τότε, ο επικυρωτής υπογράφει ψηφιακά το τυχαίο αποτύπωμα και το επιστρέφει στον ψηφοφόρο. Ο ψηφοφόρος το διαιρεί με τον τυχαίο αριθμό. Έτσι, προκύπτει ένα αποτύπωμα υπογεγραμμένο από τον επικυρωτή.

Ωστόσο, μιας και ο επικυρωτής υπέγραψε το αποτύπωμα που ήταν πολλαπλασιασμένο με τον τυχαίο αριθμό, ο επικυρωτής δεν έχει κανένα τρόπο να γνωρίζει το αρχικό αποτύπωμα ή σε ποιο ψηφοφόρο αντιστοιχεί. Τότε ο ψηφοφόρος στέλνει το υπογεγραμμένο αποτύπωμα και το αντίστοιχο κρυπτογραφημένο αποτύπωμα στον μετρητή. Ο μετρητής χρησιμοποιεί το υπογεγραμμένο αποτύπωμα για να επαληθεύσει ότι η ψήφος έχει πιστοποιηθεί από τον επικυρωτή, και παρέχει μια απόδειξη στον ψηφοφόρο ότι η ψήφος έχει γίνει αποδεκτή.

Τότε ο ψηφοφόρος στέλνει στον καταμετρητή το κλειδί που απαιτείται για να αποκρυπτογραφήσει την ψήφο, ούτως ώστε να γίνει η καταμέτρηση.

Κεφάλαιο 3

Πρωτόκολλα Ηλεκτρονικής Ψηφοφορίας

3.1 A six-authority protocol 24

3.2 Foo Protocol (Fujioka,Okamoto και Ohta) 29

3.3 An Anonymous Electronic Voting Protocol for Voting Over The Internet..... 30

3.4 REVS- A Robust Electronic Voting System 34

3.5 Wu And Sankaranarayana Protocol 36

3.6 A Novel Simple Secure Internet Voting Protocol 37

Στο παρόν κεφάλαιο παρουσιάζονται κάποια προτεινόμενα πρωτόκολλα ηλεκτρονικής ψηφοφορίας μέσω Διαδικτύου. Για κάθε πρωτόκολλο αναλύονται ξεχωριστά η λειτουργία του καθώς επίσης οι κρυπτογραφικές μέθοδοι που χρησιμοποιεί. Θα μας απασχολήσει η κατανόηση της προσέγγισης των πρωτοκόλλων που αποσκοπεί στην ανάπτυξη κριτικής σκέψης για τα συστήματα ηλεκτρονικής ψηφοφορίας μέσω του Διαδικτύου.

3.1 A six-authority protocol

Μία από τις δημοφιλής προσεγγίσεις της ηλεκτρονικής ψηφοφορίας στηρίζεται στην συμμετοχή ενός ανεξάρτητου τρίτου προσώπου, που ονομάζεται αξιόπιστη αρχή.

Τα πρωτόκολλα αξιοποιούν την ιδέα των αξιόπιστων αρχών μιας και επιχειρούν να κτίσουν βασιζόμενα στην ίδια λογική που ακολουθούσαν και οι παραδοσιακές εκλογές, δηλαδή, στην ύπαρξη ενός ή και περισσότερων αξιόπιστων μέσων τα οποία θα διαχειρίζονται ορθά την διεξαγωγή των εκλογών.

Οι ψηφοφόροι αλληλεπιδρούν με αυτές τις αρχές για να εγγραφούν και να καταχωρήσουν τις ψήφους τους και βασίζονται σε αυτές ούτως ώστε να παραχθεί μια ορθή διαδικασία χωρίς να διακυβεύεται η μυστικότητα της ψήφου.

Οι Karo και Wang πρότειναν ένα πρωτόκολλο ηλεκτρονικής ψηφοφορίας για εκλογές μεγάλης κλίμακας οι οποίες στηρίζονται στις αξιόπιστες αρχές. Το συγκεκριμένο πρωτόκολλο χρησιμοποιεί έξι διακριτές ηλεκτρονικές αρχές, οι οποίες είναι:

- ο καταχωρητής
- ο επικυρωτής
- ο διανομέας
- ο μετρητής
- ο ταυτοποιητής
- ο επαληθευτής

Το μοντέλο επικοινωνίας στηρίζεται στην χρήση ενός off-the-shelf ασφαλή πρωτοκόλλου επικοινωνίας, όπως το HTTPS , που διεξάγεται μεταξύ του ψηφοφόρου και των αρχών. Παρόλα αυτά, πολύπλοκες μέθοδοι χρησιμοποιούνται για να αποφευχθεί η συμπαιγνία μεταξύ των αρχών.

Στάδιο Εγγραφής: Ένας ψηφοφόρος πρέπει να εγγραφεί μέσω του καταχωρητή, ούτως ώστε να διερευνηθεί αν είναι νόμιμος ψηφοφόρος. Κατά την διάρκεια της εγγραφής, ο καταχωρητής προσδιορίζει ένα μοναδικό αριθμό αναγνώρισης στον ψηφοφόρο και έπειτα καταχωρείται το όνομα του ψηφοφόρου καθώς επίσης και ο μοναδικός του αριθμός σε μια λίστα η οποία εμπεριέχει όλους τους εγγεγραμμένους ψηφοφόρους.

Έπειτα ο καταχωρητής αποστέλνει μόνο τον μοναδικό αριθμό του ψηφοφόρου στον επικυρωτή χωρίς να επισυνάπτεται και το όνομα του ψηφοφόρου.

Ο επικυρωτής παράγει ένα μοναδικό ζεύγος κλειδιών που αποτελείται από δημόσια και ιδιωτικά κλειδιά για το συγκεκριμένο μοναδικό αριθμό που έλαβε και τα αποθηκεύει σε μία λίστα και εν συνεχεία, αποστέλνει το ζεύγος με το δημόσιο κλειδί s και το μοναδικό αριθμό στον καταχωρητή.

Τότε ο καταχωρητής στέλνει το ζεύγος με το δημόσιο κλειδί και το μοναδικό αριθμό πίσω στο ψηφοφόρο. Μέσω αυτής της διαδικασίας, ο επικυρωτής δεν θα γνωρίζει σε ποιο ανήκει το κλειδί ,χωρίς βέβαια να υπάρξει συνωμοσία με τον καταχωρητή.

Ο καταχωρητής στέλνει τον αριθμό των νόμιμων εγγεγραμμένων ψηφοφόρων στον μετρητή.

Ο μετρητής, με την σειρά του, παράγει ένα μεγαλύτερο αριθμό ηλεκτρονικών ψηφοδελτίων από τον αριθμό των εγγεγραμμένων ψηφοφόρων. Κάθε ηλεκτρονικό ψηφοδέλτιο συνίσταται από ένα μοναδικό αριθμό ,ένα πλήθος επιλογών καθώς επίσης και μια κρυπτογραφημένη έκδοση της κάθε επιλογής.

Ο μετρητής για το κάθε ηλεκτρονικό ψηφοδέλτιο κρατάει ιστορικό του κλειδιού αποκρυπτογράφησης και του μοναδικού αριθμού της ψήφου, ούτως ώστε ο μετρητής να έχει την δυνατότητα να κρυπτογραφήσει της ψήφους που ρίχτηκαν.

Ο μετρητής στέλνει τις ψήφους στον διανομέα, ένα αντίτυπο του πίνακα αποκρυπτογράφησης στον επαληθευτή και μία αντιστοιχία με όλα τα ζεύγη που εμπεριέχουν τις κρυπτογραφημένους ψήφους μαζί με τις αποκρυπτογραφημένες επιλογές τους στον ταυτοποιητή.

Ο καταχωρητής στέλνει στον επικυρωτή μία λίστα που περιλαμβάνει τους μοναδικούς αριθμούν των ψηφοφόρων που έχουν το δικαίωμα να ψηφίσουν στην συγκεκριμένη εκλογή.

Εάν είναι επιθυμητό, ο καταχωρητής μπορεί να δημοσιεύσει τα ονόματα αυτών των ψηφοφόρων ούτως ώστε ο επαληθευτής να μπορεί να ελέγξει τις ψήφους και το ζεύγος με τις κρυπτογραφημένες ψήφους και τις αντίστοιχες αποκρυπτογραφημένες επιλογές ώστε να επιβεβαιώσει ότι έχουν παραχθεί σωστά.

Στάδιο Ψηφοφορίας: Προκειμένου ένας ψηφοφόρος να ψηφίσει πρέπει να επικοινωνήσει με τον διανομέα και να του διανέμει το ηλεκτρονικό ψηφοδέλτιο. Ο διανομέας τυχαία επιλέγει μία ψήφο και την στέλνει στον ψηφοφόρο ο οποίος με την σειρά του ζητάει από τον ταυτοποιητή να του παραχωρήσει ένα ζεύγος κλειδιών για την συγκεκριμένη ψήφο. Ο ταυτοποιητής του τα παρέχει.

Ο ψηφοφόρος τότε υπογράφει την κρυπτογραφημένη έκδοση της επιθυμητής επιλογής του χρησιμοποιώντας το κλειδί της υπογραφής του και την αποστέλνει στον επικυρωτή, μαζί με τον μοναδικό αριθμό της ψήφου και τον δικό του. Ο επικυρωτής ενημερώνει τον διανομέα ότι η ψήφος με τον συγκεκριμένο μοναδικό αριθμό έχει ριχθεί.

Ο διανομέας καταγράφει πόσες ψήφοι έχουν πράγματι ριχθεί και ποιες είναι αυτές οι ψήφοι, με τον τρόπο αυτό εμποδίζεται η δημιουργία ψήφων από μη υπογεγραμμένες ψήφους.

Ο ψηφοφόρος επίσης ενημερώνει τον καταχωρητή ότι έχει ρίξει την ψήφο του, εντούτοις δεν είναι απαραίτητο να αναφέρει στον καταχωρητή τον μοναδικό αριθμό την ψήφου που χρησιμοποίησε.

Ο επικυρωτής ελέγχει την υπογραφή ούτως ώστε να αυθεντικοποιήσει τον ψηφοφόρο και να επαληθεύσει ότι ο εγγεγραμμένος ψηφοφόρος έχει δικαίωμα στην συγκεκριμένη ψηφοφορία.

Αφού πραγματοποιηθεί η αυθεντικοποιήση ,ο επικυρωτής περνά μόνο την νόμιμη κρυπτογραφημένη ψήφο και τον μοναδικό αριθμό της ψήφου στον μετρητή. Ο ψηφοφόρος παίρνει μια απόδειξη ,με τον τρόπο αυτό επιβεβαιώνεται ότι ο επικυρωτής έχει παραλάβει το πακέτο με τη ψήφο.

Στάδιο Καταμέτρησης και Επαλήθευσης: Για να παραχθεί η ψήφος ,ο μετρητής αποκρυπτογραφεί τις ψήφους που έχει παραλάβει. Μετά την καταμέτρηση των ψήφων ,κάθε αρχή δίνει ορισμένες πληροφορίες στο κοινό. Για την επαλήθευση της ακεραιότητας των εκλογών ,ο επαληθευτής συγκρίνει ορισμένες λίστες που έχουν δημοσιοποιηθεί. Την

διαδικασία της επαλήθευσης των στοιχείων μπορεί να την πραγματοποιήσει οποιοδήποτε άτομο επιθυμεί. Η διαδικασία της επαλήθευσης από τον ψηφοφόρο δεν απαιτείται από το σύστημα. Παρόλα αυτά, οποιοσδήποτε επιπλέον έλεγχος ενισχύει την ασφάλεια του συστήματος καθώς επίσης και την ακεραιότητα της διαδικασίας και των αποτελεσμάτων.

Ο επικυρωτής δημοσιεύει την λίστα η οποία εμπεριέχει τις κρυπτογραφημένες ψήφους μαζί με το μοναδικό αριθμό τους.

Ο μετρητής δημοσιεύει την έκδοση με την ίδια λίστα και ο επαληθευτής επαληθεύει ότι αυτές οι λίστες είναι πανομοιότυπες.

Για να εμποδιστούν φαινόμενα απόκρυψης δεδομένων, είναι επιθυμητό οι λίστες να αποστέλλονται στον επικυρωτή πρωτού να δημοσιευθούν.

Ο επικυρωτής χρησιμοποιεί επίσης αυτή την λίστα και τον αποκρυπτογραφημένο πίνακα που έχει παραχθεί από τον μετρητή κατά την διάρκεια της εγγραφής για να επαληθεύσει τα αποτελέσματα που έχουν δημοσιευθεί από τον μετρητή.

Ο ψηφοφόρος έχει την δυνατότητα να ελέγξει από τις δύο πανομοιότυπες λίστες ότι η ψήφος του βρίσκεται καταχωρημένη.

Ο διανομέας επίσης κοιτάζει αυτές τις λίστες για να βεβαιωθεί ότι μόνο επιτρεπτές ψήφοι υπάρχουν. Οποιαδήποτε μη νόμιμη ψήφος ανιχνευθεί, απομακρύνεται και υπολογίζεται εκ νέου το αποτέλεσμα.

Ο διανομέας μπορεί επίσης να ανακοινώσει την λίστα με τον μοναδικό αριθμό των ψήφων, εντούτοις αυτό είναι καλό να γίνει μετά που ο επικυρωτής και ο μετρητής ανακοινώσουν την λίστα με τις κρυπτογραφημένες ψήφους,

Ο επικυρωτής επίσης δημοσιεύει μία λίστα η οποία εμπεριέχει όλους μοναδικούς αριθμούς των ψήφων που ρίχθηκαν. Έπειτα ο καταχωρητής θα κοιτάξει αυτή την λίστα για να επιβεβαιώσει ότι μόνο εγγεγραμμένοι ψηφοφόροι έχουν ψηφίσει.

Στην περίπτωση που ζητηθεί η λίστα αυτή κοινοποιείται.

Ανάλυση του πρωτοκόλλου

Η ασφάλεια του πρωτοκόλλου στηρίζεται στον αμοιβαίο έλεγχο που πραγματοποιείται. Κάθε αρχή συμμετέχει σε ένα εσωτερικό πρωτόκολλο επικοινωνίας, που είναι σχεδιασμένο με τέτοιο τρόπο ώστε να εμποδίζει φαινόμενα συμπαιγνίας, την αποφυγή δηλαδή δόλιων ενεργειών που σκοπό έχουν την παραβίαση της μυστικότητας της ψήφους.

Με την λήξη των εκλογών , κάθε αρχή ελέγχεται δημοσίως από τις υπόλοιπες αρχές. Σύμφωνα με τους συγγραφείς του πρωτοκόλλου, το πρωτόκολλο κατασκευάστηκε με τέτοιο τρόπο ώστε το σύστημα να είναι δημοκρατικό. Με τον τρόπο αυτό διασφαλίζει ότι δεν υπάρξουν φαινόμενα εξαπάτησης κατά την διάρκειας της εγγραφής.

Το σύστημα είναι ακριβές μιας και παρέχεται στους ψηφοφόρους μία απόδειξη που επιβεβαιώνει ότι ο επικυρωτής έχει παραλάβει το πακέτο με τη ψήφο. Επίσης, κάθε ψηφοφόρος έχει την δυνατότητα να ελέγξει αν η ψήφος του καταχωρήθηκε από τις λίστες που δημοσιεύονται κατά την φάση της επαλήθευσης. Αξίζει να σημειωθεί ότι καμία αρχή δεν είναι σε θέση να δημιουργήσει ψήφο χωρίς το γεγονός να ανιχνευτεί μιας και όλες οι λίστες δημοσιεύονται μετά την λήξη των εκλογών. Ανίχνευση οποιασδήποτε αλλοίωσης ,αναπαραγωγής και διαγραφής εντοπίζεται και στις νόμιμες ψήφους εξαιτίας της κοινοποίησης των λιστών.

Αναφορικά με την μυστικότητα που διασφαλίζει το πρωτόκολλο ,η μόνη αρχή που είναι σε θέση να συνδέσει τα ονόματα των ψηφοφόρων με την ψήφο είναι ο καταχωρητής σε συνεργασία με τον μετρητή. Συγκεκριμένα ,ο καταχωρητής γνωρίζει μόνο τις κρυπτογραφημένες ψήφους οι οποίες ρίχνονται από ένα συγκεκριμένο μοναδικό αριθμό ψηφοφόρου και δεν είναι εφικτή η αποκρυπτογράφηση της ψήφου χωρίς την συνωμοσία με τον μετρητή. Για το λόγο αυτό, το μοντέλο επικοινωνίας δεν επιτρέπει οποιαδήποτε συνωμοσία.

Το μοντέλο αυτό υποστηρίζει επίσης την ατομική επαληθευσιμότητα. Κάθε ψηφοφόρος μπορεί από μόνος του να επαληθεύσει ότι η ψήφος του έχει καταχωρηθεί. Ο έλεγχος αυτός πραγματοποιείται μέσω των λιστών που αναρτώνται από τον επικυρωτή και το μετρητή που εμπεριέχουν τους μοναδικούς αριθμούς και τα κωδικοποιημένα κλειδιά. Δηλαδή, ο ψηφοφόρος διερευνά αν η ψήφος του υπάρχει στις λίστες με βάση τον μοναδικό του αριθμό και τα κωδικοποιημένα του κλειδιά.

Παρόλο που το πρωτόκολλο δεν είναι σχεδιασμένο για να είναι απαλλαγμένο από απόδειξη μιας και κάθε ψηφοφόρος εξασφαλίζει απόδειξη όταν ψηφίσει ,εντούτοις είναι εφικτό να πραγματοποιηθεί αλλαγή της ψήφου από τον ψηφοφόρο. Μιας και υπάρχει δυνατότητα της αλλαγής της ψήφου, ένα άτομο που επιδιώκει να εξαναγκάσει κάποιο ψηφοφόρο, μπορεί να το εξασφαλίσει μόνο αναγκάζοντας τον να ψηφίσει λίγο πριν το τέλος των εκλογών ούτως ώστε να μην έχει χρόνο να αλλάξει μετά την ψήφο του.

Ένας ψηφοφόρος μπορεί να επαληθεύσει την συμμετοχή του μέσω μίας λίστας που ετοιμάζεται από τον καταχωρητής ,ο οποίος γνωρίζει τους ψηφοφόρους που συμμετέχουν. Η λίστα εμπεριέχει όλους τους ψηφοφόρους που συμμετείχαν στην συγκεκριμένη εκλογή. Έτσι η επαλήθευση της συμμετοχής ενός ψηφοφόρου διασφαλίζεται.

Μέσω αυτού του πρωτοκόλλου παρέχεται στους ψηφοφόρους ευκολία στον τρόπο ψηφοφορίας καθώς επίσης δίνεται η δυνατότητα να ψηφίζει από όποιο μέρος επιθυμεί και οποιαδήποτε ώρα.

Το πρωτόκολλο αυτό μπορεί να θεωρηθεί ως αποτελεσματικό μιας και απαιτούνται ελάχιστοι υπολογισμοί.

Για μεγάλες εκλογές, κάθε περιφέρεια μπορεί να έχει τις δικές της αρχές και να υποβάλει τα αποτελέσματα σε ένα κεντρικό.

Μιας και δεν υπάρχουν περιορισμοί για την μορφή της ψήφου, το πρωτόκολλο αυτό μπορεί να χρησιμοποιηθεί σε κάθε είδος εκλογών και για τον λόγο αυτό χαρακτηρίζεται και ως ευέλικτο.

Πιο κάτω παραθέτω ένα πίνακα που συνοψίζει τις απαιτήσεις της ηλεκτρονικής ψηφοφορίας που καλύπτονται από το Six-Authority Protocol.

Voting Protocols & Schemes	**Security Requirements**											**System Wide Properties**		
	Accuracy			Democracy										
	Inalterability	Completeness	Soundness	Eligibility	Unfeasibility	Privacy	Robustness	Verifiability	Uncoercibility	Fairness	Veri. participation	"Walk-away"	Voter Mobility	Flexibility
TRUSTED AUTHORITIES														
Six authority protocol	Yes	Yes	Yes	Yes	Yes	Cmp	No	Indi	No		Yes	Yes	Yes	Yes

όπου Cmp=Computational και Indi=Individual

3.2 Foo Protocol (Fujioka,Okamoto και Ohta)

Οι Fujioka, Okamoto και Ohta εφαρμόζοντας την κρυπτογραφική μέθοδο των τυφλών υπογραφών στις ηλεκτρονικές εκλογές επίλυσαν το πρόβλημα της επικύρωσης των ψήφων καθώς επίσης και το πρόβλημα της μυστικότητας τους.

- Συμβολίζω με b την ψήφο και (e,d) τα κλειδιά του ψηφοφόρου, όπου e το ιδιωτικό του κλειδί και d το δημόσιο.

- Επίσης συμβολίζω με R ένα τυχαίο αριθμό, που θα δράσει ως παράγοντας τύφλωσης της ψήφους.
- Τέλος συμβολίζω με (ev,dv) το ιδιωτικό και δημόσιο κλειδί του επικυρωτή αντίστοιχα.

Ο ψηφοφόρος επιλέγει τον υποψήφιο που επιθυμεί και η ψήφος κρυπτογραφείται ως εξής: b^e=B.

Έπειτα η ψήφος τυφλώνεται,$(B*R^{ev})$.

Στην συνέχεια, ο ψηφοφόρος υπογράφει την ψήφο του $(B*R^{ev}$,id)όπου id η υπογραφή του ψηφοφόρου.

Αυτό το πακέτο (η τυφλή κρυπτογραφημένη υπογεγραμμένη ψήφος) υποβάλλεται με την χρήση ενός καναλιού στον επικυρωτή.

Ο επικυρωτής διερευνά αν η υπογραφή ανήκει σε ένα εγγεγραμμένο ψηφοφόρο και ελέγχει αν έχει ήδη ψηφίσει.

Σε αυτό το σημείο καθορίζεται αν μία ψήφος είναι επιτρεπτή. Στην περίπτωση που ο ψηφοφόρος έχει δικαίωμα ψήφου, ο επικυρωτής υπογράφει τη ψήφο $(B*R^{ev})^{dv}$ και επιστρέφεται στον ψηφοφόρο.

Ο ψηφοφόρος απομακρύνει το παράγοντα τύφλωσης $(B*R^{ev})^{dv}$ / R , αποκαλύπτοντας μία κρυπτογραφημένη ψήφος η οποία είναι υπογεγραμμένη από τον επικυρωτή που είναι το B^{dv}.

Έπειτα αυτή η κρυπτογραφημένη υπογεγραμμένη ψήφος στέλνεται στην Αρχή μέσω ενός ανώνυμου καναλιού επικοινωνίας για να δημοσιευθεί αν είναι έγκυρη μετά την λήξη της προθεσμίας υποβολής ψήφων.

Κάθε ψηφοφόρος κλείνεται για λόγους ασφαλείας να ελέγξει αν η ψήφος του έχει κατοχυρωθεί στον πίνακα ανακοινώσεων.

Στην περίπτωση που η ψήφος δεν είναι δημοσιευμένη, έχει την δυνατότητα να καταγγείλει ανώνυμα την διαδικασία.

Αν η ψήφος του είναι δημοσιευμένη κανονικά, ο ψηφοφόρος υποβάλλει στην Αρχή χρησιμοποιώντας ξανά το ανώνυμο κανάλι επικοινωνίας, τα κλειδιά αποκρυπτογράφησης που είναι απαραίτητα για να ανοίξουν την ψήφο του.

Η Αρχή αφού παραλάβει τα κλειδιά αποκρυπτογράφησης των ψηφοφόρων είναι σε θέση να αποκρυπτογραφήσει τις ψήφους και να τις προσθέσουν στο αποτέλεσμα των εκλογών. Μετά τις εκλογές, η Αρχή δημοσιεύει τα κλειδιά αποκρυπτογράφησης μαζί με τις κρυπτογραφημένες ψήφους (B,b,d)ούτως ώστε οι ψηφοφόροι να είναι σε θέση να επαληθεύουν οι ίδιοι τα αποτελέσματα των εκλογών.

3.3 An Anonymous Electronic Voting Protocol for Voting Over The Internet

Οι Indrajit Ray, Natarajan Narasimhamurthi και Indrakshi Ray πρότειναν ένα πρωτόκολλο ηλεκτρονικής ψηφοφορίας μέσω του Διαδικτύου [15]. Το πρωτόκολλο επιτρέπει σε εγγεγραμμένους ψηφοφόρους να ψηφίσουν τον υποψήφιο που επιθυμούν. Κάθε ψηφοφόρος μπορεί να ψηφίσει μόνο μία φορά και έχει τη δυνατότητα να επαληθεύσει ότι η ψήφος του έχει καταχωρηθεί. Το πρωτόκολλο διασφαλίζει ότι δεν θα υπάρξει συσχετισμός των ψήφων με τους ψηφοφόρους.

Το πρωτόκολλο χρησιμοποιεί τρεις αρχές για την λειτουργία του, το διανομέα των ψήφων, την αρχή πιστοποίησης και τον καταμετρητή. Ο **διανομέας των ψήφων (BD)** ετοιμάζει λευκά ψηφοδέλτια και τα διανέμει στους ψηφοφόρους. Η **αρχή πιστοποίησης** (CA) πιστοποιεί ότι ένα ψηφοδέλτιο έχει καταχωρηθεί από ένα εγγεγραμμένο ψηφοφόρο ο οποίος ασκεί το εκλογικό του δικαίωμα για πρώτη φορά και τέλος ο **καταμετρητής** (VC) έχει ως αρμοδιότητα την καταμέτρηση των ψήφων που έχουν καταχωρηθεί και την ανακοίνωση των αποτελεσμάτων.

Στη περιγραφή του πρωτοκόλλου χρησιμοποιούνται οι πιο κάτω συμβολισμοί:

- X_e το δημόσιο κλειδί της αρχής X.
- X_d το ιδιωτικό κλειδί της αρχής X.
- h(M) ο κατατεμαχισμός του μηνύματος M.
- [m, X_e] το μήνυμα m κρυπτογραφείται με το δημόσιο κλειδί του X.
- [m, X_d] το μήνυμα m υπογράφεται με το ιδιωτικό κλειδί του X.

Η διαδικασία της ψηφοφορίας διακρίνεται σε πέντε διακριτές φάσεις:

- Έναρξη Ψηφοφορίας
- Κατανομή Λευκών Ψηφοδελτίων
- Πιστοποίηση Ψηφοφόρου
- Ψηφοφορία
- Καταμέτρηση Ψήφων

Πριν την διεξαγωγή της ψηφοφορίας, οι ψηφοφόροι επικοινωνούν με την αρχή καταχώρησης, η οποία είναι αρμόδια για την εγγραφή των ψηφοφόρων που έχουν δικαίωμα να ασκήσουν το εκλογικό τους δικαίωμα. Οι ψηφοφόροι που πληρούν τα κριτήρια άσκησης ψήφους καταχωρούνται στην λίστα με τους νόμιμους ψηφοφόρους. Εναπόκειται στους κανόνες της κάθε ψηφοφορίας για το ποιοι ψηφοφόροι πληρούν τα κριτήρια για να ενταχθούν στη λίστα με τους νόμιμους ψηφοφόρους. Η αρχή καταχώρησης εκδίδει ένα πιστοποιητικό για κάθε νόμιμο ψηφοφόρο που περιέχει την ταυτότητα του ψηφοφόρου και το δημόσιο του κλειδί. Η διαδικασία της εγγραφής είναι έξω από το πεδίο του πρωτοκόλλου ψηφοφορίας.

Ο ψηφοφόρος παραχωρεί στο διανομέα των ψήφων το πιστοποιητικό που έλαβε από την αρχή καταχώρησης που εμπεριέχει την ταυτότητα και το δημόσιο του κλειδί, για να διερευνηθεί αν ο ψηφοφόρος είναι νόμιμος να ασκήσει το εκλογικό του δικαίωμα. Στην περίπτωση που εξακριβωθεί ότι ο ψηφοφόρος είναι νόμιμος, ο διανομέας των ψήφων δημιουργεί ένα λευκό ψηφοδέλτιο. Το κάθε ψηφοδέλτιο αντιστοιχεί σε ένα και μόνο ψηφοφόρο και απαρτίζεται από δύο πεδία. Στο πρώτο πεδίο βρίσκεται ο σειριακός αριθμός του ψηφοδελτίου, y. Το δεύτερο πεδίο εμπεριέχει την υπογεγραμμένη σύνοψη του αριθμού του ψηφοδελτίου από το διανομέα των ψήφων. Η υπογραφή στη σύνοψη έχει πραγματοποιηθεί με το ιδιωτικό κλειδί του διανομέα των ψήφων[h(y),BD_d].

Εν συνεχεία, ο διανομέας των ψήφων κρυπτογραφεί με το δημόσιο κλειδί του ψηφοφόρου το ψηφοδέλτιο και υπογράφει με το ιδιωτικό του κλειδί το αποτέλεσμα του κατατεμαχισμού με παράμετρο το πιστοποιητικό και τα αποστέλλει στο ψηφοφόρο $([\{y, [h(y), BD_d]\}, V_e], [h\,(voter\ certificate), BD_d])$. Ο διανομέας των ψήφων διατηρεί μια λίστα με τους σειριακούς αριθμούς των ψηφοδελτίων και τις αντίστοιχες ταυτότητες των εγγεγραμμένων ψηφοφόρων.

Ο ψηφοφόρος παραλαμβάνει το μήνυμα από το διανομέα των ψήφων και ανακτά τον μοναδικό αριθμό του ψηφοδελτίου y και του προσθέτει ένα σταθερού μεγέθους τυχαίο αριθμό και προκύπτει ο x.Ο ψηφοφόρος υπολογίζει ένα μετασχηματισμό του x και προκύπτει το m, από το όποιο είναι υπολογιστικά αδύνατο να μεταβούμε στο x.Ο σειριακός αριθμός y είναι μοναδικός για κάθε ψηφοφόρο και για το λόγο αυτό η σύνοψη m είναι επίσης μοναδική. Μέσω του m είναι ανέφικτο να εντοπιστεί ο σειριακός αριθμός y και για το λόγο αυτό, είναι αδύνατο να υπάρξει οποιαδήποτε σύνδεση με το ψηφοφόρο.

Ο ψηφοφόρος τυφλώνει το m με ένα τυχαίο αριθμό r και εν συνεχεία την κρυπτογραφεί με το δημόσιο κλειδί της αρχής πιστοποίησης , $m * [r, CA_e]$. Επίσης, ο ψηφοφόρος υπολογίζει τη σύνοψη της συνάρτησης κατακερματισμού με παράμετρο το τυφλωμένο υπογεγραμμένο m του ψηφοφόρου και το υπογράφει με το ιδιωτικό του κλειδί και εν συνεχεία το κρυπτογραφεί με το δημόσιο κλειδί της αρχής πιστοποίησης, $[[h(m * [r, CA_e]), V_d], CA_e]$ και το αποστέλλει μαζί με το τυφλωμένο κρυπτογραφημένο m, $[\{m * [r, CA_e]\}, CA_e]$ στην αρχή πιστοποίησης. Ο ψηφοφόρος επίσης, κρυπτογραφεί με το δημόσιο κλειδί της αρχής πιστοποίησης το πιστοποιητικό που παρέλαβε από το διανομέα τον ψήφο και τη σύνοψη του πιστοποιητικού του και τα αποστέλλει στην αρχή πιστοποίησης, δηλαδή αποστέλλει$[\{voter\ certificate, [h(voter - certificate), BD_d]\}, CA_e]$.

Η αρχή πιστοποίησης διερευνά αν ο ψηφοφόρος είναι εγγεγραμμένος ελέγχοντας την αυθεντικότητα του πιστοποιητικού του ψηφοφόρου και εξετάζει αν ο ψηφοφόρος έχει ψηφίσει προηγουμένως. Στην συνέχεια, υπογράφει με το ιδιωτικό του κλειδί το τυφλωμένο

κρυπτογραφημένο m του ψηφοφόρου που έχει παραλάβει και εν συνεχεία το κρυπτογραφεί με το δημόσιο κλειδί του ψηφοφόρου και του το αποστέλλει $[\{[\{m * [r, CA_e]\}, CA_d]\}, V_e]$. Η αρχή πιστοποίησης διατηρεί μία λίστα με τα τυφλωμένα κρυπτογραφημένα m των ψηφοφόρων μαζί τους αντίστοιχους αριθμούς ταυτότητας.

Ο ψηφοφόρος απομακρύνει τον παράγοντα τύφλωσης από το m που του έχει σταλεί και με τον τρόπο αυτό εξασφαλίζει το m με την υπογραφή της αρχής πιστοποίησης.

Ο ψηφοφόρος διαλέγει τον υποψήφιο που επιθυμεί. Κάθε υποψήφιος χαρακτηρίζεται από ένα μοναδικό αριθμό. Στο μοναδικό αριθμό του υποψηφίου που έχει επιλέξει ο ψηφοφόρος προστίθεται το υπογεγραμμένο m και εν συνεχεία δημιουργείται ένα κατατεμαχισμένο μήνυμα με την ψήφο και το υπογεγραμμένο m. Ο ψηφοφόρος τα κρυπτογραφεί με το δημόσιο κλειδί του καταμετρητή, $\left[\{\{vote, [m, CA_d]\}, h(vote, [m, CA_d])\}, VC_e\right]$ και τα αποστέλλει στο καταμετρητή. Ο καταμετρητής ελέγχει αν έχει παραλάβει προηγουμένως το m και εν συνεχεία υπογράφει με το ιδιωτικό του κλειδί την σύνοψη της ψήφους και το m και τα αποστέλλει στο ψηφοφόρο.

Μετά το τέλος των εκλογών, κανένας ψηφοφόρος δεν έχει δικαίωμα να ασκήσει το εκλογικό του δικαίωμα. Κατά τη διαδικασία της καταμέτρησης, ο διανομέας των ψήφων δημοσιεύει τον αριθμό των λευκών ψήφων που έχει εκδώσει και τον σειριακό αριθμό της κάθε ψήφου μαζί με την αντίστοιχη ταυτότητα του ψηφοφόρου. Ο αριθμός των λευκών ψήφων πρέπει να είναι ίσος ή μεγαλύτερος από τον αριθμό των ψήφων που έχουν καταχωρηθεί στο σύστημα κατά τη διαδικασία της ψηφοφορίας καθώς επίσης είναι ίσος ή μικρότερος από τον αριθμό των εγγεγραμμένων ψηφοφόρων. Η αρχή πιστοποίησης δημοσιεύει το σύνολο των τυφλωμένων κρυπτογραφημένων m που έχει λάβει από τους ψηφοφόρους με τις αντίστοιχες ταυτότητες τους. Ο αριθμός αυτός πρέπει να είναι μικρότερος ή ίσος με τον αριθμό των λευκών ψήφων. Ο καταχωρητής δημοσιεύει όλες τις ψήφους μαζί με τα αντίστοιχα υπογεγραμμένα με το ιδιωτικό κλειδί της αρχής πιστοποίησης m. Ο ψηφοφόρος μπορεί να ελέγξει τη δημοσιευμένη λίστα με τις ψήφους ούτως ώστε να βεβαιωθεί ότι η ψήφος του έχει μετρήσει στη τελική καταμέτρηση. Μετά από κάποιο χρονικό διάστημα, καταμετρούνται οι ψήφοι και ανακοινώνονται τα αποτελέσματα.

Αξιολόγηση Πρωτοκόλλου

- Επαληθευσιμότητα: Η επαληθευσιμότητα εξασφαλίζει μιας και κατά την λήξη της ψηφοφορίας κοινοποιείται μία λίστα η οποία εμπεριέχει τις ψήφους που καταχωρήθηκαν στο σύστημα για καταμέτρηση. Ο ψηφοφόρος έχει τη δυνατότητα να ελέγξει τη ψήφο του διερευνώντας αν το m που τον αφορά εμφανίζεται στη λίστα.

- Δημοκρατικό: Στη τελική καταμέτρηση των ψήφων δεν υπάρχουν ψήφοι από μη εγγεγραμμένους ψηφοφόρους καθώς επίσης δεν υπάρχουν πολλαπλές ψήφους από ένα ψηφοφόρο. Κάθε ψηφοφόρος έχει δικαίωμα ψήφους μόνο μία φορά.
- Μυστικό: Όταν ο ψηφοφόρος επιλέξει τον υποψήφιο που επιθυμεί αποστέλει την ανάλογη ψήφο του στο καταμετρητή κρυπτογραφώντας τη με το δημόσιο κλειδί του καταχωρητή. Συνεπώς, μόνο ο καταχωρητής έχει τη δυνατότητα να γνωρίζει τον μοναδικό αριθμό του ψηφοδελτίου και μόνο αν συνεργαστεί με τον κατανομέα των ψήφων θα μπορεί να συνδέσει μία ψήφο με τον αντίστοιχο ψηφοφόρο της.
- Ακριβές: Ο ψηφοφόρος μπορεί να επαληθεύσει ότι η ψήφος του δεν έχει αλλοιωθεί ή διαγραφεί από το σύστημα ελέγχοντας τις λίστες που κοινοποιούνται μετά τη λήξη των εκλογών. Επίσης, διασφαλίζεται ότι ο κατανομέας των ψήφων δίνει λευκά ψηφοδέλτια μόνο σε εγγεγραμμένους ψηφοφόρους και επίσης υπογράφει το κατατεμαχισμό του πιστοποιητικού του ψηφοφόρου. Όταν ο ψηφοφόρος επιδιώκει να εξασφαλίσει υπογραφή στην τυφλωμένο m παρουσιάζει το πιστοποιητικό του και το υπογεγραμμένο m στη αρχή πιστοποίησης. Αυτοί οι δύο έλεγχοι μαζί εξασφαλίζουν ότι ένας μη εγγεγραμμένος ψηφοφόρος δεν θα ψηφίσει. Επίσης, διασφαλίζεται ότι δεν θα υπογραφούν δύο τυφλωμένα m για τον ίδιο ψηφοφόρο. Κάθε m αντιστοιχεί σε ένα και μόνο ψηφοφόρο και είναι μοναδικό.

3.4 REVS- A Robust Electronic Voting System

Οι Joaquim , Zúquete και Ferreira πρότειναν ένα πρωτόκολλο ηλεκτρονικής ψηφοφορίας μέσω του Διαδικτύου που χρησιμοποιεί τυφλές υπογραφές και βασίζεται σε μία εργασία του DuRette το 1999. Μία πρώτη υλοποίηση του REVS έγινε στο Τεχνολογικό Πανεπιστήμιο της Λισαβόνας στο Ινστιτούτο Superior Técnico για την αξιολόγηση της ποιότητας των μαθημάτων [12].

Στο **REVS** πρωτόκολλο υπάρχουν πέντε διακομιστές:

- Κύριος Επίτροπος
- Κατανομέας Ψήφων
- Διαχειριστές
- Ανώνυμος Διακομιστής
- Καταμετρητής

Ο κύριος επίτροπος είναι ο επιβλέπων των εκλογών. Λαμβάνει τα παράπονα που γίνονται από τους ψηφοφόρους και διερευνά τα αίτια των παραπόνων. Έχει επίσης την ευθύνη για την προετοιμασία των εκλογών, τη δημιουργία και την διατήρηση της μυστικότητας των

κλειδιών, την υπογραφή των ερωτήσεων ψηφοφορίας. Ο κατανομέας των ψήφων είναι υπεύθυνος για τη διανομή των ψήφων στους ψηφοφόρους. Οι διαχειριστές του συστήματος έχουν τη δύναμη να αποδεχθούν ή να απορρίψουν μία ψήφο από ένα ψηφοφόρο. Ο ανώνυμος διακομιστής παρέχει ανωνυμία στη μηχανή του ψηφοφόρου απαλείφοντας έτσι τη συσχέτιση μιας ψήφου με την αντίστοιχη μηχανή. Τέλος, ο καταμετρητής είναι υπεύθυνος για την επαλήθευση της εγκυρότητας των ψήφων και την καταμέτρηση τους.

Ο ψηφοφόρος επικοινωνεί με τον κατανομέα των ψήφων αποστέλλοντας του τον αριθμό της ταυτότητας ψηφοφορίας ούτως ώστε να εξασφαλίσει μία λίστα με τις ψηφοφορίες στις οποίες μπορεί να συμμετέχει. Ο ψηφοφόρος επιλέγει μια ψηφοφορία στην οποία επιθυμεί να συμμετέχει και ζητά μία ψήφο. Ο κατανομέας αποστέλλει στο ψηφοφόρο ένα λευκό ψηφοδέλτιο και το δημόσιο κλειδί της συγκεκριμένης ψηφοφορίας υπογεγραμμένα από τον κύριο Επίτροπο. Ο ψηφοφόρος υπολογίζει τη σύνοψη m της συνάρτησης κατατεμαχισμού με παράμετρο τον αριθμό του ψηφοδελτίου. Εν συνεχεία τυφλώνει τη σύνοψη με ένα τυχαίο αριθμό σταθερού μήκους και την αποστέλλει στον διαχειριστή μαζί τον αριθμό του ψηφοφόρου. Ο διαχειριστής εξετάζει αν έχει υπογράψει προηγουμένως για το συγκεκριμένο ψηφοφόρο. Κάθε ψηφοφόρος έχει μόνο μία φορά δικαίωμα για υπογραφή από ένα συγκεκριμένο διαχειριστή. Στην περίπτωση που ο ψηφοφόρος δεν έχει ζητήσει αίτημα για υπογραφή προηγουμένως από το συγκεκριμένο διαχειριστή, ο διαχειριστής υπογράφει την τυφλωμένη σύνοψη του μηνύματος και την αποστέλλει στον ψηφοφόρο. Μία ψήφος είναι δέκτη από το τελικό καταμετρητή στην περίπτωση που έχει ένα ελάχιστο αριθμό από υπογραφών από διαφορετικούς διαχειριστές. Εάν οι διαχειριστές είναι n τότε ο ψηφοφόρος πρέπει να πάρει $t>N/2$ έγκυρες υπογραφές από διαφορετικούς διαχειριστές για να είναι μία ψήφος αποδεκτή. Με τον τρόπο αυτό είναι αδύνατο για οποιοδήποτε ψηφοφόρο να έχει δύο έγκυρες ψήφους. Ο ψηφοφόρος απομακρύνει τον παράγοντα τύφλωσης από την υπογεγραμμένη σύνοψη και χρησιμοποιώντας το δημόσιο κλειδί του διαχειριστή που είναι ευρέως γνωστό επαληθεύει την εγκυρότητα της υπογραφής. Η διαδικασία της υπογραφής της τυφλωμένης σύνοψης διεξάγεται για t διαφορετικούς διακομιστές. Ο ψηφοφόρος αφού συλλέξει t διαφορετικές υπογραφές επιλέγει τον υποψήφιο που επιθυμεί και αποστέλλει στον καταχωρητή μέσω της ανώνυμης αρχής τον αριθμό του υποψηφίου μαζί με τις υπογεγραμμένες συνόψεις κρυπτογραφημένες με το δημόσιο κλειδί της ψηφοφορίας. Στην περίπτωση που υπάρχουν πολλαπλοί καταμετρητές ο ψηφοφόρος μπορεί να αποστείλει το μήνυμα που μόλις αναφέραμε σε οποιοδήποτε καταμετρητή όσες φορές επιθυμεί ούτως ώστε να είναι βέβαιος ότι το μήνυμα του θα φθάσει στον προορισμό. Στην αντίθετη περίπτωση που χρησιμοποιείται ένας καταμετρητής, ο ψηφοφόρος έχει πάλει τη δυνατότητα να στείλει το μήνυμα όσες φορές επιθυμεί.

Με την λήξη της ψηφοφορίας ο καταμετρητής δημοσιεύει όλα τα μηνύματα που έχει παραλάβει και ο διαχειριστής δημοσιεύει όλες τις τυφλωμένες υπογεγραμμένες συνόψεις που έχει παραλάβει. Ο ψηφοφόρος έχει τη δυνατότητα να ελέγξει αν η ψήφος του έχει υπολογιστεί στην τελική καταμέτρηση μέσω των λιστών που κοινοποιούνται από τις προαναφερόμενες αρχές.

Εν συνεχεία, ο καταμετρητής αποκρυπτογραφεί με το ιδιωτικό κλειδί της εκλογής όλα τα μηνύματα που έχει παραλάβει και διερευνά την εγκυρότητα της ψήφου ελέγχοντας τον αριθμό και την εγκυρότητα των υπογραφών στις συνόψεις του ψηφοφόρου. Έπειτα αφαιρούνται όλες οι πολλαπλές ψήφους και υπολογίζεται και κοινοποιείται το αποτέλεσμα. Στην περίπτωση πολλαπλών καταμετρητών αποστέλλονται στο κύριο καταμετρητή οι ψήφοι και υπολογίζονται εκεί το τελικό αποτέλεσμα.

Αξιολόγηση Πρωτοκόλλου

- Δημοκρατικό: Κάθε ψηφοφόρος μπορεί να ψηφίσει μόνο μία φορά μιας και ο απαιτούμενος αριθμός υπογραφών που ο χρήστης πρέπει να συλλέξει από τους διαχειριστές του συστήματος είναι t>N/2 και με τον τρόπο αυτό εξαλείφεται το ενδεχόμενο ένας ψηφοφόρος να έχει περισσότερες από μία έγκυρες ψήφους.
- Επαληθευσιμότητα: Κάθε ψηφοφόρος έχει τη δυνατότητα να ελέγξει ότι η ψήφος του έχει ληφθεί υπόψη στην τελική καταμέτρηση ελέγχοντας τη λίστα που κοινοποιείται από τον καταχωρητή.
- Διαθεσιμότητα: Το σύστημα είναι διαθέσιμο για όσο διάστημα τρέχουν οι ελάχιστοι διακομιστές που απαιτούνται για την ολοκλήρωση της διαδικασίας της ψηφοφορίας δηλαδή, ένας κατανομέας ψήφων, t διαχειριστές και ένα ζεύγος ανώνυμης αρχής και καταμετρητή.
- Αντοχή σε Συμπαιγνία: Αυτή η απαίτηση εξαρτάται από τον αριθμό των διαχειριστών n και από τον ελάχιστο αριθμό υπογραφών t. Ένας ψηφοφόρος για να ψηφίσει χρειάζεται την συνεργασία t διαχειριστών.
- Επίσης, όλες οι επικοινωνίες στο σύστημα πραγματοποιούνται με τη χρήση SSL.

3.5 Wu And Sankaranarayana Protocol

Το 2002, οι Wu και Sankaranarayana πρότεινα ένα πρωτόκολλο ηλεκτρονικής ψηφοφορίας μέσω του Διαδικτύου για να μειώσουν το φαινόμενο της διπλής ψήφους από κάποιο ψηφοφόρο. Το πρωτόκολλο έχει δύο μόνο αρχές: τον καταχωρητή και τον μετρητή και η διαδικασία της ψηφοφορίας διακρίνεται σε δύο φάσεις, την διαδικασία της εγγραφής και την διαδικασία της ψηφοφορίας. Κατά τη διαδικασία της εγγραφής, οι εγγεγραμμένοι ψηφοφόροι παραχωρούν τα κατάλληλα αναγνωριστικά στην αρχή καταχώρησης που αποδεικνύουν την

ταυτότητα τους και τους παραχωρείται πιστοποιητικό ψηφοφορίας. Σε κάθε νόμιμο ψηφοφόρο του παραχωρείται μόνο ένα πιστοποιητικό ψηφοφορίας. Η αρχή καταχώρησης διατηρεί μία λίστα με τους εγγεγραμμένους ψηφοφόρους και τα αντίστοιχα πιστοποιητικά ψηφοφορίας. Κατά τη διαδικασία της ψηφοφορίας, ο ψηφοφόρος που επιθυμεί να ασκήσει το εκλογικό του δικαίωμα, επιλέγει τον υποψήφιο που επιθυμεί και ένα αριθμό έκδοσης και τα κρυπτογραφεί με το πιστοποιητικό ψηφοφορίας που του έχει παραχωρηθεί από την αρχή καταχώρησης και τα αποστέλλει στον καταμετρητή. Σε περίπτωση που ένας ψηφοφόρος επιθυμεί να αλλάξει τη ψήφο του, χρησιμοποιεί το πιστοποιητικό που του έχει παραχωρηθεί από την αρχή καταχώρησης για να κρυπτογραφήσει τον αριθμό υποψήφιου και τον καινούριο αριθμό έκδοσης που είναι μεγαλύτερος από την προηγούμενη έκδοση που έχει χρησιμοποιήσει προηγουμένως. Μετά τη λήξη της διαδικασία ψηφοφορίας, δεν επιτρέπεται οποιασδήποτε ψηφοφόρος να ψηφίσει. Εν συνεχεία εντοπίζονται οι πολλαπλές ψήφοι για κάθε ψηφοφόρο και με βάση τον αριθμό έκδοσης παραμένει η τελευταία ψήφος με το μεγαλύτερο αριθμός έκδοσης, ενώ οι υπόλοιπες ψήφοι για το συγκεκριμένο ψηφοφόρο διαγράφονται. Η διαδικασία πραγματοποιείται για όλους τους ψηφοφόρους και έπειτα πραγματοποιείται η καταμέτρηση των ψήφων.

Στο πρωτόκολλο εγκυμονεί ο κίνδυνος συνωμοσίας των δύο αρχών, του καταχωρητή και του μετρητή, παραβιάζοντας την ανωνυμία του ψηφοφόρου. Ο καταχωρητής έχει στη διάθεση του μία λίστα με τους εγγεγραμμένους ψηφοφόρους και τα αντίστοιχα πιστοποιητικά ψηφοφορίας, ενώ ο καταχωρητής έχει στη διάθεση του τις ψήφους του ψηφοφόρου μαζί με τους αριθμούς εκδόσεων και τα αντίστοιχα πιστοποιητικά.

3.6 A Novel Simple Secure Internet Voting Protocol

Οι Kumar, Sahay και Hegde πρότειναν ένα πρωτόκολλο ηλεκτρονικής ψηφοφορίας μέσω του Διαδικτύου. Το πρωτόκολλο ηλεκτρονικής ψηφοφορίας περιέχει τέσσερις φάσεις: εγγραφή, ψηφοφορία, επαλήθευση και καταμέτρηση. Η κάθε φάση διαχειρίζεται από ξεχωριστή αρχή, η οποία έχει την δική της βάση δεδομένων για να αποθηκεύει πληροφορίες αναφορικά με τους ψηφοφόρους. Οι τέσσερις αρχές του πρωτοκόλλου είναι ο καταχωρητής, η αρχή αυθεντικοποίησης, η αρχή ψηφοφορίας και τέλος ο μετρητής.

Πριν την έναρξη της ψηφοφορίας εγκαθιδρύονται τα ακόλουθα κλειδιά μεταξύ των αρχών:

- Πρώτο Κλειδί: μεταξύ του καταχωρητή και της αρχής ψηφοφορίας,
- Δεύτερο Κλειδί: μεταξύ της αρχής ψηφοφορίας και της αρχής αυθεντικοποίησης.
- Τρίτο Κλειδί: μεταξύ του καταχωρητή και της αρχής αυθεντικοποίησης.

Επίσης, υπάρχει μια μεταβλητή που υποδηλώνει αν ο ψηφοφόρος έχει ψηφίσει ή όχι.

Ο ψηφοφόρος κατά τη διαδικασία της εγγραφής παραχωρεί τα κατάλληλα αναγνωριστικά που πιστοποιούν την ταυτότητα του και ο καταχωρητής τα επαληθεύει. Στην περίπτωση που ο ψηφοφόρος είναι ένας εγγεγραμμένος ψηφοφόρος, δημιουργούνται δυο τυχαίοι κωδικοί. Χρησιμοποιώντας μια μονόδρομη συνάρτηση κατατεμαχισμού με παράμετρο τους δύο κωδικούς δημιουργείται ένας τρίτος κωδικός. Στην βάση του καταχωρητή, διατηρείται μία λίστα που περιέχει το όνομα του κάθε ψηφοφόρου μαζί με τους αντίστοιχους δύο κωδικούς, κωδικός ένα και κωδικός δύο. Εν συνεχεία, η αρχής καταχώρησης αποστέλλει τον πρώτο κωδικό στο ψηφοφόρο με τη χρήση του ηλεκτρονικού ταχυδρομείου, τον πρώτο και τον τρίτο κωδικό κρυπτογραφημένα με τη χρήση του πρώτου κλειδιού στην αρχή ψηφοφορίας και τέλος αποστέλλει το δεύτερο και τρίτο κωδικό κρυπτογραφημένα με την χρήση του τρίτου κλειδιού στην αρχή αυθεντικοποίησης.

Εν συνεχεία πραγματοποιείται η διαδικασία της ψηφοφορίας κατά την οποία ο ψηφοφόρος χρησιμοποιεί τον πρώτο κωδικό που έχει παραλάβει από την αρχή καταχώρησης για να ψηφίσει τον υποψήφιο που επιθυμεί. Στη βάση της αρχής ψηφοφορίας αποθηκεύονται ο πρώτος και τρίτος κωδικός για κάθε ψηφοφόρο μαζί με την ψήφο, τα οποία αποστέλλονται από το ψηφοφόρο. Η ψήφος κρυπτογραφείται με το δημόσιο κλειδί της ψηφοφορίας και ενώνεται με το πρώτο και το τρίτο κλειδί και εν συνεχεία κρυπτογραφείται με το δεύτερο κλειδί. και αποστέλλεται στην αρχή αυθεντικοποίησης.

Η αρχή αυθεντικοποίησης αποκρυπτογραφεί με τη χρήση του δεύτερου κλειδιού το κρυπτογραφημένο πακέτο που παρέλαβε από την αρχή ψηφοφορίας. Με τη βοήθεια του τρίτου κωδικού, η αρχή αυθεντικοποίησης ανακτά το δεύτερο κωδικό και το κρυπτογραφεί με τη χρήση του τρίτου κλειδιού. Η αρχή καταχώρησης αποκρυπτογραφεί το μήνυμα που παρέλαβε και ανακτά το δεύτερο κλειδί. Εν συνεχεία, η αρχή καταχώρησης διερευνά από τη βάση του το πρώτο κωδικό για το αντίστοιχο δεύτερο κωδικό του ψηφοφόρου, το κρυπτογραφεί με το τρίτο κλειδί και το στέλλει στην αρχή ταυτοποιήσης. Εν συνεχεία, η αρχή πιστοποίησης συγκρίνει το πρώτο κωδικό που παρέλαβε από τον καταχωρητή και από την αρχή ψηφοφορίας. Εάν οι κωδικοί είναι οι ίδιοι, τότε η ταυτότητα του ψηφοφόρου εγκρίνεται ως έγκυρη. Έπειτα διερευνάται αν ο ψηφοφόρος έχει ψηφίσει ξανά, μέσω της μεταβλητής που υποδηλώνει αν έχει ψηφίσει. Στην περίπτωση που δεν έχει ξαναψηφίσει τροποποιούμε αυτή τη μεταβλητή και αποστέλλουμε την κρυπτογραφημένη ψήφο στον μετρητή.

Ο μετρητής μετά το λήξη της διαδικασίας της ψηφοφορίας αποκρυπτογραφεί κάθε κρυπτογραφημένη ψήφο μέσω του ιδιωτικού κλειδιού της ψηφοφορίας, καταμετρά τις ψήφους και ανακοινώνει το αποτέλεσμα των εκλογών στο κοινό.

Κεφάλαιο 4

Πρωτόκολλο Ψηφοφορίας βασισμένο στο IIS

4.1 Πρωτόκολλο IIS 39

4.1.1 Φάση Εγγραφής 41

4.1.2 Φάση Ψηφοφορίας 43

4.1.3 Φάση Καταμέτρησης 45

4.2 Αξιολόγηση Πρωτοκόλλου 49

4.3 Βασικές Τεχνικές που χρησιμοποιούνται στο Πρωτόκολλο 51

Στο προηγούμενο κεφάλαιο κάναμε μία εκτενής μελέτη προτεινόμενων πρωτοκόλλων ηλεκτρονικής ψηφοφορίας μέσω του Διαδικτύου. Στο παρόν κεφάλαιο θα εστιάσουμε την προσοχή μας στο πρωτόκολλο ISS [14], το οποίο είναι το πρωτόκολλο που έχει επιλογή για υλοποίηση. Το πρωτόκολλο αυτό μας κίνησε το ενδιαφέρον από τα προαναφερόμενα πρωτόκολλα του προηγούμενου κεφαλαίου μιας και μας εντυπωσίασε η λειτουργία του καθώς επίσης τα πλεονεκτήματα που παρουσίασε έναντι άλλων πρωτοκόλλων.

Στο παρόν κεφάλαιο θα αναφέρουμε τους λόγους που επιλέξαμε το πρωτόκολλο τόσο για μελέτη όσο και για υλοποίηση του και αναλύουμε εκτενώς τη λειτουργία του παραθέτοντας παραδείγματα και επεξηγήσεις. Εν συνεχεία παρατίθεται μία αξιολόγηση του πρωτοκόλλου και οι βασικές τεχνικές που χρησιμοποιούνται στο πρωτόκολλο.

4.1 Πρωτόκολλο IIS

Έχουμε επιλέξει το πρωτόκολλο αυτό, λόγω του ότι δίνεται η δυνατότητα αναίρεσης της ψήφου στο ψηφοφόρο κάτι που δεν προσφέρεται από τα υπόλοιπα, ή στην περίπτωση που

προσφέρεται, αυτό δεν γίνεται αποδοτικά.. Έτσι διασφαλίζεται ότι ο ψηφοφόρος, θα ψηφίσει τον υποψήφιο που επιθυμεί, αφού δεν τίθεται θέμα πώλησης των ψήφων.

Επίσης το πρωτόκολλο αυτό είναι πολύ ανθεκτικό στις επιθέσεις, καθώς δεν χρειάζονται όλοι οι εξυπηρετητές για να λειτουργήσει η διαδικασία της ψηφοφορίας και της καταμέτρησης ορθά. Σε περίπτωση που κάποιοι δεχθούν επίθεση DDOS, ή για κάποιο λόγο δεν είναι προσβάσιμοι, δεν επηρεάζονται καθόλου καμία εκ των δύο πιο πάνω διαδικασιών.

Ακόμη ένα πολύ σημαντικό πλεονέκτημα του πρωτοκόλλου αυτού, είναι το γεγονός, ότι σε καμία περίπτωση δεν μπορεί να συσχετιστεί μία ψήφος με τον υποψήφιο που την υπέβαλε. Αυτό αποτελεί ένα πολύ σημαντικό θέμα σε μια ηλεκτρονική ψηφοφορία, καθώς αρκετά άτομα ίσως να πιστεύουν ότι τα ηλεκτρονικά συστήματα θα αποκαλύψουν τους ψήφους τους σε άλλους.

Σε προσπάθεια απάτης από τους εμπλεκόμενους εξυπηρετητές, μπορούμε να βρούμε με μαθηματικό τρόπο ο οποίος περιγράφεται στο πρωτόκολλο, από ποιον έχει γίνει απόπειρα για απάτη. Οι λόγοι αυτοί, είναι αρκετοί, και ιδιαίτερα σημαντικοί, και ικανοί για να μας ωθήσουν στο να επιλέξουμε το πρωτόκολλο αυτό, έναντι άλλων πρωτοκόλλων.

Επίσης, το πρωτόκολλο το οποίο έχουμε επιλέξει, παρουσιάζει μια μέθοδο ψηφοφορίας, η οποία διαφέρει από τα υπόλοιπα πρωτόκολλα. Χρησιμοποιεί μια έμμεση αρχιτεκτονική ασφάλειας δεδομένων (Implicit data security architecture). Αυτή η έμμεση ασφάλεια δεδομένων, μας κίνησε το ενδιαφέρον. Όπως υποδηλώνει και το όνομα της, η λέξη έμμεσος προσδιορίζει ότι δεν έχουν χρησιμοποιηθεί άμεσα κάποια κλειδιά κρυπτογράφησης κατά τη διαδικασία της ψηφοφορίας, αλλά τα δεδομένα αποθηκεύονται με τέτοιο τρόπο ούτως ώστε κάθε κομμάτι έμμεσα διασφαλίζεται ότι είναι ασφαλές.

Θα ξεκινήσουμε τη μελέτη μας για το πρωτόκολλο IIS, με μία συνοπτική περιγραφή.

Ο ψηφοφόρος επικοινωνεί με την αρχή η οποία είναι υπεύθυνη για την εγγραφή ενός ψηφοφόρου χρησιμοποιώντας την αληθινή του ταυτότητα. Ο ψηφοφόρος παράγει ένα τυχαίο αριθμό και τον τυφλώνει και τον παίρνει πίσω υπογεγραμμένο από τον καταχωρητή. Όταν παραλάβει τον υπογεγραμμένο αριθμό απομακρύνει τον παράγοντα τύφλωσης και τον χρησιμοποιεί ως το ανώνυμο αριθμό του. Ως εκ τούτου, για να ψηφίσει ο ψηφοφόρος δεν τυφλώνει την ψήφο του αλλά χρησιμοποιεί την ανώνυμη ταυτότητα του για να ψηφίσει. Παρόλα αυτά για να προστατεύσει τα αποτελέσματα των εκλογών ,ο ψηφοφόρος διαχωρίζει

την ψήφο του σε πολλά κομμάτια και τα στέλνει σε διαφορετικούς διακομιστές. Αυτό παρέχει μια ασφαλή κατανεμημένη αρχιτεκτονική.

Προτού να διαχωρίσει την ψήφο σε κομμάτια, ο ψηφοφόρος κωδικοποιεί ορισμένες απόρρητες πληροφορίες μέσα στα κομμάτια της ψήφους και διανέμει μία μονόδρομη συνάρτηση κατακερματισμού της απόρρητης πληροφορίας στους διακομιστές μαζί με τα κομμάτια από την ψήφο.

Παρουσιάζεται μια διαδικασία η οποία διαμοιράζει τις ψήφους σε κομμάτια έτσι ώστε η επιπρόσθετη πληροφορία να μπορεί να είναι κρυμμένη μέσα στα κομμάτια. Αυτές οι κρυμμένες πληροφορίες μπορεί να χρησιμοποιηθούν για την επικύρωση των κομματιών κατά την φάση της μέτρησης των ψήφων. Επιπρόσθετα, οι επιπρόσθετες πληροφορίες δεν αυξάνουν την αλγοριθμική πολυπλοκότητα του συστήματος που χρησιμοποιείται.

Το πρωτόκολλο αυτό ξεκινά και οι χρήστες έχουν τις πραγματικές τους ταυτότητες

Η φάση της εγγραφής στην βάση δεδομένων πραγματοποιείται κάποιο χρονικό διάστημα πριν από την έναρξη της ψηφοφορίας. Οι ψηφοφόροι καλούνται να παρουσιάσουν κάποια προσωπικά στοιχεία τους ούτως ώστε να διερευνηθεί αν έχουν την δυνατότητα να ψηφίσουν και τους παραχωρείται μία ταυτότητα. Συνήθως, η ταυτότητα που χρησιμοποιείται στα συστήματα ψηφοφορία είναι η πολιτική ταυτότητα.

Πρωτού προχωρήσουμε σε μία εκτενέστερη αναφορά των λειτουργιών του πρωτοκόλλου, θα ορίσουμε κάποιες μεταβλητές που χρησιμοποιούνται ευρέως από το πρωτόκολλο και παρατίθενται πιο κάτω:

- p : Πρώτος αριθμός και είναι δημόσιος γνωστός [26].
- g : Πρωταρχική ρίζα (primitive root) και είναι δημόσια γνωστή.
- g^x : Το δημόσιο κλειδί του καταχωρητή.
- x: Το ιδιωτικό κλειδί του καταχωρητή.
- h(.): Μονόδρομη Συνάρτηση Κατατεμαχισμού.
- n: Ο αριθμός των διακομιστών του συστήματος.
- k: Ο ελάχιστος αριθμός διακομιστών που απαιτούνται για την ανασυγκρότηση της ψήφου και της μυστικής λέξης.
- m^x: Η υπογραφή στο μήνυμα m, όπου $1<m< p-1$.
- ri_d: Ανώνυμη ταυτότητα του ψηφοφόρου.
- V_{id}: Πραγματική ταυτότητα του ψηφοφόρου.
- M: Μυστική λέξη που καταχωρεί ο ψηφοφόρος κατά τη διαδικασία της ψηφοφορίας.

4.1.1 Φάση Εγγραφής

Ο ψηφοφόρος δίνει μία λέξη στο σύστημα που αν στην συνέχεια εγκριθεί από τον καταχωρητή θα αποτελεί την ανώνυμη ταυτότητα (r_{id}) του ψηφοφόρου. Εν συνεχεία, επιλέγεται τυχαία και ομοιόμορφα από το σύστημα ένας αριθμός ο οποίος θα δράσει ως παράγοντα τύφλωσης (b).

Στην περίπτωση αυτή ο κώδικας θα ήταν συνετό να είναι open source ούτως ώστε να διασφαλίζεται ότι δεν θα υπάρξει απάτη, για παράδειγμα ο αριθμός που θα προκύπτει να είναι προκαθορισμένος. Για αυτό πρέπει να διασφαλίζεται η τυχαιότητα και η μυστικότητα του αριθμού κάθε φορά.

Αμέσως μετά κρυπτογραφείται η ανώνυμη ταυτότητα με την πιο κάτω μαθηματική πράξη: $υ = r_{id}\ g^b \bmod p$, και αποστέλλεται μαζί με την πραγματική ταυτότητα του ψηφοφόρου (V_{id}) και το αποτέλεσμα της συνάρτησης κατακερματισμού που παίρνει σαν παράμετρο τη ανώνυμη ταυτότητα του ψηφοφόρου $h(r_{id})$. Δηλαδή, αποστέλλονται στον καταχωρητή τα ακόλουθα: υ, V_{id}, $h(r_{id})$.

Ο καταχωρητής καλείται να ελέγξει αν ο ψηφοφόρος έχει δυνατότητα να ψηφίσει. Η διαδικασία του ελέγχου αποτελεί κομβικό σημείο για το σύστημα μας μιας και κρίνεται η ορθότητα των αποτελεσμάτων μέσω του σωστού ελέγχου των ατόμων που έχουν δυνατότητα να ασκήσουν το εκλογικό τους δικαίωμα στην συγκεκριμένη ψηφοφορία.

Συγκεκριμένα, εξετάζει αν η πραγματική ταυτότητα που του στάλθηκε παρουσιάζεται στη βάση δεδομένων με τους εγγεγραμμένους χρήστες. Στην περίπτωση που διασφαλιστεί η νομιμότητα του ψηφοφόρου, διεξάγεται ένας δεύτερος έλεγχος που αφορά την ανώνυμη ταυτότητα που έχει δώσει ο ψηφοφόρος.

Διερευνάται αν εμφανίζεται το $h(r_{id})$ στην λίστα L του καταχωρητή.

Η λίστα L είναι μία λίστα που διατηρεί ο καταχωρητής και εμπεριέχει όλες τις μονόδρομες συναρτήσεις κατακερματισμού που έχουν χρησιμοποιηθεί ούτως ώστε να αποφευχθούν συγκρούσεις μεταξύ των ανώνυμων ταυτοτήτων. Οι ανώνυμες ταυτότητες είναι μοναδικές, κάθε ανώνυμη ταυτότητα αντιστοιχεί σε ένα και μόνο ψηφοφόρο.

Διαφορετικά, στέλνεται μήνυμα στο ψηφοφόρο που τον ενημερώνει ότι η πραγματική ταυτότητα που έχει δοθεί δεν είναι υπαρκτή και ζητάει από το χρήστη να επαναλάβει την διαδικασία.

Στην περίπτωση που το $h(r_{id})$ εμφανίζεται στην λίστα, ο καταχωρητής ζητά από τον ψηφοφόρο να επαναλάβει την διαδικασία δημιουργίας ανώνυμης ταυτότητας και την αποστολή των τριών του στοιχείων. Στην αντίθετη περίπτωση που ο κατακερματισμός δεν υφίσταται, ο καταχωρητής προσθέτει το h(rid) του ψηφοφόρου στη λίστα L και υπογράφει με το ιδιωτικό του κλειδί (x) την κρυπτογραφημένη ανώνυμη ταυτότητα του ψηφοφόρου(u). Εν συνεχεία, το αποστέλλει στο ψηφοφόρο(δηλαδή αποστέλλεται το u^x) .

Ο ψηφοφόρος παραλαμβάνει το υπογεγραμμένο r_{id} ως ακολούθως:

Χρησιμοποιώντας το δημόσιο κλειδί του καταχωρητή υπολογίζει το $v=(g^x)^b \bmod p$ και ακολούθως υπολογίζει τον αντίστροφο του v.

Έπειτα υπολογίζει το $r=u^x *(v^{-1})=(r_{id})^x \bmod p$

Ο ψηφοφόρος τυχαία και ομοιόμορφα επιλέγει ένα εκθετικό c και παράγει:

$D=((rid)^x *g^x)^c$ και το αποστέλλει στον καταχωρητή.

Ο καταχωρητής του αποστέλλει πίσω το $e=d^{(1/x)}$.

Η φάση της εγγραφής ολοκληρώνεται με τον έλεγχο που πραγματοποιεί ο ψηφοφόρος, διερευνώντας αν είναι ίσα το $(rid*g)^c$ είναι το ίδιο με e. Σε περίπτωση ισότητας, πιστοποιείται το rid^x και η υπογραφή είναι έγκυρη και αποδεκτή.

4.1.2 Φάση Ψηφοφορίας

Ο ψηφοφόρος επικοινωνεί με το Online Εκλογικό Κέντρο χρησιμοποιώντας μία ασφαλή σύνδεση (SSL) μέσω του Διαδικτύου και στέλνει την υπογραμμένη ανώνυμη ταυτότητα και την ανώνυμη ταυτότητα.

Το Online Εκλογικό Κέντρο επαληθεύει την εγκυρότητα της ανώνυμης ταυτότητας του ψηφοφόρου επικοινωνώντας μέσω ενός zero-knowledge challenge/response protocol με τον καταχωρητή για να επαληθεύσει την υπογραφή στην ανώνυμη ταυτότητα και συνεπώς την νομιμότητα του ψηφοφόρου στις εκλογές.

Στην περίπτωση που η υπογραφή είναι έγκυρη, το Online Εκλογικό Κέντρο αποθηκεύει την ανώνυμη ταυτότητα του ψηφοφόρου και παρέχει στον ψηφοφόρο ένα μυστικό κλειδί συνόδου ούτως ώστε να το χρησιμοποιήσει για να ψηφίσει επικοινωνώντας με τους n διακομιστές.

Το σύστημα ζητάει από τον χρήστη να εισαγάγει μία λέξη η οποία να εμπεριέχει έξι γράμματα, η οποία θα διασπαστεί μαζί με την ψήφο στους διακομιστές του συστήματος.

Ο ψηφοφόρος επιλέγει τον υποψήφιο που επιθυμεί.

Εν συνεχεία, πραγματοποιείται μια αναδρομική διαδικασία για την κατάτμηση της ψήφου και της μυστικής λέξης σε n κομμάτια. Κάθε κομμάτι στέλνεται σε ένα διαφορετικό διακομιστή. Αυτό παρέχει μια κατανεμημένη ασφαλή αρχιτεκτονική. Διασφαλίζεται ότι σε περίπτωση που κάποια κομμάτια χαθούν, δεν θα χαθεί ολόκληρη η ψήφος.

Πιο κάτω παρουσιάζουμε τον αλγόριθμο που χρησιμοποιείται για την διάσπαση της ψήφους ψήφου και της μυστικής λέξης σε n κομμάτια.

Algorithm DealingPhase (V, M, k, n), όπου V είναι η ψήφος, M είναι η μυστική λέξη που δίνει ο ψηφοφόρος και τέλος k, n είναι ακέραιοι αριθμοί που αντιπροσωπεύουν τους διακομιστές του συστήματος.

1. Διαμοιρασμός της μυστικής λέξης που έχει δώσει ο ψηφοφόρος σε k-2 κομμάτια: $m_1, m_{2,\dots,} m_{k-2} \in \mathbb{Z}_p$ τέτοια ώστε η συνένωση των m_i κομματιών, να αναπαριστούν το M.
2. Τυχαία και ομοιόμορφα επιλέγεται από το σύστημα ένας αριθμός r_1 και υπολογίζεται $r_{2=} m_1 (r_1)^{-1} \bmod p$
3. Από i=2 μέχρι k-2

   Υπολογίζουμε $r_{i+1} = m_i * \left(\prod_{j=1}^{i} r_j\right)^{-1} \bmod p$.
4. Ορίζω τα r_i ως σημεία (i, r_i) έτσι ώστε, $1 < i < k - 1$.
5. Ορίζω την ψήφο V ως το σημείο $(0, V)$.
6. Δημιουργώ το πολυώνυμο f(x) χρησιμοποιώντας τα σημεία $(0, V)$ και $(i, r_i), 1 \leq i \leq k - 1$.

   Η παραγωγή πολυωνυμικής εξίσωσης από τα δοθέντα σημεία σημεία (0,V) και (i,r_i), θα πραγματοποιηθεί με τη βοήθεια του Lagrange Polynomial .
7. Αντικατάσταση n τιμών στην πολυωνυμική εξίσωση $f(x)$.

   $D_i = f(x)$ όπου $x = k, k + 1, k + 2, \dots, (k + n - 1)$ $και$. $1 \leq i \leq n$.
8. Το αποτέλεσμα της αλγορίθμου είναι$(i + k - 1, Di)$, $1 \leq i \leq n$.

Ας εξετάσουμε ένα παράδειγμα, ούτως ώστε να γίνει κατανοητή η διαδικασία της ψηφοφορίας:

Έστω ότι ο ψηφοφόρος έχει στη διάθεση του οκτώ διακομιστές για να ασκήσει το εκλογικό του δικαίωμα. Στην υλοποίηση του συστήματος, αναπαριστούμε τους πολλαπλούς διακομιστές με πολλαπλές βάσεις που τρέχουν στην ίδια μηχανή. Ας προσδιορίσουμε ότι ο ελάχιστος αριθμός διακομιστών οι οποίοι πρέπει να παραμείνουν ασφαλείς ούτως ώστε στη διαδικασία της συνένωσης, να συνεργαστούν για να ανακατασκευάσουν την ψήφο ορθά είναι πέντε και ο πρώτος αριθμός (p) ο οποίος επιλέχθηκε είναι ο αριθμός 257. Ο κάθε υποψήφιος, αντιπροσωπεύεται με ένα αριθμό. Ο ψηφοφόρος αφού επιλέξει τον υποψήφιο που επιθυμεί θα πρέπει ο αριθμός αυτός, να κατανεμηθεί στους διακομιστές και για να διασφαλίσουμε αυθεντικοποίση ζητούμε από το ψηφοφόρο να καταχωρήσει μία μυστική λέξη. Ο ψηφοφόρος στο παράδειγμα, επιθυμεί να ψηφίσει τον υποψήφιο με τον μοναδικό αριθμό 157 και η μυστική λέξη που καταχωρεί είναι η λέξη “USA”. Το σύστημα λαμβάνει ως είσοδο την λέξη του ψηφοφόρου και παράγει την αντίστοιχη ASCII συμβολοσειρά, η οποία είναι 85,83,65.

Με βάση τις πιο πάνω προυποθέσεις και σύμφωνα με τον αλγόριθμο διάσπασης που περιγράψαμε θα πραγματοποιηθούν τα ακόλουθα βήματα:

1. Η μυστική λέξη που καταχωρεί ο ψηφοφόρος διαιρείται σε τρία κομμάτια, τέτοια ώστε

   m_1=85, m_2 =83, m_3=65.
2. Τυχαία και ομοιόμορφα επιλέγεται ένας αριθμός ,r_1 =101.

   Υπολογίζεται το r_2,

$$r_{2\equiv} m_1 {r_1}^{-1} \equiv 85(101)^{-1} \equiv 85 * 28 \equiv 67\ mod\ 257$$

3. Υπολογίζεται το r_3,

$$r_{3\equiv} m_2 (r_1 * r_2)^{-1} \equiv 83(101 * 67)^{-1} \equiv 83 * 127 \equiv 4\ mod\ 257$$

4. Υπολογίζεται το r_4,

$$r_{4\equiv} m_3 (r_1 * r_2 * r_3)^{-1} \equiv 65(101 * 67 * 4)^{-1} \equiv 65 * 96 \equiv 72\ mod\ 257$$

5. Ορίζουμε τα r_i ως σημεία

   $(1, r_1) = (1{,}101), (2, r_2) = (2{,}67), (3, r_3) = (3{,}4), (4, r_4) = (4{,}72)$
6. Ορίζουμε την ψήφο V ως σημείο $(0, V) = (0{,}157)$.
7. Δημιουργούμε το πολυώνυμο f(x) χρησιμοποιώντας τα σημεία (0,V) και (i, r_i) και με τη βοήθεια του Lagrange Polynomial, εντοπίζεται η ακόλουθη πολυωνυμική εξίσωση:

$$f(x) = 148x^4 + 3x^3 + 251x^2 + 56x + 157\ mod\ 257$$

8. Πραγματοποιούμε αντικαταστάσεις στο πολυώνυμο $f(x)$.

   $D_1 = f(5) = 128,\ D_2 = f(6) = 240,\ D_3 = f(7) = 173,\ D_4 = f(8) = 160,\ D_5 = f(9) = 131, D_6 = f(10) = 227, D_7 = f(11) = 29, D_8 = f(12) = 100.$
9. $(i + k - 1, Di), όπου\ k = 5\ και\ j = 1\ μέχρι\ το\ n.$.

4.1.3 Φάση Καταμέτρησης

Στη φάση της καταμέτρησης πραγματοποιείται η συνένωση και συνάμα η επικύρωση των κομματιών της ψήφους. Έχουμε υποθέσει ότι ο ελάχιστος αριθμός διακομιστών, οι οποίοι πρέπει να παραμείνουν ασφαλείς ούτως ώστε να συνεργαστούν για να ανακατασκευάσουν την ψήφο ορθά είναι πέντε.

Χρησιμοποιώντας τον αλγόριθμο συνένωσης που λαμβάνει ως είσοδο τα σημεία που προέκυψαν από την φάση της κατάτμησης, ανακατασκευάζουμε τα κομμάτια που απαρτίζουν την μυστική λέξη καθώς επίσης παράγουμε ένα καινούριο πολυώνυμο από τα δοθέντα σημεία. Εν συνεχεία, ενώνουμε τα κομμάτια για να πάρουμε την λέξη που προκύπτει από τον συνδυασμό των κομματιών. Υπολογίζουμε τη συνάρτηση κατατεμαχισμού με παράμετρο τη λέξη που προέκυψε και διεξάγουμε μία σύγκριση με το αποτέλεσμα της συνάρτησης κατατεμαχισμού με τη λέξη που καταχώρησε ο χρήστη. Στην περίπτωση που η διαδικασία της ψηφοφορίας κύλησε ομαλά, δηλαδή, δεν πραγματοποιήθηκε

οποιαδήποτε αλλοίωση στα κομμάτια που διανεμήθηκαν στους διακομιστές που απώτερο σκοπό θα είχε την αλλοίωση του τελικού αποτελέσματος, λαμβάνεται ο αριθμός της ψήφου για να υπολογιστεί στην καταμέτρηση. Διαφορετικά, διαπιστώνεται απάτη και ασφαλώς η ψήφος δεν θα ληφθεί υπόψη για καταμέτρηση.

Τα βήματα για τη διαδικασία της καταμέτρησης της ψήφου έχουν ως ακολούθως:

1. Εκτελούμε τον αλγόριθμο συνένωσης ούτως ώστε να πάρουμε καινούριο πολυώνυμο $f(x)'$ και τα κομμάτια για να ανακατασκευάσουμε τη μυστική λέξη.
2. Ενώνουμε τα κομμάτια m' που προέκυψαν από τον αλγόριθμό της συνένωσης. Το αποτέλεσμα της συνένωσης είναι μία λέξη M' που ευελπιστούμε ότι θα είναι ίδια με την λέξη M που ο ψηφοφόρος είχε καταχωρήσει. Για να το διερευνήσουμε, πράττουμε ως εξής:
3. Υπολογίζουμε τη συνάρτηση κατατεμαχισμού με παράμετρο τη λέξη που προέκυψε από τον αλγόριθμο συνένωσης $h(M')$.
4. Στην περίπτωση που το αποτέλεσμα $h(M')$ είναι ίσο με το αποτέλεσμα $h(M)$, τότε συμπεραίνουμε ότι τα κομμάτια είναι έγκυρα, δεν έχει πραγματοποιηθεί καμία αλλοίωση και οι πολυωνυμικές εξισώσεις $f(x')$ και $f(x)$ είναι ίσες.
5. Ανακτάται η ψήφος , $V = f'(0)$.

Παράδειγμα Φάσης Καταμέτρησης

Η φάση της καταμέτρησης πραγματοποιείται έπειτα από τη φάση της έγγραφής και της κατάτμησης και μετά από το κλείσιμο της ψηφοφορίας μιας και οι ψηφοφόροι έχουν το δικαίωμα να αλλάζουν την ψήφο τους, στην περίπτωση που το επιθυμούν.

Η ψήφος όπως έχουμε δει στην φάση της κατάτμησης, κομματιάζεται σε n κομμάτια και κάθε κομμάτι αποστέλλεται σε διαφορετικό διακομιστή. Εν συνεχεία του παραδείγματος που μόλις έχουμε περιγράψει, της διαδικασία της κατάτμησης, οι διακομιστές καλούνται να συνενώσουν τα κομμάτια τους για να ανακατασκευάσουν την ψήφο. Αφού έχουμε προσδιορίσει ότι μόνο πέντε κομμάτια χρειάζονται για να δημιουργηθεί ξανά η ψήφος, επιλέγουμε πέντε από αυτά. Έστω ότι τα κομμάτια που επιλέγονται είναι τα ακόλουθα:

$(6, D_2) = (6{,}240), \quad (7, D_3) = (7{,}173), \quad (9, D_5) = (9{,}131),$

$(11, D_7) = (11{,}29), \quad (12, D_8) = (12{,}100)$

Μέσω των πέντε αυτών σημείων θα διεξάγουμε τη φάση της συνένωσης που έχει ως εξής:

1. Δημιουργούμε το πολυώνυμο f(x) χρησιμοποιώντας τα σημεία και με τη βοήθεια του Lagrange Polynomial, εντοπίζεται η ακόλουθη πολυωνυμική εξίσωση:

$$f'(x) = 148x^4 + 3x^3 + 251x^2 + 56x + 157 \; mod \; 257$$

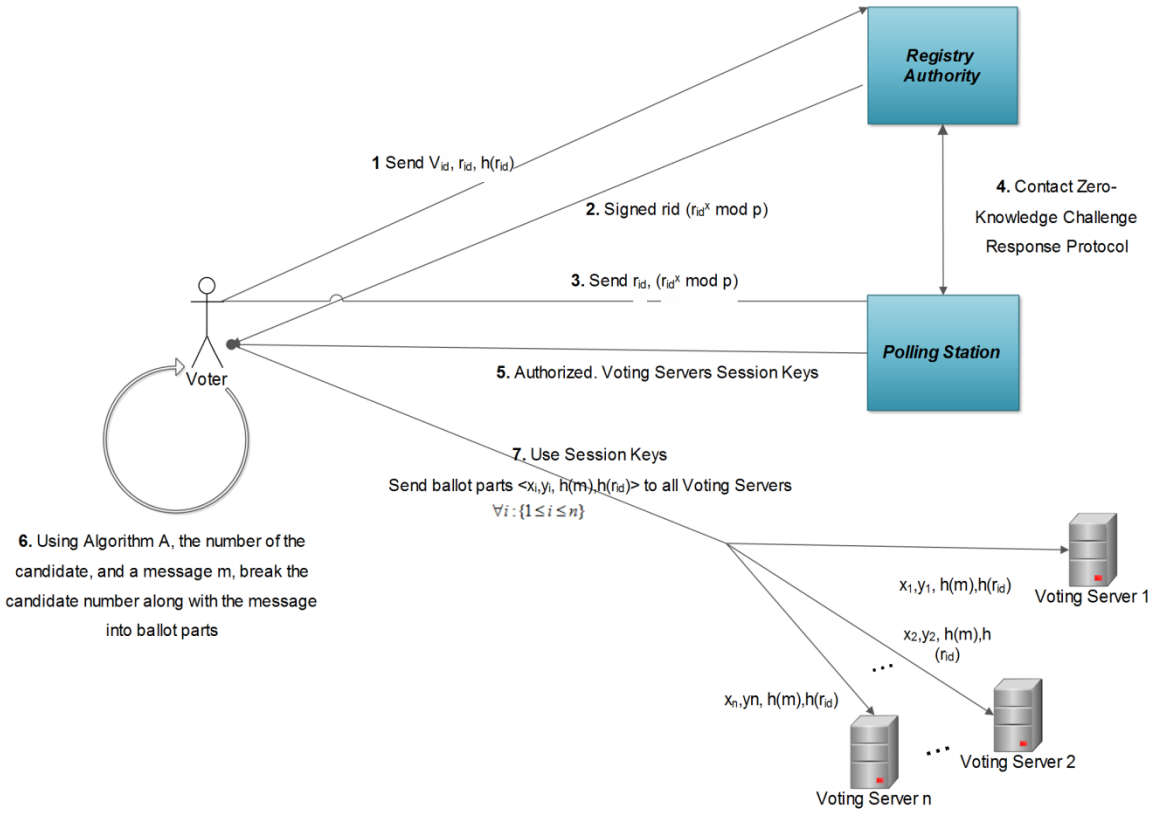
2. Αντικαθιστούμε στην εξίσωση $f'(x)$ το x με την τιμή μηδέν ούτως ώστε να ανακτήσουμε την τιμή της ψήφου, $V' = f'(0)$

   Να σημειωθεί ότι στην φάση της καταμέτρησης, η ψήφος συμβολίζεται με V' και όχι με V μιας και ακόμη δεν έχει διερευνηθεί αν η ψήφος είναι έγκυρη ή είναι μία αλλοιωμένη ψήφος.
3. Πραγματοποιούμε τέσσερις αντικαταστάσεις στο πολυώνυμο $f'(x)$ $για\ τιμές\ x =$ 1,2,3, .

   $r_1{}' = f'(2) = 101, r_2{}' = f'(2) = 67, r_3{}' = f'(3) = 4, r_4{}' = f'(4) = 72.$
4. Ανασχηματίζουμε τα κομμάτια που απαρτίζουν την μυστική λέξη με τον ακόλουθο τρόπο:
   a) $m_1{}' = r_1{}' r_2{}' = 85,$
   b) $m_2{}' = r_1{}' r_2{}' r_3{}' = 83,$
   c) $m_3{}' = r_1{}' r_2{}' r_3{}' r_4{}' = 65.$
5. Συνενώνουμε τα κομμάτια $m_1{}', m_2{}'$ και $m_3{}'$ ούτως ώστε να ανασχηματίσουμε τη λέξη M'.
6. Εκτιμούμε τη συνάρτηση κατατεμαχισμού που έχει σαν παράμετρο τη λέξη M', δηλαδή, H(M').
7. Διερευνούμε αν $h(M') = h(M)$. Στην περίπτωση που είναι ίσα, τότε τα κομμάτια είναι έγκυρα και συνεπώς ,V $(M') = V(M)$ και η ψήφος υπολογίζεται στην καταμέτρηση. Στην αντίθετη περίπτωση, έχει πραγματοποιηθεί αλλοίωση της ψήφους. Ασφαλώς η ψήφος δεν υπολογίζεται και διερευνάται η αιτία που της αλλοίωση της ψήφους.

Εν συνεχεία, θα παρουσιάσουμε μέσω ενός σχήματος την αρχιτεκτονική του πρωτοκόλλου.

Αρχιτεκτονική του πρωτοκόλλου



Το πιο πάνω σχεδιάγραμμα καθορίζει τον τρόπο επικοινωνίας των οντοτήτων μεταξύ τους και προσδιορίζει την σειρά της επικοινωνίας τους. Αναφέρονται επίσης, οι πληροφορίες που στέλνονται από την κάθε οντότητα σε κάποια άλλη και είναι οι ακόλουθες:

Βήμα 1: Ο ψηφοφόρος στέλνει το V_{id}, r_{id}, $h(r_{id})$ στον καταχωρητή.

Βήμα 2: Αυτό που παραλαμβάνει ο ψηφοφόρος στο τέλος της επικοινωνίας τους, είναι η υπογεγραμμένη ανώνυμη ταυτότητα του.

Βήμα 3: Ο ψηφοφόρος, αποστέλλει την ανώνυμη του ταυτότητα και την υπογεγραμμένη ανώνυμη του ταυτότητα στο σταθμό ψηφοφορίας.

Βήμα 4: Διεξάγεται το πρωτόκολλο Zero-Knowledge Challenge-Response μεταξύ του σταθμού ψηφοφορίας και του καταχωρητή, για να επαληθεύσει ο καταχωρητής την εγκυρότητα του r_{id}.

Βήμα 5: Αφού ο σταθμός ψηφοφορίας εγκρίνει την νομιμότητα του ψηφοφόρου, τον προμηθεύει με κλειδιά συνόδου για να επικοινωνήσει με τους εξυπηρετητές για να ψηφίσει.

Βήμα 6: Ο ψηφοφόρος καταχωρεί μία εξαφήφια μυστική λέξη m και επιλέγει τον υποψήφιο που επιθυμεί. Στη συνέχεια εκτελείται ο αλγόριθμος Α, για να διασπάσει τη μυστική λέξη και τον αριθμό του υποψηφίου σε n σημεία (x,y).
Βήμα 7: Ο ψηφοφόρος χρησιμοποιεί τα κλειδιά συνόδου για να επικοινωνήσει με όλους τους εξυπηρετητές ψηφοφορίας. Στέλνει στον κάθε ένα εξυπηρετητή, ένα διαφορετικό σημείο (x,y) από τα n σημεία που δημιούργησε, καθώς επίσης τη σύνοψη του μηνύματος m και τη σύνοψη της ανώνυμης ταυτότητάς του. Δηλαδή ο κάθε ένας από τους εξυπηρετητές ψηφοφορίας j, στο τέλος της διαδικασίας αυτής παίρνει από τον ψηφοφόρο τα δεδομένα $(x_j,f(x_j),h(m),h(r_{id}))$ όπου $1\leq j \leq n$.

4.2 Αξιολόγηση Πρωτοκόλλου

Απαιτήσεις Συστήματος Ηλεκτρονικής Ψηφοφορίας που πληρούνται

Ασφαλές

Ένα σύστημα είναι ασφαλές αν είναι δημοκρατικό ,ακριβές , μυστικό, προστατευμένο από καταναγκασμό, οικουμενικά επαληθεύσιμο, ανθεκτικό.

- **Δημοκρατικό (Democratic) :** Το πρωτόκολλο IIS κατά την φάση της εγγραφής πραγματοποιεί έλεγχο για να εντοπίσει ποια είναι τα εγγεγραμμένα μέλη και παρέχει δυνατότητα ψηφοφορίας μόνο στα άτομα που είναι εγγεγραμμένα για την συγκεκριμένη ψηφοφορία. Συγκεκριμένα, ζητείται από τον ψηφοφόρο να στείλει την πραγματική του ταυτότητα στον καταχωρητή. Ο καταχωρητής με βάση την ταυτότητα διερευνά κατά πόσο η ταυτότητα αυτή υφίσταται στην λίστα με τους εγγεγραμμένους ψηφοφόρους.

  Στην περίπτωση που ένας εγγεγραμμένος ψηφοφόρος δεν πραγματοποιήσει το στάδιο της εγγραφής και κατευθυνθεί απευθείας στο στάδιο της ψηφοφορίας τότε χρειάζεται να παράξει ένα τυχαίο αριθμό και εν συνεχεία να πλαστογραφήσει την υπογραφή του καταχωρητή που αυτό είναι υπολογιστικά ανέφικτο για να την αποστείλει στο online polling station. Σε αυτό το σημείο ,το polling station θα επικοινωνήσει με τον καταχωρητή για να διερευνήσει αν το συγκεκριμένο rid υφίσταται.

  Για κάθε εγγεγραμμένο ψηφοφόρο εκδίδεται μόνο ένα rid. Στην περίπτωση που ένας εγγεγραμμένος ψηφοφόρος επιχειρήσει να ψηφίσει περισσότερο από μία φορές, τότε οι διακομιστές θα αντικαταστήσουν την παλαιά ψήφο με το συγκεκριμένο rid με την

καινούρια. Έτσι πραγματοποιείται έλεγχος από τους διακομιστές με βάση το rid κάθε φορά που εισέρχεται μία ψήφος, για να εντοπιστεί αν ο ψηφοφόρος έχει ψηφίσει ξανά ούτως ώστε να αντικαταστήσει την παλιά ψήφο με την καινούρια με βάση το rid του ψηφοφόρου.

- **Ακριβές (Accurate):** Κατά την διαδικασία της ψηφοφορίας, η ψήφος κατατμίζεται στους διακομιστές του συστήματος. Επίσης, ο ψηφοφόρος καλείται να δώσει ένα μυστικό μήνυμα το οποίο κατατμίζεται και αυτό στους διακομιστές.

  Κατά την φάση της καταμέτρησης , τα κομμάτια της ψήφους συνενώνονται και διερευνάται αν η συνάρτηση κατακερματισμού που εμπεριέχει το μυστικό μήνυμα που προέκυψε κατά την διαδικασία της συνένωσης είναι η ίδια με την συνάρτηση κατακερματισμού με το μυστικό μήνυμα που έδωσε ο χρήστης κατά την διαδικασία της ψηφοφορίας.
  Επίσης, η διαδικασία της ψηφοφορίας πραγματοποιείται με την χρήση SSL ούτως ώστε να διασφαλίζεται η ακεραιότητα και η μυστικότητα των δεδομένων. Επιπρόσθετα, κατά την διαδικασία της ψηφοφορίας η ψήφος κατατμίζεται σε n διακομιστές, k διακομιστές από αυτούς πρέπει να παραμένουν ασφαλείς για να ανασχηματίσουν την ψήφο. Σε περίπτωση που κάποιος από τους διακομιστές τεθεί εκτός λειτουργίας τότε δεν εγκυμονεί κίνδυνος να χαθεί η ψήφος.
- **Μυστικό(Secret) :** Ο καταχωρητής έχει μία λίστα με τις πραγματικές ταυτότητες των ψηφοφόρων ούτως ώστε να είναι σε θέσει να ελέγχει αν ένας ψηφοφόρος έχει την δυνατότητα να ψηφίσει. Επίσης, έχει μία λίστα με τις συναρτήσεις κατακερματισμού για τους τυχαίους αριθμούς. Το polling station έχει μία λίστα με τις ανώνυμες ταυτότητες των ψηφοφόρων. Ακόμη και σε περίπτωση συνεργασίας μεταξύ του καταχωρητή και του polling station δεν είναι δυνατό η σύνδεση της ψήφου με τον ψηφοφόρο μιας και ο καταχωρητής δεν συνδέει το h(rid) με κάποιο ψηφοφόρο.
- **Προστατευμένο από Καταναγκασμό (Uncoercible) :** Μετά την υποβολή της ψήφου δεν εμφανίζεται στο χρήστη τι έχει ψηφίσει, κάποιο είδος απόδειξης, που με τον τρόπο αυτό να αποκαλύπτει το περιεχόμενο της ψήφου του. Συνεπώς, είναι ανέφικτο να αποδείξει σε κάποιο τρίτο πρόσωπο ότι έχει ψηφίσει κάποιο συγκεκριμένο υποψήφιο. Αν αναλογιστούμε και το γεγονός ότι παρέχεται στο ψηφοφόρο δυνατότητα να ξαναψηφίσει αυτό δυσκολεύει ακόμη περισσότερο το φαινόμενο του καταναγκασμού και της πούλησης ψήφους μιας και ο ψηφοφόρος θα έχει την δυνατότητα να αλλάξει την ψήφο του όποτε και όπου επιθυμεί. Σε περίπτωση που ένας ψηφοφόρος πουλήσει την πραγματική ταυτότητα του σε κάποιο τρίτο άτομο,

τότε το τρίτο άτομο θα είναι σε θέση να ψηφίσει στην θέση του ψηφοφόρου. Το σύστημα δεν αποτρέπει τέτοια ενέργεια.

- **Οικουμενικά Επαληθεύσιμο (Universally Verifiable) :** Μετά την λήξη των εκλογών δεν κοινοποιείται στο ευρύ κοινό ποιες ψήφοι καταχωρήθηκαν στο σύστημα. Θα ήταν συνετό αν δημοσιευόταν ένας πίνακας με τις συναρτήσεις κατακερματισμού των ανώνυμων ταυτοτήτων ούτως ώστε να επαληθεύσει κάποιος ότι έχει καταχωρηθεί η ψήφος του. Εντούτοις, ο υποψήφιος δεν μπορεί να γνωρίζει αν η ψήφος του καταχωρήθηκε ορθά. Η ορθότητα της ψήφου διασφαλίζεται μέσω του προγράμματος και θα μπορούσε ο κώδικα να ήταν ανοικτός ούτως ώστε ο κάθε ψηφοφόρος να ελέγχει την ορθότητα της διαδικασίας.
- **Ανθεκτικό(Robust):** Κατά τη διαδικασία της ψηφοφορίας η ψήφος κατατμίζεται σε n διακομιστές εκ τον οποίο k διακομιστές από αυτούς πρέπει να παραμένουν ασφαλείς για να ανασχηματίσουν την ψήφο. Σε περίπτωση που κάποιος από τους διακομιστές τεθεί εκτός λειτουργίας τότε δεν εγκυμονεί κίνδυνος να χαθεί η ψήφος. Με τον τρόπο αυτό προσφέρεται η δυνατότητα ύπαρξης n-k σφαλμάτων στους διακομιστές, γεγονός που δε θα επηρέαζε τη λειτουργία του πρωτοκόλλου.

4.3 Βασικές Τεχνικές που χρησιμοποιούνται στο Πρωτόκολλο

4.3.1 Συνάρτηση Κατατεμαχισμού (Hash function)

Μία συνάρτηση κατατεμαχισμού, δέχεται ως είσοδο ένα μεγάλο μήνυμα M ,μεταβλητού μεγέθους ,και παράγει ως έξοδο μια μικρότερη αλυσίδα από bits σταθερού μήκους H(M),που ονομάζεται σύνοψη ή διαφορετικά κατατεμαχισμός (hash ή digest) .

Έχει τις πιο κάτω ενδιαφέρουσες ιδιότητες :

1. Η πιθανότητα δύο διαφορετικά μηνύματα, έστω χ και ψ, να έχουν το ίδιο κατατεμαχισμένο μήνυμα, είναι πρακτικά μηδαμινή.

2. Επίσης, είναι εξίσου αδύνατο να αναιρέσουμε τη διαδικασία κατατεμαχισμού και να καταλήξουμε στο πρωτότυπο κείμενο, ξεκινώντας από τον κατατεμαχισμένο μήνυμα.

3. Τέλος, δοθέντος (M, H(M)) , δηλαδή, το πρωτότυπο μήνυμα του αποστολέα και ο κατατεμαχισμός του μηνύματος, είναι υπολογιστικά αδύνατο να βρεθεί κάποιο άλλο μήνυμα, έστω M΄, τέτοιο ώστε H(M’)=H(M).

Και οι τρεις προαναφερόμενες ιδιότητες δρουν ως ασφάλεια στο περιεχόμενο του μηνύματος, μιας και ένας εισβολέας είναι υπολογιστικά αδύνατο να εντοπίσει το μήνυμα που αποστέλλεται το οποίο προστατεύεται από την συνάρτηση κατακερματισμού.

Μονόδρομες συναρτήσεις κατατεμαχισμού (one-way hash functions)

Υπάρχουν εφαρμογές οι οποίες χρειάζονται ορισμένες από τις πιο πάνω ιδιότητες και για το λόγο αυτό υπάρχει ενδιαφέρον στην ανάπτυξη κρυπτογραφικών οικογενειών συναρτήσεων κατακερματισμού.

Ειδικότερα, οι συναρτήσεις κατακερματισμού οι οποίες ικανοποιούν τις ιδιότητες (2) και (3) ονομάζονται μονόδρομες συναρτήσεις κατατεμαχισμού(one-way hash functions), ενώ οι συναρτήσεις που πληρούν τις ιδιότητες (1) και (3) ονομάζονται ανθεκτικές σε συγκρούσεις συναρτήσεις κατατεμαχισμού (collision resistance hash functions).

Οι μονόδρομες συναρτήσεις κατατεμαχισμού διαχωρίζονται σε δύο κατηγορίες, στις συναρτήσεις άνευ κλειδιού και στις συναρτήσεις με κλειδί.

Αυθεντικοποίηση Μηνύματος στις Συναρτήσεις Κατατεμαχισμούς

Η αυθεντικοποίηση των μηνυμάτων είναι μία διαδικασία που επιτρέπει στα συναλλασσόμενα μέρη να κατοχυρώσουν αφενός την ακεραιότητα των δεδομένων, δηλαδή, τη διασφάλιση ότι στα δεδομένα δεν θα παρατηρηθεί οποιαδήποτε αλλοίωση της πληροφορίας των μηνυμάτων και αφετέρου την αυθεντικότητα της πηγής που έχει μεταδώσει το μήνυμα. Σε μερικές περιπτώσεις, στο μήνυμα ενσωματώνεται χρονοσήμανση για να διασφαλιστεί ότι το μήνυμα δεν αποτελεί αναμετάδοση παλαιότερου μηνύματος ή για τον έλεγχο καθυστέρησης.

Τρεις Τρόποι Αυθεντικοποίησης Μηνύματος

Ο κατατεμαχισμός του μηνύματος μπορεί να κρυπτογραφηθεί μέσω **συμμετρικής κρυπτογράφησης**. Η αυθεντικότητα διασφαλίζεται στην περίπτωση που αποδεχθούμε ότι το κλειδί κρυπτογράφησης διαμοιράζεται μονάχα από τα εξουσιοδοτημένα επικοινωνούντα μέρη, τον αποστολέα και τον νόμιμο παραλήπτη.

Ένας δεύτερος τρόπος προσέγγισης , είναι η **κρυπτογράφηση με τη χρήση δημόσιου κλειδιού**. Η αυθεντικοποίηση του μηνύματος επιτυγχάνεται χωρίς να απαιτείται να γίνει διαμοιρασμός μυστικών κλειδιών μεταξύ των συναλλασσόμενων μέρη.

Ο αποστολέας κρυπτογραφεί το κατατεμαχισμένο μήνυμα μέσω του ιδιωτικού του κλειδιού και εν συνεχεία στέλνει το κρυπτογραφημένο μήνυμα και την κρυπτογράφηση του κατατεμαχισμένου μηνύματος στον παραλήπτη.

Ο παραλήπτης ανακτά τις πληροφορίες και με τη βοήθεια του δημόσιου κλειδιού του αποστολέα αποκρυπτογραφεί το μήνυμα που περιέχει τον κατατεμαχισμό. Ακολούθως, εφαρμόζει την συνάρτηση κατατεμαχισμού και παίρνει το κατατεμαχισμένο μήνυμα, το οποίο το συγκρίνει με το κατατεμαχισμένο μήνυμα που παρέλαβε από τον αποστολέα. Στην περίπτωση που τα κατατεμαχισμένα μηνύματα είναι τα ίδια, ο παραλήπτης μπορεί να είναι σίγουρος ότι κανείς δεν αλλοίωσε το περιεχόμενου του μηνύματος καθώς επίσης επαληθεύει την ταυτότητα του αποστολέα. Να σημειωθεί σε αυτό το σημείο, ότι θεωρούμε ότι ο παραλήπτης έχει γνώση ποια συνάρτηση κατακερματισμού καλείται να χρησιμοποιήσει.

Η συμμετρική κρυπτογράφηση και η κρυπτογράφηση με χρήση δημόσιου κλειδιού παρέχουν ένα σημαντικό πλεονέκτημα σε σχέση με τις προσεγγίσεις που κρυπτογραφούν ολόκληρο το μήνυμα, ότι απαιτείται πολύ μικρότερη υπολογιστική ισχύς.

Παρόλα αυτά, υπάρχει σημαντικό επιστημονικό ενδιαφέρον στην ανάπτυξη τεχνικών κατατεμαχισμού που δεν χρησιμοποιούν κρυπτογραφικές μεθοδολογίες μιας και έχει παρατηρηθεί ότι το λογισμικό κρυπτογράφησης είναι σχετικά αργό. Μολονότι, το μέγεθος των δεδομένων κρυπτογράφησης ανά μήνυμα είναι αρκετά μικρότερο, συνεχίζει να υφίσταται μία χρονοβόρα ροή εισερχόμενων και εξερχόμενων μηνυμάτων από το σύστημα. Επιπλέον, το κόστος του υλικού κρυπτογράφησης είναι ιδιαίτερα σημαντικό μιας και όλοι οι κόμβοι που εμπεριέχονται στο δίκτυο χρειάζεται να προσφέρουν δυνατότητα κρυπτογράφησης και αποκρυπτογράφησης των δεδομένων. Αξίζει να σημειωθεί ότι για μεγάλο όγκων δεδομένων η απόδοση στην εφαρμογή βελτιώνεται αρκετά όταν η κρυπτογράφηση υλοποιείται σε υλικό. Όμως, για μικρά τμήματα δεδομένων δαπανάται σημαντικό χρόνος για την απαιτούμενη αρχικοποίηση.

Οι πιο πάνω λόγοι ήταν αρκετοί για να προσθέσουν ακόμη μια **τεχνική που χρησιμοποιεί συνάρτηση κατατεμαχισμού αλλά εντούτοις δεν χρησιμοποιεί κρυπτογράφηση** για την αυθεντικοποίηση ενός μηνύματος. Αντιθέτως, διαμοιράζεται μια κοινή μυστική τιμή μεταξύ των συναλλασσόμενων μερών. Ο αποστολέας όταν επιθυμεί να αποστείλει ένα μήνυμα στον παραλήπτη, εισαγάγει στη συνάρτηση κατατεμαχισμού τη συνένωση της μυστικής τιμής και του μηνύματος. Ο αποστολέας αποστέλλει στον παραλήπτη τη συνένωση του μηνύματος και το αποτέλεσμα της συνάρτησης κατακερματισμού. Ο παραλήπτης ο οποίος γνωρίζει τη μυστική τιμή, επανυπολογίζει τη συνάρτηση κατατεμαχισμού για να ελέγξει την ακεραιότητα

του μηνύματος. Ενόσω διασφαλίζεται μυστική, η τιμή που διαμοιράζεται μεταξύ των επικοινωνούντων μερών είναι αδύνατο από ένα ωτακουστή να αλλοιώσει το μήνυμα χωρίς να εντοπιστεί από το παραλήπτη. Στην αντίθετη περίπτωση , ένας ωτακουστής μπορεί όχι μόνο να υποκλέψει το μήνυμα αλλά και να το τροποποίηση χωρίς να γίνει αντιληπτός.

Το πρωτόκολλο δεν καθορίζει κάποια συγκεκριμένη τεχνική για κατατεμαχισμό των μηνυμάτων και έτσι η επιλογή γίνεται από εμάς. Στην υλοποίηση του συστήματος έχουμε χρησιμοποιήσει τον αλγόριθμο SHA256.

4.3.2 SSL (Secure Socket Layer)

Το SSL δεν είναι ένα τρίτο πρωτόκολλο μεταφοράς Διαδικτύου, εκτός των TCP και UDP, αλλά είναι ένα επαυξημένο TCP και οι επαυξήσεις έχουν υλοποιηθεί στο επίπεδο εφαρμογής [22].

Το επαυξημένο με SSL TCP κάνει όλες τις εργασίες που κάνει το παραδοσιακό TCP, αλλά επίσης παρέχει κρίσιμες υπηρεσίες ασφαλείας ανάμεσα σε διεργασίες:

- Εμπιστευτικότητα (Κρυπτογράφηση)
- Ακεραιότητα δεδομένων
- Επαλήθευση στα άκρα.

Αυτές οι υπηρεσίες είναι υψίστης σημασίας μιας και αν δεν χρησιμοποιηθεί εμπιστευτικότητα, ένας εισβολέας μπορεί να υποκλέψει τα απόρρητα στοιχεία. Σε περίπτωση που δεν χρησιμοποιηθεί ακεραιότητα των δεδομένων, ένας εισβολέας μπορεί να τροποποιήσει στοιχεία και τέλος αν δεν υπάρχει αυθεντικοποίηση του εξυπηρέτη, ένας εξυπηρέτης μπορεί με δόλιο τρόπο να παραπλανήσει τους χρήστες ισχυρίζοντας ότι είναι κάποιος άλλος με απώτερο σκοπό την υποκλοπή στοιχείων.

Το SSL αρχικά σχεδιάστηκε από την Netscape και από την ημέρα της σύλληψης της ιδέας, το SSL έτυχε ευρείας αποδοχής. Το SSL διασφαλίζει το TCP και μπορεί να χρησιμοποιηθεί από οποιαδήποτε εφαρμογή εκτελείται επί του TCP. Έτσι το SSL υποστηρίζεται από όλα τα δημοφιλή προγράμματα περιήγησης και από όλους τους εξυπηρετητές Web και χρησιμοποιείται από πολλούς εμπορικούς ιστότοπους, για παράδειγμα, Amazon, eBay. Δεκάδες εκατομμύρια δολάρια διακινούνται μέσω SSL κάθε χρόνο.

Μπορείτε να καταλάβετε ότι χρησιμοποιείται το SSL από το πρόγραμμα περιήγηση σας, όταν το URL αρχίζει με https: και όχι http:.

Από τεχνικής πλευράς το SSL βρίσκεται στο επίπεδο εφαρμογής, από την σκοπιά του προγραμματιστή είναι ένα πρωτόκολλο μεταφοράς, που παρέχει υπηρεσίες TCP εμπλουτισμένες με υπηρεσίες ασφάλειας.

Το SSL παρέχει μια απλή Διεπαφή Προγραμματισμού Εφαρμογών (Application Programming Interface,API) με sockets. Όταν μια εφαρμογή χρησιμοποιεί SSL, η διεργασία αποστολής μεταβιβάζει δεδομένα καθαρού κειμένου στην SSL socket. Κατόπιν, το SSL στον υπολογιστή αποστολής κρυπτογραφεί τα δεδομένα και μεταβιβάζει τα κρυπτογραφημένα δεδομένα στην TCP socket. Τα κρυπτογραφημένα δεδομένα ταξιδεύουν επάνω στο Διαδίκτυο προς την TCP socket της διεργασίας λήψης. Η socket λήψης μεταβιβάζει τα κρυπτογραφημένα δεδομένα στο SSL,το οποίο τα αποκρυπτογραφεί. Τέλος, το SSL μεταβιβάζει τα δεδομένα καθαρού κειμένου μέσω της SSL socket του στην διεργασία λήψης.

4.3.3 Απόδειξη με μηδενική γνώση Zero-knowledge challenge/response protocol

Μία από τις δυσκολίες που αντιμετωπίζουν οι τεχνικές ταυτοποίησης ,όπως για παράδειγμα, ταυτότητες, πιστωτικές κάρτες, κωδικοί πρόσβασης στον υπολογιστή είναι ότι μία οντότητα P καλείται να αποδείξει την ταυτότητα του, αποκαλύπτοντας ένα τμήμα της πληροφορίας, έστω i(P),που ενδεχομένως θυμάται ή είναι τυπωμένη στη κάρτα του.

Ας υποθέσουμε ότι ο P(the Prover) είναι μία οντότητα η οποία καλείται να αποδείξει σε μία άλλη οντότητα ότι γνωρίζει κάποιες πληροφορίες. Οι πληροφορίες του P πρέπει να είναι επαληθεύσιμες, δηλαδή, πρέπει να υπάρχει μία αποτελεσματική διαδικασία για τον έλεγχο της εγκυρότητας των πληροφοριών. Σε συνδυασμό με ένα μαθηματικό θεώρημα αυτό προϋποθέτει ότι κάθε βήμα της απόδειξης μπορεί να επικυρωθεί. Ο P θέλει να πείσει τον επαληθευτή V (Varifier) πέραν πάση αμφιβολίας ότι είναι ο πραγματικός κάτοχος της πληροφορίας.

Ο P θα μπορούσε να γνωστοποιήσει αυτές τις πληροφορίες στον επαληθευτή, έτσι ώστε ο επαληθευτής να πραγματοποιήσει ο ίδιος τον έλεγχο.

Για παράδειγμα, ας εξετάσουμε το πρόβλημα παραγοντοποίησης σε πρώτους αριθμούς (factoring problem). Ο P θα μπορούσε να πει στον επαληθευτή, τους πρώτους παράγοντες p και q του ακέραιου αριθμού n. Κατά συνέπεια, θα ήταν εφικτό ο επαληθευτής να κάνει την πράξη n = pq και να ελέγξει την εγκυρότητα της πράξης. Ο επαληθευτής μιας και έχει γνώση των πληροφοριών που συνίσταται ο αριθμός n, δηλαδή τους αριθμούς p και q, είναι εφικτό να αποδείξει σε μία τρίτη οντότητα την εγκυρότητα της διαδικασίας.

Εντούτοις, μία κακόβουλη οντότητα που συνεργάζεται με ένα αναξιόπιστο επαληθευτή μπορεί να ανακτήσει είτε ένα αντίγραφο της κάρτας ή να μάθει το τμήμα i(P) και στη συνέχεια να τα χρησιμοποιήσει προσποιώντας ότι είναι ο P, και κατά συνέπεια να του παρέχεται πρόσβαση ή υπηρεσίες που ανήκουν στον P.

Μια προφανής λύση στο πρόβλημα είναι η χρήση απόδειξης με μηδενική γνώση, για να πειστεί ο επαληθευτής V ότι η οντότητα P γνωρίζει το i (P) χωρίς όμως, να αποκαλύψει το i(P) [19].

Η απόδειξης με μηδενική γνώση είναι μία διαδικασία η οποία περιλαμβάνει τα ακόλουθα σημεία:

- Η διαδικασία αρχίζει με ένα challenge της οντότητας verifier και ένα response της οντότητας Prover.
- Περιλαμβάνει ένα μήνυμα από την μία οντότητα. Εν συνεχεία η άλλη οντότητα εκτελεί ένα υπολογισμό και στέλνει ένα μήνυμα στην άλλη οντότητα.
- Στο τέλος, η οντότητα verifier είτε θα αποδεχτεί ή θα απορρίψει την προσπάθεια της άλλης οντότητας.

Στο σύστημα μας, η απόδειξη με μηδενική γνώση πραγματοποιείται ως ακολούθως:

- Αρχικά ο σταθμός ψηφοφορίας στέλλει τα πρώτα 20 ψηφία της σύνοψης της σύνοψης της ανώνυμης ταυτότητας του ψηφοφόρου ($h(h(r_{id}))$) στον καταχωρητή.
- Στη συνέχεια ο καταχωρητής πραγματοποιεί κατατεμαχισμό στις εγγραφές της λίστας που διαθέτει με τις συνόψεις των ανώνυμων ταυτοτήτων και διερευνά αν υπάρχει κάποιο αποτέλεσμα που τα πρώτα 20 ψηφία είναι ίδια με αυτά που παρέλαβε. Στην περίπτωση που υπάρχει χρησιμοποιεί το ιδιωτικό του κλειδί για να κρυπτογραφήσει τη συγκεκριμένη εγγραφή και εν συνεχεία πραγματοποιεί κατατεμαχισμό στο αποτέλεσμα της κρυπτογράφησης, δηλαδή εκτελείται η πράξη ($h(rid^x \bmod p)$).
- Ακολούθως απαντά με τα επόμενα 20 ψηφία της σύνοψης της υπογεγραμμένης ανώνυμης ταυτότητας του ψηφοφόρου. Έτσι ο σταθμός ψηφοφορίας μπορεί να επαληθεύσει ότι πράγματι ο καταχωρητής περιέχει εγγραφή με το συγκεκριμένο ψηφοφόρο, που είναι το ζητούμενο, χωρίς όμως διαρροή της πραγματικής πληροφορίας εντός των δύο αρχών.

4.3.4 Polynomial interpolation

Στο σύστημα μας, κατά τη διαδικασία της κατάτμησης και της συνένωσης καλούμαστε από δοθέντα σημεία να δημιουργήσουμε μια πολυωνυμική εξίσωση. Ο εντοπισμός μιας πολυωνυμικής εξίσωσης μπορεί να επιτευχθεί με ποικίλους τρόπους, όπως για παράδειγμα με τον πίνακα Vandermonde και με την βοήθεια των πολυωνύμων Lagrange [5] [6] [7] [8] [9]. Στο σύστημα μας, έχει επιλεγεί η χρήση των πολυωνύμων Lagrange.

Στο πιο κάτω υποκεφάλαιο παρουσιάζονται η μέθοδος παραγωγής πολυωνυμικής εξίσωσης με τη χρήση πίνακα Vandermonde και τη χρήση πολυωνύμων Lagrange. Παρουσιάζοντας

αρχικά τη λειτουργία της πρώτης τεχνικής με τη χρήση πίνακα Vandermonde διαπιστώνουμε ότι είναι πιο εποικοδομητικό να αναπαριστάς το πολυώνυμο της παρεμβολής με τη χρήση πολυωνύμων Lagrange.

Vandermonde matrix

Ένας Vandermonde matrix είναι ένας πίνακας στον οποίο οι όροι του σε κάθε σειρά είναι μία γεωμετρική πρόοδος και έχει την ακόλουθη μορφή:

$$A=\begin{matrix} 1 & x_1 & x_1^2 & . & . & . & x_1^{n-1} \\ 1 & x_2 & x_2^2 & . & . & . & x_2^{n-1} \\ 1 & x_3 & x_3^2 & . & . & . & x_3^{n-1} \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ 1 & x_n & x_n^2 & . & . & . & x_n^{n-1} \end{matrix}$$

Ένας πίνακας Vandermonde είναι αντιστρέψιμος αν και μόνο αν οι n παράμετροι του $x_1,x_2,\ldots,x_n$ είναι διακριτοί. Χρησιμοποιείται σε προβλήματα παρεμβολής για την εξεύρεση ενός πολυώνυμου της μορφής $p(x)= c_{n-1}\, x^{n-1} +c_{n-2}\, x^{n-2}+\ldots+c_1\, x+c_0$ βαθμού το πολύ n-1, με συντελεστές έτσι ώστε:

$P(x_1)= c_0+c_1x_1+c_2x_1^2+\ldots..+c_{n-1}x_1^{n-1}=y_1$

$P(x_2)= c_0+c_1x_2+c_2x_2^2+\ldots..+c_{n-1}x_2^{n-1}=y_2$

. . .

. . .

. . .

$P(x_n)= c_0+c_1x_n+c_2x_n^2+\ldots..+c_{n-1}x_n^{n-1}=y_n$

Όπου $x_1,x_{2,\ldots},x_n$ και $y_1,y_2,\ldots,y_n$ είναι κάποια δοθέντα στοιχεία.

Οι πιο πάνω συνθήκες παρεμβολής εμπεριέχουν ένα σύστημα από n εξισώσεις για τους n άγνωστους συντελεστές $c_0,c_1,\ldots,c_{n-1}$ και έχουν την ακόλουθη μορφή:

$Ac=y$

Όπου $c=[c_0,c_1,\ldots,c_n]^T$ και $y=[y_1,y_2,\ldots,y_n]^T$

Το πρόβλημα παρεμβολής έχει πάντα λύση, εάν τα σημεία $x_1,x_2,\ldots,x_n$ είναι διακριτά.

Στην περίπτωση που τα σημεία $x_1,x_{2,\ldots},x_n$ είναι διακριτά, οι συντελεστές του πολυωνύμου παρεμβολής θα μπορούσαν να εντοπιστούν επιλύοντας το σύστημα, αλλά συνήθως είναι πιο

εποικοδομητικό να αναπαριστάς το πολυώνυμο της παρεμβολής p(x) μέσω Lagrange interpolating polynomials.

$$L_i(x) = \frac{\prod_{j=1_{j\neq i}}^{n}(x - x_j)}{\prod_{j=1_{j\neq i}}^{n}(x_i - x_j)}$$

για τιμές i=1,2,…,n όπου κάθε πολυώνυμο $L_i(x)$ έχει βαθμό n-1.

Η μορφή της Lagrange παρεμβολής είναι η ακόλουθη:

$P(x) = y_1L_1(x) + y_2L_2(x) + \ldots + y_nL_n(x)$

Για πολυώνυμο P(x) με βαθμό το πολύ n-1, που ικανοποιεί τις προαναφερόμενες εξισώσεις $P(x_1)$ έως και $P(x_n)$.

Πολυωνυμικές Εξισώσεις Lagrange

Στην αριθμητική ανάλυση, τα πολυώνυμα Lagrange χρησιμοποιούνται για την πολυωνυμική παρεμβολή καθώς επίσης είναι ιδιαίτερα χρήσιμα στην κρυπτογραφία, για παράδειγμα στο σχήμα Shamir's secret sharing. Το όνομα των πολυωνυμικών εξισώσεων αποδίδεται στο Γάλλο μαθηματικό Joseph Louis Lagrange, ο οποίος τις δημοσίευσε το 1795. Εντούτοις, ανακαλύφθηκαν για πρώτη φορά το 1779 από τον Edward Waring.

Ορισμός Πολυωνυμικών Εξισώσεων Lagrange

Δοθέντων κάποιων k+1 σημείων$(x_0, y_0), \ldots, (x_j, y_j), \ldots, (x_k, y_k)$ εκ των οποίων δεν υπάρχουν σημεία των οποίων οι συντεταγμένες στον άξονα x να είναι ίδια, τότε το πολυώνυμο παρεμβολής στην Lagrange μορφή είναι ένας γραμμικός συνδυασμός τέτοιος ώστε:

$$L(x) = \sum_{j=0}^{k} y_j \, l_j(x)$$

όπου οι συντελεστές $l_{j(x)}$ ονομάζονται συντελεστές Lagrange και δίνονται από την πιο κάτω μαθηματική σχέση:

$$l_j(x) = \prod_{0\leq m\leq k_{m\neq j}} \frac{x - x_m}{x_j - x_m} = \frac{(x - x_0)}{(x_j - x_0)} \ldots \frac{(x - x_{j-1})}{(x_j - x_{j-1})} \frac{(x - x_{j+1})}{(x_j - x_{j+1})} \ldots \frac{(x - x_k)}{(x_j - x_k)}$$

Η παρεμβολή Lagrange διακατέχεται από απλότητα, μιας και είναι εφικτό να την προσδιορίσουμε χωρίς να χρειάζεται να επιλύσουμε το συστήματος ή εκτελώντας επαναλαμβανόμενους υπολογισμούς.

Θα ήταν εποικοδομητικό να εξετάσουμε ένα παράδειγμα με την μέθοδο Lagrange ούτως ώστε να μας διευκολύνει η κατανόηση του.

$(x_0, y_0) = (-1.5, -14.1014)$

$(x_1, y_1) = (-0.75, -0.93596)$

$(x_2, y_2) = (0,0)$

$(x_3, y_3) = (0.75,0.931596)$

$(x_4, y_4) = (1.5,14.1014)$

Έπειτα δημιουργώ τις εξισώσεις για τους συντελεστές Lagrange που εμπεριέχουν k-1 παράγοντες :

$$l_0(x) = \frac{(x-x_1)}{(x_0-x_1)}\frac{(x-x_2)}{(x_0-x_2)}\frac{(x-x_3)}{(x_0-x_3)}\frac{(x-x_4)}{(x_0-x_4)}$$

$$l_1(x) = \frac{(x-x_0)}{(x_1-x_0)}\frac{(x-x_2)}{(x_1-x_2)}\frac{(x-x_3)}{(x_1-x_3)}\frac{(x-x_4)}{(x_1-x_4)}$$

$$l_2(x) = \frac{(x-x_0)}{(x_2-x_0)}\frac{(x-x_1)}{(x_2-x_1)}\frac{(x-x_3)}{(x_2-x_3)}\frac{(x-x_4)}{(x_2-x_4)}$$

$$l_3(x) = \frac{(x-x_0)}{(x_3-x_0)}\frac{(x-x_1)}{(x_3-x_1)}\frac{(x-x_2)}{(x_3-x_2)}\frac{(x-x_4)}{(x_3-x_4)}$$

$$l_4(x) = \frac{(x-x_0)}{(x_4-x_0)}\frac{(x-x_1)}{(x_4-x_1)}\frac{(x-x_2)}{(x_4-x_2)}\frac{(x-x_3)}{(x_4-x_3)}$$

Αφού δημιουργηθούν οι πολυώνυμες εξισώσεις για τους συντελεστές Lagrange πραγματοποιείται μία αντικατάσταση των σημείων, ούτως ώστε να υπολογιστούν οι τιμές των εξισώσεων.

$$l_0(x) = \frac{\big(x—(-0{,}75)\big)}{\big((-1{,}5)-(-0{,}75)\big)}\frac{(x-0)}{\big((-1{,}5)-x_2\big)}\frac{(x-0{,}75)}{\big((-1{,}5)-0{,}75\big)}\frac{(x-1{,}5)}{\big((-1{,}5)-1{,}5\big)}$$

$$l_1(x) = \frac{\big(x-(-1{,}5)\big)}{\big((-0{,}75)-x_0\big)}\frac{(x-0)}{\big((-0{,}75)-0\big)}\frac{(x-0{,}75)}{\big((-0{,}75)-0{,}75\big)}\frac{(x-1{,}5)}{\big((-0{,}75)-1{,}5\big)}$$

$$l_2(x) = \frac{\big(x-(-1{,}5)\big)}{\big(0-(-1{,}5)\big)}\frac{\big(x-(-0{,}75)\big)}{\big(0-(-0{,}75)\big)}\frac{(x-0{,}75)}{(0-0{,}75)}\frac{(x-1{,}5)}{(0-1{,}5)}$$

$$l_3(x) = \frac{\big(x-(-1{,}5)\big)}{\big(0{,}75\_(-1{,}5)\big)}\frac{\big(x-(-0{,}75)\big)}{\big(0{,}75\_(-0{,}75)\big)}\frac{(x-0)}{(0{,}75\_0)}\frac{(x-1{,}5)}{(0{,}75\_1{,}5)}$$

$$l_4(x) = \frac{\big(x-(-1{,}5)\big)}{\big(1{,}5\_(-1{,}5)\big)}\frac{\big(x-(-0{,}75)\big)}{\big(1{,}5\_(-0{,}75)\big)}\frac{(x-0)}{(1{,}5-0)}\frac{(x-0{,}75)}{(1{,}5-0{,}75)}$$

Εν συνεχεία του παραδείγματος, προκύπτουν οι ακόλουθες τιμές:

$$l_0(x) = \frac{1}{243}x\,(2x-3)(4x-3)(4x+3)$$

$$l_1(x) = -\frac{8}{243}x\,(2x-3)(2x+3)(4x-3)$$

$$l_2(x) = \frac{3}{243}\,(2x+3)(4x+3)(4x-3)(2x-3)$$

$$l_3(x) = -\frac{8}{243}\,(2x-3)(2x+3)(4x+3)$$

$$l_4(x) = \frac{1}{243}x\,(2x+3)(4x-3)(4x+3)$$

Έτσι, το πολυώνυμο της παρεμβολής που προκύπτει είναι το ακόλουθο:

$L(x) = \frac{1}{243}(f(x_0)x(2x-3)(4x-3)(4x+3) - 8f(x1)x(2x-3)(2x+3)(4x-3) +$
$3fx22x+34x+34x-32x-3-8fx3x2x-32x+34x+3+fx4x2x+34x-3(4x+3)$

$= \frac{1}{243}\big((-14.1014)x(2x-3)(4x-3)(4x+3) - 8(-0{,}93596)x(2x-3)(2x+$
$34x-3+302x+34x+34x-32x-3-80{,}931596x2x-32x+34x+3+14{,}1014x2x+34x-3(4x+3)$

$= 4.834848x^3 - 1.477474x$

Κεφάλαιο 5

Προδιαγραφές

5.1 Απαιτήσεις Χρήστη 61

5.2 Προοπτική Συστήματος (Product Perspective) 62

5.3 Διαγράμματα Ροής Δεδομένων 64

5.4 Περιπτώσεις Χρήσεις 71

5.5 Αποθήκευση Δεδομένων 76

5.6 Διαγράμματα Ακολουθίας 79

5.7 Υλοποίηση 82

Στο κεφάλαιο αυτό, δίνονται τα απαραίτητα σχεδιαγράμματα και επεξηγήσεις για να κατανοήσουμε καλύτερα τη λειτουργία του πρωτοκόλλου αυτού. Πιο συγκεκριμένα παρέχονται τα σχεδιαγράμματα περιπτώσεων χρήσεων, διαγράμματα ροής δεδομένων και διαγράμματα ακολουθίας. Επίσης περιγράφονται οι απαιτήσεις χρήστη, η αποθήκευση των δεδομένων και αναφέρονται τα χαρακτηριστικά της κάθε βάσης δεδομένων.

5.1 Απαιτήσεις Χρήστη

Το ηλεκτρονικό σύστημα ψηφοφορίας παρέχει δυνατότητα πρόσβασης μόνο στους εγγεγραμμένους ψηφοφόρους για την συγκεκριμένη ψηφοφορία. Διαχειρίζεται τρεις βασικές λειτουργίες, την φάση της εγγραφής, της ψηφοφορίας και της καταμέτρησης.

- Το ηλεκτρονικό σύστημα ψηφοφορίας έχει τη δυνατότητα να διαχειρίζεται τη φάση της εγγραφής των ψηφοφόρων, ούτως ώστε οι ψηφοφόροι να αποκτήσουν ανώνυμη ταυτότητα και να είναι σε θέση να ασκήσουν το εκλογικό τους δικαίωμα.
- Σε κάθε ψηφοφόρο αποδίδεται μια και μόνο μοναδική ανώνυμη ταυτότητα που δρα ως αναγνωριστικό για την άσκηση του εκλογικού δικαιώματος των ψηφοφόρων.

- Οι ψηφοφόροι έχουν την ευχέρεια προτού ασκήσουν το εκλογικό τους δικαίωμα, να πληροφορηθούν για τον υποψήφιο, ούτως ώστε να είναι σίγουροι για την απόφαση τους. Συγκεκριμένα, για κάθε υποψήφιο εμφανίζεται η αντίστοιχη φωτογραφία και πληροφορίες για το έργο του.
- Οι ψηφοφόροι ασφαλώς, έχουν την δυνατότητα να επιλέξουν τον υποψήφιο που επιθυμούν και να ασκήσουν το εκλογικό τους δικαίωμα.
- Παρέχεται η δυνατότητα ακύρωσης της αρχικής ψήφους, ψηφίζοντας ξανά.
- Το σύστημα είναι σε θέση να διαχειρίζεται με ασφαλές τρόπο τις ψήφους του συστήματος, πραγματοποιώντας κατάτμηση της κάθε ψήφου και αποστέλλοντας το κάθε κομμάτι σε διαφορετικούς διακομιστές.
- Σε περίπτωση που κάποιος διακομιστής τεθεί εκτός λειτουργίας, η ψήφος δεν χάνεται.
- Για την ευκολότερη χρήση του συστήματος, υπάρχει εγχειρίδιο χρήσης που αναρτάται στη γραφική διεπαφή του συστήματος.

5.2 Προοπτική Συστήματος (Product Perspective)

User Interfaces

Στη γραφική διεπαφή του ψηφοφόρου, με τη χρήση του μενού ο ψηφοφόρος θα μπορεί να εγγραφεί ούτως ώστε να αποκτήσει ανώνυμη ταυτότητα και να είναι σε θέση να ασκήσει το εκλογικό του δικαίωμα, να ενημερωθεί για τους υποψηφίους, να διαβάσει το εγχειρίδο χρήσης σε περίπτωση που χρειάζεται οποιαδήποτε καθοδήγηση και τέλος να επικοινωνήσει με το εκλογικό σύστημα.

Πιο συγκεκριμένα, στη γραφική διεπαφή για την εγγραφή, ο ψηφοφόρος καλείται να καταχωρήσει μία λέξη σε ένα πεδίο κειμένου (text box) που θα αποτελεί την ανώνυμη ταυτότητα του στην περίπτωση που εγκριθεί από το σύστημα.

- Στην περίπτωση που έχει ήδη δημιουργήσει ανώνυμη ταυτότητα, εμφανίζεται στο ψηφοφόρο μήνυμα λάθους που τον ενημερώνει ότι δεν είναι εφικτή η δημιουργία ανώνυμης ταυτότητας μιας και έχει ήδη.
- Στην περίπτωση που καταχωρήσει μία λέξη για ανώνυμη ταυτότητα που ήδη υπάρχει, εμφανίζεται μήνυμα που του επεξηγεί ότι η ανώνυμη ταυτότητα έχει δοθεί σε κάποιο άλλο υποψήφιο και του ζητείται να καταχωρήσει μία άλλη λέξη για ανώνυμη ταυτότητα.

- Διαφορετικά σε μία επιτυχή καταχώρηση, εμφανίζεται μήνυμα στο ψηφοφόρο που τον ενημερώνει ότι η λέξη που έχει καταχωρήσει αποτελεί την ανώνυμη ταυτότητα του και του εμφανίζει την υπογεγραμμένη ανώνυμη ταυτότητα. Ο ψηφοφόρος ενημερώνεται ότι την ανώνυμη ταυτότητα και την υπογεγραμμένη ανώνυμη ταυτότητα πρέπει να τις θυμάται για να μπορεί έπειτα να ψηφίσει.

Εν συνεχεία, θα εξετάσουμε τη γραφική διεπαφή για τη ψηφοφορία.
Ο ψηφοφόρος αφού αποκτήσει ανώνυμη ταυτότητα μπορεί να ασκήσει το εκλογικό του δικαίωμα. Στην περίπτωση που ένας ψηφοφόρος χωρίς ανώνυμη ταυτότητα ή ένας μη εγγεγραμμένος ψηφοφόρος επιχειρήσουν να ψηφίσουν τους εμφανίζεται μήνυμα λάθος. Ο ψηφοφόρος επιλέγει από το μενού την επιλογή "Vote" και μετακινείται στη ιστοσελίδα με τους υποψηφίους. Η σελίδα αυτή περιλαμβάνει τα ονόματα και οι αντίστοιχες φωτογραφίες των υποψηφίων. Στην περίπτωση που ο ψηφοφόρος πατήσει την εικόνα ή το όνομα ενός υποψηφίου, εμφανίζεται η αντίστοιχη περιγραφή του υποψηφίου, ενώ όταν πατήσει τον σύνδεσμό "click to vote <Candidate Name>" κάτω από την εικόνα του υποψηφίου εμφανίζεται ένα παράθυρο για να ψηφίσει τον υποψήφιο της αρεσκείας του. Εν συνεχεία, ζητείται από τον ψηφοφόρο να καταχωρήσει την ανώνυμη ταυτότητα του και την υπογεγραμμένη ανώνυμη ταυτότηττα. Αφού πραγματοποιηθεί έλεγχος των στοιχείων που έχει καταχωρήσει ο ψηφοφόρος του ζητείται να καταχωρήσει μία εξαψήφια λέξη. Αφού καταχωρήσει την εξαψήφια λέξη, του εμφανίζεται μήνυμα που τον ενημερώνει ότι η ψήφος του έχει καταχωρηθεί επιτυχώς.

Ο ψηφοφόρος μέσω του μενού μπορεί να επιλέξει την επιλογή "contact us" και να μετακινηθεί στην σελίδα επικοινωνίας. Στη σελίδα υπάρχει ένας διαδραστικός χάρτης με πινέζα στην διεύθυνση του Πανεπιστημίου Κύπρου καθώς επίσης και μία φόρμα επικοινωνίας.

Ο ψηφοφόρος έχει επίσης την ευχέρεια να διαβάσει το εγχειρίδιο χρήσης επιλέγοντας την επιλογή "Manual" από το μενού. Σε περίπτωση που επιθυμεί να αποσυνδεθεί από το σύστημα ηλεκτρονικής ψηφοφορίας, επιλέγει την επιλογή "Exit" από το μενού.

Hardware Interfaces

Το σύστημα επικοινωνεί με ένα εξυπηρετητή και με προσωπικούς υπολογιστές με την χρήση browser.

Software Interfaces: Το σύστημα θα μπορεί να τρέχει σε κάθε λειτουργικό σύστημα μέσω του φυλλομετρητή. Για να παρέχονται υπηρεσίες διακομιστή ιστού, χρειάστηκε η

εγκατάσταση του WampServer έκδοσης 2.2 ο οποίος υποστηρίζει, Server Apache, PHP και MySQL. Έτσι, για την υλοποίηση του συστήματος έχουμε χρησιμοποιήσει τις γλώσσες προγραμματισμού PHP έκδοσης 5.4.3, HTML, HTML5, JavaScript και για βάση δεδομένων την MySQL με έκδοση 5.5.24. Για διαχείριση της βάσης δεδομένων χρησιμοποιούμε την διεπαφή του PhpMyAdmin, καθώς επίσης ο εξυπηρετητής ιστού είναι Apache έκδοσης 2.2.22.

Communications Interfaces: Το Σύστημα επικοινωνεί με τερματικούς υπολογιστές με την χρήση του διαδικτύου. Επίσης, κατά την διαδικασία της ψηφοφορίας η ψήφος διασπάται σε κομμάτια και αποστέλλεται σε διαφορετικούς διακομιστές. Οι διακομιστές στο σύστημα, για σκοπούς υλοποίησης, αναπαριστώνται ως διαφορετικές βάσεις δεδομένων. Εναλλακτικά, θα μπορούσαν να είναι είναι διαφορετικοί εξυπηρετητές που θα βρίσκονται σε διαφορετικές τοποθεσίες.

5.3 Διαγράμματα Ροής Δεδομένων

Τα διαγράμματα ροής δεδομένων εκφράζουν τη λογική ροή των δεδομένων του συστήματος, δηλαδή την αλληλεπίδραση μεταξύ εξωτερικών πρακτόρων, διαδικασιών και αποθηκευτικών μονάδων. Είναι ένας τρόπος αναπαράστασης συναρτησιοστρεφών συστημάτων, το οποίο δεν παρέχει πληροφορίες για το χρονισμό των διεργασιών ή αν αυτές λειτουργούν ακολουθιακά ή παράλληλα. Το πλεονέκτημα των διαγραμμάτων ροής δεδομένων είναι ότι δείχνουν την επεκεργασία από άκρο σε άκρο. Μπορείτε δηλαδή να δείτε όλες τις συναρτήσεις που επενεργούν στα δεδομένα καθώς αυτά περνούν από διάφορα στάδια στο σύστημα.

Δομικά στοιχεία ενός ΔΡΔ:

Εξωτερικός Πράκτορας:

Αντιπροσωπεύει σημεία αλληλεπίδρασης συστήματος με το εξωτερικό περιβάλλον. Επίσης, καθορίζουν την εμβέλειά του. Οι εξωτερικοί πράκτορες αναπαριστούν πρόσωπα, μονάδες οργανισμού, κάποιο άλλο σύστημα, οργανισμούς που αλληλεπιδρούν με το σύστημα για ανταλλαγή δεδομένων.

Διαδικασία:

Αντιπροσωπεύει διαδικασία που εκτελεί ή προκαλείται από την εισροή δεδομένων στο σύστημα, απεικονίζει δηλαδή, μία συνάρτηση που υλοποιεί κάποιο μετασχηματισμό δεδομένων.

Αποθηκευτική Μονάδα:

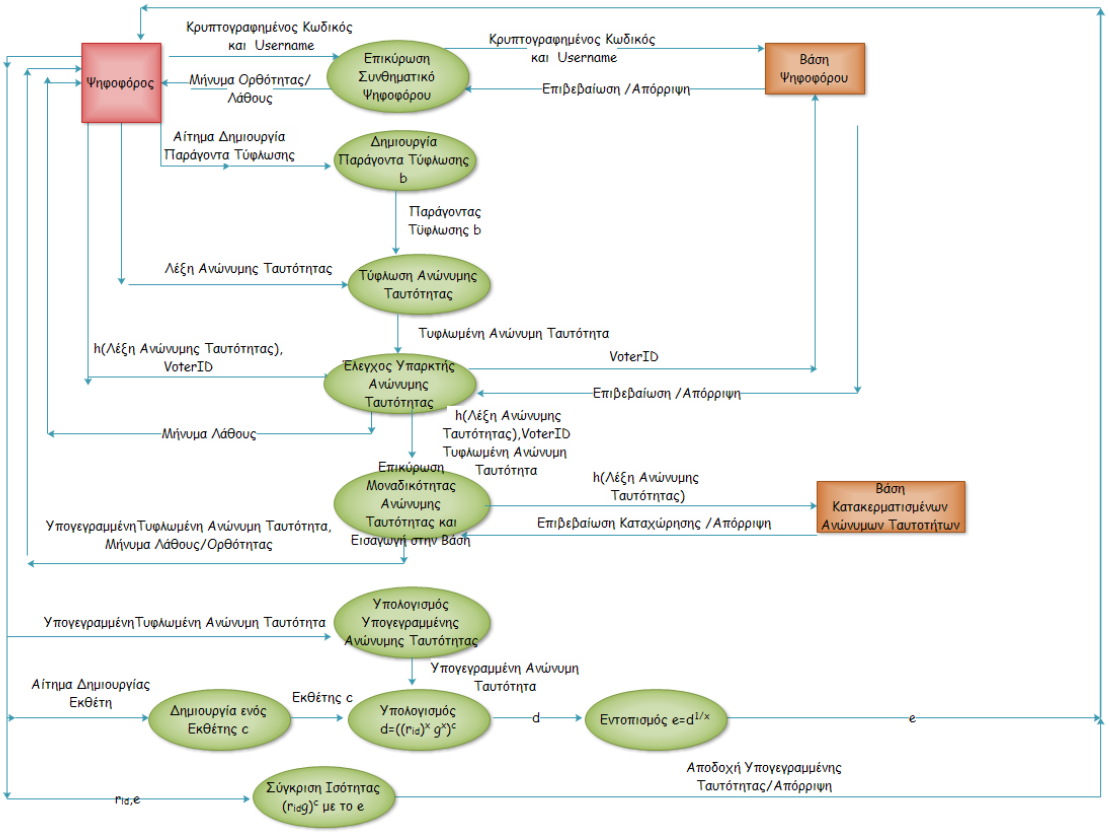
Αντιπροσωπεύει την αποθηκευτική μονάδα όπου αποθηκεύονται τα δεδομένα του συστήματος. Συνήθως, υλοποιούνται ως αρχεία ή βάσεις δεδομένων.

Ροές Δεδομένων:

Αναπαριστούν τις εισόδους και εξόδους προς και από μια διαδικασία. Προέρχονται από ή καταλήγουν σε εξωτερικούς πράκτορες, αποθηκευτικές μονάδες ή άλλες διαδικασίες.

´

Φάση Εγγραφής



Το διάγραμμα αυτό παρουσιάζει τη διαδικασία της εγγραφής ενός ψηφοφόρου στο σύστημα, ούτως ώστε να εξασφαλίσει ανώνυμη ταυτότητα και να είναι σε θέση να ασκήσει το εκλογικό του δικαίωμα. Είναι μία καθοριστική φάση, μιας και πρέπει να διασφαλιστεί ότι ο νόμιμος ψηφοφόρος θα αποκτήσει μονάχα μία μοναδική ανώνυμη ταυτότητα.

Οι διαδικασίες που λαμβάνουν χώρα κατά την διαδικασία της εγγραφής είναι οι ακόλουθες:

- Επικύρωση Συνθηματικό Ψηφοφόρου
- Δημιουργία Παράγοντα Τύφλωσης
- Τύφλωση Ανώνυμης Ταυτότητας
- Έλεγχος Υπαρκτής Ανώνυμης Ταυτότητας
- Επικύρωση μοναδικότητας Ανώνυμης Ταυτότητας και Εισαγωγή στη Βάση
- Υπολογισμός Υπογεγραμμένης Ανώνυμης Ταυτότητας
- Δημιουργία Εκθέτη
- Υπολογισμός του d
- Εντοπισμός του e

- Σύγκριση Ισότητα
- Επικύρωση Συνθηματικό Ψηφοφόρου

Ο κάθε ψηφοφόρος ενώνεται με το σύστημα, καταχωρώντας το μοναδικό του συνθηματικό, το οποίο του παραχωρήθηκε νωρίτερα από την αρχή ψηφοφορίας ούτως ώστε να εξασφαλίσει πρόσβαση στο σύστημα. Το συνθηματικό του απαρτίζεται από το όνομα χρήστη και το μοναδικό κωδικό πρόσβασης. Για την επικύρωση του συνθηματικού πρόσβασης πρέπει να διερευνηθεί από την βάση δεδομένων που εμπεριέχει τα δεδομένα που αφορούν τους νόμιμους ψηφοφόρους του συστήματος, ότι το συνθηματικό είναι ορθό και δηλαδή ο χρήστης είναι νόμιμος. Σε περίπτωση που τα δεδομένα που εισαγάγει είναι λανθασμένα τότε εμφανίζεται ενημερωτικό μήνυμα που τον πληροφορεί για το λάθος του και του ζητάει να επανεισάγει τα σωστά στοιχεία του. Διαφορετικά, ο χρήστης εισαγάγετε στο σύστημα για την απόκτηση της ανώνυμης ταυτότητας.
Οι είσοδοι και οι έξοδοι για την διαδικασία επικύρωσης συνθηματικού είναι :
Εισόδος:
Κρυπτογραφημένος Κωδικός και κωδικός πρόσβασης (Username).
Έξοδος:
Μήνυμα Ορθότητας /Λάθους.

Ο ψηφοφόρος αφού ενταχθεί επιτυχώς στο σύστημα, ξεκινά η φάση της εγγραφής, ούτως ώστε να εξασφαλίσει μία ανώνυμη ταυτότητα. Το σύστημα του ζητάει να καταχωρήσει μία λέξη για ανώνυμη ταυτότητα. Εν συνεχεία, πραγματοποιούνται οι ακόλουθες διαδοχικές διαδικασίες:

- Δημιουργία Παράγοντα Τύφλωσης

Ο ψηφοφόρος τυχαία και ομοιόμορφα λαμβάνει ένα παράγοντα τύφλωσης ούτως ώστε να τυφλώσει την λέξη που έχει καταχωρήσει στο σύστημα, που στην περίπτωση που εγκριθεί από το σύστημα θα αποτελεί την ανώνυμη ταυτότητα του. Η έξοδος αυτής της διαδικασίας είναι ο παράγοντας τύφλωσης (b), ο οποίος αποστέλλεται στην επόμενη διαδικασία για τη τύφλωση της ανώνυμης ταυτότητας.

- Τύφλωση Ανώνυμης Ταυτότητας

Η διαδικασία της τύφλωσης της λέξης που έχει καταχωρήσει ο ψηφοφόρος για ανώνυμη ταυτότητα είναι ιδιαίτερα σημαντική μιας και διασφαλίζεται κρυπτογράφηση της λέξης. Για αυτή τη διαδικασία απαιτείται ασφαλώς η λέξη που έχει καταχωρήσει ο ψηφοφόρος και ο

παράγοντας τύφλωσης που μόλις έχει δημιουργηθεί. Η διαδικασία της τύφλωσης της λέξης έχει ως ακολούθως: r_{id} g^b mod p, όπου g είναι μια primitive root και p είναι ένας πρώτος αριθμός, που είναι δημόσιοι γνωστοί και καθορίζονται από το σύστημα. Η έξοδος της διαδικασίας της τύφλωσης της ανώνυμης ταυτότητας είναι η τυφλωμένη ανώνυμη ταυτότητα. Συνεπώς, οι είσοδοι και οι έξοδοι για την διαδικασία τύφλωσης της ανώνυμης ταυτότητας είναι :

Εισόδοι:

Παράγοντας τύφλωσης και η λέξη που έχει καταχωρήσει ο ψηφοφόρος ως ανώνυμη ταυτότητα.

Έξοδος:

Τυφλωμένη Ανώνυμη Ταυτότητα.

- Έλεγχος Υπαρκτής Ανώνυμης Ταυτότητας

Μιας και η λέξη που καταχώρησε ο ψηφοφόρος έχει τυφλωθεί, το σύστημα καλείται σύμφωνα με το πρωτόκολλο να διερευνήσει αν ο ψηφοφόρος που επιδιώκει να δημιουργήσει την ανώνυμη ταυτότητα έχει δημιουργήσει ήδη ανώνυμη ταυτότητα. Στην περίπτωση που ο ψηφοφόρος έχει ήδη πραγματοποιήσει τη φάση της δημιουργίας ανώνυμης ταυτότητας, το σύστημα τον αποτρέπει να δημιουργήσει κάποια άλλη ανώνυμη ταυτότητα. Με τον τρόπο αυτό διασφαλίζεται ότι η ψήφος οποιουδήποτε ψηφοφόρου μετράει ισάξια με την ψήφο οποιουδήποτε άλλου ψηφοφόρου.

Ο ψηφοφόρος εισαγάγει στο σύστημα το αποτέλεσμα της συνάρτησης κατατεμαχισμού που παίρνει σαν παράμετρο τη λέξη που έχει καταχωρήσει ο ψηφοφόρος ως ανώνυμη ταυτότητα, την πραγματική του ταυτότητα και την τυφλωμένη ανώνυμη ταυτότητα. Η πραγματική ταυτότητα του ψηφοφόρου έχει οριστεί να είναι ίδια με τον κώδικα πρόσβασης.

Πραγματοποιείται έλεγχος από τη βάση που κρατάει πληροφορίες για τους ψηφοφόρους, αν ο συγκεκριμένος ψηφοφόρος έχει ήδη δημιουργήσει ανώνυμη ταυτότητα. Στην περίπτωση που έχει παράγει ανώνυμη ταυτότητα, του αποστέλλεται ενημερωτικό μήνυμα που τον πληροφορεί ότι δεν είναι εφικτή η δημιουργία άλλης ανώνυμης ταυτότητας.

Οι είσοδοι και οι έξοδοι για την διαδικασία του ελέγχου της ύπαρξη ανώνυμης ταυτότητας είναι:

Είσοδοι:

Το αποτέλεσμα της συνάρτησης κατατεμαχισμού που παίρνει σαν παράμετρο τη λέξη που έχει καταχωρήσει ο ψηφοφόρος ως ανώνυμη ταυτότητα , την πραγματική ταυτότητα του ψηφοφόρου και την τυφλωμένη ανώνυμη ταυτότητα.

Έξοδοι:

Μήνυμα Λάθους, σε περίπτωση που ο ψηφοφόρος έχει ήδη δημιουργήσει ανώνυμη ταυτότητα. Στην αντίθετη περίπτωση, τα προαναφερόμενα στοιχεία που έχει δώσει ο ψηφοφόρος (το αποτέλεσμα της συνάρτησης κατατεμαχισμού που παίρνει σαν παράμετρο τη λέξη που έχει καταχωρήσει ο ψηφοφόρος ως ανώνυμη ταυτότητα , την πραγματική ταυτότητα του ψηφοφόρου και την τυφλωμένη ανώνυμη ταυτότητα.

θα σταλθούν στην επόμενη διαδικασία για να πραγματοποιηθεί ένας δεύτερος έλεγχος, αναφορικά με την μοναδικότητα της ανώνυμης ταυτότητας.

- Επικύρωση μοναδικότητας Ανώνυμης Ταυτότητας και Εισαγωγή στη Βάση

Η διαδικασία αυτή είναι υπεύθυνη για να πιστοποίηση τη μοναδικότητα της ανώνυμης ταυτότητας. Καθώς επίσης, στην περίπτωση που διασφαλιστεί η μοναδικότητα της ανώνυμης ταυτότητας, πραγματοποιείται εισαγωγή του αποτελέσματος της συνάρτησης κατακερματισμού με παράμετρο την λέξη που έχει καταχωρήσει ο ψηφοφόρος ,στη κατάλληλη βάση.

Η λειτουργία της διαδικασίας, είναι η διερεύνηση από τη βάση που εμπεριέχει τα αποτελέσματα των συναρτήσεων κατακερματισμού με παράμετρο τις ανώνυμες ταυτότητες, οι οποίες έχουν εγκριθεί από το σύστημα ως ανώνυμες ταυτότητες, εάν το αποτέλεσμα της συνάρτησης κατακερματισμού με παράμετρο τη λέξη που καταχώρησε ο ψηφοφόρος υπάρχει ήδη. Δηλαδή, διερευνάται αν κάποιος ψηφοφόρος έχει ήδη καταχωρήσει αυτή τη λέξη ως ανώνυμη ταυτότητα. Στην περίπτωση που εμφανίζεται στην βάση, τότε αποστέλλεται στο ψηφοφόρο ενημερωτικό μήνυμα στο ψηφοφόρο και του ζητάει να επαναλάβει τη διαδικασία δημιουργίας ανώνυμης ταυτότητας, καταχωρώντας καινούρια λέξη ως ανώνυμη ταυτότητα. Στην αντίθετη περίπτωση, το αποτέλεσμα εισάγεται στη βάση δεδομένων και αποστέλλεται στο ψηφοφόρο ενημερωτικό μήνυμα που τον πληροφορεί ότι η λέξη που είχε καταχωρήσει στο σύστημα, αποτελεί την ανώνυμη ταυτότητα του καθώς επίσης του αποστέλλεται η τυφλωμένη ανώνυμη ταυτότητα που είναι υπογεγραμμένη από τον ψηφοφόρο.

Εισόδοι:

Το αποτέλεσμα της συνάρτησης κατατεμαχισμού που παίρνει σαν παράμετρο τη λέξη που έχει καταχωρήσει ο ψηφοφόρος ως ανώνυμη ταυτότητα, την πραγματική ταυτότητα του ψηφοφόρου και την τυφλωμένη ανώνυμη ταυτότητα.

Εξόδοι:

Μήνυμα Λάθους στην περίπτωση που η ανώνυμη ταυτότητα που καταχώρησε, έχει δωθεί σε κάποιο άλλο ψηφοφόρο.

Διαφορετικά, του αποστέλλεται ενημερωτικό μήνυμα που τον πληροφορεί ότι η λέξη που είχε καταχωρήσει στο σύστημα, αποτελεί την ανώνυμη ταυτότητα του καθώς επίσης του αποστέλλεται η τυφλωμένη ανώνυμη ταυτότητα που είναι υπογεγραμμένη από τον ψηφοφόρο.

- Υπολογισμός Υπογεγραμμένης Ανώνυμης Ταυτότητας

Η διαδικασία υπολογισμού της υπογεγραμμένης ταυτότητας αποσκοπεί στον εντοπισμό της υπογεγραμμένη ανώνυμης ταυτότητας του ψηφοφόρου, δοθέντος της τυφλωμένης υπογεγραμμένης ανώνυμης ταυτότητας.
Ο ψηφοφόρος παραλαμβάνει το υπογεγραμμένο r_{id} ως εξής:
Χρησιμοποιώντας το δημόσιο κλειδί του καταχωρητή υπολογίζει το $v=(g^x)^b \bmod p$ και ακολούθως υπολογίζει τον αντίστροφο του v.
Έπειτα υπολογίζει το $r=u^x *(v^{-1})=(r_{id})^x \bmod p$.
Είσοδοι: Η τυφλωμένη υπογεγραμμένη ανώνυμη ταυτότητα.
Έξοδοι: Η υπογεγραμμένη ανώνυμη ταυτότητα.

- Δημιουργία Εκθέτη

Ο ψηφοφόρος τυχαία και ομοιόμορφα λαμβάνει ένα εκθέτη ούτως ώστε να πιστοποιήσει στη συνέχεια ότι η υπογραφή στην ανώνυμη ταυτότητα προέρχεται από την αρχή ψηφοφορίας και όχι από ένα εξωτερικό παράγοντα. Η έξοδος αυτής της διαδικασίας είναι ο εκθέτης (c) ο οποίος αποστέλλεται στην επόμενη διαδικασία για τον υπολογισμό μιας μαθηματικής πράξης που θα συμβάλλει στην ορθή ανίχνευση της υπογραφής στην ανώνυμη ταυτότητα.

- Υπολογισμός του d

Λαμβάνεται στην είσοδο ο εκθέτης c και η υπογεγραμμένη ανώνυμη ταυτότητα. Με τη βοήθεια του δημόσιου κλειδιού του συστήματος(g^x), που είναι ευρέως γνωστό πραγματοποιείται η ακόλουθη μαθηματική πράξη:
$D=((rid)^x *g^x)^c$.
Το αποτέλεσμα της εξίσωσης δίνεται ως είσοδο στην επόμενη μαθηματική πράξη.

- Εντοπισμός του e

Χρησιμοποιώντας το ιδιωτικό κλειδί του συστήματος πραγματοποιείται η ακόλουθη πράξη:
$e=d^{(1/x)}$.

- Σύγκριση Ισότητας

Ο ψηφοφόρος συγκρίνει $(r_{id}g)^c$ με το e. Στην περίπτωση που σημειωθεί ισότητα μεταξύ αυτών των δύο αριθμών, πιστοποιείται ότι η υπογραφή στην ανώνυμη ταυτότητα προέρχεται από την αρχή ψηφοφορίας και όχι από ένα εξωτερικό παράγοντα. Διαφορετικά, ανιχνεύεται απάτη στην διαδικασία της υπογραφής της ανώνυμης ταυτότητας.

5.4 Περιπτώσεις Χρήσεις

Actors

Οι χρήστες που αλληλεπιδρούν με το ηλεκτρονικό σύστημα ψηφοφορίας είναι:

- Χρήστες
- Καταχωρητής
- Σταθμός Εκλογών
- Εξυπηρετητές

Στο σύστημα υπάρχουν 3 διαφορετικά είδη βάσεων δεδομένων και μία γραφική διεπαφή χρήστη. Οι βάσεις δεδομένων του συστήματος είναι οι ακόλουθες:

- Της αρχής καταχώρησης
- Του σταθμού εκλογών
- Των n Εξυπηρετητών. Υπάρχουν n διαφορετικές βάσεις δεδομένων, μία για κάθε εξυπηρετητή, με διαφορετικά δεδομένα η κάθε μία, αλλά με την ίδια μορφή.
- Οι εγγραμμένοι ψηφοφόροι του συστήματος, οι οποίοι είναι οι χρήστες του συστήματος, είναι σε θέση να πραγματοποιούν την φάση της εγγραφής για την απόκτηση της ανώνυμης ταυτότητας ούτως ώστε να έχουν στην συνέχεια, τη δυνατότητα άσκησης του εκλογικού τους δικαιώματος.

Στους πιο κάτω πίνακες φαίνονται οι σχέσεις των χρηστών με το σύστημα.

Actor descriptions

Βάση Δεδομένων Καταχωρητή	
Description	Ο ψηφοφόρος του συστήματος έχει τη δυνατότητα να ασκήσει το εκλογικό του δικαίωμα. Πρωτίστως, πρέπει να εξασφαλίσει

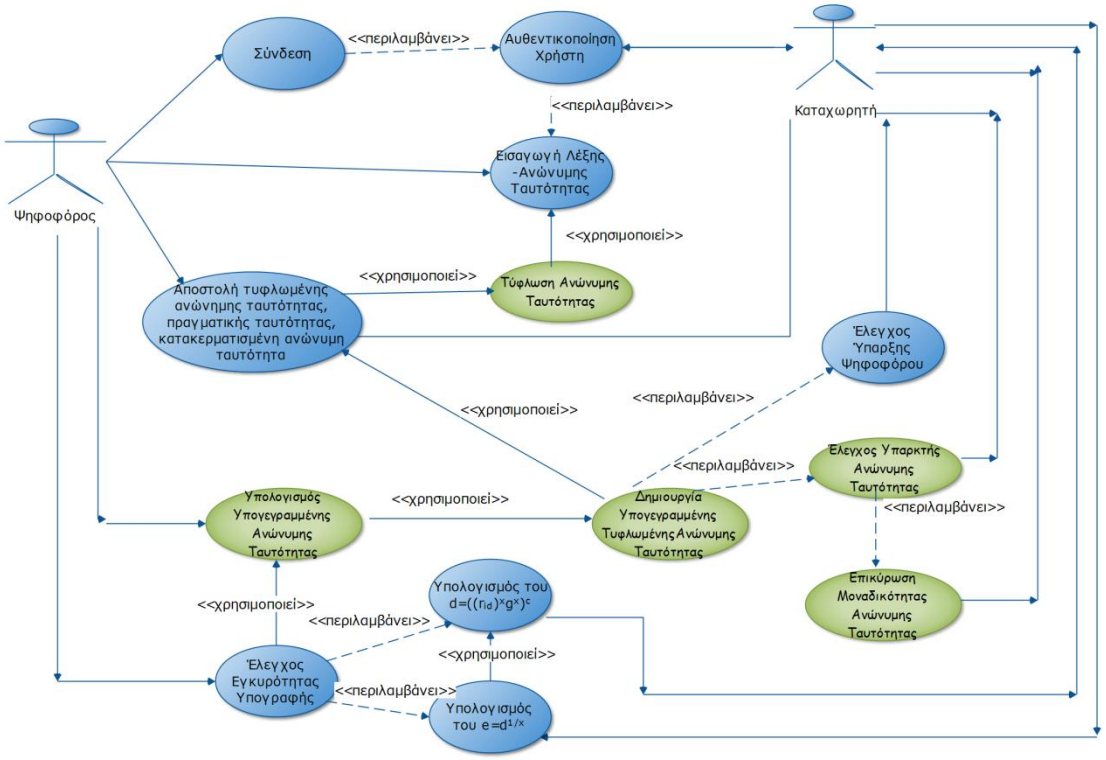
	μία ανώνυμη ταυτότητα και εν συνεχεία να επιλέξει τον υποψήφιο που επιθυμεί και να ψηφίσει.
Aliases	None
Inherits	None
Actor Type	Active-person

Βάση Δεδομένων Καταχωρητή	
Description	Περιέχει στοιχεία για τους ψηφοφόρους και τους υποψήφιους. Διατηρεί επίσης, μία λίστα με τα αποτελέσματα των συναρτήσεων κατακερματισμού με παράμετρο την λέξη που έχει δοθεί από το ψηφοφόρο ως ανώνυμη ταυτότητα. Η λίστα αυτή εμπεριέχει όλους τους ψηφοφόρους που επιτυχώς έχουν πραγματοποιήσει τη διαδικασία της απόκτησης ανώνυμης ταυτότητας.
Aliases	None
Inherits	None
Actor Type	Active-External System

Βάση Δεδομένων Σταθμού Εκλογών	
Description	Περιέχει όλες τις ανώνυμες ταυτότητες των ψηφοφόρων που άσκησαν το εκλογικό τους δικαίωμα. Συνεπώς, οι ψηφοφόροι οι οποίοι έχουν πραγματοποιήσει επιτυχώς τη διαδικασία απόκτηση ανώνυμης ταύτοτητας και δεν έχουν ψηφίσει δεν περιλαμβάνονται σε αυτή τη βάση δεδομένων.
Aliases	None
Inherits	None
Actor Type	Active-External System

Βάση Δεδομένων των πολλαπλών εξυπηρετητών	
Description	Η ψήφος μαζί με τη μυστική λέξη διαμοιράζεται σε κομμάτια και αποστέλλεται το κάθε κομμάτι σε διαφορικούς διακομιστές. Έτσι, η βάση των n εξυπηρετητών, όπου n =8 ,εμπεριέχουν τμήματα από την κομματιασμένη ψήφο. Στην διαδικασία της καταμέτρησης, k διακομιστές , όπου k=5,συνεργάζονται για να ανακατασκευάσουν την ψήφο.
Aliases	None
Inherits	None
Actor Type	Active-External System

Φάση Εγγραφής

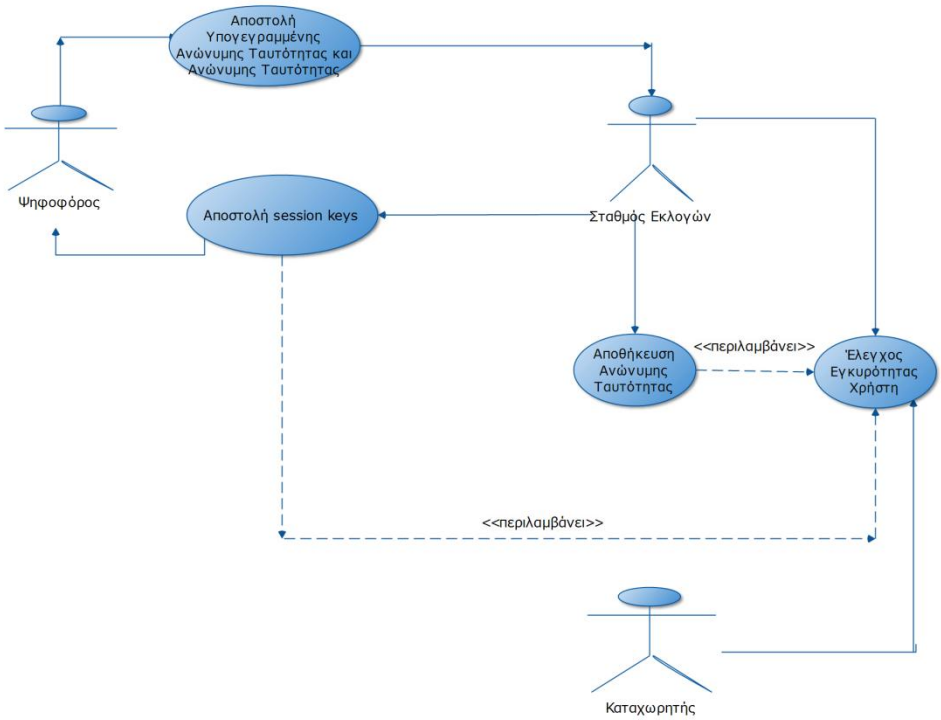


Περιγραφή

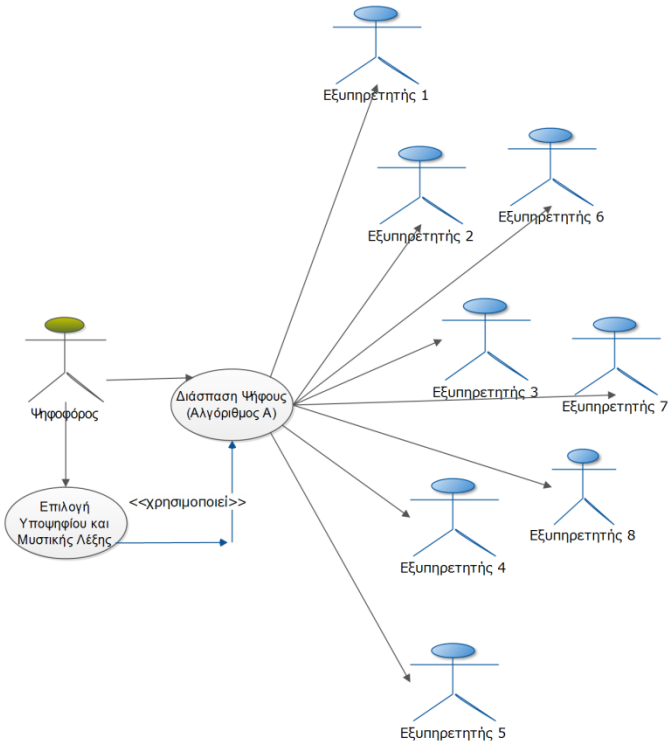
Ο ψηφοφόρος για να ψηφίσει πρέπει πρώτα να εξασφαλίσει ανώνυμη ταυτότητα. Η διαδικασία της απόκτησης ανώνυμης ταυτότητας καθώς και της ψηφοφορίας απαιτούν τη σύνδεση του ψηφοφόρου στο σύστημα ηλεκτρονικής ψηφοφορίας. Η λειτουργία της σύνδεσης περιλαμβάνει την αυθεντικοποίηση του χρήστη. Υπεύθυνος για την όλη διαδικασία είναι ο καταχωρητής, ο οποίος περιέχει τα στοιχεία σύνδεσης του ψηφοφόρου (κωδικός και συνθηματικό) καθώς και επιπρόσθετα στοιχεία του ψηφοφόρου όπως το όνομα, επίθετο, αν έχει ψηφίσει. Αφού πραγματοποιηθεί αυθεντικοποίηση της νομιμότητας του ψηφοφόρου, ο ψηφοφόρος εισάγει μία λέξη, η οποία θα αποτελέσει την ανώνυμη ταυτότητά του ψηφοφόρου στην περίπτωση που εγκριθεί από τον καταχωρητή. Στην συνέχεια η λέξη τυφλώνεται και αποστέλλεται μαζί με την ανώνυμη ταυτότητα και την πραγματική ταυτότητα του ψηφοφόρου στον καταχωρητή. Στην συνέχεια ο καταχωρητής πραγματοποιεί δύο ελέγχους. Πρωτίστως, ελέγχει αν ο χρήστης έχει δικαίωμα να ψηφίσει στις εκλογές και στη συνέχεια διερευνά αν η συγκεκριμένη ανώνυμη ταυτότητα υπάρχει ήδη στη λίστα του. Η ύπαρξη της ανώνυμης ταυτότητας στη λίστα του ψηφοφόρου υποδηλώνει

ότι ο ψηφοφόρος έχει αποκτήσει ήδη μία ανώνυμη ταυτότητα. Διαφορετικά, αποθηκεύει τη σύνοψη της ανώνυμης ταυτότητας του ψηφοφόρου στη λίστα του και ακολούθως την υπογράφει και την αποστέλλει στον ψηφοφόρο. Ο ψηφοφόρος ανακτά την υπογεγραμμένη ανώνυμη τυφλωμένη ταυτότητα και ελέγχει την εγκυρότητα της υπογραφής. υπολογίζοντας το $d=((r_{id})^x g^x)^c$ και στην συνέχεια το $e=d^{1/x}$. Στην περίπτωση ισότητας, ο ψηφοφόρος αποδέχεται την ανώνυμη ταυτότητα. Η ανώνυμη ταυτότητα καθώς επίσης και η υπογεγραμμένη ταυτότητα θα χρησιμοποιηθούν στην συνέχεια στην φάση της ψηφοφορίας.

Φάση Ψηφοφορίας



Ο ψηφοφόρος για να είναι σε θέση να ψηφίσει, πρέπει να επικοινωνήσει με τον σταθμό εκλογών και να του αποστείλει την υπογεγραμμένη ανώνυμη ταυτότητά του καθώς και την ανώνυμη ταυτότητά του. Στην συνέχεια ο σταθμός εκλογών ελέγχει την εγκυρότητα του χρήστη, η οποία γίνεται σε συνεργασία με τον καταχωρητή, επικοινωνώντας και ανταλλάσσοντας πληροφορίες σύμφωνα με το zero-knowledge challenge-responce πρωτόκολλο. Αφού ενημερωθεί για την εγκυρότητα του χρήστη, αποθηκεύει την ανώνυμη του ταυτότητα, και του αποστέλλει κλειδιά συνόδου, για να είναι σε θέση να ψηφίσει αργότερα.



Ο ψηφοφόρος επιλέγει τον υποψήφιο που επιθυμεί για να τον ψηφίσει, και στην συνέχειά εκτελεί τον αλγόριθμο Α όπως τον έχουμε περιγράψει στο πρωτόκολλο, με είσοδο την μυστική λέξη και τον αριθμό του επιθυμητού υποψηφίου και δημιουργείται ένα σύνολο από n κομμάτια της ψήφου. Σε κάθε διακομιστή θα αποσταλεί ένα διαφορετικό κομμάτι από αυτό το σύνολο τα οποία έχουν την μορφή σημείου (x,y). Μαζί με το κάθε κομμάτι θα αποσταλεί σε κάθε διακομιστή το h(rid) που είναι η σύνοψη της ανώνυμης του ταυτότητας και το h(m) που είναι η σύνοψη του μηνύματος που έχει καταχωρήσει ο ψηφοφόρος ως μυστική λέξη .

5.5 Αποθήκευση Δεδομένων

Βάσεις Δεδομένων

Στο σύστημα υπάρχουν 3 διαφορετικά είδη βάσεων δεδομένων
Υπάρχουν οι βάσεις δεδομένων

1. Της αρχής καταχώρησης
2. Του σταθμού εκλογών
3. Των n Εξυπηρετητών. Εδώ υπάρχουν n διαφορετικές βάσεις δεδομένων, μία σε κάθε εξυπηρετητή, με διαφορετικά δεδομένα η κάθε μία, αλλά με την ίδια μορφή που περιγράφεται και στο διάγραμμα σχέσεων οντοτήτων.

Ανάλυση Βάσεων Δεδομένων

Βάση Δεδομένων Αρχής Καταχώρησης

Έχει τις οντότητες:

- Candidate: Υποψήφιος σε μία ψηφοφορία
- Voter : Ο ψηφοφόρος
- One Way Hash Of Anonymous ID : Είναι λίστα με τις εξόδους της συνάρτησης κατακερματισμού που παίρνει σαν είσοδο την ανώνυμη ταυτότητα rid του ψηφοφόρου

Candidate
Name: Το όνομα του υποψήφιου
Surname: Το επίθετο του υποψήφιου
CandidateNoInVoting Ο αριθμός – ταυτότητα- του υποψήφιου στη συγκεκριμένη ψηφοφορία

Voter
Voter_ID: Ο μοναδικός αριθμός του υποψηφίου στο σύστημα (ταυτότητα).
Name: Το όνομα του ψηφοφόρου
Surname : Το επίθετο του ψηφοφόρου
Password: Το συνθηματικό του ψηφοφόρου με το οποίο συνδέεται στο σύστημα

One Way hash of Anonymous ID
Anonymous Id Hash: Είναι η έξοδος της συνάρτησης κατακερματισμού που παίρνει σαν είσοδο την ανώνυμη ταυτότητα rid του ψηφοφόρου

Σχέσεις πολλά προς πολλά:
Votes: Σχέση μεταξύ του ψηφοφόρου και ψηφοφορίας. Περιέχει μεταβλητές όπως αν ο ψηφοφόρος έχει δικαίωμα να ψηφίσει στην ψηφοφορία, καθώς και αν έχει ήδη ψηφήσει.

Βάση Δεδομένων Σταθμού Εκλογών

Registered User: Περιέχει μία λίστα με τα rids των ψηφοφόρων
Rid: Το rid των ψηφοφόρων

Βάση Δεδομένων n Εξυπηρετητών

Ballot Part

x-Coordinate: το χ στην συνάρτηση f η οποία χρησιμοποιείται για να διαχωρίσουμε την ψήφο σε κομμάτια.

y-Coordinate: το αποτέλεσμα της συνάρτησης f με είσοδο χ (δηλαδή το f(x))

MessageMHash: Είναι η έξοδος του μυνήματος M αφού πρώτα περάσει από την συνάρτηση κατακερματισμού

AnonymousIDHash : Είναι το h(rid)

Αντιστοιχήσεις από μεταβλητές του αλγορίθμου σε μεταβλητές της βάσης δεδομένων:

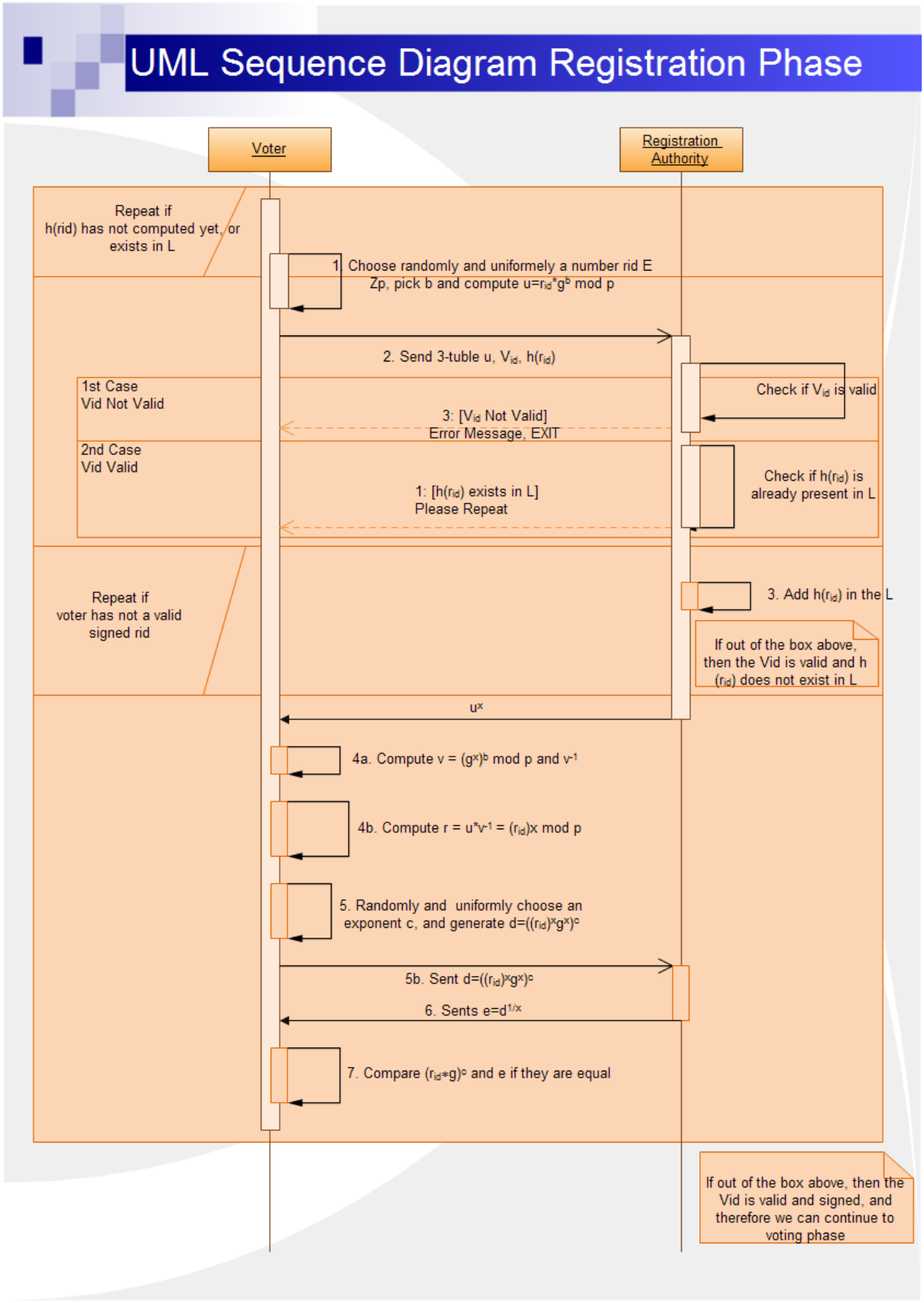
h(rid) = "Anonymous IDHash" On Entity "One Way hash of Anonymous ID"

Vid = Voter_ID on Entity "Voter"

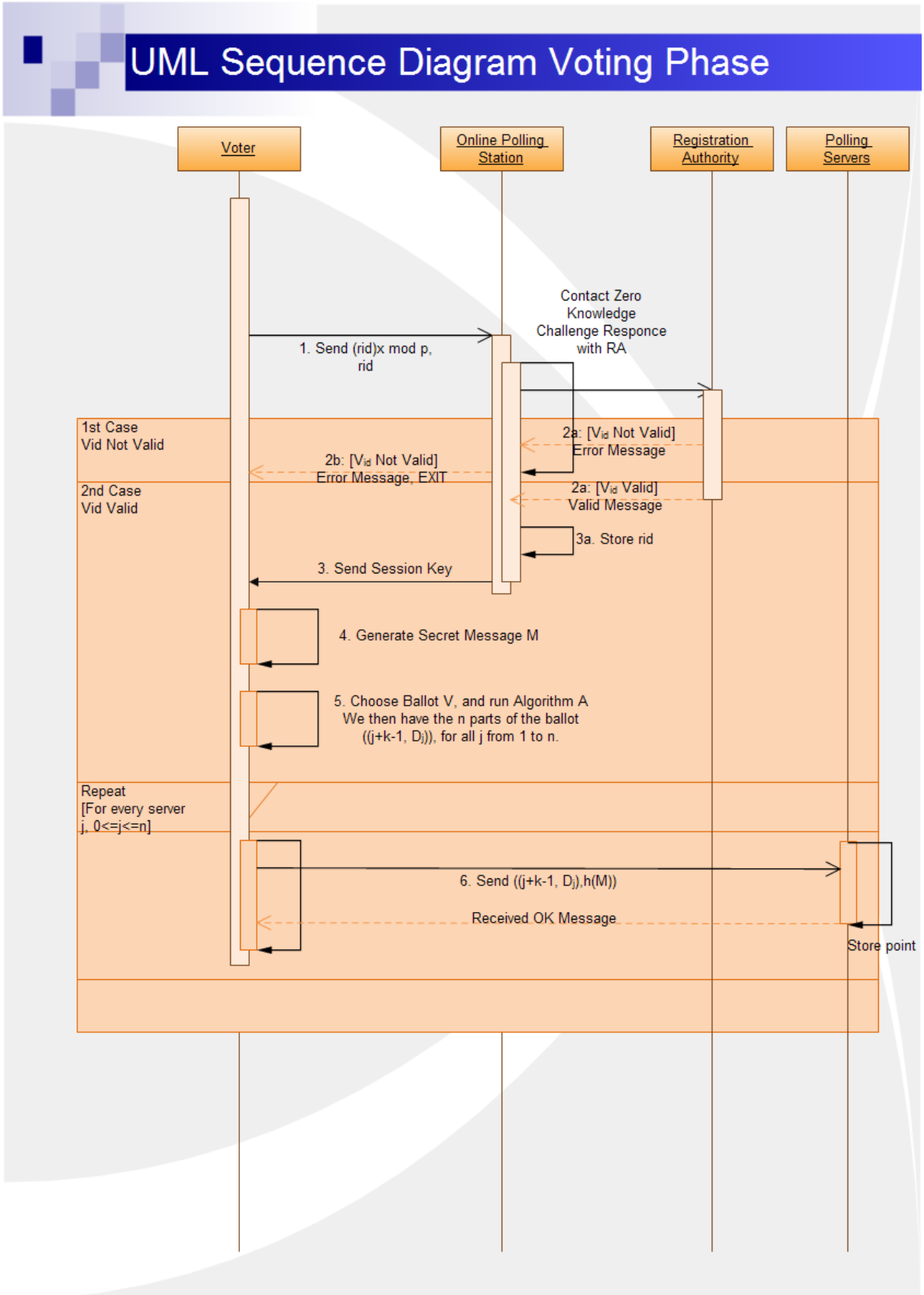
CandidateNoInVoting : The number of candidate in Voting $\in \mathbb{Z}$ p

5.6 Διαγράμματα Ακολουθίας

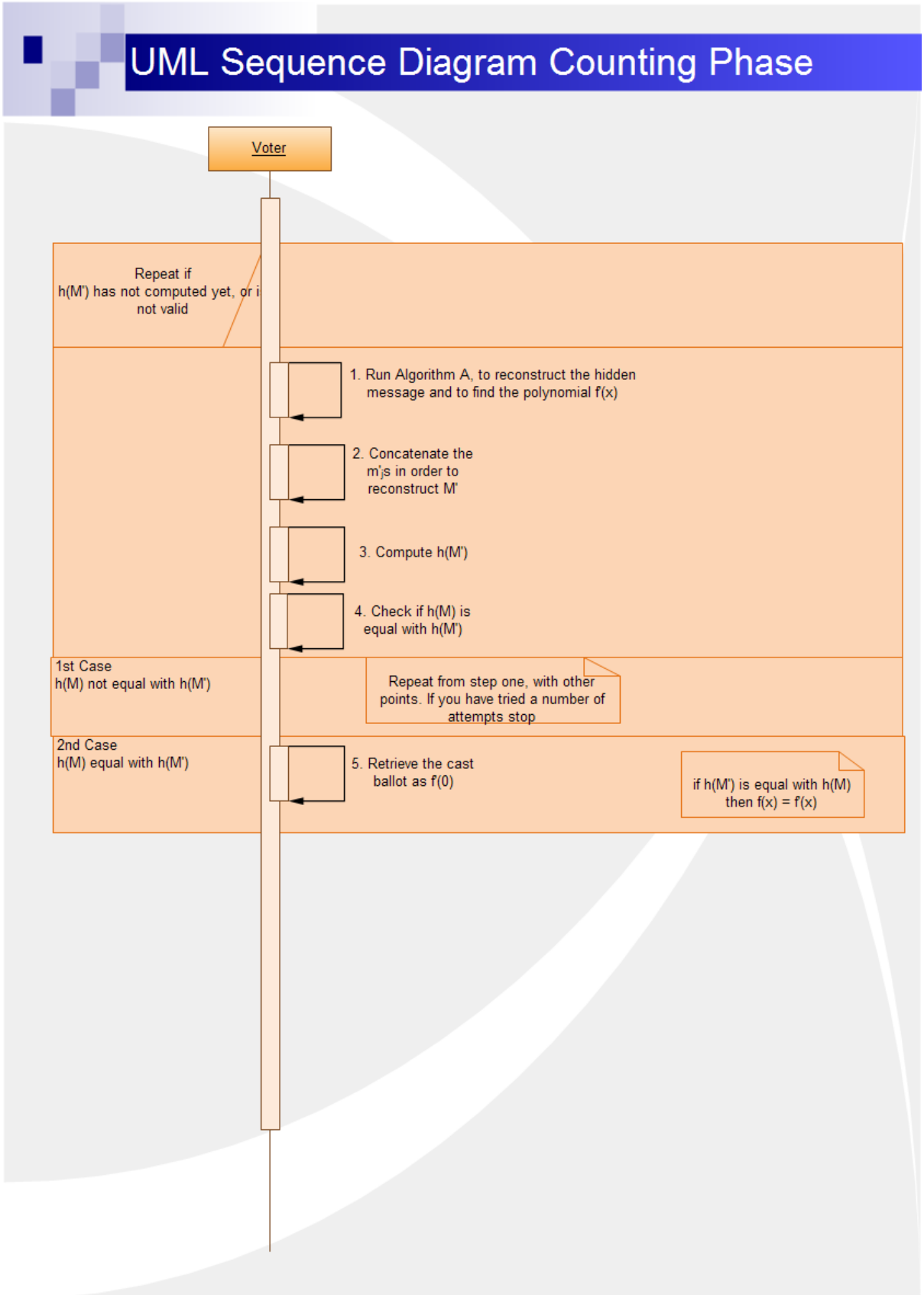
Φάση Εγγραφής



Φάση Ψηφοφορίας



Φάση Καταμέτρησης



5.7 Υλοποίηση

Το σύστημα το οποίο έχω υλοποιήσει, ικανοποιεί πλήρως το πρωτόκολλο IIS. Σε αυτό το υποκεφάλαιο αναφέρονται κάποιες λεπτομέρειες για την υλοποίηση του συστήματος. Μερικές από αυτές τις λεπτομέρειες σχετίζονται με τις μεταβλητές και τις συναρτήσεις που έχουν καθοριστεί στο σύστημα καθώς επίσης με τα εργαλεία και τις βιβλιοθήκες που έχουν χρησιμοποιηθεί.

Θα ξεκινήσουμε τη περιγραφή της υλοποίησης του συστήματος, αναφέροντας πως έχουμε καθορίσει τις βασικές μεταβλητές και συναρτήσεις του συστήματος μας.

Καθορισμός μεταβλητών και συναρτήσεων: Σημαντικές παράμετροι του πρωτοκόλλου και κατά συνέπεια και του συστήματος μας, αποτελούν οι παράμετροι n και k όπου n είναι ο αριθμός των εξυπηρετητών του συστήματος και k ο ελάχιστος αριθμός εξυπηρετών ανασυγκρότηση της μυστικής λέξης που έχει καταχωρήσει ο ψηφοφόρος. Στην τρέχουσα έκδοση του συστήματος έχει επιλεγεί ως αριθμός εξυπηρετητών n, ο αριθμός 8, ενώ ως αριθμός ελάχιστων εξυπηρετητών για ανασυγκρότηση του μηνύματος k, ο αριθμός 5. Οι αριθμοί αυτοί έχουν επιλεγεί με αυτόν τον τρόπο, λόγω του ότι είναι οι τιμές των μεταβλητών που περιγράφονται και στα παραδείγματα της δημοσίευσης του πρωτοκόλλου. Οι τιμές των μεταβλητών μπορούν να αλλάξουν πολύ εύκολα, καθώς η υλοποίηση του αλγορίθμου έχει γίνει λαμβάνοντας υπόψη την επεκτασιμότητα του συστήματος.

Επίσης για επιλογή πρωταρχικής ρίζας (primitive root) η οποία χρησιμοποιείται σαν η παράμετρος g στο σύστημά μας, έχουμε επιλέξει τιμή μέσω πινάκων οι οποίοι υπάρχουν στο διαδίκτυο και έχουν προκαθορισμένες τιμές πρωταρχικών ριζών για αρκετούς πρώτους αριθμούς.

Το πρωτόκολλο αναφέρει τη χρήση μίας συνάρτησης κατακερματισμού h, εντούτοις δεν αναφέρει ρητά ποια συνάρτηση κατακερματισμού χρησιμοποιεί και έτσι στην υλοποίηση του συστήματος έχουμε επιλέξει τη συνάρτηση κατακερματισμού SHA 256 και η οποία καλείται μέσω της PHP. Πιο συγκεκριμένα, στην γλώσσα προγραμματισμού PHP υπάρχει ήδη η συνάρτηση string hash (string $algo , string $data [, bool $raw_output = false]) στην οποία η παράμετρος $algo υποδηλώνει το όνομα του αλγορίθμου που θα χρησιμοποιηθεί. Έτσι εμείς καλούμε τη συνάρτηση ως hash ("sha256",$data).

Κατά τη διαδικασία της ψηφοφορίας, χρειάζεται να πραγματοποιηθεί επικοινωνία του σταθμού ψηφοφορίας με τον καταχωρητή μέσω της χρήσης ενός Zero-Knowledge Challenge-Response πρωτοκόλλου. Μιας και δεν διευκρινίζεται από το πρωτόκολλο ο τρόπος με τον οποίο θα ανταλλάζονται τα δεδομένα η επιλογή γίνεται από εμάς. Πιο συγκεκριμένα, αρχικά ο σταθμός ψηφοφορίας στέλλει τα πρώτα 20 ψηφία της σύνοψης της

σύνοψης της ανώνυμης ταυτότητας του ψηφοφόρου ($h(h(r_{id}))$) στον καταχωρητή. Στη συνέχεια ο καταχωρητής πραγματοποιεί κατατεμαχισμό στις εγγραφές της λίστας που διαθέτει με τις συνόψεις των ανώνυμων ταυτοτήτων και διερευνά αν υπάρχει κάποιο αποτέλεσμα που τα πρώτα 20 ψηφία είναι ίδια με αυτά που παρέλαβε. Στην περίπτωση που υπάρχει χρησιμοποιεί το ιδιωτικό του κλειδί για να κρυπτογραφήσει τη συγκεκριμένη εγγραφή και εν συνεχεία πραγματοποιεί κατατεμαχισμό στο αποτέλεσμα της κρυπτογράφησης, δηλαδή εκτελείται η πράξη ($h(rid^x \bmod p)$). Ακολούθως απαντά με τα επόμενα 20 ψηφία της σύνοψης της υπογεγραμμένης ανώνυμης ταυτότητας του ψηφοφόρου. Έτσι ο σταθμός ψηφοφορίας μπορεί να επαληθεύσει ότι πράγματι ο καταχωρητής περιέχει εγγραφή με το συγκεκριμένο ψηφοφόρο, που είναι το ζητούμενο, χωρίς όμως διαρροή της πραγματικής πληροφορίας εντός των δύο αρχών.

Επίσης, κατά τη διαδικασία της ψηφοφορίας ο ψηφοφόρος για να ψηφίσει καταχωρεί μία 6ψήφια μυστική λέξη και η οποία θα διασπαστεί σε k-2 κομμάτια. Συνεπώς, στην περίπτωση μας που το k είναι ίσο με 5, απαιτείται η διάσπαση της λέξης σε 3 διαφορετικά κομμάτια. Στο παράδειγμα το οποίο αναφέρεται στο πρωτόκολλο IIS, διασπάται η λέξη στους αριθμούς ASCII του κάθε γράμματος που την αποτελούν. Έτσι η λέξη USA διασπάται σε τρία τμήματα τα οποία έχουν τιμή τους αριθμούς 85, 83 και 65 αντίστοιχα, οι αριθμοί αυτοί αντιστοιχούν στα γράμματα U, S και A στον κώδικα ASCII. Εμείς, για περισσότερη ασφάλεια θέλουμε ο ψηφοφόρος να μην εισάγει μόνο τρία γράμματα όπως στο συγκεκριμένο παράδειγμα αλλά έξι. Δηλαδή σε κάθε ένα από τα τμήματα θα αντιστοιχούν δύο γράμματα.

Έτσι, χρειάστηκε να συνδυάσουμε τους κώδικες ASCII δύο διαδοχικών γραμμάτων της λέξης σε ένα και μόνο αριθμό. Αυτό το χειριστήκαμε ως ακολούθως:

1. Διασπούμε τη λέξη σε k-2 ακολουθίες, των δύο γραμμάτων η κάθε μία.
2. Δημιουργούμε ένα αριθμό ο οποίος προκύπτει από το μαθηματικό τύπο ASCII(A1)*128+ASCII(A2) όπου A1 και A2 το πρώτο και δεύτερο γράμμα της κάθε ακολουθίας αντίστοιχα.

Έτσι για παράδειγμα έχουμε διασπάσει τη λέξη RUSSIA στους ακόλουθους τρεις αριθμούς:

(82)*128+85 = 10581

(83)*128+83 = 10707

(73)*128+65 = 9409

Για τη διαδικασία της συνένωσης εκτελούμε την ακριβώς αντίθετη διαδικασία, δηλαδή,

A1 = Πάτωμα(10581/128) = 82 = R

A2 = 10581 mod 128 = 85 = U

Στην ουσία κάνουμε μετακίνηση(shift) των δυφίων του αριθμού, κατά 7 δυφία αριστερά. Έτσι σχηματίζονται 7 μηδενικά δυφία στα δεξιά στα οποία προσθέτουμε τον κώδικα ASCII

του δεύτερου γράμματος. Έχουμε πολλαπλασιάσει τον κώδικα ASCII του πρώτου γράμματος με το 128 (2^7) λόγω του ότι ο κώδικας ASCII χρειάζεται 7 δυφία.

Εν συνεχεία αναφέρουμε τα εργαλεία και τις βιβλιοθήκες που χρησιμοποιήθηκαν για την υλοποίηση του συστήματος.

Εργαλεία: Για την υλοποίηση του συστήματος έχουμε χρησιμοποιήσει την γλώσσα προγραμματισμού PHP έκδοσης 5.4 και για βάση δεδομένων την MySQL με έκδοση 5.5.24. Για διαχείριση της βάσης δεδομένων χρησιμοποιούμε την διεπαφή του PhpMyAdmin, καθώς επίσης έχουμε εγκαταστήσει τον εξυπηρετητή ιστού Apache έκδοσης 2.2.22. Τα παραπάνω εργαλεία τα είχαμε προμηθευτεί από το πακέτο εργαλείων WampServer.

Βιβλιοθήκες: Στο σύστημα υπολογίζονται εξαιρετικά μεγάλοι αριθμοί, οι οποίοι δεν είναι δυνατό να αποθηκευτούν σε μία μεταβλητή τύπου Integer ή long. Έτσι έχουμε χρησιμοποιήσει τις βιβλιοθήκες BigInteger για τον κώδικα ο οποίος έχει υλοποιηθεί από εμάς στην γλώσσα Javascript, ενώ την βιβλιοθήκη GMP για τους μεγάλους αριθμούς στην γλώσσα προγραμματισμού PHP. Οι βιβλιοθήκες αυτές αποθηκεύουν τους αριθμούς με μορφή γραμματοσειράς, και έχουν τις δικές τους συναρτήσεις για πράξεις μεταξύ των τελεστών αυτών. Ένα σημαντικό γεγονός, είναι ότι η βιβλιοθήκη GMP είναι προκαθορισμένη να είναι ανενεργή στην PHP. Για να την ενεργοποιήσουμε και να μπορούμε να την χρησιμοποιήσουμε έπρεπε να φύγουμε από σχόλιο την γραμμή extension=php_gmp.dll που βρίσκεται στο αρχείο php.ini και να επανεκκινήσουμε τον εξυπηρετητή.

Συνεχίζουμε προσδιορίζοντας κάποια βασικά στοιχεία που χρησιμοποιήθηκαν για την εμφάνιση της ιστοσελίδας.

Εμφάνιση Ιστοσελίδας: Ένας βασικός πυλώνας κατά την ανάπτυξη του συστήματος ήταν η φιλικότητα του συστήματος προς το χρήστη. Για το λόγο αυτό έχουμε χρησιμοποιήσει αρκετές βιβλιοθήκες, φόρμες με τεχνολογία HTML5, διαδραστικούς χάρτες στη γραφική διεπαφή του συστήματος.

Πρωτίστως, έχουμε χρησιμοποιήσει τη δωρεάν βιβλιοθήκη Fancybox, η οποία χρησιμοποιείται ευρέως τα τελευταία χρόνια. Η βιβλιοθήκη αυτή προσφέρει τη δυνατότητα εμφάνιση μίας σελίδας εντός μίας άλλης, με εντυπωσιακό τρόπο χωρίς να χρειάζεται να μετακινηθούμε από την πρώτη σελίδα. Έχει χρησιμοποιηθεί στο σύστημα μας για την εμφάνιση των πληροφοριών για τους υποψήφιους καθώς επίσης και για την εμφάνιση του εγχειρίδιου χρήσης.

Η εμφάνιση των ιστοσελίδων του συστήματος επιτυγχάνεται από τα αρχεία CSS τα οποία χρησιμοποιεί η εφαρμογή. Επίσης χρησιμοποιείται ολισθητής (slider), για να την ομαλή

μεταφορά από τη μια σελίδα του συστήματος στην άλλη. Η μετάβαση αυτή φαίνεται σαν μία μετακίνηση προς τα δεξιά ή τα αριστερά. Να σημειωθεί ότι η τεχνική αυτή δεν χρησιμοποιείται για μετάβαση σε σελίδα η οποία αφορά σύστημα άλλης αρχής.

Οι φόρμες που υπάρχουν στο σύστημα χρησιμοποιούν τεχνολογία HTML5. Ο χρήστης ενημερώνεται μέσω μηνυμάτων στην περίπτωση που έχει καταχωρήσει λάθος στοιχεία σε κάποιο από τα πεδία της φόρμας. Στην περίπτωση που ο ψηφοφόρος επιλέξει ένα πεδίο κειμένου (text box) για να εισαγάγει δεδομένα, πραγματοποιείται μεγέθυνση του πεδίου κειμένου και πριν πραγματοποιηθεί η συμπλήρωση οποιουδήποτε πεδίου από τον ψηφοφόρο υπάρχει μέσα σε αυτό, κείμενο με μεγάλα γκρίζα γράμματα που αναφέρει στον ψηφοφόρο το τι αναμένεται να καταχωρήσει. Εκτός αυτού, στην περίπτωση που το κείμενο που εντάσσει ο ψηφοφόρος στα πεδία κειμένου πληρούν τις απαιτήσεις, εμφανίζεται ένα μικρό πράσινο √ δίπλα από το πεδίο, ενώ εάν δεν τις πληροί εμφανίζεται ένα μικρό κόκκινο x. Ακόμη, η φόρμα δεν καταχωρείται εάν δεν συμπληρωθούν όλα τα απαραίτητα πεδία με την μορφή που ζητείται στο κάθε ένα.

Στην προσπάθειά μας να κάνουμε ένα ολοκληρωμένο και εμφανίσιμο σύστημα ηλεκτρονικής ψηφοφορίας, έχουμε προσθέσει στην σελίδα contact us ένα διαδραστικό χάρτη με πινέζα στην διεύθυνση του Πανεπιστημίου Κύπρου, τον οποίο έχουμε πάρει από την σελίδα των Google Maps. Στην ίδια σελίδα έχουμε προσθέσει μία φόρμα επικοινωνίας, καθώς επίσης και τη διεύθυνση ηλεκτρονικού ταχυδρομείου του πανεπιστημίου, στην οποία ένα μέρος της είναι κρυμμένο. Η διεύθυνση αυτή, είναι προστατευμένη με την τεχνολογία reCaptcha για αποφυγή των spammers.Ένας ψηφοφόρος για να την δει πρέπει να πατήσει επάνω της, και να πληκτρολογήσει ορθά τις λέξεις που θα του εμφανιστούν (Captcha).

Στην υλοποίηση του προτοκόλου IIS, είχαμε κάποιες μικρές διαφοροποιήσεις για να γίνει η εφαρμογή πιο φιλικιά προς το χρήστη.

Διαφοροποιήσεις πρωτοκόλλου από το σύστημα: Κατά τη διαδικασία της εγγραφής, στο πρωτόκολλο αναφέρεται ότι ο χρήστης δίνει ένα αριθμό ο οποίος θα αποτελέσει την ανώνυμη ταυτότητά του, r_{id}, ένα παράγοντα τύφλωσης b και ένα εκθέτη c. Για ευκολία όμως του ψηφοφόρου, ο ψηφοφόρος μπορεί να καταχωρήσει μία λέξη για ανώνυμη ταυτότητά. Την λέξη αυτή, τη μετατρέπουμε σε αριθμό χρησιμοποιώντας την ακόλουθη μαθηματική πράξη:

$$r_{id} = \sum_{i=1}^{n} \mathrm{ASCII}(\mathrm{word}[i]) * (i + 1)$$

Όπου η συνάρτηση ASCII επιστρέφει τον κώδικα ASCII του γράμματος που παίρνει σαν είσοδο, ενώ η έκφραση word[i], το i-οστό γράμμα της λέξης word.

Επίσης ο παράγοντας τύφλωσης και ο εκθέτης παράγονται τυχαία και ομοιόμορφα από το σύστημα για απλοποίηση της διαδικασίας για τον ψηφοφόρο.

Έλεγχοι

Κατά την δημιουργία του συστήματός μας χρειάστηκε να υλοποιήσουμε κάποιους ελέγχους, κάποιους από αυτούς αναφέρονται ρητά στο πρωτόκολλο και κάποιοι όχι. Μερικοί από τους βασικούς ελέγχους αυτούς ανάγονται πιο κάτω:

- Κατά την εισαγωγή του ψηφοφόρου στο σύστημα μέσω της ιστοσελίδας login.php, οι ψηφοφόροι καλούνται να εισάγουν τα κατάλληλα αναγνωριστικά, την ταυτότητα τους και το αντίστοιχο συνθηματικό. Στην περίπτωση που ο ψηφοφόρος δεν καταχωρήσει ορθά την ταυτότητα του ή το αντίστοιχο συνθηματικό του ο ψηφοφόρος δεν εισάγεται στο σύστημα και εμφανίζεται μήνυμα λάθους.
- Ελέγχεται η περίπτωση που ο ψηφοφόρος επιχειρεί να πάρει δεύτερη ανώνυμη ταυτότητα για να ψηφίσει. Το σύστημα δεν του το επιτρέπει και του εμφανίζει μήνυμα λάθους.
- Κατά την διαδικασία της ψηφοφορίας, ο ψηφοφόρος πρέπει να καταχωρήσει την ανώνυμη ταυτότητα του και την αντίστοιχη υπογεγραμμένη ανώνυμη ταυτότητα του, τα οποία έχει διασφαλίσει από τον καταχωρητή. Στην περίπτωση που ο ψηφοφόρος τοποθετήσει λάθος την ανώνυμη ταυτότητά του ή την υπογεγραμμένη ανώνυμη ταυτότητά του, του εμφανίζει μήνυμα λάθους και δεν είναι εφικτή η ψηφοφορία.
- Στην περίπτωση που ο ψηφοφορός επιθυμεί να ψηφίσει εκτός από τον έλεγχο της ανώνυμης ταυτότητας και της υπογεγραμμένης ταυτότητας, υφίσταται ακόμη ένας έλεγχος. Διερευνάται εάν ο κατατεμαχισμός με παράμετρο την ανώνυμη ταυτότητα του ψηφοφόρου, δηλαδή το $h(r_{id})$ βρίσκεται στους εξυπηρετητές ψηφοφορίας, τότε εκτελείται επερώτημα βάσης δεδομένων (sql query) τύπου ενημέρωσης (update). Διαφορετικά, εκτελείται επερώτημα τύπου εισαγωγής (insert). Έτσι στην πρώτη περίπτωση ο παλιός ψήφος του ψηφοφόρου αντικαθίσταται με τον καινούριο, ενώ στην δεύτερη εισάγεται καινούρια ψήφος.
- Γίνεται επίσης έλεγχος για τη μοναδικότητα της ανώνυμης ταυτότητας κατά τη διαδικασία της εγγραφής. Ο ψηφοφόρος για να εξασφαλίσει ανώνυμη ταυτότητα καταχωρεί μία λέξη. Στην περίπτωση που υπάρχει ήδη η ανώνυμη ταυτότητα που εισήγαγε ο ψηφοφόρος στην βάση δεδομένων του καταχωρητή, εμφανίζεται κατάλληλο μήνυμα στον ψηφοφόρο που τον ενημερώνει να καταχωρήσει κάποια

άλλη επιθυμητή ανώνυμη ταυτότητα. Διαφορετικά, καταχωρείται η ανώνυμη ταυτότητα στη βάση δεδομένων του καταχωρητή.

Επίσης πραγματοποιούνται έλεγχοι επικύρωσης των δεδομένων σε όλα τα πλαίσια κειμένου, τα οποία υπάρχουν στις φόρμες του συστήματός μας. Τα πλαίσια κειμένου που υπάρχουν είναι τα εξής:

1. Εισαγωγή Ανώνυμης Ταυτότητας(R_{id}): Γίνεται έλεγχος εάν η ανώνυμη ταυτότητα που καταχωρεί ο ψηφοφόρος περιλαμβάνει κεφαλαία, μικρά γράμματα ή αριθμούς. Οι επιτρεπτοί χαρακτήρες είναι γράμματα και αριθμοί.
2. Εισαγωγή Υπογεγραμμένης Ανώνυμης Ταυτότητας: Γίνεται έλεγχος εάν η υπογεγραμμένη ανώνυμη ταυτότητα είναι αριθμός.
3. Εισαγωγή Μυστικής λέξης: Γίνεται έλεγχος εάν αποτελείται από γράμματα ή αριθμούς, και εάν το μέγεθός της είναι έξι ψηφία.

Συναρτήσεις οι οποίες έχουν υλοποιηθεί

Για την υλοποίηση του πρωτοκόλλου όπως αναφέρεται, χρειάστηκε η δημιουργία συναρτήσεων οι οποίες επικοινωνούν με την βάση δεδομένων της κάθε αρχής. Έτσι παραθέτουμε τις πιο κάτω συναρτήσεις, τις οποίες έχουμε υλοποιήσει για να προσκομίζουμε δεδομένα από τις βάσεις δεδομένων:

- Σύνδεση και τερματισμός σύνδεσης με τις βάσεις δεδομένων.
- Εύρεση ψηφοφόρου από τη βάση δεδομένων του καταχωρητή.
- Εύρεση εάν κάποιο $h(r_{id})$ υπάρχει στην λίστα L του καταχωρητή.
- Εισαγωγή ενός συγκεκριμένου $h(r_{id})$ στη βάση δεδομένων.
- Έλεγχος εάν ο ψηφοφόρος έχει ήδη εξασφαλίσει $R_{id.}$
- Εύρεσης ενός υποψηφίου στη βάση δεδομένων του καταχωριτή και εμφάνιση των πληροφοριών του στην γραφική διεπαφή του συστήματος.
- Εύρεση του ονόματος ενός υποψηφίου παίρνοντας σαν είσοδο τον μοναδικό του αριθμό.

Επίσης εκτός από τις λειτουργίες οι οποίες περιγράφονται από το πρωτόκολλο, έχουμε υλοποιήσει την προβολή των στοιχείων του υποψηφίου στη σελίδα "Vote". Στην περίπτωση που ο ψηφοφόρος πατήσει την εικόνα ή το όνομα ενός υποψηφίου, εμφανίζεται η αντίστοιχη περιγραφή του υποψηφίου, ενώ όταν πατήσει τον σύνδεσμό "click to vote <Candidate Name>" κάτω από την εικόνα του υποψηφίου εμφανίζεται ένα παράθυρο για να ψηφίσει τον υποψήφιο της αρεσκείας του.

Τα στοιχεία των υποψηφίων μαζί με τις αντίστοιχες φωτογραφίες τους, δεν είναι ενσωματωμένα στον κώδικα της σελίδας αλλά εισάγονται δυναμικά από τη βάση δεδομένων.

Ανάλογα με την κατάταξη τους στη βάση δεδομένων εμφανίζονται στην κατάλληλη θέση στην ιστοσελίδα. Σε κάθε σειρά της ιστοσελίδας, υπάρχει δυνατότητα εμφάνισης τριών υποψηφίων, τα ονόματα και οι αντίστοιχες φωτογραφίες τους. Οι φωτογραφίες των υποψηφίων βρίσκονται αποθηκευμένες στη βάση δεδομένων σε τύπο BLOB.

Μία συνάρτηση η οποία είναι εύκολα υλοποιήσιμη με μεγάλη χρήση είναι η συνάρτηση mod. Κρίθηκε αναγκαίο η υλοποίηση της, μιας και ο τελεστής % στην γλώσσα PHP στην περίπτωση που ο τελεστέος είναι αρνητικός τότε το αποτέλεσμά της εφαρμογής του τελεστή mod στον τελεστέο είναι αρνητικό. Η συνάρτησή η οποία έχει υλοποιηθεί από εμάς, προσθέτει στο αποτέλεσμα της εφαρμογής του τελεστή τον πρώτο αριθμό p τον οποίο χρησιμοποιούμε στην δεξιά πλευρά του τελεστή, ούτως ώστε να παράγεται ένα θετικό αποτέλεσμα όπως και είναι το θεμιτό αποτέλεσμα της συνάρτησης.

Γενικά στοιχεία υλοποίησης

Κλείνοντας την περιγραφή της υλοποίησης, θα αναφέρουμε κάποια γενικά στοιχεία που αφορούν την υλοποίηση του συστήματός μας ως σύνολο. Τα κυριότερα από αυτά αναφέρονται πιο κάτω:

- Κάθε εξυπηρετητής και αρχή έχει υλοποιηθεί ανεξάρτητα, όπως επίσης και οι βάσεις δεδομένων για κάθε μία αρχή και εξυπηρετητή. Αυτό σημαίνει ότι ο κώδικας ιστού και οι βάσεις δεδομένων θα μπορούσαν κάλλιστα να τρέχουν σε διαφορετικές μηχανές, αλλάζοντας απλά τις διευθύνσεις IP οι οποίες αναφέρονται στους συνδέσμους του κώδικα.
- Η ιστοσελίδα κάθε αρχής έχει επικοινωνία μόνο με την βάση δεδομένων της συγκεκριμένης αρχής.
- Η μετάβαση πληροφοριών από μία ιστοσελίδα στον εξυπηρετητή, γίνεται με τρεις διαφορετικούς τρόπους. Στην πρώτη, εάν ο ψηφοφόρος καλείται να συμπληρώσει μία φόρμα, όπως για παράδειγμα να συμπληρώσει την λέξη που θα αποτελεί την ανώνυμη ταυτότητά του, ο εξυπηρετητής παίρνει τα στοιχεία με την μέθοδο POST. Η δεύτερη μέθοδος η οποία έχει χρησιμοποιηθεί ήταν με το πέρασμα παραμέτρων στη διεύθυνση της σελίδας, όπως για παράδειγμα την example.php?show_results=1, τις οποίες παραλαμβάνει ο εξυπηρετητής με την μέθοδο GET. Η τελευταία μέθοδος γίνεται χρησιμοποιώντας cookies.

Κεφάλαιο 6

Συμπεράσματα και Μελλοντικές Επεκτάσεις

Η ηλεκτρονική ψηφοφορία είναι ένα ενδιαφέρον και συνάμα περίπλοκο θέμα. Ένα σύστημα ηλεκτρονικής ψηφοφορίας πρέπει να διέπεται από ένα σύνολο απαιτήσεων, τόσο ασφάλειας, όσο και πρακτικότητας, οι οποίες πιθανόν αλληλοεπηρεάζονται. Έτσι, χρειάζεται να γίνεται εκτενής μελέτη στα προτεινόμενα πρωτόκολλα ούτως ώστε να μειώνονται τα πιθανά μειονεκτήματά τα οποία ίσως να έχουν. Απώτερος στόχος είναι η δημιουργία πρωτοκόλλων και κατά επέκταση συστημάτων που επικεντρώνονται και ικανοποιούν ολοένα και παραπάνω απαιτήσεις.

Η ηλεκτρονική ψηφοφορία, είναι μία μέθοδος ψηφοφορίας, η οποία ίσως στο μέλλον αντικαταστήσει πλήρως την παραδοσιακή έντυπη μορφή ψηφοφορίας. Σε κάθε περίπτωση, η ηλεκτρονική ψηφοφορία έχει πολλά να προσφέρει, όπως μείωση των δαπανών ενός κράτους ή οργανισμού τις οποίες θα χρειάζονταν για εκτύπωση ψηφοδελτίων, χαρτί, μελάνι, και προσωπικό. Επίσης προσφέρει ταχύτητα στην μέτρηση των ψήφων και καταμέτρηση αποτελεσμάτων καθώς επίσης και ένα μεγάλο φάσμα άλλων πλεονεκτημάτων.

Η Διπλωματική αυτή εργασία, μου έχει δώσει την ευκαιρία να ασχοληθώ τόσο με τα στάδια και τις απαιτήσεις ενός συστήματος ηλεκτρονικής ψηφοφορίας, με τη μελέτη υπάρχον συστημάτων και πρωτοκόλλων, όσο και με τη δημιουργία ενός δικού μου συστήματος ηλεκτρονικής ψηφοφορίας. Έχουμε μελετήσει και αξιολογήσει συστήματα ηλεκτρονικής ψηφοφορίας ως προς τις απαιτήσεις ηλεκτρονικής ψηφοφορίας που πληρούν, καθώς επίσης έχουμε μελετήσει αναλυτικά το σύστημα της Εσθονίας και της Ελβετίας, από τα οποία έχουμε πάρει σημαντικές πληροφορίες, για τον τρόπο που μπορούν να εφαρμοστούν πρωτόκολλα στην πράξη. Επίσης έχουμε μελετήσει το πως τα πρωτόκολλα ηλεκτρονικής ψηφοφορίας χρησιμοποιούν ένα φάσμα κρυπτογραφικών τεχνικών και κρυπτογραφικών μοντέλων, για να διασφαλίσουν την ασφάλεια του συστήματος, καθώς επίσης ότι οι ψήφοι δεν πρόκειται να συνδυαστούν με τους ψηφοφόρους οι οποίοι τις έχουν υποβάλλει.

Πιο συγκεκριμένα έχουμε μελετήσει τα πρωτόκολλα Six-authority protocol, Foo Protocol, An Anonymous Electronic Voting Protocol for Voting Over The Internet, το πρωτόκολλο REVS, το πρωτόκολλο των Wu και Sankaranarayana καθώς επίσης το A Novel Simple Secure Internet Voting Protocol. Κάθε ένα από αυτά έχει μερικά ισχυρά πλεονεκτήματα, όσο και κάποια μειονεκτήματα.

Στην συνέχεια επιλέξαμε ένα πρωτόκολλο ψηφοφορίας, βασισμένο στο IIS. Το πρωτόκολλο το οποίο έχουμε επιλέξει, παρουσιάζει μια μέθοδο ψηφοφορίας, η οποία διαφέρει από τα υπόλοιπα πρωτόκολλα, λόγω του γεγονότος ότι η ασφάλεια της ψήφους, δε διασφαλίζεται άμεσα μέσω κάποιων κρυπτογραφικών κλειδιών αλλά κυρίως μέσα από την διάσπαση της ψήφους και τη διανομή των τμημάτων που προκύπτουν σε πολλαπλούς εξυπηρετητές. Το έχουμε επιλέξει ως καλύτερο έναντι των υπολοίπων, προσφέρει ακόμη το πλεονέκτημα του δικαιώματος του ψηφοφόρου να ξαναψηφίσει, κάτι που δεν προσφέρεται από τα υπόλοιπα, ή στην περίπτωση που προσφέρεται, αυτό δεν γίνεται αποδοτικά.

Το πρωτόκολλο αυτό, έχει υλοποιηθεί πλήρως, με τη χρήση κυρίως των γλωσσών PHP, Javascript και MySQL. Το σύστημα το οποίο έχουμε υλοποιήσει τρέχει σε όλους του φυλλομετρητές και παρέχει τις απαιτήσεις ασφάλειας και πρακτικότητας οι οποίες πληρούνται από το πρωτόκολλο. Επίσης εξασφαλίζουμε ακόμη μεγαλύτερη ασφάλεια από το γεγονός ότι τρέχει σε Secure Socket Layer. Γίνονται αρκετοί έλεγχοι για να διασφαλιστεί η ασφάλεια του συστήματος.

Εν κατακλείδι η δημιουργία αλλά και η εφαρμογή ενός πρωτοκόλλου ηλεκτρονικής ψηφοφορίας, θα πρέπει να γίνεται δίνοντας προσοχή σε λεπτομέρειες της διαδικασίας. Η χρήση λεπτών διαδικασιών, επιβάλλεται, αφού κάθε τι ίσως να επηρεάσει τα δημοκρατικά δικαιώματα του κάθε ψηφοφόρου. Ακόμη μπορούμε να προσθέσουμε, ότι εφόσον υπάρχουν ήδη πρωτόκολλα, τα οποία έχουν υιοθετηθεί από χώρες με επιτυχία, τότε η εφαρμογή τους και στις υπόλοιπες χώρες είναι εφικτή, και ίσως είναι θέμα χρόνου για να επεκταθεί η μέθοδος της ηλεκτρονικής ψηφοφορίας σε περισσότερες χώρες. Υπάρχει ένα μεγάλο σύνολο κρυπτογραφικών μοντέλων και τεχνικών, οι οποίες θα μπορούσαν, συνδυασμένες ή μη, να χρησιμοποιηθούν για ανάπτυξη ενός ισχυρότερου πρωτοκόλλου. Ακόμη, η έμφαση σε μια απαίτηση της ασφάλειας ή πρακτικότητας ίσως να επηρεάζει κάποια άλλη απαίτηση. Έτσι αυτό που είναι θεμιτό, είναι να πληρούνται όλες οι απαιτήσεις αυτές, στο μεγαλύτερο δυνατό βαθμό.

Ίσως το πιο σημαντικό σημείο το οποίο έχω αντιληφθεί μέσω της διπλωματικής αυτής εργασίας, είναι το γεγονός ότι οι απαιτήσεις ασφάλειας και πρακτικότητας ενός συστήματος, πρέπει να είναι πάντα στη σκέψη του δημιουργού, και το σύστημα το οποίο δημιουργείται να αναπτύσσεται έχοντας πάντοτε γνώμονα τις απαιτήσεις αυτές. Έτσι, μελλοντικά ίσως όλος ο κόσμος να είναι σε θέση να εμπιστεύεται τα συστήματα αυτά, και να τα χρησιμοποιεί, οπουδήποτε, και οποτεδήποτε. Αυτό θα είχε ως αποτέλεσμα την αύξηση των ποσοστών των ψηφοφόρων εφόσον θα είναι πλέον σίγουροι, ότι η ψήφος τους θα καταμετρηθεί όπως ακριβώς έχει καταχωρηθεί, μέσα σε ένα πλαίσιο απολύτως ασφαλές, νόμιμο και δημοκρατικό.

Μελλοντικές Επεκτάσεις

Το σύστημα το οποίο έχω υλοποιήσει, τηρεί επακριβώς την περιγραφή του πρωτοκόλλου IIS. Είναι ένα ολοκληρωμένο σύστημα, και έχουμε δείξει ότι η όλη διαδικασία της ψηφοφορίας γίνεται ορθά, καθώς μπορούμε να ελέγξουμε τα αποτελέσματά της μέσω της σελίδας των αποτελεσμάτων.

Παρόλα αυτά θα μπορούσε το σύστημα αυτό να επεκταθεί περαιτέρω.

Θα μπορούσαμε να εντοπίζουμε έναν εξυπηρετητή, ο οποίος προσπαθεί να εξαπατήσει και να αλλοιώσει τα αποτελέσματα. Θα μπορούσε δηλαδή να υπάρχει ακόμη μία διαδικασία η οποία θα τρέχει, για να ανακαλύπτει πιθανές απάτες και συγκεκριμένα ποιος διακομιστής ή υπολογιστής έχει κάνει την απάτη.

Η είσοδος ενός ψηφοφόρου στο σύστημα χρησιμοποιώντας την ταυτότητα και το συνθηματικό του, το οποίο χρησιμοποιείται σχεδόν σε όλα τα διαδικτυακά συστήματα εγκυμονεί πολλούς κινδύνους. Στην περίπτωση ηλεκτρονικής ψηφοφορίας, κάποιος τρίτος, ίσως και άτομο της οικογένειας, ο οποίος γνωρίζει τα συνθηματικά για κάποιο ψηφοφόρο, θα ταυτοποιηθεί ως τον ψηφοφόρο από το σύστημα, και θα είναι σε θέση να ψηφίσει για αυτόν. Αυτό είναι μεγάλο μειονέκτημα, καθώς πλήττει τα δημοκρατικά δικαιώματα κάποιου ψηφοφόρου.

Έτσι, ακόμη μία πιθανή επέκταση του συστήματος μου η εισδοχή στο σύστημα να γίνεται με τη χρήση βιομετρικών στοιχείων. Στη σελίδα εισδοχής του συστήματος, θα μπορούσε να γίνεται αναγνώριση προσώπου ή ίριδας, για να πιστοποιείται ότι το άτομο το οποίο έχει καθίσει μπροστά από τον υπολογιστή για να ψηφίσει είναι νόμιμος ψηφοφόρος, και ότι είναι όντως αυτός και όχι μία φωτογραφία του. Σε μία τέτοια περίπτωση όμως, θα πρέπει και να υπάρχει μία βάση δεδομένων με όλα τα βιομετρικά στοιχεία των ανθρώπων, πράγμα το οποίο ίσως και να παραβιάζει ένα μέρος της ανθρώπινης ιδιωτικότητας. Επίσης αυτό ταυτόχρονα θα προϋπόθετε αγορά κάμερας, ενώ όσον αφορά αναγνώριση μέσω ίριδας, θα χρειαζόταν κάμερα με υψηλό κόστος, η οποία θα είχε και υψηλότερη ανάλυση.

Μια άλλη ακόμη πιθανή επέκταση του συστήματος μου, είναι το να επιτρέπει την ψηφοφορία περισσότερων του ενός ατόμου. Σε αρκετές περιπτώσεις, αυτό που επιζητούμε δεν είναι να ψηφίσουμε ένα άτομο (όπως στις προεδρικές εκλογές), αλλά πολλά όπως στις

βουλευτικές εκλογές, ή ακόμη και στις εκλογές φοιτητικών αντιπροσώπων. Το πρωτόκολλο θα μπορούσε να μετατραπεί ελαφρώς, καθώς επίσης και το σύστημα, ούτως ώστε η ψηφοφορία περισσότερων του ενός ατόμου να είναι πλέων επιτρεπτή.

Μία μελλοντική επέκταση του συστήματος μου, θα ήταν να αυξηθούν οι τιμές των παραμέτρων του συστήματος n και k ούτως ώστε να διασφαλίζεται ακόμη περισσότερο η ασφάλεια του συστήματος καθώς επίσης να διασφαλιστεί ότι οι εξυπηρετητές οι οποίοι συμμετέχουν στην ηλεκτρονική αυτή ψηφοφορία, είναι αρκετά ισχυροί και δεν πρόκειται να πέσουν από επιθέσεις τύπου DDOS. Ένα άλλο θέμα είναι και η μελέτη του τρόπου με τον οποίο οι ψηφοφόροι εξασφαλίζουν το όνομα χρήστη και τον κωδικό τους, καθώς επίσης και τον τρόπο που τα παραλαμβάνουν ξανά σε περίπτωση που τα ξεχάσουν.

Επίσης εφόσον παρουσιάζουμε το βιογραφικό ενός υποψηφίου, θα μπορούσε ίσως να εμφανίζεται και κάποιο τηλεοπτικό spot το οποίο έχει γίνει για τον συγκεκριμένο υποψήφιο.

Η εμπιστοσύνη του συστήματος από τους ψηφοφόρους είναι κλειδί για επιτυχία του συστήματος. Συνεπώς εάν ο κώδικας αυτός μετατραπεί σε ανοικτό κώδικα, ίσως πιθανά λάθη ασφαλείας τα οποία θα προέκυπταν να αναγνωρίζονταν από το κοινό, καθώς επίσης θα μπορούσε οποιοσδήποτε να ελέγξει την ορθότητα της διαδικασίας.

Βιβλιογραφία

[1] Chen, T.S. 2003, Electronic Voting, [online], https://files.nyu.edu/tsc223/public/ElectronicVoting.pdf (accessed: 26 June 2012)

[2] Edenbrandt A., "Chordal graph recognition is in NC," Inform, Process, Lett., vol. 24, pp 239-241, 1987.

[3] Estonian National Electoral Committee 2010, *E-Voting System*, [online] http://www.vvk.ee/public/dok/General_Description_E-Voting_2010.pdf (accessed: 25 June 2012)

[4] Estonian National Electoral Committee, *Be, know, do*: Internet Voting in Estonia, [online], http://www.vvk.ee/voting-methods-in-estonia/engindex/id-card/the-estonian-id-card/ (accessed: 26 June 2012)

[5] Fulekrson D.R. and Gross O.A. "Incidence matrices and interval graphs," Pacific J.Math., vol. 15, pp. 835-855, 1965.

[6] Gilmore P.C. and Hoffaman A.J., "A characterization of comparability graphs and of interval graphs, "Canad. J.Math., vol. 16, pp. 539-548, 1964.

[7] Golumbic M.C., Algorithmic Graph Theory and Perfect Graphs, Academic Press, Inc., New York, 1980.

[8] Gupta N, Kumar P, Chhokar S 2011, 'A secure blind Signature Application in E Voting', Proceedings of the 5th National Conference; INDIACom-2011,Computing For Nation Development, March 10 – 11,2011, Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi

[9] Horn, R, and Johnson, C 1990, *Matrix Analysis*, Cambridge University Press, United States of America

[10] Ibrahim, S., Kamat, M., Salleh, M. And Aziz, S.R.A., 2003. Secure E-voting with blind signature, Telecommunication Technology, 2003. NCTT 2003 Proceedings. 4th National Conference on 2003, pp. 193-197

[11] Ion, M., Posea,I., 2011. An Electronic Voting System Based On The Blind Signature Protocol. *Computer Science Master Research*, 1(1)

[12] R. Joaquim, A. Zúquete, and P. Ferreira. REVS - A Robust Electronic Voting System. *IADIS Int. Journal on WWW/ Internet*, 1(2):47--63, Dec. 2003.

[12] Joyce J, Understanding Digital Certificates – A beginner's guide, [online] http://www.scientificcomputing.com/understanding-digital-certificates.aspx (accessed: 10 September 2012)

[13] Payton , L 2012 **,** 'NDP voting disruption deliberate, hard to track**',** *CBC News*, [online] http://www.cbc.ca/news/politics/story/2012/03/27/pol-ndp-voting-disruption-deliberate.html (accessed: 28 June 2012)

[14] Parakh A, Kak S (2010): Internet Voting Protocol Based on Improved Implicit Security, Cryptologia, 34:3, 258-268

[15] Indrajit Ray, Indrakshi Ray, and Natarajan Narasimhamurthi. 2001. An Anonymous Electronic Voting Protocol for Voting Over The Internet. In Proceedings of the Third International Workshop on Advanced Issues of E-Commerce and Web-Based Information Systems (WECWIS '01)(WECWIS '01). IEEE Computer Society, Washington, DC, USA, 188-.

[16] *Rosner* ,IM & Rosner G 2002, *Electronic Voting Protocols and Schemes*,1 September, The Hebrew University of Jerusalem, [online] http://www.cs.huji.ac.il/~ns/Voting2.pdf (accessed: 22 June 2012)

[17] Rivest R.L, Shamir A & Adleman L.M February 1978, 'A method for obtaining digital signatures and public-key cryptosystems ', *Communications of the ACM*,21(2):120-126

[18] Rosner, I.M. And Rosner, G., Spring Semester 2002. *Electronic Voting Protocols and Schemes, Lecture Notes Based on Lectures by Dahlia Malkhifor the course "Advanced Topics in Computer Security" (67916).* School of Engineering and Computer Science The Hebrew University of Jerusalem, Israel.

[19] Salomaa, A 1996,'Zero-knowledge Proofs of Identity' in Brauer W, Rozenberg G, Salomaa A (ed.) *Public-Key Kryptography*, Second Edition,Springer,Berlin, pp.213-18

[20] Wikipedia 2012, *New Democratic Party*, [online] http://en.wikipedia.org/wiki/New_Democratic_Party (accessed: 1 July 2012)

[21] Wikipedia 2012, *Electronic Voting*, [online] http://en.wikipedia.org/wiki/Electronic_voting (accessed: 26 June 2012)

[22] The Linux Documentation Project, SSL, What is SSL and what are Certificates?, [online] http://tldp.org/HOWTO/SSL-Certificates-HOWTO/x64.html (accessed: 13 September 2012)

Ελληνική Βιβλιογραφία

[23] Βικιπαίδεια 2012, Κρυπτογράφιση Δημόσιου Κλειδιού, MediaWiki, [online] http://el.wikipedia.org/wiki/Κρυπτογράφηση_Δημόσιου_Κλειδιού (accessed: 01 September 2012)

[24] Βικιπαίδεια 2012, Κρυπτογραφία, MediaWiki, [online] http://el.wikipedia.org/wiki/Κρυπτογραφία (accessed: 25 Αύγουστος 2012)

[25] Βικιπαίδεια 2012, Προστασία της Ιδιωτικότητας στην Ηλεκτρονική Ψηφοφορία, MediaWiki, [online] http://el.wikipedia.org/wiki/Προστασία_της_Ιδιωτικότητας_στην_Ηλεκτρονική_Ψηφοφορία (accessed: 29 Αύγουστος 2012)

[26] Βικιπαίδεια 2012, Σχετικά Πρώτοι, MediaWiki, [online] http://el.wikipedia.org/wiki/Σχετικά_πρώτοι (accessed: 25 Αύγουστος 2012)

[27] Δημοσιογραφική Ομάδα Πολίτη 2011,'Αύξηση Της Συμμετοχής Στις Εκλογές. Η ηλεκτρονική ψηφοφορία στην υπηρεσία του πολίτη', *ΕΝΕΡΓΟΣ ΠΟΛΙΤΗΣ*,5 April, [online] http://www.politis-europe.com/cgibin/hweb?-A=106,printer.html&-V=webcontent (accessed: 27 June 2012)

[28] Δημητρίου, Τ., 2011. *Κρυπτογραφία και Ελλειπτικές Καμπύλες*, Διπλωματική Εργασία, Εθνικό Μετσόβιο Πολυτεχνείο.

[29] Μάγκος, Ε 2003, 'Ασφάλεια σε Συστήματα Ηλεκτρονικής Ψηφοφορίας', *Ασφαλή Ηλεκτρονικά Συστήματα Συναλλαγών στο Διαδίκτυο*, Διδακτορική Διατριβή, Παν/μιο Πειραιά, Πειραιάς

[30] Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων, Ψηφιακές Υπογραφές, [online] http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html (accessed: 16 September 2012)

[31] Κάτος Β., Στεφανίδης Γ. 2003, 'Συμμετρική Κρυπτογραφία', σε Τεχνικές Κρυπτογραφίας και κρυπτανάλυσης, εκδόσεις Ζυγός, σελ 157-209

[32] Κάτος Β., Στεφανίδης Γ. 2003, 'Ψηφιακές Υπογραφές', σε Τεχνικές Κρυπτογραφίας και κρυπτανάλυσης, εκδόσεις Ζυγός, σελ 285-310

[33] Μάγκος, Ε., 2003. *Διδακτορική Διατριβή, Ασφαλή Ηλεκτρονικά Συστήματα Συναλλαγών στο Διαδίκτυο*, University of Piraeus.

[34] Μάγκος Κ., Νιξαρλίδης 1999, Κρυπτογραφία σε 'Ασφάλεια στο Διαδύκτιο', Πτυχιακή Εργασία, Α. Ε.Κ.Ε.Φ.Ε Δημόκριτος και ΤΕΙ ΑΘΗΝΩΝ

[35] Παναγιώτης Ε. Νάστου, Παύλος Γ. Σπυράκης & Γιάννης Κ. Σταματίου 2003, *Σύγχρονη κρυπτογραφία : Μια ξέγνοιαστη διαδρομή στα μονοπάτια της,* Ελληνικά Γράμματα, Αθήνα

[37] Παπαδάκης Δ. 2001, Πως λειτουργούν τα ψηφιακά πιστοποιητικά, Δημήτρης Παπαδάκης, [online] http://www.e-papadakis.gr/ola18.htm (accessed: 16 September 2012)

Παράρτημα Α

Εγχειρίδιο χρήσης

Σύστημα Ηλεκτρονικής Ψηφοφορίας,
βασισμένο στο IIS

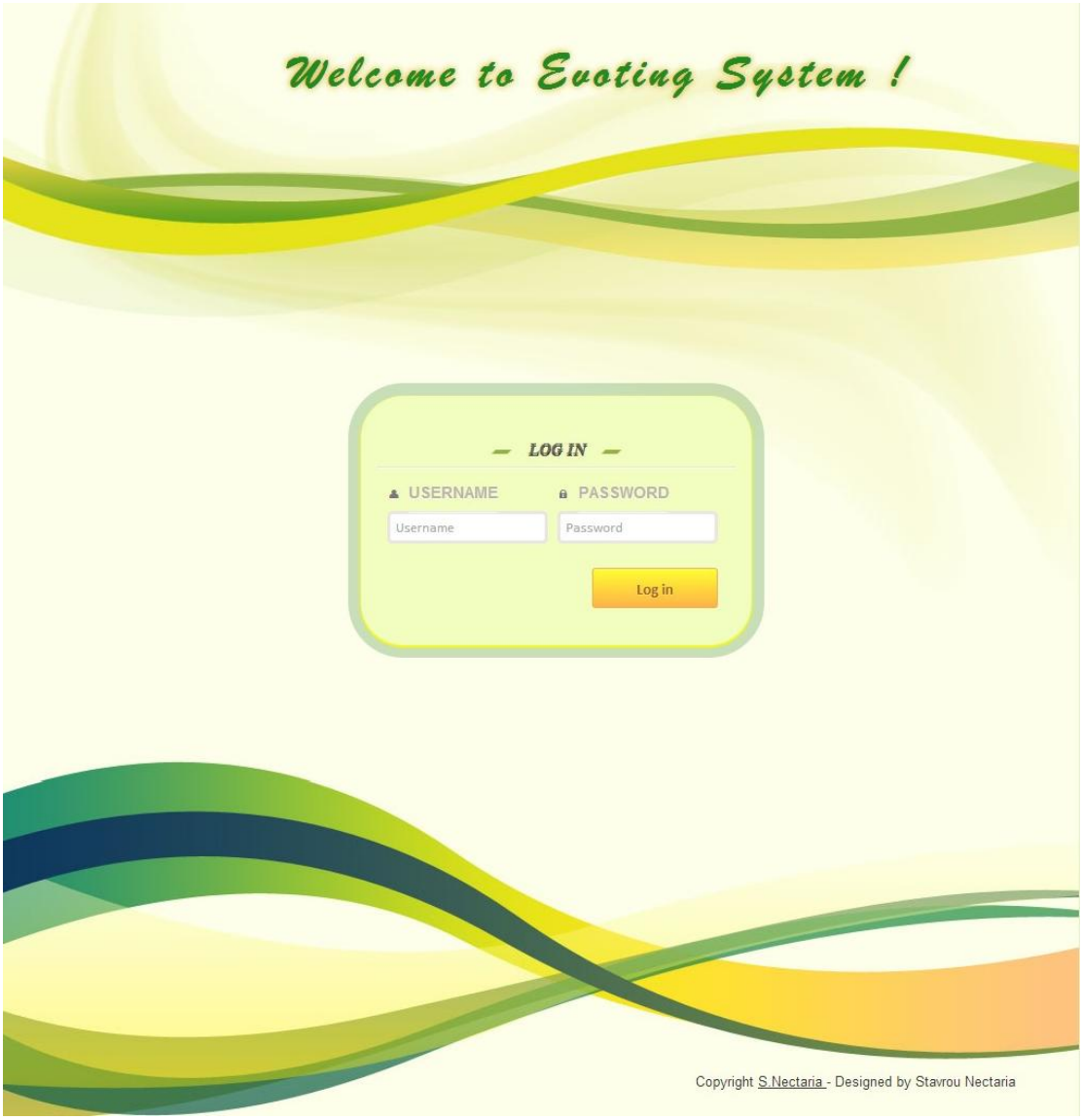
Νεκταρία Σταύρου

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

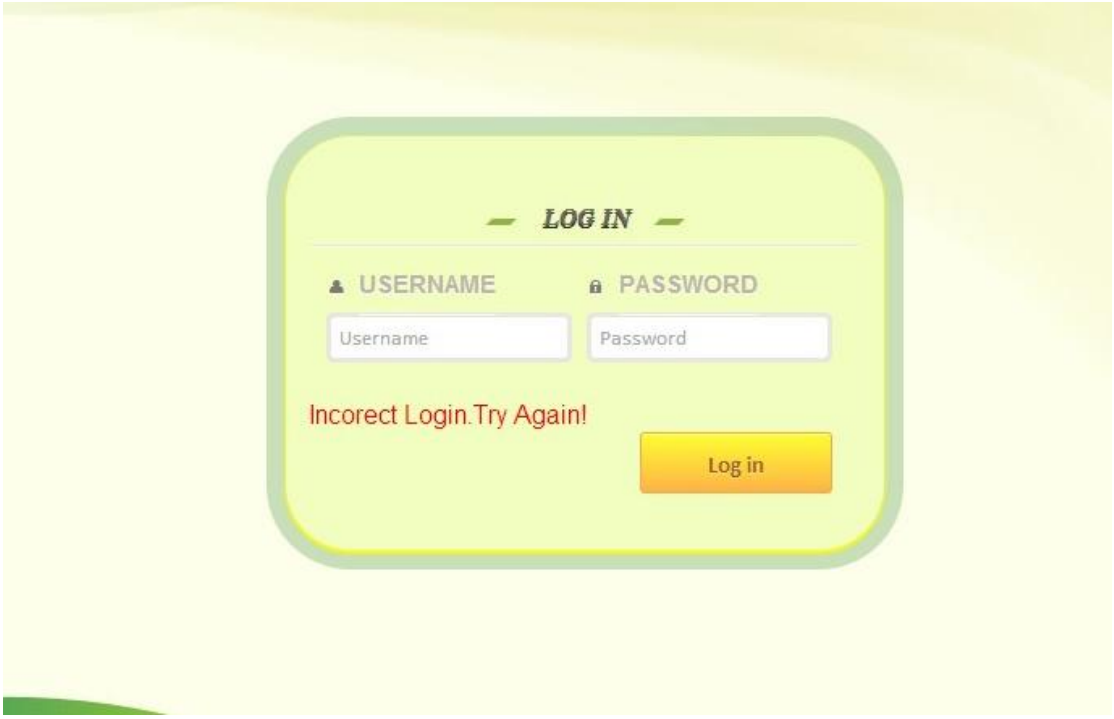
Μάιος 2013

Βήμα 1: Εισδοχή στο σύστημα



Εικόνα Α.1: Η σελίδα εισδοχής στο σύστημα.

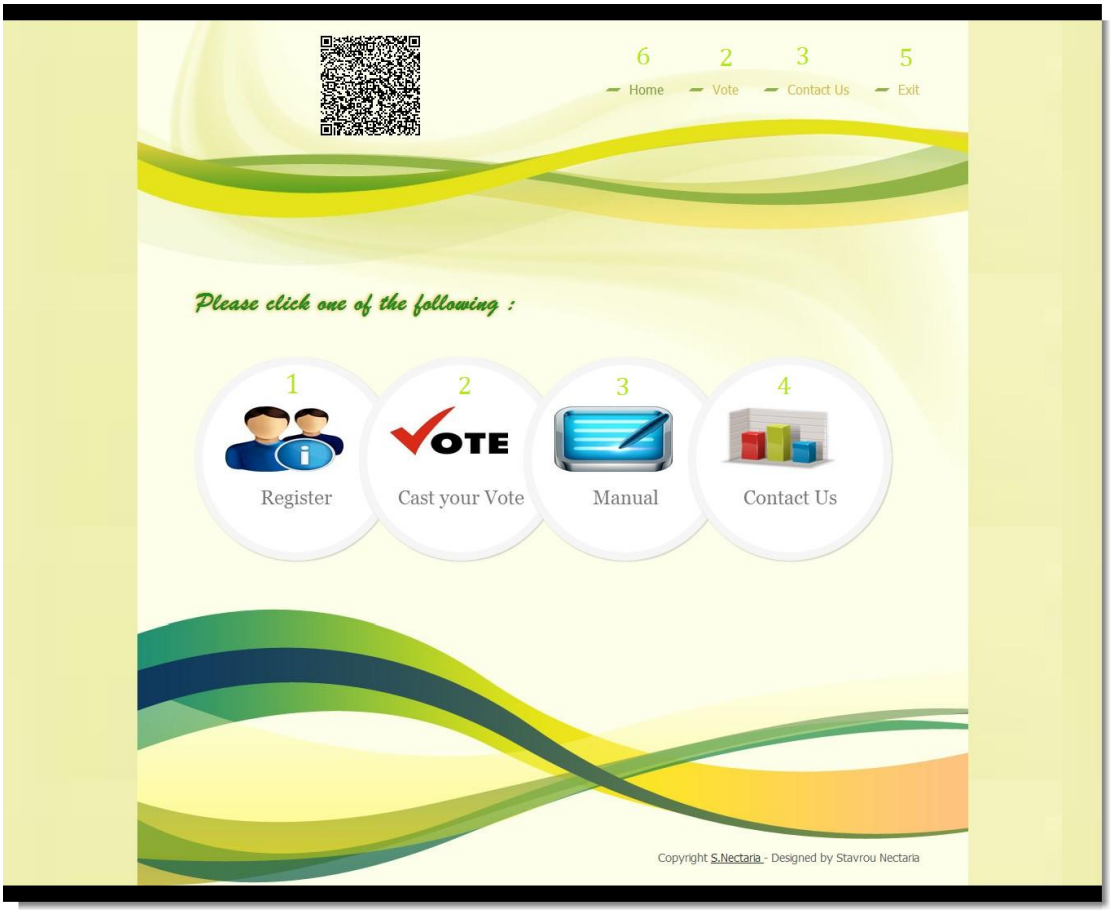
Για να συνδεθούμε με το σύστημα ηλεκτρονικής ψηφοφορίας, και να μπορούμε να ψηφίσουμε, θα πρέπει να πληκτρολογήσουμε την διεύθυνση της σελίδας του συστήματος. Στην συνέχεια, η πιο πάνω σελίδα, είναι η πρώτη σελίδα την οποία θα δούμε.
Για να εισαχθούμε στο σύστημα, θα πρέπει να καταχωρήσουμε το όνομα χρήστη το οποίο έχουμε, το συνθηματικό μας, καθώς επίσης και να πατήσουμε στην συνέχεια το κουμπί Log In.



Εικόνα Α.2: Εμφάνιση μηνύματος λάθους στην σελίδα εισδοχής στο σύστημα.

Στην περίπτωση που στην σελίδα εισδοχής στο σύστημα, η οποία παρουσιάζεται στην Εικόνα Α.1, ο εισάγουμε λάθος στοιχεία, τότε θα μας εμφανιστεί το μήνυμα “Incorrect Login. Try Again”. Έτσι θα μπορέσουμε να ξαναπροσπαθήσουμε να συνδεθούμε με το σύστημα.

Βήμα 2: Παραλαβή ανώνυμης ταυτότητας, και υπογεγραμμένης ανώνυμης ταυτότητας.



Εικόνα Α.3: Η κύρια σελίδα του συστήματος.

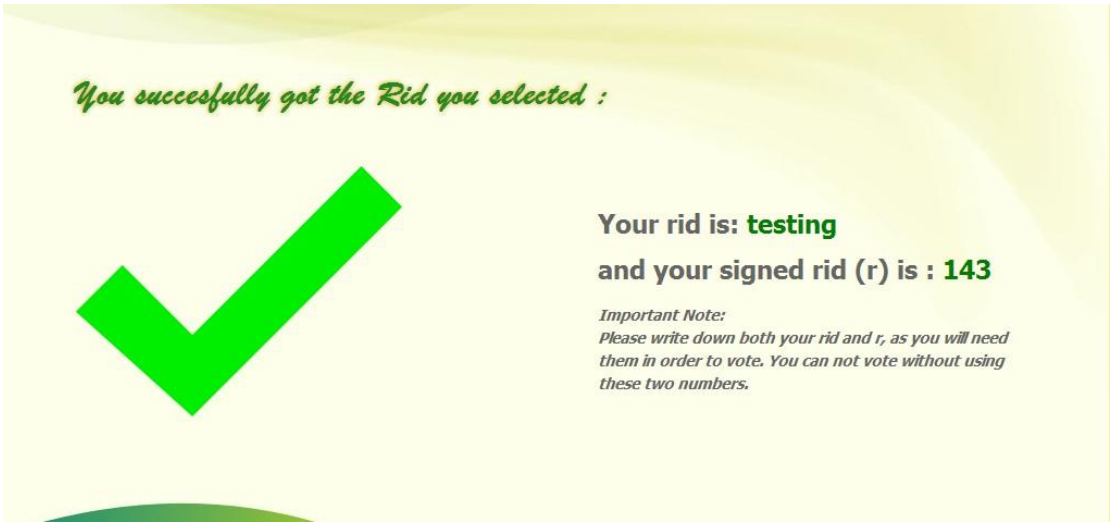
Αμέσως μετά από την είσοδο μας στο σύστημα, εμφανίζεται η κύρια σελίδα του συστήματος, η οποία είναι η πιο πάνω. Αυτό το οποίο θα πρέπει να κάνουμε στην συνέχεια, είναι να παραλάβουμε μία ανώνυμη ταυτότητα, και την υπογραφή της.
Αυτό θα γίνει πατώντας στο κουμπί Register το οποίο βρίσκεται στο σημείο 1. Έτσι, θα μεταβούμε στην σελίδα η οποία παρουσιάζεται στην εικόνα Α.4 για να πάρουμε ανώνυμη ταυτότητα.

Λόγω του ότι η σελίδα αυτή είναι η κεντρική, να αναφέρουμε ακόμη ότι πατώντας στο Cast Your Vote ή Vote στον αριθμό 2, θα μεταβούμε στην σελίδα η οποία παρουσιάζεται στο Α.8, όπου θα μας παρουσιαστούν οι υποψήφιοι για να ψηφίσουμε. Επίσης, πατώντας στο σημείο 3, «Manual», θα μας εμφανιστεί το εγχειρίδιο χρήσης του συστήματος ενώ πατώντας στο Contact us το οποίο βρίσκεται στο σημείο 4, θα μεταβούμε στην σελίδα επικοινωνίας με τον

φορέα της ηλεκτρονικής ψηφοφορίας. Επίσης θα μπορεί ανά πάσα στιγμή να πατήσει στον σύνδεσμο exit, ο οποίος και μας αποσυνδέσει από το σύστημα,. Μπορούμε να μεταβούμε ξανά στην συγκεκριμένη σελίδα, εάν πατήσουμε στον σύνδεσμο home (σημείο 6).

Εικόνα Α.4: Η σελίδα στην οποία ο ψηφοφόρος μπορεί να πάρει μία ανώνυμη ταυτότητα.

Αφού έχουμε πατήσει τον σύνδεσμο Register στην προηγούμενη σελίδα, στη συνέχεια θα μεταβούμε εδώ. Στην φόρμα αυτή, καλούμαστε να γράψουμε μία λέξη αποτελούμενη από γράμματα, αριθμούς ή συνδυασμό των δύο, για να δηλώσουμε την ανώνυμη ταυτότητά την οποία επιθυμούμε να πάρουμε, στο πεδίο κειμένου (σημείο 1). Στην συνέχεια θα χρειαστεί να πατήσουμε το κουμπί στο σημείο 2, για να καταχωρήσουμε την επιθυμητή μας ανώνυμη ταυτότητα.



Εικόνα Α.5: Η σελίδα δήλωσης της επιτυχούς καταχώρησης ανώνυμης ταυτότητας στον ψηφοφόρο.

Η σελίδα αυτή εμφανίζει την ανώνυμη ταυτότητα την οποία έχουμε πάρει ως ψηφοφόροι, την οποία είχαμε δηλώσει στην προηγούμενη σελίδα, καθώς επίσης και την υπογεγραμμένη ανώνυμη ταυτότητά μας.

Στο σημείο αυτό, θα πρέπει να σημειώσουμε σε κάποιο χαρτί και τους δύο αριθμούς, τους οποίους θα χρειαστούμε στην φάση της ψηφοφορίας. Στην περίπτωση που ξεχάσουμε τους αριθμούς αυτούς, δεν θα είμαστε σε θέση να ψηφίσουμε τον υποψήφιο που επιθυμούμε

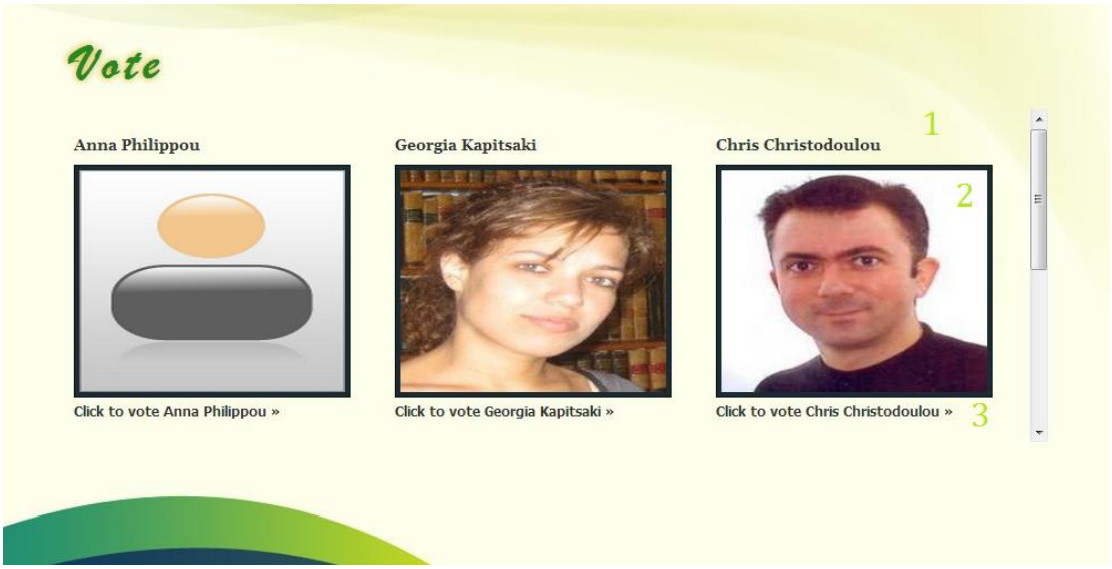
Εικόνα Α.6: Εμφάνιση μυνήματος λάθους στην σελίδα καταχώρησης ανώνυμης ταυτότητας .

Όταν καταχωρήσουμε στην σελίδα καταχώρησης επιθυμητής ανώνυμης ταυτότητας, ανώνυμη ταυτότητα η οποία ήδη έχει καταχωρηθεί σε άλλον ψηφοφόρο, τότε μας εμφανίζεται το μήνυμα ότι η συγκεκριμένη ανώνυμη ταυτότητα έχει ήδη δοθεί, και έτσι θα πρέπει να διαλέξουμε κάποια άλλη.

Εικόνα Α.7: Εικόνα ενημέρωσης ότι ο χρήστης έχει προσπαθήσει να πάρει δεύτερη ανώνυμη ταυτότητα.

Κάθε ψηφοφόρος, δικαιούται να πάρει μόνο μία ανώνυμη ταυτότητα. Στην περίπτωση που προσπαθήσουμε να πάρουμε δεύτερη ανώνυμη ταυτότητα, τότε το μήνυμα αυτό θα μας εμφανιστεί, για να μας ενημερώσει, αλλά και να μας αποτρέψει.

Βήμα 3: Ψήφιση υποψηφίου



Εικόνα Α.8: Η σελίδα εμφάνισης υποψηφίων της ηλεκτρονικής ψηφοφορίας.

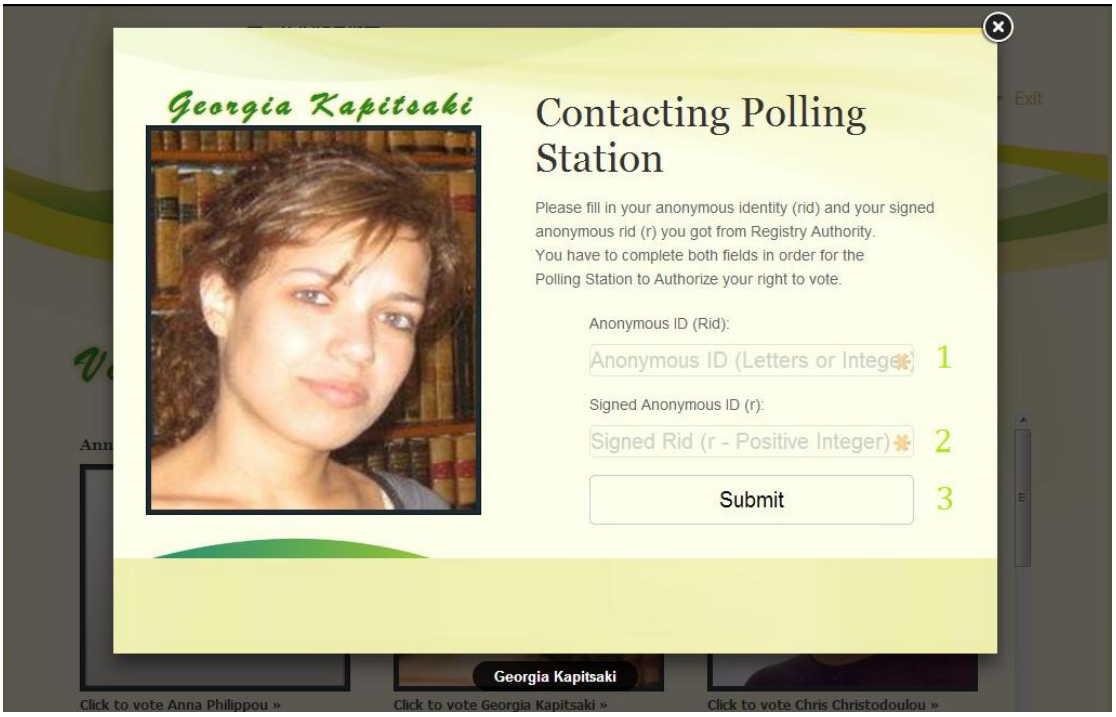
Αφού πάρουμε μία ανώνυμη ταυτότητα, και την υπογραφή της, θα πρέπει να ψηφίσουμε τον υποψήφιο που επιθυμούμε.

Για να το επιτύχουμε αυτό, θα πρέπει να πατήσουμε στον σύνδεσμο “Vote” στο μενού του συστήματος, ή “Cast your Vote” στην κεντρική σελίδα του συστήματος. Έτσι στην συνέχεια θα μεταβούμε στην σελίδα αυτή, η οποία παρουσιάζει όλους τους υποψήφιους του συστήματος.

Εδώ πατώντας στο όνομα (σημείο 1) ή στην φωτογραφία του ψηφοφόρου (σημείο 2) θα εμφανιστούν οι πληροφορίες των υποψηφίων όπως παρουσιάζονται στην εικόνα Α.9. Για να ξεκινήσει την διαδικασία ψήφισης ενός υποψηφίου, θα πρέπει να πατήσουμε στον σύνδεσμο «click to vote» ο οποίος βρίσκεται κάτω από την φωτογραφία του κάθε υποψηφίου όπως φαίνεται στο σημείο 3.

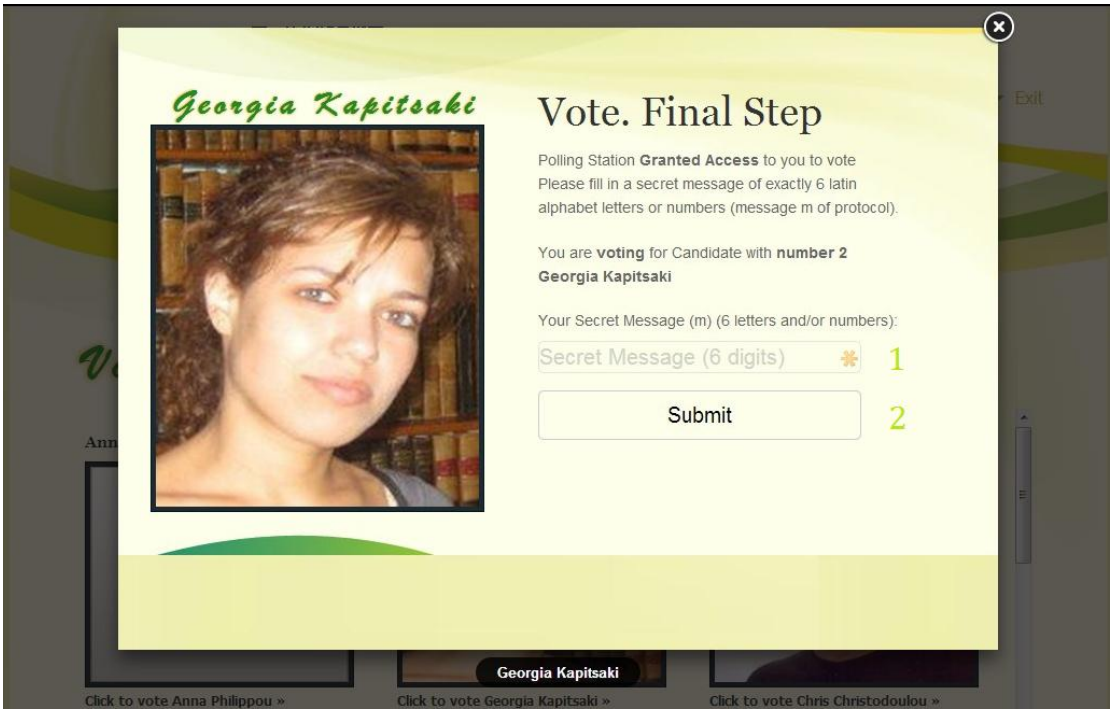
Εικόνα Α.9: Σελίδα εμφάνισης πληροφοριών υποψηφίου.

Πατώντας στο όνομα ή στην φωτογραφία ενός υποψηφίου στην προηγούμενη σελίδα, εμφανίζονται οι πληροφορίες σχετικά με τον υποψήφιο. Πατώντας στο x πάνω δεξιά το παράθυρο κλείνει, και έτσι αφού έχουμε ενημερωθεί, έχουμε την δυνατότητα είτε να ψηφίσουμε είτε να μάθουμε περισσότερες πληροφορίες για κάποιον
άλλον υποψήφιο.



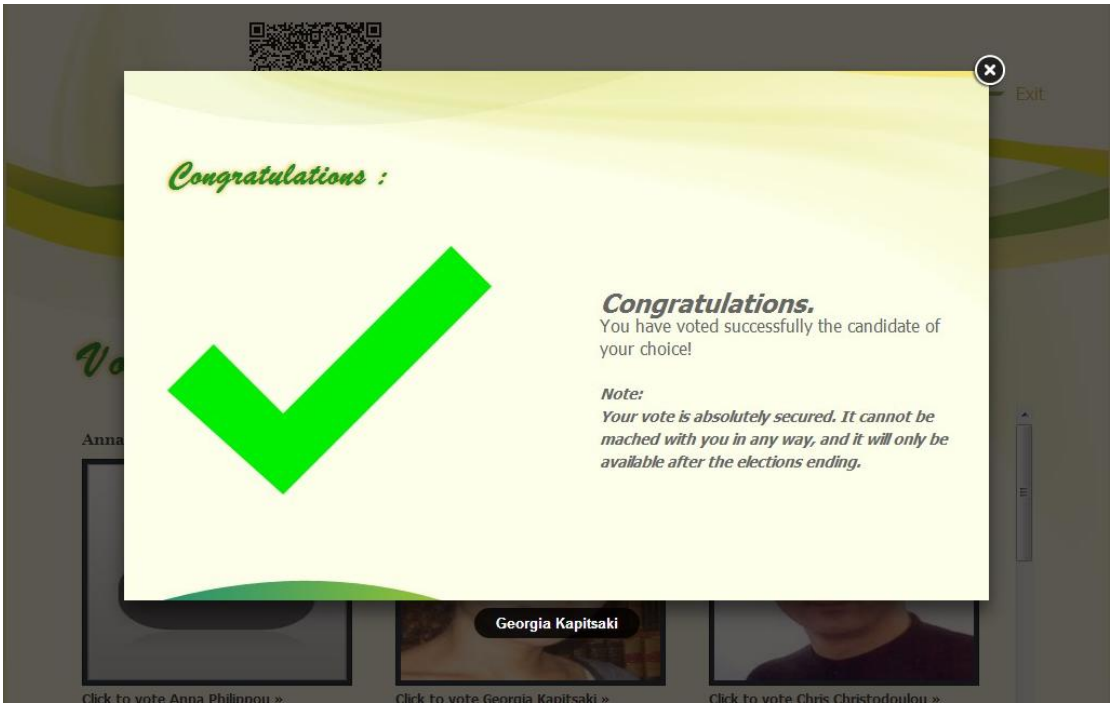
Εικόνα Α.10: Η σελίδα έναρξης της ψηφοφορίας.

Πατώντας στον σύνδεσμο “Click to Vote” κάτω από τον κάθε υποψήφιο, θα μας μεταφέρει στην σελίδα αυτή. Εδώ, ξεκινά η διαδικασία για ψήφιση, ενός υποψηφίου. Στο σημείο αυτό, θα πρέπει να καταχωρήσουμε την ανώνυμη ταυτότητά μας (σημείο 1), και την υπογεγραμμένη ανώνυμη ταυτότητά μας τις οποίες έχουμε πάρει και σημειώσει από την προηγούμενη φάση. Στην συνέχεια θα πρέπει να καταχωρήσουμε τα στοιχεία μας, πατώντας το κουμπί submit το οποίο φαίνεται στο σημείο 3.



Εικόνα Α.11: Η δεύτερη και τελευταία σελίδα ψηφοφορίας υποψηφίου.

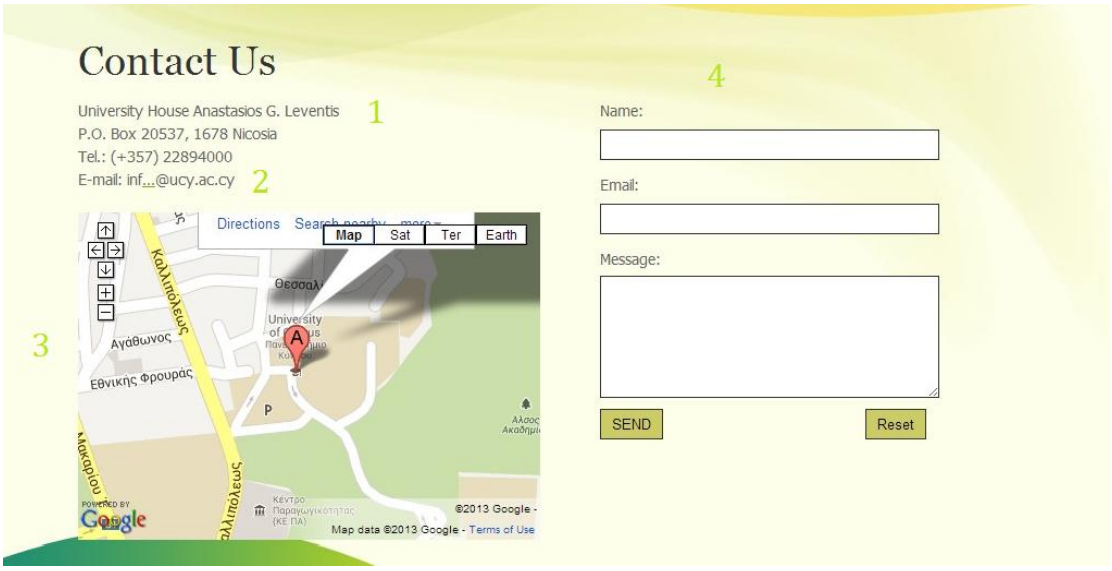
Αφού πατήσουμε submit στην προηγούμενη σελίδα, τότε θα έχουμε μπροστά μας την σελίδα αυτή. Εδώ, χρειάζεται να καταχωρήσουμε στο πεδίο κειμένου στο σημείο 1, μία λέξη 6 γραμμάτων η οποία θα αποτελέσει το μυστικό μας μήνυμα. Η λέξη αυτή είναι αναγκαία να καταχωρηθεί για να ψηφίσουμε. Αφού συμπληρωθεί το πεδίο αυτό, θα πρέπει να πατήσουμε στο κουμπί submit για να καταχωρηθεί η ψήφος μας.



Εικόνα Α.12: Η σελίδα εμφάνισης επιτυχής ψηφοφορίας.

Στην συνέχεια θα μας εμφανιστεί η σελίδα αυτή, η οποία δηλώνει επιτυχία στην ψηφοφορία, και ότι η ψήφος μας έχει καταχωρηθεί σωστά.

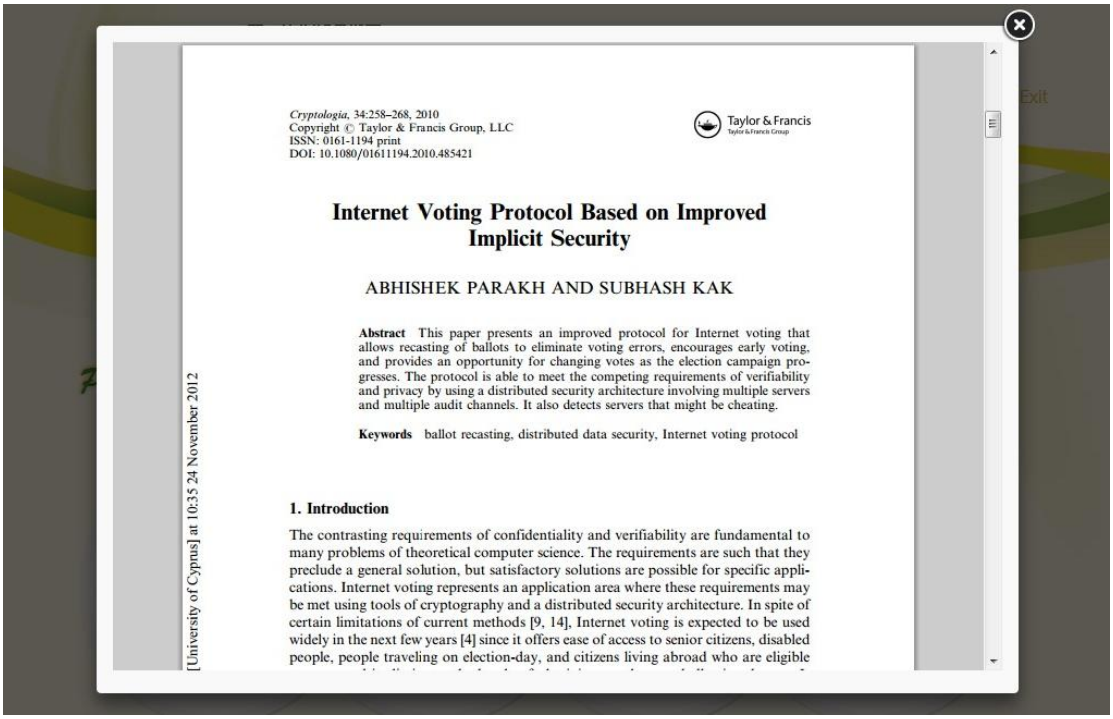
Εμφάνιση πληροφοριών επικοινωνίας



Εικόνα Α.13: Σελίδα επικοινωνίας με τους διαχειριστές του πανεπιστημίου.

Η σελίδα αυτή εμφανίζει τις απαραίτητες πληροφορίες για επικοινωνία με τον φορέα των ηλεκτρονικών εκλογών. Στο σημείο 1 εμφανίζεται η διεύθυνση του καθώς επίσης στο σημείο 2 η διεύθυνση ηλεκτρονικού ταχυδρομείου. Η διεύθυνση αυτή, προστατεύεται με την χρήση της τεχνολογίας reCaptcha, και χρειάζεται να πατήσουμε πάνω στη διεύθυνση και να πληκτρολογήσουμε τις λέξεις που εμφανίζονται, για να μας παρουσιαστεί η διεύθυνση. Επίσης στο σημείο 3 εμφανίζεται διαδραστικός χάρτης της περιοχής, ενώ στο σημείο 4, μία φόρμα επικοινωνίας με τον υπεύθυνο της ηλεκτρονικής ψηφοφορίας. Η σελίδα αυτή εμφανίζεται πατώντας στον σύνδεσμο “Contact us” στην αρχική σελίδα στην σελίδα Α.3.στο μενού του συστήματος, ή στην αρχική σελίδα.

Εμφάνιση εγχειριδίου χρήσης



Εικόνα Α.14: Η σελίδα εμφάνισης εγχειριδίου χρήσης του συστήματος.

Πατώντας στον σύνδεσμο “Manual” στην κεντρική σελίδα θα μας παρουσιαστεί το εγχειρίδιο χρήσης του συστήματος.

Εμφάνιση Αποτελεσμάτων

Εικόνα Α.15: Η σελίδα αποτελεσμάτων της ηλεκτρονικής ψηφοφορίας.

Η σελίδα αυτή εμφανίζεται μόνο μετά το πέρας των εκλογών. Στην πιο πάνω σελίδα εμφανίζονται τα αποτελέσματα της ψηφοφορίας. Πιο συγκεκριμένα, εμφανίζονται στο σημείο 1, όλοι οι υποψήφιοι, ταξινομημένοι από τον υποψήφιο ο οποίος έχει πάρει τους περισσότερους ψήφους, προς τον υποψήφιο ο οποίος έχει πάρει τους λιγότερους.

Στο σημείο 2, εμφανίζονται οι ψήφοι οι οποίοι έχουν καταχωρηθεί, μαζί με τις λέξεις οι οποίες έχουν καταχωρηθεί.

Παράρτημα Β

Ερωτηματολόγιο

Το ερωτηματολόγιο αυτό έχει δημιουργηθεί για να βοηθήσει στην εκπόνηση της Διπλωματικής Εργασίας με θέμα «Ανωνυμία σε πρωτόκολλα ηλεκτρονικής ψηφοφορίας» φοιτήτριας Πληροφορικής του Πανεπιστημίου Κύπρου. Απευθύνεται καθαρά και μόνο στους φοιτητές του πανεπιστημίου Κύπρου, και έχει ως σκοπό να αποκτήσουμε μια ολοκληρωμένη εικόνα της γνώμης που έχετε σχετικά με την ηλεκτρονική ψηφοφορία. Το ερωτηματολόγιο αυτό είναι ανώνυμο, και θα παρακαλούσαμε να απαντήσετε στις παρακάτω απλές ερωτήσεις με προσοχή και συνέπεια. Ευχαριστούμε εκ των προτέρων για τον ελάχιστο, αλλά πολύτιμο χρόνο που θα διαθέσετε.

Ερώτηση	Καθόλου	Λίγο	Μέτρια	Πολύ	Πάρα πολύ
1. Η Κυπριακή κοινωνία είναι έτοιμη να αποδεχθεί την ηλεκτρονική ψηφοφορία.	☐	☐	☐	☐	☐
2. Θα προτιμούσα αν οι εκλογές εκπροσώπων τμημάτων και σχολών του πανεπιστημίου μας ήταν ηλεκτρονικές.	☐	☐	☐	☐	☐
3. Πιστεύω ότι θα ήταν ενδιαφέρον αν η ψηφοφορία ήταν ηλεκτρονική.	☐	☐	☐	☐	☐
4. Το ποσοστό συμμετοχής αναμένεται να αυξηθεί αν χρησιμοποιηθεί η ηλεκτρονική ψηφοφορία.	☐	☐	☐	☐	☐
5. Δεν πιστεύω ότι η ηλεκτρονική ψηφοφορία είναι κατάλληλη γιατί δεν	☐	☐	☐	☐	☐

πιστεύω ότι οι ψήφοι θα παραμένουν μυστικοί.					
6. Η ηλεκτρονική ψηφοφορία δεν είναι κατάλληλη κινδύνων ασφαλείας(ιοί, hackers etc) .	☐	☐	☐	☐	☐
7. Θα προτιμούσα να ψήφιζα ηλεκτρονικά.	☐	☐	☐	☐	☐
8. Οι φίλοι μου θα προτιμούσαν να ψήφιζαν ηλεκτρονικά.	☐	☐	☐	☐	☐
9. Θα μπορούσα εύκολα και γρήγορα να ψηφίσω αν η ψηφοφορία ήταν ηλεκτρονική.	☐	☐	☐	☐	☐
10. Θα προτιμούσα να ψηφίζω μέσω SMS.	☐	☐	☐	☐	☐
11. Δεν θέλω να ψηφίζω, ανεξάρτητα από τον τρόπο ψηφοφορίας, γιατί η ψηφοφορία δεν αλλάζει κάτι.	☐	☐	☐	☐	☐
12. Γνωρίζατε αν έχει εφαρμοστεί η ηλεκτρονική ψηφοφορία σε κάποια χώρα.	☐				☐
13. Αν ναι, αναφέρατε την χώρα εφαρμογής της ηλεκτρονικής ψηφοφορίας. **.....**					

14. Αν είστε αρνητικοί ,με την εφαρμογή της ηλεκτρονικής ψηφοφορίας στην Κύπρο ,αυτό θα ήταν για τους πιο κάτω λόγους.

.....
.....
.....
.....
.....

15. Αν είστε θετικοί της εφαρμογής αναφέρετε τους λόγους.

.....
.....
.....
.....
.....

Ευχαριστούμε για τον χρόνο που έχετε διαθέσει!