ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ
ΕΡΓΑΣΤΗΡΙΟ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρακτικές Βελτιώσεις Επαληθευσιμότητας για το Σύστημα Ηλεκτρονικών Ψηφοφοριών Ζευς

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Δημήτριου Τερζόπουλου

Επιβλέπων: Παναγιώτης Τσανάκας
Καθηγητής ΕΜΠ

Αθήνα, Οκτώβριος 2016

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΕΡΓΑΣΤΗΡΙΟ ΥΠΟΛΟΓΙΣΤΙΚΩΝ
ΣΥΣΤΗΜΑΤΩΝ

Πρακτικές Βελτιώσεις Επαληθευσιμότητας για το Σύστημα Ηλεκτρονικών Ψηφοφοριών Zeus

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Δημήτριου Τερζόπουλου

Επιβλέπων: Παναγιώτης Τσανάκας
Καθηγητής ΕΜΠ

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 31η Οκτωβρίου 2016.

.....	.....	.....
Παναγιώτης Τσανάκας Καθηγητής ΕΜΠ	Αριστείδης Παγουρτζής Αναπληρωτής Καθηγητής ΕΜΠ	Παναγιώτης Λουρίδας Αναπληρωτής Καθηγητής ΟΠΑ

Αθήνα, Οκτώβριος 2016

.....
Δημήτριος Τερζόπουλος
Διπλωματούχος Ηλεκτρολόγος Μηχανικός & Μηχανικός Υπολογιστών

Περίληψη

΄Οπως κάθε εκλογικό σύστημα, τα ακραίως επαληθεύσιμα συστήματα πρέπει να διασφαλίζουν τις δύο σημαντικότερες ιδιότητες ασφαλείας για την διεξαγωγή μιας εκλογικής διαδικασίας, την μυστικότητα της ψήφου και την ακεραιότητα της ψήφου.

Στις παραδοσιακές εκλογές, ο φυσικός θάλαμος ψηφοφορίας και η σφράγιση της ψήφου σε ανώνυμο φάκελο εξασφαλίζουν την μυστικότητα της ψήφου, ενώ μια έντιμη εφορευτική επιτροπή εξασφαλίζει στον ψηφοφόρο ότι η ψήφος του δεν παραποιήθηκε και καταμετρήθηκε σωστά.

Στις ηλεκτρονικές εκλογές, η μυστικότητα της ψήφου εξασφαλίζεται μέσω κρυπτογράφησης και στη συνέχεια μίξης των ψηφοδελτίων. Η ακεραιότητα των ψήφων εξασφαλίζεται μέσω ελέγχου και επαλήθευσης. Η ιδιότητα της επαληθευσιμότητας είναι καίριας σημασίας για τα ακραίως επαληθεύσιμα συστήματα εκλογών.

Η παρούσα εργασία θα εστιαστεί στην ιδιότητα της επαληθευσιμότητας και πως αυτή μπορεί να γίνει με απλό και πρακτικό τρόπο. Στο πλαίσιο αυτό θα μελετηθούν οι τρόποι με τους οποίους εξασφαλίζεται η επαληθευσιμότητα σε διάφορα διάσημα ακραίως επαληθεύσιμα συστήματα εκλογών.

Στη συνέχεια, θα γίνει παρουσίαση του τρόπου λειτουργίας του συστήματος Ζευς, στο οποίο η εξασφάλιση της ακεραιότητας της ψήφου γίνεται από τον ίδιο τον ψηφοφόρο. Η μέθοδος αυτή θα μελετηθεί και θα αξιολογηθεί. ΄Οπως θα αναλυθεί, η μέθοδος αυτή έχει αρκετά πλεονεκτήματα, όταν αυτή χρησιμοποιείται από επαρκές και τυχαίο δείγμα ψηφοφόρων. Εάν, όμως, δεν χρησιμοποιηθεί, το σύστημα στερείται την ιδιότητα της επαληθευσιμότητας.

Στόχος της παρούσας εργασίας είναι η πρόταση ενός εναλλακτικού τρόπου εξασφάλισης της ιδιότητας της επαληθευσιμότητας, ο οποίος δεν βασίζεται στον ψηφοφόρο και δεν απαιτεί καμία επιπλέον δράση εκ μέρους του. Η πρόταση βασίζεται στην εισαγωγή μιας ανεξάρτητης έμπιστης τρίτης αρχής της οποίας ο ρόλος θα είναι να επαληθεύει την ορθή καταγραφή των ψηφοδελτίων και να ελέγχει το σύστημα εκλογών. ΄Ετσι η εμπιστοσύνη που πρέπει να έχει ο ψηφοφόρος διαμοιράζεται μεταξύ του συστήματος των ηλεκτρονικών εκλογών και της ανεξάρτητης αρχής. Στην πρόταση αυτή η αλλοίωση του αποτελέσματος μπορεί να γίνει και να μην εντοπιστεί μόνο εάν η αρχή συνωμοτήσει με το σύστημα των εκλογών.

Λέξεις κλειδιά: Ηλεκτρονική Ψηφοφορία, Ακραίως Επαληθεύσιμα Συστήματα Εκλογών, Ζευς, Επαληθεύσιμη καταγραφή της υποβληθείσας ψήφου, Επαληθεύσιμη υποβολή της προτιθέμενης ψήφου

Abstract

As any electoral system, the end-to-end verifiable voting systems must ensure the two most important security features for the conduct of an electoral process, which are no other than the secrecy and the integrity of the vote.

During a traditional election process, the voting booth and the sealing of the vote in an unmarked envelope can ensure the secrecy of the vote, while an honest election committee ensures the voter that his vote is not distorted in any way and will be counted correctly.

On the contrary, during the conduct of an electronic election, the secrecy of voting is ensured through encryption followed by the mixing of the ballots. The integrity of the vote is ensured through monitoring and verification. Verifiability property is of major importance for any end-to-end verifiable election system.

This project will focus on the verifiability notion and how this can be done in a simple and practical way. In this context, we will address ways to ensure the verifiability, as they are implemented in various popular end-to-end verifiable election systems.

Moreover, we will present the logic behind the Zeus electoral system, in which verifiability depends on the voter himself, as he needs to verify his vote. This method will be studied and evaluated. As it will be furtherly discussed in this project, this method has several advantages when used in a sufficient and random enough voter sample. However, in any other case, the system lacks verifiability.

The objective of this project is the proposal of an alternative way of securing the property of verifiability, which is not based on the voters themselves and requires no additional action on their part. The proposal is based on the introduction of an third trusted and independent authority whose role is to verify that the ballots were cast as intended and will monitor the electoral process. So the trust the voter previously had to place only in the system itself is now shared between the electronic electoral system and the independent authority. In this proposal, a corrupted voting system can tamper with the votes and avoid being detected only if it manages to conspire with the independent authority.

Keywords: Electronic Voting, End to end verifiable voting systems, Zeus, Cast as intended verifiability, Recorded as cast verifiability

Περιεχόμενα

Κατάλογος Πινάκων

Κατάλογος Σχημάτων

Κεφάλαιο 1

Εισαγωγή στα ακραίως επαληθεύσιμα συστήματα εκλογών

Η ιδέα της χρήσης κρυπτογραφίας για την ασφαλή διεξαγωγή εκλογών προτάθηκε αρκετά χρόνια πριν, όταν ο David Chaum[1] το 1981 δημοσίευσε ένα άρθρο που αφορούσε την ανώνυμη επικοινωνία. Οι απομακρυσμένες ηλεκτρονικές εκλογές ήταν τότε απλά μία πρακτική εφαρμογή των όσων πρότεινε η δημοσίευση. Η ριζοσπαστική αυτή ιδέα για την εποχή είχε απήχηση στην ακαδημαϊκή κοινότητα και τις επόμενες δύο δεκαετίες διάφορα συστήματα εκλογών εμφανίστηκαν στην βιβλιογραφία. Αν και τα περισσότερα δεν υλοποιήθηκαν ποτέ σε πραγματικά συστήματα εκλογών, ένα - δύο από αυτά πήραν την μορφή αρχικών πρωτοτύπων[2].

Οι αρχικές αυτές προσπάθειες εξελίχθηκαν τα τελευταία δεκαπέντε χρόνια σε ένα αρκετά ενδιαφέρον κλάδο της επιστήμης των υπολογιστών. Πλέον, υπάρχει ιδιαίτερο ενδιαφέρον για την έρευνα και την μελέτη επαληθεύσιμων συστημάτων ηλεκτρονικών εκλογών. Οι λόγοι που έστρεψαν το ενδιαφέρον της ακαδημαϊκής κοινότητας στο θέμα των επαληθεύσιμων ηλεκτρονικών εκλογών είναι βασικά δύο και έχουν να κάνουν με τα εκλογικά συστήματα των Ηνωμένων Πολιτειών και ορισμένων άλλων χωρών.

Η ανάγκη για ένα επαληθεύσιμο σύστημα εκλογών προέκυψε αρχικά το 2000 στις προεδρικές εκλογές των Ηνωμένων Πολιτειών της Αμερικής[3]. Στις εκλογές αυτές, η διαφορά του νικητή George H. W. Bush από τον δεύτερο Al Gore ήταν μία από τις μικρότερες στην ιστορία των Ηνωμένων Πολιτειών. Το αποτέλεσμα των εκλογών κρίθηκε από την πολιτεία της Florida, όπου η πολύ μικρή διαφορά των δύο υποψηφίων (μόλις 930 ψήφοι) απαίτησε την υποχρεωτική από τον νόμο

επανακαταμέτρηση των ψηφοδελτίων από τα μηχανήματα καταμέτρησης. Το αποτέλεσμα αμφισβητήθηκε από τον Al Gore και ζητήθηκε η καταμέτρηση των ψήφων με το χέρι σε ορισμένους νομούς της Florida. Η αντιδικεία αυτή έφτασε στο Ανώτατο Δικαστήριο των Ηνωμένων Πολιτειών το οποίο, όμως, αποφάσισε να μην επιτρέψει την καταμέτρηση και έτσι ο Bush ανακοινώθηκε ως νικητής των εκλογών. Υπάρχουν αντικρουόμενες μελέτες για το ποιος θα είχε νικήσει μετά την επανακαταμέτρηση εάν αυτή είχε επιτραπεί.

Πολλά από τα προβλήματα που προέκυψαν στην Florida είχαν να κάνουν με την χρηστικότητα και τον σχεδιασμό του ψηφοδελτίου. Επίσης πολλοί ψηφοφόροι αντιμετώπισαν δυσκολίες με τα μηχανήματα των εκλογών καθώς δεν μπορούσαν να καταλάβουν την απαιτούμενη διαδικασία που έπρεπε να ακολουθήσουν ή αντιμετώπιζαν δυσκολίες στο να την εφαρμόσουν. Αυτό προκάλεσε ένα ασυνήθιστο αριθμό ψηφοδελτίων τα οποία περιείχαν περισσότερους από τους επιτρεπόμενους σταυρούς. Αρκετά ήταν και τα ψηφοδέλτια με λιγότερους σταυρούς από ότι έπρεπε, γεγονός το οποίο οφειλόταν σε αστοχίες των τρυπητών καρτών - ψηφοδελτίων και λάθη των ψηφοφόρων.

Η αναστάτωση που προκάλεσε το γεγονός αυτό οδήγησε στην δημιουργία του νόμου Help America Vote Act[4] με σκοπό τον εξοπλισμό των εκλογικών κέντρων με μηχανήματα νέας τεχνολογίας και την διευκόλυνση των ψηφοφόρων να ψηφίσουν. ΄Ετσι ξεκίνησαν να επενδύονται αρκετά κεφάλαια στην έρευνα για την βελτίωση της τεχνολογίας των ηλεκτρονικών εκλογών[5].

Επιπρόσθετα, τα τελευταία χρόνια πολλές έρευνες έφεραν στο φως πολλά και σημαντικά προβλήματα αξιοπιστίας και ασφάλειας των ηλεκτρονικών μηχανών ψηφοφορίας και των ηλεκτρονικών συστημάτων εκλογών που χρησιμοποιούνταν τόσο στις Ηνωμένες Πολιτείες[6] όσο και σε άλλες χώρες όπως η Ινδία[7] και η Εσθονία[8], δείχνοντας ότι ήταν ευάλωτα σε επιθέσεις οι οποίες θα μπορούσαν να παραβιάσουν το αδιάβλητο των εκλογών και την μυστικότητα των ψήφων. Μάλιστα, έχουν καταγραφεί αρκετές περιπτώσεις όπου οι ηλεκτρονικές μηχανές ψηφοφορίας δυσλειτούργησαν κατά την διάρκεια των εκλογών, αλλάζοντας τις ψήφους των ψηφοφόρων ή τυχαία προσθέτοντας ή αφαιρώντας ψήφους σε υποψηφίους. ΄Ετσι, τα τελευταία χρόνια, το ακαδημαϊκό ενδιαφέρον για την προστασία του αδιάβλητου των εκλογών αυξήθηκε[9][10].

Το αυξημένο αυτό ενδιαφέρον οδήγησε στην ανάπτυξη ενός νέου τύπου συστημάτων εκλογών, τα οποία έχουν ακραίως επαληθεύσιμες ιδιότητες ασφαλείας. Για να γίνει κατανοητή η έννοια των από άκρη σε άκρη επαληθεύσιμων συστημάτων εκλογών, παρουσιάζεται ένα τυπικό σενάριο χρήσης το οποίο περιγράφει την ιδέα αυτών των συστημάτων.

΄Εστω ένας ψηφοφόρος ο οπόιος πάει την ημέρα των εκλογών στο εκλογικό κέντρο για να ψηφίσει. Η διαδικασία της ψηφοφορίας είναι όμοια με αυτή που ήδη γνωρίζουμε από τις παραδοσιακές εκλογές. Με την είσοδό του στο εκλογικό κέντρο ο ψηφοφόρος πιστοποιείται από την εφορευτική επιτροπή ως έγκυρος ψηφοφόρος και οδηγείται στον θάλαμο ψηφοφορίας, το γνωστό "παραβάν". Ο θάλαμος αυτός εξασφαλίζει στον ψηφοφόρο ότι κανείς δεν μπορεί να δει τι ψηφίζει, δηλαδή διασφαλίζει την μυστικότητα της ψήφου. Στον θάλαμο υπάρχει ένα σύστημα (για παράδειγμα ένας υπολογιστής με οθόνη αφής) με το οποίο ο ψηφοφόρος επιλέγει τους υποψήφιους που θέλει να ψηφίσει. Αφού ο ψηφοφόρος ρίξει το ψηφοδέλτιο στην κάλπη, το μηχάνημα δίνει στον ψηφοφόρο μία απόδειξη (για παράδειγμα την εκτυπώνει), η οποία είναι στην ουσία ένα κρυπτογραφημένο αντίγραφο της ψήφου του. ΄Οσο βρίσκεται πίσω από το παραβάν, ο ψηφοφόρος μπορεί επίσης να επιβεβαιώσει ότι το μηχάνημα έριξε την σωστή ψήφο στην κάλπη και δεν την άλλαξε. Αυτό μπορεί να γίνει είτε οπτικά, είτε προκαλώντας το μηχάνημα (για παράδειγμα με το να κρυπτογραφήσει ο ίδιος την ψήφο του και να την συγκρίνει με αυτή που του έδωσε σαν απόδειξη το μηχάνημα και που έριξε στην κάλπη). Ο ψηφοφόρος μπορεί δηλαδή να επαληθεύσει ότι το ψηφοδέλτιο του ρίχθηκε στην κάλπη όπως ακριβώς συμπληρώθηκε και δεν αλλάχτηκε από το μηχάνημα.

Μετά το κλείσιμο των καλπών, το σύστημα των εκλογών δημοσιεύει όλες τις αποδείξεις που έχει δώσει στους ψηφοφόρους σε ένα δημόσιο πίνακα ανακοινώσεων (για παράδειγμα σε μια ιστοσελίδα). Εκεί, ο ψηφοφόρος μπορεί να επιβεβαιώσει ότι η ψήφος του καταγράφηκε στην κάλπη χωρίς να αλλαχθεί (δηλαδή η απόδειξη που έλαβε μετά την ψηφοφορία υπάρχει στον πίνακα ανακοινώσεων και δεν έχει αλλαχθεί). Αυτό σημαίνει ότι ο ψηφοφόρος μπορεί να επαληθεύσει ότι το ψηφοδέλτιό του καταγράφηκε από το σύστημα όπως ακριβώς υποβλήθηκε στην κάλπη.

Το τελευταίο βήμα είναι η καταμέτρηση των ψήφων και η έκδοση του αποτελέσματος των εκλογών. Για να γίνει αυτό, γίνεται επεξεργασία όλων των αποδείξεων που βρίσκονται στον πίνακα ανακοινώσεων και μέσω κρυπτογραφικών υπολογισμών υπολογίζεται το τελικό αποτέλεσμα. Με σκοπό να είναι επαληθεύσιμο και αυτό το κρίσιμο για τις εκλογές βήμα, όλοι οι αλγόριθμοι που χρησιμοποιούνται αναρτώνται δημόσια. ΄Ετσι κάποιος ο οποίος γνωρίζει την χρήση των μεθόδων αυτών (ίσως ακόμα και ο ίδιος ο ψηφοφόρος) μπορεί να επαληθεύσει ότι η καταμέτρηση των ψήφων έγινε σωστά και συνεπώς το ότι το αποτέλεσμα των εκλογών είναι έγκυρο. Συνεπώς, ο ψηφοφόρος μπορεί να επαληθεύσει ότι το ψηφοδέλτιό του καταμετρήθηκε όπως ακριβώς καταγράφηκε.

Το σενάριο αυτό, εάν και μοιάζει σε πολλά σημεία με τον παραδο-

σιακό τρόπο εκλογών διαφέρει σημαντικά από αυτόν. Στις παραδοσιακές εκλογές, ο ψηφοφόρος πρέπει να εμπιστευτεί την εφορευτική επιτροπή (ή αντίστοιχα το σύστημα των εκλογών) για το αδιάβλητο των εκλογών. Μια ανέντιμη εφορευτική επιτροπή μπορεί να αλλάξει το αποτέλεσμα των εκλογών, χωρίς αυτό να γίνει αντιληπτό από τους ψηφοφόρους. Επίσης, ο ψηφοφόρος δεν έχει εικόνα για το τι συμβαίνει στο εσωτερικό των μηχανημάτων εκλογών που χρησιμοποιούνται σήμερα και συνεπώς πρέπει να εμπιστευτεί την εταιρία που τα κατασκεύασε και την αρχή που τα έλεγξε για την ακεραιότητα της ψήφου του.

Αντίθετα, στην περίπτωση των ακραίως επαληθεύσιμων συστημάτων εκλογών, ο ψηφοφόρος δεν χρειάζεται να εμπιστευτεί κανέναν για το αδιάβλητο της διαδικασίας. Αυτό συμβαίνει γιατί σε κάθε βήμα μπορεί ο ίδιος να επαληθεύσει ότι το σύστημα λειτουργεί σωστά. ΄Ετσι, εάν ένα μηχάνημα χάσει την ψήφο του ψηφοφόρου ή την τροποποιήσει, η απόδειξη που θα έχει στα χέρια του δεν θα ταιριάζει με αυτή στον πίνακα ανακοινώσεων. Αυτό συνεπάγεται ότι ο ψηφοφόρος θα εντοπίσει την αλλοίωση στην ψήφο του και θα μπορεί να κάνει ένσταση, χρησιμοποιώντας την απόδειξη που έλαβε ως αποδεικτικό στοιχείο. Επίσης, εάν κάποιο μέλος της εφορευτικής επιτροπής αλλοιώσει το τελικό αποτέλεσμα, οποιοσδήποτε παρατηρητής ο οποίος τρέξει τους κρυπτογραφικούς αλγόριθμους στα δικά του συστήματα θα το εντοπίσει.

Τέλος, αφού η απόδειξη που λαμβάνει ο ψηφοφόρος είναι μια κρυπτογράφηση της ψήφου του, δεν μπορεί να χρησιμοποιηθεί ως απόδειξη για το περιεχόμενο της ψήφου. Βέβαια, αυτό δεν συμβαίνει σε όλα τα ακραίως επαληθεύσιμα συστήματα εκλογών και η αντίσταση στον εξαναγκασμό ή την πώληση της ψήφου είναι ένα ζήτημα που απασχολεί τους ερευνητές.

Κεφάλαιο 2

Ιδιότητες ασφαλείας των ακραίως επαληθεύσιμων συστημάτων ηλεκτρονικών εκλογών - Επεξήγηση όρων και συμβολισμών

2.1 Ιδιότητες ασφαλείας των ακραίως επαληθεύσιμων συστημάτων ηλεκτρονικών εκλογών

Στο σημείο αυτό, είναι χρήσιμο να περιγραφούν οι βασικές ιδιότητες ασφαλείας που χαρακτηρίζουν τα ακραίως επαληθεύσιμα συστήματα εκλογών, δίνοντας ιδιαίτερη έμφαση στην ιδιότητα της επαληθευσιμότητας. Πολλές από τις παρακάτω ιδιότητες είναι άρρηκτα συνδεδεμένες η μία στην άλλη ενώ άλλες δεν μπορούν να συνυπάρχουν.

Μυστικότητα - Privacy:

- **Μυστικότητα ψήφου (Ballot-privacy):** Κανείς εξωτερικός παρατηρητής δεν δύναται να διαβάσει το περιεχόμενο της ψήφου ενός ψηφοφόρου.
- **Απουσία απόδειξης(Receipt-freeness):** Ο ψηφοφόρος δεν μπορεί να αποδείξει τι ψήφισε. Η ιδιότητα αυτή δεν μπορεί να υπάρξει χωρίς να εξασφαλίζεται η μυστικότητα της ψήφου.
- **Αδυναμία εξαγοράς ψήφου (Coercion-resistance):** Ο ψηφοφόρος να μην μπορεί να μην αλληλεπιδράσει με κανέναν την ώρα της ψηφοφορίας και να αποδείξει το περιεχόμενο της ψήφου του. Η ιδιότητα αυτή συνδέεται με την προηγούμενη.

Επαληθευσιμότητα - Verifiability:

- **Ατομική επαληθευσιμότητα (Individual verifiability):** Ο ψηφοφόρος μπορεί να επαληθεύσει ότι το ψηφοδέλτιο που έριξε στην κάλπη ανήκει όντως στο σύνολο των ψηφοδελτίων που βρίσκονται στην τελική κάλπη.
- **Γενική επαληθευσιμότητα (Universal verifiability):** Οποιοσδήποτε εξωτερικός παρατηρητής μπορεί να επαληθεύσει ότι όλα τα ψηφοδέλτια της τελικής κάλπης καταμετρήθηκαν σωστά και το αποτέλεσμα προέκυψε από αυτά και μόνο αυτά τα ψηφοδέλτια.
- **Από άκρη σε άκρη επαληθευσιμότητα (End-to-end verifiability)**: Ο ψηφοφόρος μπορεί να επαληθεύσει ότι το ψηφοδέλτιό του καταμετρήθηκε όπως συμπληρώθηκε (tallied-as-intended). Δηλαδή ότι το ψηφοδέλτιό του:
  - **Υποβολή της προτιθέμενης (ψήφου) (Cast-as-intended):** Το σφραγισμένο ψηφοδέλτιο που ρίχθηκε στην κάλπη περιέχει την ψήφο που επέλεξε ο ψηφοφόρος.
  - **Καταγραφή της υποβληθείσας (ψήφου) (Recorded-as-cast):** Το ψηφοδέλτιο που ρίχθηκε στην κάλπη καταγράφηκε από σύστημα ως έχει και προστέθηκε στην τελική κάλπη χωρίς καμία τροποποίηση.
  - **Καταμέτρηση των καταγεγραμμένων (ψήφων)(Tallied-as-recorded):** Η ψήφος που καταμετρήθηκε στο τελικό αποτέλεσμα είναι αυτή που περιέχεται στο ψηφοδέλτιο όπως αυτό λήφθηκε και καταγράφηκε από το σύστημα.

Είναι σημαντικό να σχολιαστεί ότι η απόλυτη μυστικότητα δεν μπορεί να συνυπάρξει με την επαληθευσιμότητα. Αυτό γιατί, απόλυτη μυστικότητα σημαίνει ότι δεν υπάρχει διαρροή καμίας πληροφορίας. Από την άλλη, η επαληθευσιμότητα απαιτεί επαρκή διαρροή πληροφορίας με σκοπό να μπορεί να επαληθευτεί το αποτέλεσμα. Ο στόχος ενός επαληθεύσιμου συστήματος εκλογών είναι να εξασφαλίζει όσο τον δυνατόν περισσότερη μυστικότητα σε συνδυασμό με την επαληθευσιμότητα.

2.2 Επεξήγηση όρων και συμβολισμών

Πέρα από τις ιδιότητες ασφαλείας των συστημάτων εκλογών, είναι σημαντικό να εξηγηθούν ορισμένες έννοιες οι οποίες θα χρησιμοποιηθούν στη συνέχεια της εργασίας.

2.2.1 Δίκτυα μίξης (Mixnets)

Πολλά ακραίως επαληθεύσιμα συστήματα εκλογών αποθηκεύουν επώνυμα τα ψηφοδέλτια των ψηφοφόρων δίνοντας παράλληλα στους ψηφοφόρους αποδείξεις για το τι ψήφισαν. Η μυστικότητα των ψήφων διασφαλίζεται συνήθως μέσω κρυπτογράφησης. Για την καταμέτρηση όμως των ψήφων, το περιεχόμενο κάθε ψηφοδελτίου πρέπει να αποκαλυφθεί. Είναι συνεπώς σημαντικό πριν την αποκάλυψη του περιεχομένου των ψήφων να γίνει ανωνυμοποίηση των ψηφοδελτίων. Σε πολλά ακραίως επαληθεύσιμα συστήματα η ανωνυμοποίηση επιτυγχάνεται μέσω δικτύων μίξης.

Τα δίκτυα μίξης [11] είναι πρωτόκολλα δρομολόγησης τα οποία δημιουργούν συνδέσεις οι οποίες είναι δύσκολο να εδιχνιαστούν, χρησιμοποιώντας μια αλυσίδα από ενδιάμεσων κόμβων, γνωστών ως μίκτες. Οι μίκτες λαμβάνουν μηνύματα από ποικίλους αποστολείς, τα "ανακατεύουν" και τα στέλνουν στον επόμενο προορισμό σε τυχαία σειρά (ο οποίος μπορεί να είναι και αυτός κόμβος μίξης). Η διαδικασία αυτή ¨σπάει¨ την σύνδεση μεταξύ της πηγής του μηνύματος και του προορισμού του, καθιστώντας δυσκολότερο στους ωτακουστές να εδιχνιάσουν από άκρη σε άκρη επικοινωνίες

Επιπλέον, καθώς οι μίκτες ξέρουν μόνο τον αμέσως προηγούμενο κόμβο από τον οποίο έλαβαν το μήνυμα και τον αμέσως επόμενο στον οποίον έστειλαν τα "ανακατεμένα" μηνύματα, το δίκτυο είναι ανθεκτικό σε κακόβουλους κόμβους μίξης. Επίσης, κάθε μήνυμα κρυπτογραφείται σε κάθε κόμβο χρησιμοποιώντας κρυπτογράφηση δημοσίου κλειδιού. Κάθε κόμβος προσθέτει ένα επίπεδο κρυπτογράφησης. Το αποτέλεσμα μπορεί να προσομοιαστεί με ένα κρεμμύδι, στο οποίο κάθε φλοιός είναι ένα επίπεδο κρυπτογράφησης και το οποίο στο εσωτερικό του έχει το μήνυμα. Κάθε κόμβος αφαιρεί το δικό του επίπεδο κρυπτογράφησης για να αποκαλύψει που πρέπει να αποσταλεί το μήνυμα στη συνέχεια. ΄Ετσι ακόμα και όλοι πλην ενός κόμβοι να παραβιαστούν από κάποιον κακόβουλο χρήση, η αδυναμία εδιχνιασης μπορεί να εξασφαλιστεί (υπό συγκεκριμένες προϋποθέσεις).

Μια σημαντική ιδιότητα των δικτύων μίξης που χρησιμοποιούνται στα συστήματα εκλογών είναι η δυνατότητα επαλήθευσης ότι η μίξη έγινε σωστά. ΄Ενα παράδειγμα μιας μεθόδου επαλήθευσης παρουσιάζεται στη συνέχεια[12].

Κατά την διαδικασία επαλήθευσης, τα κρυπτογραφημένα μηνύματα κάθε κόμβου χωρίζονται σε ανεξάρτητες ομάδες σύμφωνα με μια τυχαία διαδικασία η οποία καθορίζεται από τον επαληθευτή (π.χ. η αρχή που ελέγχει το σύστημα). Είναι σημαντικό να σημειωθεί ότι η ομαδοποίηση των μηνυμάτων γίνεται αφού ολοκληρωθεί η διαδικασία της μίξης, αποτρέποντας έτσι την αποκάλυψη ευαίσθητων πληροφοριών σε κάποιο κόμβο (με αποτέλεσμα αυτός να "κλέψει" κατά την

διαδικασία της επαλήθευσης). Ο υπό έλεγχο κόμβος μίξης ονομάζεται αποδείκτης, καθώς προσπαθεί να αποδείξει στον επαληθευτή ότι έκανε σωστά την μίξη. Κάθε κόμβος μίξης - αποδείκτης μαρτυρά στον επαληθευτή την θέση στην έξοδο που έχουν τα μηνύματα κάθε ομάδας που έλαβε στην είσοδο του. Η θέση αυτή των μηνυμάτων μίας ομάδας εξόδου δεν αποκαλύπτει την θέση που είχε κάθε μήνυμα στην ομάδα του στην είσοδο του κόμβου.

Επίσης, όταν ο επαληθευτής χωρίζει τα μηνύματα σε ομάδες, πολλαπλασιάζει τα μηνύματα κάθε ομάδας ώστε να λάβει μία Απόδειξη Ακεραιότητας Εισόδου (Input Integrity Proof), χρησιμοποιώντας ομομορφικές ιδιότητες. Αφού ο αποδείκτης υποδείξει ποια μηνύματα στην έξοδο του αντιστοιχούν σε κάθε ομάδα εισόδου, ο επαληθευτής μπορεί να πολλαπλασιάσει τα μηνύματα κάθε ομάδας για να λάβει μια Απόδειξη Ακεραιότητας Εξόδου (Output Integrity Proof). Για κάθε ζεύγος Αποδείξεων Ακεραιότητας Εισόδου και Εξόδου, ο αποδείκτης παρέχει μια Απόδειξη Μηδενικής Γνώσης για να δείξει ότι η Απόδειξη Ακεραιότητας Εξόδου είναι μια επανακρυπτογράφηση της Απόδειξης Ακεραιότητας Εισόδου. Καθώς οι αποδείξεις ακεραιότητας μπορούν να υπολογιστούν και να επαληθευτούν από έναν εξωτερικό παρατηρητή, η μέθοδος αυτή εξασφαλίζει την ιδιότητα της γενικής επαληθευσιμότητας.

2.2.2 Αποδείξεις μηδενικής γνώσης (Zero Knowledge Proofs)

Στην κρυπτογραφία, μία απόδειξη μηδενικής γνώσης [13] είναι μία μέθοδος με την οποία μια οντότητα (ο αποδείκτης) μπορεί να αποδείξει σε μία άλλη (τον επαληθευτή) ότι μία πρόταση είναι αληθής, χωρίς να αποκαλύψει καμία πληροφορία εκτός από το γεγονός ότι η πρόταση όντως είναι αληθής. Εάν η απόδειξη της πρότασης απαιτεί την γνώση κάποιας μυστικής πληροφορίας από την πλευρά του αποδείκτη, ο ορισμός συνεπάγεται ότι ο επαληθευτής δεν μπορεί να αποδείξει την πρόταση προσποιούμενος ότι είναι ο αποδείκτης, αφού ο επαληθευτής δεν γνωρίζει την μυστική αυτή πληροφορία. Είναι σημαντικό να σημειωθεί ότι η πρόταση προς απόδειξη πρέπει να περιέχει τον ισχυρισμό ότι ο αποδείκτης γνωρίζει την μυστική πληροφορία.

Κάθε απόδειξη μηδενικής γνώσης πρέπει να ικανοποιεί τρεις ιδιότητες:

1. Πληρότητα (Completeness): Εάν η πρόταση είναι αληθής, ο έντιμος επαληθευτής (δηλαδή ο επαληθευτής που ακολουθεί σωστά το πρωτόκολλο επαλήθευσης) θα μπορεί πειστεί από έναν έντιμο αποδείκτη.

2. Ορθότητα (Soundness): Εάν η πρόταση είναι ψευδής, κανένας κακόβουλος αποδείκτης δεν μπορεί να πείσει έναν έντιμο επαλη-

θευτή για το αντίθετο - η πιθανότητα να συμβεί αυτό είναι πολύ μικρή.

3. Μηδενική Γνώση (Zero Knowledge): Εάν η πρόταση είναι αληθής, ένας έντιμος επαληθευτής δεν μπορεί να μάθει τίποτα πέρα από το γεγονός αυτό - ότι η πρόταση είναι αληθής.

2.2.3 Σχήμα δέσμευσης (Commitment scheme)

Στην κρυπτογραφία, ένα σχήμα δέσμευσης[14] επιτρέπει σε κάποιον να δεσμευτεί σε μία επιλεγμένη τιμή ή δήλωση αποκρύπτοντας το περιεχόμενο της και έχοντας την δυνατότητα να αποκαλύψει αργότερα το περιεχόμενο αυτό. Τα σχήματα δέσμευσης έχουν σχεδιαστεί έτσι ώστε αυτός που δεσμεύεται δεν μπορεί να αλλάξει την τιμή ή την δήλωσή του αφού έχει δεσμευτεί σε αυτή.

2.2.4 Συνάρτηση κατακερματισμού (Hash Function)

Η συνάρτηση κατατεμαχισμού[15], γνωστή και ως συνάρτηση κατακερματισμού, είναι μια μαθηματική συνάρτηση που δέχεται ως είσοδο κάποιο δεδομένο τυχαίου μεγέθους και επιστρέφει ένα αλφαριθμητικό σταθερού μεγέθους. Οι τιμές που επιστρέφει η συνάρτηση κατατεμαχισμού ονομάζονται τιμές κατατεμαχισμού (hash values), κώδικες κατατεμαχισμού (hash codes), αθροίσματα κατατεμαχισμού (hash sums) ή απλά τιμές κατατεμαχισμού (hashes). Οι τιμές αυτές θα πρέπει να είναι διαφορετικές για διαφορετική είσοδο, καθώς η κύρια χρησιμότητα αυτών των συναρτήσεων είναι να ταυτοποιούν δεδομένα. Μια άλλη εφαρμογή είναι στη δημιουργία ψηφιακών υπογραφών. Στις περιπτώσεις αυτές χρησιμοποιούνται τιμές κατατεμαχισμού μεγάλου μεγέθους για να ελαχιστοποιηθεί ο κίνδυνος πλαστογράφησης τους.

2.3 Σημειογραφία

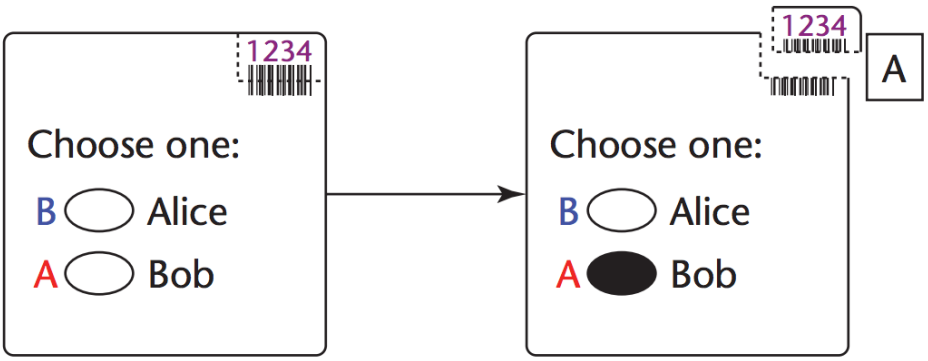
Για την καλύτερη κατανόηση της παρούσας εργασίας παρουσιάζονται οι διάφοροι συμβολισμοί που θα χρησιμοποιηθούν. Η κρυπτογράφηση c ενός μηνύματος m με κλειδί K συμβολίζεται ως $Enc_K\{m\}$ Το κρυπτοκείμενο μπορεί να αποκρυπτογραφηθεί με το αντίστροφο κλειδί του K^{-1}. Η αποκρυπτογράφηση του κρυπτοκειμένου c με κλειδί K^{-1} συμβολίζεται ως $Dec_{K^{-1}}\{c\}$. Για συμμετρική κρυπτογραφεία το αντίστροφο κλειδί K^{-1} είναι ίδιο με το K. Για ασύμετρη κρυπτογραφία, συμβολίζουμε το δημόσιο κλειδιί και το ιδιωτικό κλειδή ενός δράστη A με $PK(A)$ και $SK(A)$ αντίστοιχα. Η ψηφιακή υπογραφή σ ενός μηνύματος m με ιδιωτικό κλειδί SK συμβολίζεται ως $Sig_{SK}\{m\}$.

Η επαλήθευση μιας ψηφιακής υπογραφής σ ενός μηνύματος m με το δημόσιο κλειδί PK συμβολίζεται ως $Ver_{PK}\{m, \sigma\}$ και επιτυγχάνει εάν $Ver_{PK}\{m, \sigma\} = True$.

Κεφάλαιο 3

Μελέτη συστημάτων εκλογών ως προς την ιδιότητα της επαληθευσιμότητας

Για την καλύτερη κατανόηση της έννοιας της επαληθευσιμότητας αλλά για το πως αυτή μπορεί να εξασφαλισθεί, είναι σημαντική η μελέτη υπαρχόντων ακραίως επαληθεύσιμων συστημάτων εκλογών. Τα συστήματα αυτά χωρίζονται σε κατηγορίες με βάση τον τύπο ψηφοδελτίου που χρησιμοποιούν, δηλαδή εάν χρησιμοποιούν φυσικό ψηφοδέλτιο (όπως χάρτινο ψηφοδέλτιο) ή ηλεκτρονικό ψηφοδέλτιο, και με βάση τον τρόπο διεξαγωγής της ψηφοφορίας, δηλαδή εάν απαιτείται φυσικός χώρος εκλογών (φυσική παρουσία στο εκλογικό κέντρο) ή η ψηφοφορία γίνεται απομακρυσμένα. Ιδιαίτερη έμφαση θα δοθεί σε συστήματα τα οποία έχουν πρακτική εφαρμογή σε πραγματικές εκλογές. Επίσης θα μελετηθούν κυρίως συστήματα που χρησιμοποιούν κρυπτογράφηση για την εξασφάλιση της μυστικότητας της ψήφου. Για την κάλυψη, όμως, του πλήρους φάσματος των ακραίως επαληθεύσιμων συστημάτων ηλεκτρονικών εκλογών θα μελετηθούν και συστήματα που δεν χρησιμοποιούν κρυπτογράφηση Μερικά από τα συστήματα που θα περιγραφούν μπορεί να μην εξασφαλίζουν όλες τις ιδιότητες ενός ακραίως επαληθεύσιμου συστήματος, αλλά είναι σημαντικού ενδιαφέροντος και η συνεισφορά τους στον τομέα της επαληθευσιμότητας είναι σημαντική.



Σχήμα 3.1: Το ψηφοδέλτιο του Scantegrity

3.1 Ακραίως επαληθεύσιμα συστήματα που απαιτούν φυσικό χώρο εκλογών και βασίζονται σε φυσικό ψηφοδέλτιο

Η κατηγορία αυτή αποτελείται από συστήματα που απαιτούν την ύπαρξη φυσικού εκλογικού κέντρου και στα οποία το αποτέλεσμα προκύπτει από την καταμέτρηση χάρτινων ψηφοδελτίων τα οποία συμπληρώθηκαν είτε με το χέρι είτε μέσω μίας μηχανής. "Πατέρας" αυτών των συστημάτων θεωρείται το σύστημα Votegrity [16] το οποίο εφευρέθηκε από τον David Chaum το 2004 και αποτέλεσε έμπνευση για το Scantegrity[17]. Το ενδιαφέρον της παρούσας μελέτης θα επικεντρωθεί στο Scantegrity λόγω του γεγονότος ότι είχε πρακτική εφαρμογή.

3.1.1 Scantegrity

Το Scantegrity αναπτύχθηκε το 2008 από μια ομάδα ερευνητών, συμπεριλαμβανομένων των David Chaum και Ron Rivest και αποτελεί μια βελτιωμένη και πιο ασφαλή μέθοδο εκλογών με χρήση οπτικών σκάνερ. Το σύστημα αυτό χρησιμοποιεί την υπάρχουσα τεχνολογία των οπτικών σκάνερ εξασφαλίζοντας ταυτόχρονα ακραία επαληθευσιμότητα. Το ψηφοδέλτιο του Scantegrity μοιάζει αρκετά με αυτό που χρησιμοποιείται από τα κλασσικά οπτικά σκάνερ, έχει όμως τις ακόλουθες διαφορές. Κάθε ψηφοδέλτιο έχει έναν μοναδικό σειριακό αριθμό. Ο σειριακός αριθμός γράφεται σε δύο σημεία του ψηφοδελτίου, στο βασικό σώμα του ψηφοδελτίου καθώς και σε ένα αποσπώμενο μέρος. Επίσης, δίπλα από το όνομα του κάθε υποψηφίου υπάρχει ένα τυχαίο κωδικό γράμμα. ΄Ενα παράδειγμα του ψηφοδελτίου του Scantegrity παρουσιάζεται στο Σχήμα 3.1

Κατά την διάρκεια της ψηφοφορίας, ο ψηφοφόρος σημαδεύει τους υποψηφίους της επιλογής του και σκανάρει το ψηφοδέλτιο στο οπτικό σκάνερ. Στη συνέχεια κόβει το αποσπώμενο μέρος του ψηφοδελτίου και σημειώνει σε αυτό τα γράμματα - κωδικούς που βρίσκονται δίπλα από τα ονόματα των υποψηφίων που ψήφισε. Το αποσπώμενο αυτό μέρος αποτελεί την απόδειξη για το τι ψήφισε ο ψηφοφόρος. Είναι σημαντικό να σημειωθεί ότι ο σειριακός αριθμός και γράμματα επιλέγονται με τέτοιο τρόπο έτσι ώστε να εξασφαλίζουν την μυστικότητα της ψήφου. Καθώς το αντικείμενο μελέτης της εργασίας αυτής είναι η ιδιότητα της επαληθευσιμότητας δεν θα σχολιαστεί η μέθοδος δημιουργίας των κωδικών αυτών.

Στην περίπτωση του Scantegrity δεν χρησιμοποιείται δίκτυο μίξης για την αποσύνδεση της επώνυμης απόδειξης από το περιεχόμενο της ψήφου. Το Scantegrity εξασφαλίζει τις ιδιότητες των δικτύων μίξης χρησιμοποιώντας μια πιο απλή διαδικασία, το Switchboard. Το Switchboard είναι και αυτό ένα δίκτυο που πραγματοποιεί μια μυστική αναδιάταξη των διάφορων καταστάσεων των περιοχών που συμπληρώνει ο χρήστης (συμπληρωμένη / μη συμπληρωμένη). ΄Ετσι το Scantegrity χρησιμοποιεί την αναδιάταξη αυτή για να ανακτήσει την ψήφο κρύβοντας ταυτόχρονα την σύνδεση μεταξύ του σειριακού αριθμού και της ψήφου. Το Switchboard εξασφαλίζει και αυτό την ιδιότητα της γενικής επαληθευσιμότητας, όπως και τα δίκτυα μίξης.

Κατά την διαδικασία της καταμέτρησης, η κατάσταση κάθε περιοχής συμπλήρωσης μεταφράζεται μέσω του Switchboard σε ψήφο σε κάποιον συγκεκριμένο υποψήφιο στα αποτελέσματα των εκλογών.

Μετά το κλείσιμο των κάλπεων, όλοι οι σειριακοί αριθμοί των ψηφοδελτίων μαζί με τα κωδικά γράμματα αναρτώνται σε ένα δημόσιο πίνακα ανακοινώσεων. Στον πίνακα αυτό οι ψηφοφόροι μπορούν να επαληθεύσουν ότι οι ψήφοι τους καταγράφηκαν σωστά από το σύστημα συγκρίνοντας τα δεδομένα του πίνακα ανακοινώσεων με τις αποδείξεις τους. Τα κωδικά γράμματα από μόνα τους δεν αποκαλύπτουν την ψήφο του ψηφοφόρου αφού είναι τυχαία.

Η μέθοδος αυτή έχει ένα μειονέκτημα, δεν υπάρχει εγγύηση ότι ο ψηφοφόρος θα σημειώσει στην απόδειξη τους σωστούς κωδικούς - γράμματα που αντιστοιχούν στους υποψηφίους που έχει επιλέξει. Συνεπώς, στη περίπτωση που τα κωδικά γράμματα στην απόδειξη δεν ταιριάζουν με αυτά του πίνακα ανακοινώσεων, η επίλυση του προβλήματος είναι δύσκολη καθώς μπορεί να οφείλεται σε λάθος του ψηφοφόρου και όχι του συστήματος.

Το Scantegrity II[18] λύνει τα προβλήματα αυτά με το να τυπώνει τα κωδικά γράμματα των υποψηφίων με ένα αόρατο μελάνι, το οποίο

αποκαλύπτεται μόνο όταν ο ψηφοφόρος σημειώσει και ψηφίσει έναν υποψήφιο χρησιμοποιώντας ένα ειδικό στυλό. Καθώς οι κωδικοί αυτοί είναι τυχαίοι και δεν είναι μικροί σε μήκος, η πιθανότητα ο ψηφοφόρος να τους μαντέψει στην τύχη είναι μικρή. Συνεπώς, εάν κάποιος ψηφοφόρος διαμαρτυρηθεί για την μη σωστή καταγραφή της ψήφου του και έχει σωστό κωδικό, είναι μάλλον πιθανό ότι η διαμαρτυρία είναι βάσιμη και σωστή.

Πέρα από τον έλεγχο της σωστής καταγραφής των ψήφων, το Scantegrity δίνει την δυνατότητα επαλήθευσης της ορθής λειτουργίας του Switchboard.

Πριν τις εκλογές, όταν η εφορευτική επιτροπή δημιουργεί τα ψηφοδέλτια και ρυθμίζει το Switchboard, δεσμεύεται σε αυτή την μυστική πληροφορία χρησιμοποιώντας μία κρυπτογραφηκά ασφαλή μέθοδο δέσμευσης. Οι δεσμεύσεις αυτές δημοσιοποιούνται στον πίνακα ανακοινώσεων και μπορούν να χρησιμοποιηθούν από οποιαδήποτε ανεξάρτητη αρχή για την επιβεβαίωση ότι κανείς δεν τροποποίησε τα ψηφοδέλτια ή το Switchboard με σκοπό να αλλοιώσει την διαδικασία της επαλήθευσης.

Το πρώτο σκέλος επαλήθευσης αφορά τα ψηφοδέλτια, δηλαδή την επαλήθευση ότι οι κωδικοί δίπλα στους υποψηφίους αντιστοιχούν όντως στους σωστούς υποψηφίους.

Πριν τις εκλογές, οι ελεγκτές διαλέγουν τυχαία τα μισά από τα ψηφοδέλτια και τα αποκαλύπτουν δημόσια, μαζί με τους σειριακούς τους αριθμούς και τις συνδέσεις τους μέσω του Switchboard. ΄Ετσι, μπορούν να επαληθεύσουν ότι το μονοπάτι μέσω του Switchboard για κάθε υποψήφιο σε κάθε ένα από τα επιλεγμένα δημόσια ψηφοδέλτια οδηγεί σε μία ψήφο στον σωστό υποψήφιο στα αποτελέσματα. Στη συνέχεια τα ψηφοδέλτια αυτά καταστρέφονται. Εάν τα ψηφοδέλτια επιλεχθούν με τρόπο δίκαιο και τυχαίο τότε η πιθανότητα κάποιος να κλέψει και αυτό να μην γίνει αντιληπτό (τυπώνοντας μη έντιμα ψηφοδέλτια, με λάθος κωδικούς υποψηφίων ή χρησιμοποιώντας ένα ανέντιμο Switchboard, το οποίο δεν δρομολογεί σωστά τις επιλογές των ψηφοφόρων) είναι πολύ μικρή.

Τον ίδιο έλεγχο μπορούν να πραγματοποιήσουν και οι ψηφοφόροι κατά την διάρκεια της ψηφοφορίας. Μπορούν να ζητήσουν και ένα δεύτερο ψηφοδέλτιο (το οποίο θα σημειωθεί ως άκυρο), να το κρατήσουν και μετά το πέρας των εκλογών να επιβεβαιώσουν ότι το μονοπάτι μέσω του Switchboard για κάθε υποψήφιο στο ψηφοδέλτιο οδηγεί σε ψήφο στο σωστό υποψήφιο στα αποτελέσματα.

Το δεύτερο σκέλος επαλήθευσης αφορά την καταμέτρηση, δηλαδή ότι οι κωδικοί που σημειώθηκαν στα ψηφοδέλτια μεταφράστηκαν σε ψήφους στους σωστούς υποψηφίους. Μετά το κλείσιμο των κάλπεων, η ελεγκτική αρχή χωρίζει το Switchboard σε δύο τυχαία υποδίκτυα.

Οι ψήφοι των ψηφοφόρων ταξιδεύουν στο πρώτο υποδίκυο, φτάνουν σε μια ενδιάμεση θέση (στην τομή του δικτύου) και μέσω του δεύτερο υποδικτύου καταλήγουν στην τελική θέση στον πίνακα των αποτελεσμάτων. Η αποκάλυψη των συνδέσεων στο ένα μέρος του δικτύου δεν αποκαλύπτει όλο το μονοπάτι. Για κάθε μία ψήφο στην ενδιάμεση θέση, η ελεγκτική αρχή ζητάει από την εφορευτική επιτροπή να αποκαλύψει είτε τις συνδέσεις το πρώτο υποδίκτυο είτε τις συνδέσεις στο δεύτερο υποδίκτυο - ποτέ όμως και τις δύο. Συνεπώς, η σύνδεση μεταξύ της επώνυμης απόδειξης του ψηφοφόρου και της τελικής θέσης στα αποτελέσματα δεν αποκαλύπτεται ποτέ στο σύνολό της.

Για κάθε μία από αυτές τις συνδέσεις, κάθε παρατηρητής μπορεί να επαληθεύσει δημόσια ότι η ψήφος ταξίδεψε χωρίς να αλλαχθεί. ΄Ετσι και πάλι η πιθανότητα το Switchboard να μην δρομολογεί σωστά τις ψήφους και αυτό να μην γίνει αντιληπτό είναι πολύ μικρή.

Σύμφωνα με όσα παρουσιάστηκαν παραπάνω, το Scantegrity εξασφαλίζει την ιδιότητα της ακραίας επαληθευσιμότητας. Συγκεκριμένα:
Υποβολή της προτιθέμενης (Cast-as-intended): Εξασφαλίζεται μέσω της αποκάλυψης των ψηφοδελτίων και του ελέγχου στο Switchboard που πραγματοποιεί η ανεξάρτητη αρχή ελέγχου πριν τις εκλογές, καθώς και των ελέγχων που μπορούν να πραγματοποιήσουν οι ψηφοφόροι ζητώντας ένα δεύτερο ψηφοδέλτιο.
Καταγραφή της υποβληθείσας (Recorded-as-cast): Εξασφαλίζεται μέσω του ελέγχου που μπορούν να πραγματοποιήσουν οι ψηφοφόροι συγκρίνοντας τις αποδείξεις που έχουν λάβει (σειριακών αριθμών και κωδικών γραμμάτων υποψηφίων) με αυτές που έχουν αναρτηθεί στον δημόσιο πίνακα ανακοινώσεων.
Καταμέτρηση των καταγεγραμμένων (Tallied-as-recorded): Εξασφαλίζεται μέσω του ελέγχου που πραγματοποιείται από την ελεγκτική αρχή στο Switchboard μετά το κλείσιμο των κάλπεων.

Το Scantegrity II ήταν το πρώτο από άκρη σε άκρη επαληθεύσιμο σύστημα με μυστικό ψηφοδέλτιο που χρησιμοποιήθηκε σε πραγματικές κυβερνητικές εκλογές. Στις 3 Νοεμβρίου του 2009, 1728 από τους 11000 περίπου εγγεγραμμένους ψηφοφόρους της πόλης Takoma Park στο Maryland των Ηνωμένων Πολιτειών της Αμερικής ψήφισαν στις δημοτικές εκλογές χρησιμοποιώντας το Scantegrity II[19].Η διαδικασία στέφθηκε με απόλυτη επιτυχία καθώς το Scantegrity έδωσε σωστό αποτέλεσμα και πέρασε όλους τους ελέγχους επαλήθευσης.

Η διαδικασία επαλήθευσης και ελέγχου ήταν όμοια με αυτή που περιγράφηκε προηγουμένως. Ως ανεξάρτητοι ελεγκτές επιλέχθηκαν οι Dr. Ben Adida, Dr. Filip Zagorski και Ms. Lillie Coney. Αρκετά πριν την έναρξη των εκλογών, στις 13 Οκτωβρίου 2009, η εφορευτική επιτροπή δημοσίευσε τις δεσμεύσεις για τα μονοπάτια αποκρυπτογράφη-

σης των 5000 ψηφοδελτίων του Scantegrity. Την επόμενη ημέρα, τα μισά από τα μονοπάτια κρυπτογράφησης των ψηφοδελτίων ανοίχτηκαν δημόσια και δημοσιοποιήθηκαν οι συνδέσεις μεταξύ των κωδικών των υποψηφίων και των υποψηφίων.

Οι εκλογές ξεκίνησαν στις 7 το πρωί της 3ης Νοεμβρίου και ολοκληρώθηκαν στις 8 το βράδυ. Κατά την διάρκεια των εκλογών η Ms. Coney επέλεξε τυχαία περίπου 50 ψηφοδέλτια από όλους τους θαλάμους με ομοιόμορφο τρόπο και δημοσιοποίησε τους σειριακούς τους αριθμούς και τους κωδικούς των υποψηφίων. Η Ms. Coney κράτησε αντίγραφο από κάθε ένα από τα ψηφοδέλτια, τα οποία υπογράφηκαν από τον πρόεδρο της εφορευτικής επιτροπής. Η Ms. Coney δεν είχε καμία αλληλεπίδραση με τους ψηφοφόρους.

Η επιβεβαίωση για την ορθή καταμέτρηση των ψήφων έγινε στις 5 Νοεμβρίου όπου ολοκληρώθηκε η καταμέτρηση των ψηφοδελτίων με το χέρι. Αν και τα αποτελέσματα της ψηφιακής καταμέτρησης δεν ταίριαζαν απόλυτα με τα αποτελέσματα της χειροκίνητης καταμέτρησης, το αποτέλεσμα κρίθηκε σωστό. Η διαφορά οφειλόταν σε 48 ψηφοδέλτια στα οποία οι επιλογές για τους υποψηφίους είχαν σημειωθεί εκτός των προκαθορισμένων περιοχών. Ενώ το οπτικό σκάνερ δεν αναγνώρισε τις ψήφους αυτές, η νομοθεσία της πόλης ορίζει πως οι ψήφοι έπρεπε να καταμετρηθούν.

Την επόμενη ημέρα δημοσιεύτηκαν όλοι οι κωδικοί των ψηφοδελτίων που καταμετρήθηκαν καθώς και όλα τα στοιχεία των ψηφοδελτίων που περίσσεψαν (όσα δεν ακυρώθηκαν και δεν χρησιμοποιήθηκαν για ψηφοφορία).

Στις 9 Νοεμβρίου, οι εξωτερικοί ελεγκτές Dr. Adida και Dr. Zagorski επιβεβαίωσαν ο κάθε ένας ανεξάρτητα ότι το Scantegrity πέρασε σωστά όλες τις δοκιμασίες. Συγκεκριμένα, επιβεβαίωσαν ότι οι ψήφοι καταμετρήθηκαν σωστά. Επίσης, δημοσιοποίησαν, ο κάθε ένας στην ιστοσελίδα του, κώδικα που οι ίδιοι έγραψαν με τον οποίον οποιοσδήποτε μπορεί να επιβεβαιώσει ότι οι δεσμεύσεις της εφορευτικής επιτροπής για τον υπολογισμό του αποτελέσματος είναι σωστές.

Για την δημοσιοποίηση των αρχικών δεσμεύσεων για το σύστημα αλλά και όλων των σειριακών κωδικών και των κωδικών γραμμάτων κατασκευάστηκε ειδική ιστοσελίδα η οποία είχε τον ρόλο του πίνακα ανακοινώσεων. Ενώ το αρχικό σενάριο ήταν η ιστοσελίδα να φιλοξενηθεί από τον δήμο, τελικά μόνο το μέρος των αποτελεσμάτων και οι πληροφορίες για τις εκλογές φιλοξενήθηκαν από τον δήμο. Το μέρος της επαλήθευσης της σωστής καταγραφής της ψήφου φιλοξενήθηκε από το Scantegrity. Πέρα από την σελίδα του Scantegrity τα δεδομένα των αποδείξεων δημοσιεύτηκαν και στις ιστοσελίδες των ελεγκτών. ΄Ενα από τα βασικότερα προβλήματα ήταν η διασφάλιση ότι τα δεδομένα που βλέπουν οι χρήστες ήταν αυθεντικά. Για τον λόγο αυτό

χρησιμοποιήθηκαν ψηφιακές υπογραφές.

Οι ελεγκτές Adida και Zagorski έλεγχαν περιοδικά την ορθότητα των υπογραφών καθώς επίσης και εάν τα δεδομένα που παρέχει η ιστοσελίδα είναι όμοια σε κάθε έναν έλεγχο.

Η περίοδος για διαμαρτυρίες σχετικά με τις εκλογές (συμπεριλαμβανομένων και διαμαρτυριών για σειριακούς αριθμούς που λείπουν) έληξε στις 6 Νοεμβρίου. Εντός της προθεσμίας 66 άτομα (σχεδόν το 4% των συνολικών ψηφοφόρων που ψήφισαν) επισκέφθηκαν την ιστοσελίδα για να επιβεβαιώσουν ότι η ψήφος τους καταγράφηκε σωστά από το σύστημα. Ο αριθμός αυτός αν και μικρός θεωρήθηκε αρκετός για τον εντοπισμό τυχόν σφαλμάτων ή αλλοίωσης του αποτελέσματος με μεγάλη πιθανότητα. Το Scantegrity έλαβε μόνο μία ένσταση από ένα ψηφοφόρο η οποία αποδείχθηκε λανθασμένη καθώς ο ψηφοφόρος είχε σημειώσει λάθος ένα ψηφίο στον κωδικό.

3.2 Ακραίως επαληθεύσιμα συστήματα που απαιτούν φυσικό χώρο εκλογών και βασίζονται σε ψηφιακό ψηφοδέλτιο

Η κατηγορία αυτή αποτελείται από συστήματα στα οποία τα ψηφοδέλτια είναι ψηφιακά, η καταμέτρησή των ψήφων γίνεται ηλεκτρονικά και η ψηφοφορία γίνεται σε φυσικό χώρο - εκλογικό κέντρο. Η βασική διαφοροποίηση από τα συστήματα της προηγούμενης κατηγορίας είναι ότι το ψηφοδέλτιο που ρίχνεται πλέον στην κάλπη δεν είναι άμεσα ορατό από τον ψηφοφόρο. Στα συστήματα της προηγούμενης κατηγορίας οι ψηφοφόροι ρίχνουν ένα χάρτινο ψηφοδέλτιο οι ίδιοι στην κάλπη. Αυτό σημαίνει ότι εύκολα μπορούν να ελέγξουν ότι το ψηφοδέλτιο είναι σωστό πριν το ρίξουν. Στα συστήματα, όμως, όπου το ψηφοδέλτιο είναι ψηφιακό κάτι τέτοιο δεν είναι τόσο προφανές - πλέον το μηχάνημα ψηφοφορίας είναι αυτό που ρίχνει το ψηφοδέλτιο στην κάλπη και όχι ο ψηφοφόρος. Συνεπώς είναι αναγκαία η εισαγωγή νέων μεθόδων επαλήθευσης ότι το μηχάνημα εκτελεί σωστά την δουλειά του.

Κύρια χαρακτηριστικά αυτών των συστημάτων είναι ότι βασίζονται σε συνδυασμούς διαφόρων κρυπτογραφικών μεθόδων. Στο πλαίσιο της εργασίας αυτής θα μελετηθεί ένα πολύ σημαντικό σύστημα για αυτή την κατηγορία, το MarkPledge[20].

3.2.1 MarkPledge

Το MarkPledge εφευρέθηκε από τον Neff το 2004 και είναι μαζί

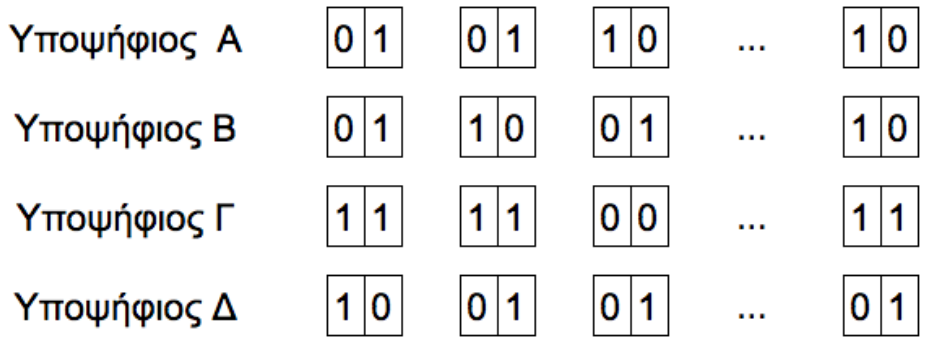
με το Votegrity του Chaum ένα από τα πρώτα ακραίως επαληθεύσιμα συστήματα εκλογών. Η πρωτοπορία στο σύστημα αυτό είναι ότι επιτρέπει στους χρήστες να επαληθεύσουν ότι η ψήφος τους κρυπτογραφήθηκε σωστά από το μηχάνημα ψηφοφορίας την ώρα που βρίσκονται στο θάλαμο ψηφοφορίας, χωρίς να απαιτείται να κάνουν σύνθετους υπολογισμούς. Αντίθετα με άλλα συστήματα που ανήκουν στην ίδια κατηγορία τα οποία έχουν σύνθετες διαδικασίες επαλήθευσης, το MarkPledge απλοποιεί την επαλήθευση της σωστής λειτουργίας του μηχανήματος ψηφοφορίας μέσω της σύγκρισης γραμμών κειμένου μήκους τεσσάρων χαρακτήρων.

Η ψηφοφορία με το MarkPledge γίνεται με τον ακόλουθο τρόπο. Εντός κάθε θαλάμου ψηφοφορίας υπάρχει ένα μηχάνημα ψηφοφορίας. Εκεί, ο ψηφοφόρος επιλέγει τον υποψήφιο της επιλογής του, χρησιμοποιώντας το γραφικό περιβάλλον του μηχανήματος ψηφοφορίας. Το μηχάνημα παράγει μία ειδικά διαμορφωμένη κρυπτογράφηση της επιλογής του ψηφοφόρου, την οποία τυπώνει σε μία απόδειξη. Στη συνέχεια, το μηχάνημα δεσμεύεται στην επιλογή του ψηφοφόρου παρουσιάζοντας στην οθόνη ένα σύντομο κείμενο. Στην απόδειξη επίσης τυπώνονται και οι ακόλουθες πληροφορίες: Το σύντομο κείμενο που εμφανίστηκε στην οθόνη, η λίστα με τους υποψηφίους, καθώς και μια λίστα με σύντομους κωδικούς, κάθε ένας από τους οποίους αντιστοιχεί σε έναν υποψήφιο. Επιπλέον τυπώνεται και μια απόδειξη για την σωστή κρυπτογράφηση της ψήφου του ψηφοφόρου. Με τα παραπάνω δεδομένα ο ψηφοφόρος μπορεί να επαληθεύσει ότι το μηχάνημα κρυπτογράφησε σωστά την ψήφο του.

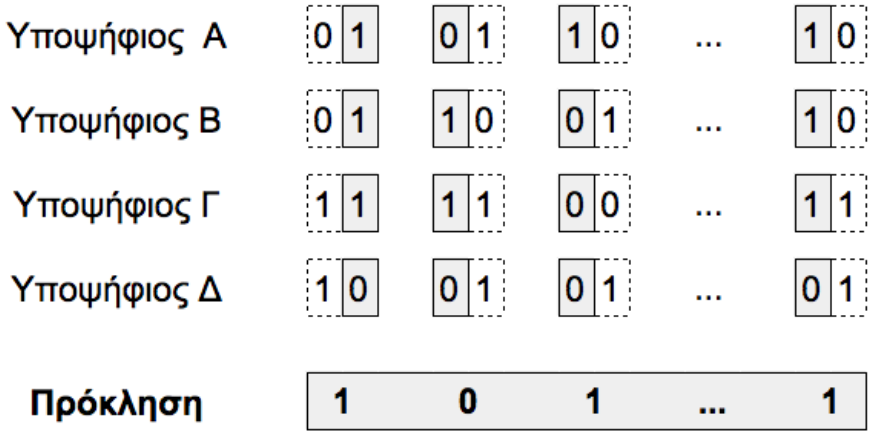
Για την επεξήγηση της διαδικασίας επαλήθευσης είναι απαραίτητη η κατανόηση της δομής του ψηφοδελτίου του MarkPledge.

Σε κάθε υποψήφιο στο ψηφοδέλτιο του MarkPledge αντιστοιχεί μια λίστα από ζεύγη δυαδικών ψηφίων. Τα ζεύγη των δυαδικών ψηφίων για κάθε υποψήφιο διαμορφώνονται ανάλογα με τον αν ο ψηφοφόρος θα επιλέξει να ψηφίσει τον εκάστοτε υποψήφιο. Μία ψήφος στον εκάστοτε ψηφοφόρο (ναι-ψήφος) συμβολίζεται από συνδυασμούς ζευγών όπου τα δυαδικά ψηφία είναι ίδια, δηλαδή (1,1) ή (0,0). Αντίστοιχα η μη ψήφος (όχι-ψήφος) στον εκάστοτε ψηφοφόρο συμβολίζεται με συνδυασμούς ζευγών από δυαδικά ψηφία που είναι διαφορετικά μεταξύ τους, δηλαδή (0,1) ή (1,0). ΄Οταν ο ψηφοφόρος επιλέγει έναν υποψήφιο το σύστημα θέτει τα ζεύγη δυαδικών ψηφίων έτσι ώστε κάθε ζεύγος να περιέχει όμοια ψηφία, βάζει δηλαδή μια Ναι-ψήφο. Για όλους τους υπόλοιπους υποψήφιους θέτει τα δυαδικά ψηφία των ζευγών τους έτσι ώστε να αναπαριστούν ΄Οχι-ψήφους.

΄Εστω ένα παράδειγμα όπου ο ψηφοφόρος επιλέγει να ψηφίσει τον υποψήφιο Γ. Στο Σχήμα 3.2 παρουσιάζεται ένα παράδειγμα συμπλήρω-



Σχήμα 3.2: Παράδειγμα συμπλήρωσης του ψηφοδελτίου του Mark-Pledge



Σχήμα 3.3: Παράδειγμα ελέγχου του ψηφοδελτίου του MarkPledge

σης των ζευγών από το σύστημα.

Τα ζεύγη στο Σχήμα 3.2 είναι αποτέλεσμα της κρυπτογράφησης των δυαδικών ψηφίων 0 και 1. Συγκεκριμένα, όταν ο ψηφοφόρος επιλέγει να ψηφίσει έναν υποψήφιο, τότε του δίνει την ψήφο 1, ενώ όσοι υποψήφιοι δεν ψηφίστηκαν παίρνουν την τιμή 0. Οι τιμές αυτές κρυπτογραφούνται με μια ειδική πιθανοτική κρυπτογράφηση El Gamal η οποία παράγει τα ζεύγη (0,0), (0,1), (1,0) και (1,1). Συνεπώς τα παραπάνω ζεύγη είναι κρυπτοκείμενα τα οποία αντιστοιχούν στα ψηφία 0 και 1.

Στη συνέχεια, το μηχάνημα κωδικοποιεί την σειρά δυαδικών ψηφίων του επιλεγμένου υποψήφιου σε κείμενο. Το κείμενο αυτό έχει

μήκος 4 χαρακτήρες και εμφανίζεται στην οθόνη.

Μετά την κρυπτογράφηση της ψήφου, ο ψηφοφόρος μπορεί να επαληθεύσει ότι η κρυπτογράφηση ήταν σωστή ζητώντας από το σύστημα να αποκαλύψει είτε το δεξί είτε το αριστερό δυαδικό ψηφίου κάθε ζεύγους για κάθε ψηφοφόρο. Η πρόκληση που ο ψηφοφόρος δίνει στο σύστημα είναι μία σειρά από δυαδικά ψηφία, όπου το 0 συμβολίζει το αριστερό δυαδικό ψηφίο κάθε ζεύγους και το 1 το δεξί. ΄Ενα τέτοιο παράδειγμα παρουσιάζεται στο Σχήμα 3.3.

΄Οπως και προηγουμένως, στην οθόνη δεν εμφανίζονται τα δυαδικά ψηφία που επέλεξε ο ψηφοφόρος αλλά η αλφαριθμητική κωδικοποίησή τους. ΄Ετσι ο ψηφοφόρος μπορεί να επιβεβαιώσει ότι η αλφαριθμητική τιμή που εμφανίζεται δίπλα στον υποψήφιο της επιλογής της ταιριάζει με τη δέσμευση που του έδωσε το μηχάνημα προηγουμένως. Καθώς ο ψηφοφόρος επιλέγει τυχαία την πρόκληση, το μηχάνημα δεν μπορεί να γνωρίζει από πριν ποιο από τα δύο ψηφία κάθε ζεύγους θα αποκαλυφθεί. ΄Ετσι, εάν το μηχάνημα άλλαξε την ψήφο του ψηφοφόρου (κρυπτογραφώντας την ψήφο σαν όχι αντί για ναι), υπάρχει πολύ μεγάλη πιθανότητα ότι η απάτη του συστήματος θα εντοπιστεί στα δυαδικά ψηφία που ο ψηφοφόρος επέλεξε να αποκαλυθφούν. Ο μηχανισμός αυτός διασφαλίζει στον ψηφοφόρο ότι η ψήφος του κρυπτογραφήθηκε σωστά και ότι η ψήφος που ρίχθηκε στην κάλπη ήταν αυτή που επέλεξε ο ψηφοφόρος.

Μόλις η πρόκληση ολοκληρωθεί, η μηχανή δημιουργεί όχι-ψήφους για όλους τους υποψηφίους στο ψηφοδέλτιο με την σημαντική λεπτομέρεια ότι συμπληρώνει τις θέσεις (δεξιά/αριστερά) που επέλεξε ο ψηφοφόρος έτσι ώστε όλες οι ψήφοι να φαίνονται σαν ναι-ψήφοι. ΄Ολη αυτή η πληροφορία, μαζί με τα κρυπροκείμενα, την δέσμευση της μηχανής, την πρόκληση του ψηφοφόρου και τα τυχαία στοιχεία που προστέθηκαν στο ψηφοδέλτιο τυπώνονται στην απόδειξη με την μορφή κωδικοποιημένου αλφαριθμητικού κειμένου.

Το εκλογικό μηχάνημα επίσης υπογράφει την απόδειξη και τυπώνει την υπογραφή πάνω στην απόδειξη.

Αμέσως μετά την ψηφοφορία, η κρυπτογραφημένη ψήφος του ψηφοφόρου μαζί με το όνομα του δημοσιεύονται σε έναν δημόσιο πίνακα ανακοινώσεων.

Με την έξοδό του από τον θάλαμο ψηφοφορίας, ο ψηφοφόρος δίνει την απόδειξη σε κάποιον βοηθητικό οργανισμό της επιλογής του. Οι βοηθητικοί οργανισμοί βρίσκονται παρόντες κατά την διάρκεια των εκλογών και μπορούν να στελεχώνονται από μέλη των διάφορων παρατάξεων που συμμετέχουν στις εκλογές. Ο βοηθητικός οργανισμός επαληθεύει ότι η απόδειξη του ψηφοφόρου δημοσιεύτηκε σωστά στον πίνακα ανακοινώσεων, ότι είναι σωστά συμπληρωμένο και ότι η υπογραφή του μηχανήματος εκλογών είναι σωστή.

Εάν τα αποτελέσματα του βοηθητικού οργανισμού δεν ικανοποιήσουν τον ψηφοφόρο, μπορεί απλά να πάει και να ψηφίσει ξανά. Σε αυτή την περίπτωση η νέα ψήφος αντικαθιστά την προηγούμενη στον πίνακα ανακοινώσεων. Ο πίνακας ανακοινώσεων κρατάει ιστορικό με όλες τις ψήφους των ψηφοφόρων, υποδεικνύοντας ποια είναι η τελευταία που θα καταμετρηθεί.

΄Οταν ο ψηφοφόρος πειστεί ότι η ψήφος του καταχωρήθηκε σωστά, μπορεί να φύγει από το εκλογικό κέντρο μαζί με την απόδειξη που του έδωσε το μηχάνημα ψηφοφορίας. Εάν το επιθυμεί, μπορεί να δώσει ένα αντίγραφο της απόδειξής του σε όσους βοηθητικούς οργανισμούς επιθυμεί.

Αφού φύγει από το εκλογικό κέντρο, ο ψηφοφόρος μπορεί να ελέγξει, χρησιμοποιώντας έμπιστο λογισμικό, ότι η ψήφος του καταχωρήθηκε και μετρήθηκε σωστά. Μετά το πέρας των εκλογών υπάρχει μια περίοδος όπου οι ψηφοφόροι μπορούν να ελέγξουν ότι οι αποδείξεις τους εμφανίζονται σωστά στον πίνακα ανακοινώσεων. Επίσης, την περίοδο αυτή οι βοηθητικοί οργανισμοί ελέγχουν και αυτοί ότι οι αποδείξεις των ψηφοφόρων εμφανίζονται σωστά στον πίνακα ανακοινώσεων.

Μετά από την διευθέτηση τυχών παραπόνων για τις εκλογές, τα ψηφοδέλτια ανωνυμοποιούνται και καταμετρώνται με την χρήση δικτύων μίξης.

Είναι σημαντικό να αναφερθεί εδώ ότι η απόδειξη δεν παρέχει καμία πληροφορία για το περιεχόμενο της ψήφου του ψηφοφόρου, αφού τα αλφαριθμητικά κείμενα αντιπροσωπεύουν όλα “ναι” ψήφους. Ο ψηφοφόρος που γνωρίζει το σωστό κείμενο στο οποίο δεσμεύτηκε το μηχάνημα ψηφοφορίας μπορεί να αναγνωρίσει ποια είναι η σωστή ψήφος. ΄Ομως, καθώς ο ψηφοφόρος ήταν μόνος του στον θάλαμο ψηφοφορίας και καθώς το κείμενο για την αληθινή ναι ψήφο εμφανίστηκε στην οθόνη και μετά εξαφανίστηκε, ο ψηφοφόρος δεν μπορεί να αποδείξει σε κανέναν ποιο από τα αλφαριθμητικά κείμενα αντιπροσωπεύει την αληθινή ναι-ψήφο. Αυτός είναι και ο λόγος που το μηχάνημα εμφανίζει μόνο το δεξί ή μόνο το αριστερό δυαδικό ψηφίο κάθε ζεύγους. Εάν ο ψηφοφόρος μπορούσε να γνωρίζει την τυχαιότητα που χρησιμοποιήθηκε για την κρυπτογράφηση και των δύο ψηφίων θα μπορούσε εύκολα να αποδείξει τι ψήφισε.

3.3 Ακραίως επαληθεύσιμα συστήματα απομακρυσμένης ψηφοφορίας με ψηφιακό ψηφοδέλτιο

Η κατηγορία αυτή αποτελείται από συστήματα τα οποία δίνουν την δυνατότητα στους ψηφοφόρους να ψηφίσουν μέσω διαδικτύου. Τα συστήματα της κατηγορίας αυτά αντιμετωπίζουν την ίδια πρόκληση με

τα συστήματα της προηγούμενης κατηγορίας, καθώς και σε αυτά ένα μηχάνημα ρίχνει το ψηφοδέλτιο στην κάλπη. Τα συστήματα, όμως, αυτά αντιμετωπίζουν και άλλη μία πρόκληση. Καθώς ο ψηφοφόρος ψηφίζει απομακρυσμένα, δεν υφίσταται πλέον ο ασφαλής και ιδιωτικός θάλαμος ψηφοφορίας. Αυτό σημαίνει ότι τα συστήματα τέτοιου τύπου καλούνται να αντιμετωπίσουν και άλλο ένα πρόβλημα, αυτό του εκβιασμού και της πώλησης της ψήφου. Στην κατηγορία αυτή ανήκουν δύο συστήματα εκλογών με ιδιαίτερο ενδιαφέρον μελέτης, το Civitas[21], το οποίο προσπαθεί να αντιμετωπίσει το πρόβλημα του εκβιασμού και της πώλησης της ψήφου, και το Helios[22] το οποίο έχει στόχο την ευκολία στην χρήση.

3.3.1 Civitas

Το Civitas σχεδιάστηκε και υλοποιήθηκε από τους Clarkson, Chong και Myers και είναι το πρώτο από άκρη σε άκρη επαληθεύσιμο σύστημα το οποίο αντιμετωπίζει αποτελεσματικά το πρόβλημα του εκβιασμού και της πώλησης της ψήφου. Η βασική λογική πίσω από την λειτουργία του Civitas, καθώς και ο τρόπος που αυτό προστατεύει τον ψήφοφόρο από τον εξαναγκασμό/πώληση της ψήφου βασίζεται σε ένα προηγούμενο σύστημα εκλογών, το JCJ[23][24], το οποίο αναπτύχθηκε από τους Juels, Catalano και Jakobsson. Η βασική διαφορά και καινοτομία του Civitas είναι ο διαμοιρασμός της εμπιστοσύνης ανάμεσα σε πολλές αρχές - δράστες αντί για έναν.

Για την κατανόηση του τρόπου λειτουργίας του Civitas, είναι σημαντική η κατανόηση του ρόλου που έχουν οι διάφοροι δράστες.

Στο Civitas υπάρχουν πέντε τύποι δραστών: ένας διαχειριστής, ένας υπεύθυνος πιστοποίησης της ταυτότητας των ψηφοφόρων, οι ψηφοφόροι, οι υπεύθυνοι εγγραφής των ψηφοφόρων στο σύστημα και οι υπεύθυνοι καταμέτρησης.

΄Ολοι οι δράστες πλην των ψηφοφόρων αποτελούν τις αρχές διεξαγωγής των εκλογών:

- Ο Διαχειριστής είναι υπεύθυνος για την διοργάνωση και για την διεξαγωγή των εκλογών. Αυτό περιλαμβάνει τον καθορισμό της μορφής του ψηφοδελτίου, των υπεύθυνων καταμέτρησης, της έναρξης και της λήξης των εκλογών.

- Οι υπέυθυνοι ταυτοποιησης, πιστοποιούν την ταυτότητα των ψηφοφόρων κατά την διάρκεια της ψηφοφορίας.

- Οι υπεύθυνοι εγγραφής των ψηφοφόρων στο σύστημα (registration tellers) δημιουργούν τα διαπιστευτήρια που θα χρησιμοποι-

ήσουν οι ψηφοφόροι για την αποστολή των ψήφων τους στην κάλπη.

- Οι υπεύθυνοι καταμέτρησης (tabulation tellers) καταμετρούν τις ψήφους.

΄Ολοι οι παραπάνω δράστες χρησιμοποιούν δημόσια αρχεία καταγραφής τα οποία έχουν την ιδιότητα ότι υποστηρίζουν μόνο την προσθήκη δεδομένων (και όχι την αλλαγή ή διαγραφή δεδομένων). Η ακεραιότητα των δεδομένων στα αρχεία καταγραφής εξασφαλίζεται μέσω ψηφιακών υπογραφών. Οι δράστες μπορούν να υπογράψουν τα δεδομένα που εισάγουν στο σύστημα καταγραφής, διασφαλίζοντας ότι το σύστημα δεν μπορεί να πλαστογραφήσει νέα δεδομένα εκ μέρους των δραστών.

Πέρα από την ακεραιότητα και την αυθεντικότητα των αποθηκευμένων δεδομένων των αρχείων καταγραφής, πρέπει να διασφαλίζεται και ότι η πληροφορία που παρουσιάζουν τα αρχεία καταγραφής στον χρήστη είναι αυθεντική και ακέραια. Για τον λόγο αυτό κάθε φορά που το σύστημα καταγραφής δίνει μια πληροφορία στον χρήστη την υπογράφει. ΄Ετσι, εάν το σύστημα καταγραφής δώσει διαφορετική πληροφορία σε δύο χρήστες, αυτό θα μπορεί να εντοπιστεί. Τέτοια συστήματα αρχείων καταγραφής χρησιμοποιούνται για την εξυπηρέτηση διάφορων λειτουργιών κατά την διάρκεια μιας εκλογικής διαδικασίας. Μία περίπτωση χρήσης τους είναι ο γνωστός πίνακας ανακοινώσεων, ο οποίος χρησιμοποιείται από τις αρχές διοργάνωσης των εκλογών για να καταγράφει όλες τις πληροφορίες που απαιτούνται για την εξασφάλιση της ιδιότητας της επαληθευσιμότητας των εκλογών. Οι κάλπες αποτελούν και αυτές υλοποιήσεις αυτού του καταγραφικού συστήματος.

Αρχικά, ο διαχειριστής δημιουργεί τις εκλογές δημοσιοποιώντας το σχέδιο του ψηφοδελτίου σε έναν άδειο πίνακα ανακοινώσεων. Ο διαχειριστής επίσης καθορίζει τους υπεύθυνους καταμέτρησης δημοσιεύοντας τα δημόσια κλειδιά τους.

Στη συνέχεια ο υπεύθυνος πιστοποίησης της ταυτότητας των ψηφοφόρων δημοσιεύει τους εκλογικούς καταλόγους, οι οποίοι περιέχουν ένα αναγνωριστικό για κάθε ψηφοφόρο (για παράδειγμα το ονοματεπώνυμο) μαζί με το δημόσιο κλειδί κάθε ψηφοφόρου. Κάθε ψηφοφόρος έχει δύο κλειδιά, ένα κλειδί εγγραφής και ένα κλειδί εξουσιοδότησης. Η χρήση των κλειδιών αυτών παρουσιάζεται στη συνέχεια.

΄Επειτα, οι υπεύθυνοι καταμέτρησης δημιουργούν συλλογικά ένα δημόσιο κλειδί για ένα διαμοιρασμένο σχήμα κρυπτογράφησης και το δημοσιεύουν στον πίνακα ανακοινώσεων. Η αποκρυπτογράφηση των μηνυμάτων τα οποία κρυπτογραφήθηκαν με αυτό το δημόσιο κλειδί απαιτεί την συνεργασία όλων των υπευθύνων καταμέτρησης.

Τέλος, οι υπεύθυνοι εγγραφής των ψηφοφόρων στο σύστημα δημιουργούν διαπιστευτήρια για κάθε έναν ψηφοφόρο. Τα διαπιστευτήρια αυτά χρησιμοποιούνται για να πιστοποιήσουν την αυθεντικότητα των ψήφων χωρίς όμως να αποκαλύψουν την ταυτότητα του ψηφοφόρου. Κάθε διαπιστευτήριο αντιστοιχεί μοναδικά σε έναν ψηφοφόρο. ΄Οπως τα κλειδιά στην ασύμμετρη κρυπτογραφία, τα διαπιστευτήρια είναι ζεύγη ενός δημόσιου και ένας ιδιωτικού κλειδιού. ΄Ολα τα δημόσια διαπιστευτήρια δημοσιεύονται στον πίνακα ανακοινώσεων ενώ τα ιδιωτικά χωρίζονται σε μέρη και κάθε υπεύθυνος εγγραφής των ψηφοφόρων στο σύστημα αποθηκεύει ένα μόνο μέρος από κάθε ένα ιδιωτικό κλειδί.

Ο διαμοιρασμός αυτός των ιδιωτικών διαπιστευτηρίων των ψηφοφόρων καθιστά σχεδόν αδύνατη την πλαστογράφηση ή την διαρροή τους από κάποιο μέλος της εφορευτικής επιτροπής, καθώς κάτι τέτοιο απαιτεί την συνεργασία όλων των υπεύθυνων εγγραφής των ψηφοφόρων στο σύστημα.

Για την απόκτηση των ιδιωτικών τους διαπιστευτηρίων, οι ψηφοφόροι πρέπει να εγγραφούν. Κάθε υπεύθυνος εγγραφής των ψηφοφόρων στο σύστημα πιστοποιεί την ταυτότητα ενός ψηφοφόρου χρησιμοποιώντας το κλειδί εγγραφής του ψηφοφόρου.

Στη συνέχεια, ο ψηφοφόρος και ο κάθε ένας υπεύθυνος εγγραφής ακολουθούν ένα πρωτόκολλο με το οποίο χρησιμοποιώντας το κλειδί εξουσιοδότησης του ψηφοφόρου απελευθερώνεται το ιδιωτικό μέρος του διαπιστευτηρίου του ψηφοφόρου που έχει στην κατοχή του ο εκάστοτε υπεύθυνος εγγραφής. Ο ψηφοφόρος συνδυάζει όλα αυτά τα μέρη για να κατασκευάσει το ιδιωτικό του διαπιστευτήριο.

Για να ψηφίσει, ο ψηφοφόρος εισάγει στο σύστημα το ιδιωτικό διαπιστευτήριο, επιλέγει τους ψηφοφόρους που επιθυμεί να ψηφίσει και δημιουργεί μια απόδειξη ότι το ψηφοδέλτιο είναι σωστά συμπληρωμένο. ΄Ολη αυτή η πληροφορία αποστέλλεται στην κάλπη. Είναι σημαντικό να σημειωθεί ότι ο ψηφοφόρος έχει την δυνατότητα να ρίξει το ψηφοδέλτιο σε πολλές κάλπες ταυτόχρονα.

΄Οπως αναφέρθηκε στην εισαγωγή της ενότητας αυτής, η βασική καινοτομία που εισάγει το Civitas είναι η αντίστασή του στον εκβιασμό και την εξαγορά της ψήφου. Αυτό γίνεται εφικτό με την δυνατότητα των ψηφοφόρων να δημιουργούν ψεύτικα διαπιστευτήρια με την ιδιότητα ότι ένας τρίτος δεν μπορεί να τα ξεχωρίσει από τα αληθινά. ΄Ετσι, στην περίπτωση εκβιασμού ή εξαγοράς της ψήφου ο ψηφοφόρος μπορεί να χρησιμοποιήσει ή να στείλει τα ψεύτικα διαπιστευτήρια αντί τα αληθινά, και όταν δεν διατρέχει κάποιον κίνδυνο ή πίεση να ψηφίσει με τα αληθινά. Οι ψήφοι που ρίχνονται στην κάλπη με ψεύτικα διαπιστευτήρια εμφανίζονται και αυτές στον πίνακα ανα-

κοινώσεων σαν πραγματικές (θα απορριφθούν όμως αργότερα από το σύστημα της καταμέτρησης των ψήφων).

Μόλις κλείσουν οι κάλπες ξεκινάει η διαδικασία της καταμέτρησης των ψήφων. Αρχικά, οι υπεύθυνοι καταμέτρησης συγκεντρώνουν όλες τις ψήφους από όλες τις κάλπες, καθώς και τα δημόσια διαπιστευτήρια από τον πίνακα ανακοινώσεων. Το επόμενο βήμα είναι ο έλεγχος των αποδείξεων για κάθε ένα ψηφοδέλτιο, έτσι ώστε να επαληθευτεί η σωστή του συμπλήρωση. Κάθε ψηφοδέλτιο που δεν έχει έγκυρη υπογραφή απορρίπτεται. ΄Εχοντας κρατήσει μόνο τα σωστά συμπληρωμένα ψηφοδέλτια γίνεται στη συνέχεια η αφαίρεση των διπλών ψήφων. Για κάθε ένα διαπιστευτήριο κρατείται το πολύ μία ψήφος. Η αφαίρεση των ψήφων με ίδια διαπιστευτήρια γίνεται σύμφωνα με την πολιτική επαναφήφισης του εκάστοτε φορέα που διεξάγει τις εκλογές.

Η λίστα με τις υποβληθείσες ψήφους καθώς και η λίστα με τα διαπιστευτήρια ανωνυμοποιούνται με την χρήση ενός δικτύου μίξης. ΄Εχοντας αφαιρέσει πλέον την σύνδεση μεταξύ των ψήφων, των διαπιστευτηρίων και των ψηφοφόρων γίνεται αφαίρεση των ψήφων οι οποίες ρίχθηκαν με ψεύτικα διαπιστευτήρια. Το γεγονός ότι η αφαίρεση των ψήφων αυτών γίνεται μετά την ανωνυμοποίηση είναι ιδιαίτερα σημαντικό. Σε αντίθετη περίπτωση θα μπορούσαν να εντοπιστούν οι ψηφοφόροι που έδωσαν ψεύτικα διαπιστευτήρια σε κάποιον που τους εκβίασε ή εξαγόρασε την ψήφο τους και να διωχθούν.

Τέλος, γίνεται η αποκρυπτογράφηση και η καταμέτρηση των ψήφων. Τα διαπιστευτήρια δεν αποκρυπτογραφούνται. Ο υπολογισμός του αποτελέσματος μέσω των αποκρυπτογραφημένων ψηφοδελτίων μπορεί να γίνει από τον οποιοδήποτε.

Πέρα από την αντίσταση στον εκβιασμό και την πώληση της ψήφου, το Civitas διασφαλίζει την ιδιότητα της ακραίας επαληθευσιμότητας. Κάθε ψηφοφόρος μπορεί να ελέγξει ότι η ψήφος του καταγράφηκε από το σύστημα όπως υποβλήθηκε στην κάλπη επιβεβαιώνοντας ότι βρίσκεται ακέραια στον πίνακα ανακοινώσεων (ατομική επαληθευσιμότητα).

Επίσης, η διαδικασία της καταμέτρησης είναι επαληθεύσιμη καθώς κάθε υπεύθυνος καταμέτρησης δημοσιεύει αποδείξεις ότι ακολούθησε σωστά το πρωτόκολλο. ΄Ολοι οι υπεύθυνοι καταμέτρησης επαληθεύουν τις αποδείξεις αυτές κατά την διάρκεια της καταμέτρησης. Εάν ένας έντιμος καταμετρητής ανακαλύψει μια άκυρη απόδειξη σταματάει την διαδικασία της καταμέτρησης. Επιπρόσθετα, οι αποδείξεις των υπευθύνων καταμέτρησης μπορούν να επαληθευτούν από τον οποιοδήποτε μετά το πέρας της καταμέτρησης (γενική επαληθευσιμότητα).

3.3.2 Helios

Το Helios εφευρέθηκε το 2008 από τον Adida. Είναι ένα διαδικτυακό σύστημα εκλογών το οποίο προορίζεται για εκλογές στις οποίες η μυστικότητα και η ακεραιότητα της ψήφου είναι ύψιστης σημασίας, ο κίνδυνος, όμως, εκβιασμού ή πώλησης της ψήφου είναι μικρός. Τέτοιες περιπτώσεις είναι οι μαθητικές εκλογές, οι εκλογές συλλόγων και οι εκλογές σε διαδικτυακές κοινότητες. Το Helios δεν εισάγει κάποια νέα τεχνολογία ή κάποιο νέο πρωτόκολλο εκλογών. Χρησιμοποιεί τεχνολογίες που ήδη υπάρχουν στην βιβλιογραφία για να φτιάξει ένα αποτελεσματικό και εύχρηστο σύστημα εκλογών.

΄Ενα από τα κύρια χαρακτηριστικά του Helios είναι η επαληθευσιμότητά του. Ως σύστημα με ψηφιακό ψηφοδέλτιο και ψηφιακή καταμέτρηση, το Helios καλείται να αντιμετωπίσει το ζήτημα της επαλήθευσης της υποβολής της προτιθέμενης. Η εξασφάλιση της υποβολή της προτιθέμενης επαληθευσιμότητας του Helios βασίζεται στην μελέτη του Josh Benaloh[25], δηλαδή στον διαχωρισμό της διαδικασίας συμπλήρωσης του ψηφοδελτίου από την διαδικασία ρίψης του στην κάλπη.

Η βασική ιδέα είναι ότι ένα ψηφοδέλτιο μιας εκλογικής διαδικασίας μπορεί να προβληθεί και να συμπληρωθεί από τον οποιοδήποτε, οποιαδήποτε χρονική στιγμή κατά την διάρκεια των εκλογών, χωρίς να απαιτείται πιστοποίηση της ταυτότητας του ψηφοφόρου. Η πιστοποίηση της ταυτότητας του ψηφοφόρου γίνεται μόνο την στιγμή πριν της ρίψης του ψηφοδελτίου στην κάλπη. ΄Ετσι, οποιοσδήποτε, ακόμα και κάποιος ελεγκτής ο οποίος δεν έχει δικαίωμα ψήφου στις εκλογές (για παράδειγμα ένα μέλος από μία παράταξη) μπορεί να ελέγξει ότι ο μηχανισμός προετοιμασίας του ψηφοδελτίου λειτουργεί σωστά.

Η διαδικασία της ψηφοφορίας είναι η ακόλουθη:

1. Ο ψηφοφόρος ξεκινάει την διαδικασία ψηφοφορίας με το να υποδείξει στο σύστημα σε ποια εκλογική διαδικασία θέλει να συμμετάσχει.

2. Το Σύστημα Προετοιμασίας Ψηφοδελτίου παρουσιάζει στον ψηφοφόρο το ψηφοδέλτιο και καταγράφει τις επιλογές του.

3. Μόλις ο ψηφοφόρος επιβεβαιώσει τις επιλογές του, το Σύστημα Προετοιμασίας Ψηφοδελτίου κρυπτογραφεί την ψήφο του και δεσμεύεται στην κρυπτογράφηση αυτή προβάλλοντας το αποτέλεσμα της εφαρμογής μιας συνάρτησης κατακερματισμού στο κρυπτοκείμενο.

4. Ο ψηφοφόρος μπορεί να επιλέξει να ελέγξει το ψηφοδέλτιο. Το Σύστημα Προετοιμασίας Ψηφοδελτίου προβάλει στην οθόνη το

κρυπτοκείμενο και την τυχαιότητα που χρησιμοποιήθηκε για την δημιουργία του, με σκοπό ο ψηφοφόρος να επαληθεύσει ότι το Σύστημα Προετοιμασίας Ψηφοδελτίου κρυπτογράφησε σωστά τις επιλογές του. Στην περίπτωση αυτή το Σύστημα Προετοιμασίας Ψηφοδελτίου προτρέπει τον ψηφοφόρο να δημιουργήσει μια νέα κρυπτογράφηση των επιλογών του.

5. Εναλλακτικά, ο ψηφοφόρος μπορεί να επιλέξει να σφραγίσει το ψηφοδέλτιο. Το Σύστημα Προετοιμασίας Ψηφοδελτίου διαγράφει όλη την τυχαιότητα και κάθε πληροφορία για την ακρυπτογράφητη ψήφο, αφήνοντας μόνο το κρυπτοκείμενο, έτοιμο για ρίψη στην κάλπη.

6. Στη συνέχεια ζητείται από τον ψηφοφόρο να πιστοποιήσει την ταυτότητά του. Εάν ταυτοποιηθεί επιτυχημένα, η κρυπτογραφημένη ψήφος, στην οποία το Σύστημα Προετοιμασίας Ψηφοδελτίου δεσμεύτηκε προηγουμένως αποστέλλεται στην ψηφιακή κάλπη.

7. Μόλις η ψήφος ριχθεί στην κάλπη, ο ψηφοφόρος λαμβάνει ένα μήνυμα ηλεκτρονικού ταχυδρομίου στο οποίο περιέχεται η επιβεβαίωση της κρυπτογραφημένης ψήφου καθώς και το αποτέλεσμα της εφαρμογής της συνάρτησης κατακερματισμού SHA1 στο κρυπτοκείμενο.

Καθώς έχει γίνει η παραδοχή ότι ο κίνδυνος εξαγοράς/πώλησης της ψήφου είναι μικρός, το Helios είναι απλούστερο από το σύστημα που πρότεινε ο Benaloh. Συγκεκριμένα το Σύστημα Προετοιμασίας Ψηφοδελτίου δεν υπογράφει το κρυπτοκείμενο πριν την αποστολή του και προβάλει στον ψηφοφόρο ως δέσμευση τον πραγματικό κατακερματισμό της κρυπτογραφημένης ψήφου του πριν την σφράγιση του ψηφοδελτίου.

΄Οπως και στα άλλα συστήματα που μελετήθηκαν, έτσι και το Helios χρησιμοποιεί έναν δημόσιο πίνακα ανακοινώσεων για την δημοσίευση των κρυπτογραφημένων ψήφων. Αμέσως μετά την ρίψη κάθε μίας ψήφου στην κάλπη, η ψήφος μαζί με το όνομα ή το αναγνωριστικό του εκάστοτε ψηφοφόρου εμφανίζονται στον πίνακα ανακοινώσεων. Στο Helios χρησιμοποιείται η πιο απλή μορφή του πίνακα ανακοινώσεων η οποία τρέχει σε έναν μόνο εξυπηρετητή. Αυτό απαιτεί ότι οι ελεγκτές των εκλογών θα ελέγχουν περιοδικά την ακεραιότητα του πίνακα ανακοινώσεων κατά την διάρκεια των εκλογών καθώς και ότι αρκετοί ψηφοφόροι θα ελέγξουν ότι οι κρυπτογραφημένες ψήφοι τους εμφανίζονται σωστά στον πίνακα ανακοινώσεων.

Μετά το κλείσιμο των κάλπεων ακολουθεί η ανωνυμοποίηση των ψήφων η οποία γίνεται και εδώ μέσω ενός δικτύου μίξης. Συγκεκριμένα, το Helios χρησιμοποιεί το Sako-Kilian πρωτόκολλο, το οποίο είναι το πρώτο αποδείξιμο δίκτυο μίξης το οποίο βασίζεται σε επανακρυπτογράφηση El-Gamal. Παρόμοια τεχνική χρησιμοποιείται και στο σύστημα που πρότεινε ο Benaloh. Το πρωτόκολλο αυτό δεν είναι το καλύτερο σε απόδοση καθώς υπάρχουν ταχύτερα πρωτόκολλα που επιτυγχάνουν τον ίδιο βαθμό εξασφάλισης της ακεραιότητας. Ο λόγος επιλογής αυτού του πρωτοκόλλου είναι η απλότητα του και η ευκολία επεξήγησης του τρόπου λειτουργίας του.

Η συνολική διαδικασία εκλογών είναι η ακόλουθη:

1. Ο ψηφοφόρος προετοιμάζει και επαληθεύει όσα ψηφοδέλτια επιθυμεί, ελέγχοντας έτσι ότι όλα τα ελεγμένα ψηφοδέλτια είναι σωστά συμπληρωμένα. Καθώς ο ψηφοφόρος είναι ανώνυμος στο σημείο αυτό, δεν μπορεί να στοχοποιηθεί από ένα διεφθαρμένο σύστημα Helios έτσι ώστε να λάβει ένα διεφθαρμένο ψηφοδέλτιο (στο οποίο ενώ θα πιστεύει ότι ψηφίζει έναν υποψήφιο, στην πραγματικότητα ψηφίζει κάποιον άλλο). Εάν το Helios επιχειρήσει να προβάλει ένα διεφθαρμένο ψηφοδέλτιο υπάρχει μεγάλη πιθανότητα αυτό να γίνει αντιληπτό από κάποιον ελεγκτή ή από κάποιον ψηφοφόρο. Για την αντιμετώπιση αυτής της επίθεσης, παρέχεται μάλιστα και το πρόγραμμα Επαλήθευσης Κρυπτογράφησης Ψηφοδελτίου, σε μορφή πηγαίου κώδικα, με το οποίο οι ελεγκτές και οι ψηφοφόροι μπορούν να επαληθεύσουν ότι τα ψηφοδέλτια τους κρυπτογραφήθηκαν σωστά. Πρέπει να σημειωθεί βέβαια ότι ένα διεφθαρμένο Helios ίσως ταυτοποιήσει τους χρήστες πριν την συμπλήρωση του ψηφοδελτίου (ορισμένοι ψηφοφόροι μπορεί να μην το αντιληφθούν), ή να χρησιμοποιήσει άλλες πληροφορίες (όπως η IP διεύθυνση) για να αναγνωρίσει τους ψηφοφόρους και να προβάλει διεφθαρμένα ψηφοδέλτια σε συγκεκριμένα θύματα.

2. ΄Οταν ικανοποιηθεί από τον έλεγχο, ο ψηφοφόρος ρίχνει την κρυπτογραφημένη ψήφο στην κάλπη, αφού πρώτα πιστοποιήσει την ταυτότητά με την χρήση κάποιου συνδυασμού ψευδωνύμου-/κωδικού. Ο πίνακας ανακοινώσεων του Helios δημοσιεύει το όνομα του ψηφοφόρου και το κρυπτογραφημένο ψηφοδέλτιο. Οποιοσδήποτε, συμπεριλαμβανομένου και του ψηφοφόρου μπορεί να ελέγξει τον πίνακα ανακοινώσεων και να βρει την κρυπτογραφημένη ψήφο. Η επαλήθευση της καταγραφής της υποβληθείσας ψήφου είναι πολύ σημαντική στο Helios. Αυτό γιατί ένα διεφθαρμένο Helios μπορεί να αλλάξει το κρυπτοκείμενο του ψηφοφόρου με ένα άλλο, αλλάζοντας την ψήφο που έχει ρίξει στην

κάλπη. Ακόμα και αν η κάλπη βρίσκεται σε διαφορετικό εξυπηρετητή στον οποίο το Helios δεν έχει πρόσβαση, το Helios γνωρίζει τα στοιχεία σύνδεσης των ψηφοφόρων στο σύστημα και συνεπώς μπορεί να συνδεθεί ψηφίσει εκ μέρους τους. Αναλύσεις έχουν δείξει ότι αρκεί μόνο ένα μικρό δείγμα των ψηφοφόρων να επαληθεύσει την ψήφο του στον πίνακα ανακοινώσεων για να ανακαλυφθεί με μεγάλη πιθανότητα μια τέτοια προσπάθεια αλλοίωσης του αποτελέσματος. Βέβαια, ο έλεγχος αυτός δεν λύνει όλα τα προβλήματα. Για παράδειγμα ένα διεφθαρμένο Helios μπορεί να συνδεθεί και να ψηφίσει εκ μέρους ενός ψηφοφόρου που δεν παρευρέθηκε στις εκλογές (δεδομένου ότι η πιθανότητα να επαληθεύσει την ψήφο του στον πίνακα ανακοινώσεων ένας απέχων από τις εκλογές ψηφοφόρος είναι μικρή). Για τον λόγο αυτόν απαιτείται εκτενής έλεγχος του συστήματος κατά την διάρκεια διεξαγωγής των εκλογών.

3. Μετά το κλείσιμο των κάλπεων, το Helios ανωνυμοποιεί όλα τα κρυπτογραφημένα ψηφοδέλτια και παράγει μία απόδειξη μηδενικής γνώσης που δεν απαιτεί αλληλεπίδραση για την σωστή μίξη τους, η οποία είναι σωστή με πολύ μεγάλη πιθανότητα.

4. Μετά από μια λογική περίοδο παραπόνων, τέτοια ώστε οι ελεγκτές να έχουν χρόνο να ελέγξουν την μίξη, το Helios αποκρυπτογραφεί όλα τα ανώνυμα ψηφοδέλτια, παρέχει μία απόδειξη σωστής αποκρυπτογράφησης για κάθε ένα και καταμετρά τις ψήφους.

΄Ενας οποιοσδήποτε ελεγκτής μπορεί να κατεβάσει όλα τα δεδομένα μια εκλογικής διαδικασίας και να επαληθεύσει την ορθότητα της μίξης, της αποκρυπτογράφησης και της καταμέτρησης. ΄Ετσι εάν ένα διεφθαρμένο Helios προσπαθήσει να “κλέψει” στην διαδικασία μίξης ή αποκρυπτογράφησης αυτό θα γίνει αντιληπτό με μεγάλη πιθανότητα ακόμα και από έναν μόνο ελεγκτή. Με τον τρόπο αυτόν διασφαλίζεται η ιδιότητα της καταμέτρησης των καταγεγραμμένων της ακραίας επαληθευσιμότητας.

Για την διευκόλυνση των ελεγκτών και των ψηφοφόρων να επαληθεύσουν ότι τα ψηφοδέλτια τους καταμετρήθηκαν σωστά, το Helios παρέχει το πρόγραμμα Επαλήθευσης Καταμέτρησης Εκλογών, το οποίο διατίθεται σε μορφή ανοιχτού κώδικα. Το πρόγραμμα Επαλήθευσης Καταμέτρησης Εκλογών εξάγει ένα αντίγραφό όλων των ψηφοδελτίων που ρίχθηκαν στην κάλπη το οποίο μπορούν να επαναδημοσιεύσουν οι ελεγκτές στους δικούς τους πίνακες ανακοινώσεων. Με το πρόγραμμα αυτό μπορούν επίσης να επαληθεύσουν ότι τα ψηφοδέλτια αποκρυπτογραφήθηκαν σωστά και ότι η καταμέτρηση δεν είχε κάποιο λάθος. Μάλιστα μπορούν να επικοινωνήσουν και με τους ψηφοφόρους και να τους ζητήσουν να επαληθεύσουν τον κατακερματι-

σμό του κρυπτογραφημένου ψηφοδελτίου τους. ΄Ετσι ακόμα και αν οι ψηφοφόροι δεν επαληθεύσουν οι ίδιοι ότι η ψήφος τους εμφανίζεται σωστά στον πίνακα ανακοινώσεων, αναμένεται ότι μια μεγάλη πλειοψηφία τους (ίσως ακόμα και όλοι οι ψηφοφόροι) θα απαντήσουν σε έναν τουλάχιστον ελεγκτή.

Πέρα από το θεωρητικό ενδιαφέρον του, το Helios είναι ένα σημαντικό σύστημα ηλεκτρονικών εκλογών λόγω της εφαρμογής του σε εκλογικές διαδικασίες διάφορων φορέων. Το 2009 χρησιμοποιήθηκε από το το Universite Catholique de Louvain για την διεξαγωγή των προεδρικών εκλογών του[26].

Αν και οι εκλογές αυτές ήταν ύψιστης σημασίας για το πανεπιστήμιο, θεωρήθηκε πως ο κίνδυνος εκβιασμού ή πώλησης της ψήφου των ψηφοφόρων δεν είναι μεγάλος. Επίσης, θεωρήθηκε πως δεν είναι πιθανό κάποιος κακόβουλος χρήστης να μολύνει τους υπολογιστές των ψηφοφόρων με σκοπό να αλλοιώσει τις ψήφους που αυτοί στέλνουν στην ηλεκτρονική κάλπη. ΄Ετσι το Helios κρίθηκε κατάλληλο για την διεξαγωγή των εκλογών.

Παρόλα αυτά το Helios δεν ήταν απόλυτα έτοιμο να διεξάγει αυτές τις εκλογές. Οι βασικοί λόγοι ήταν ότι:

- Δεν ήταν δυνατή η χρήση του δικτύου μίξης που χρησιμοποιούσε το Helios καθώς οι ψήφοι είχαν διαφορετικό βάρος ανάλογα με την κατηγορία στην οποία άνηκε ο ψηφοφόρος.
- Το Helios χρησιμοποιούσε το Google App Engine για να τρέξει, το οποίο ήταν δύσκολο να χρησιμοποιηθεί από ένα Ευρωπαϊκό Πανεπιστήμιο λόγω των Ευρωπαϊκών νόμων περί προσωπικών δεδομένων.
- Η διαδικασία επαλήθευσης που χρησιμοποιούσε το Helios δεν ήταν αποδοτική στην πράξη για την καταμέτρηση δεκάδων χιλιάδων ψήφων και δεν είχε σχεδιαστεί για να επιλύει τυχόν διαμαρτυρίες των ψηφοφόρων.
- Το Helios χρησιμοποιούσε ένα μόνο κλειδί για την αποκρυπτογράφηση των ψήφων. Αυτό σημαίνει ότι το Helios θα μπορούσε να αποκρυπτογραφήσει τις ψήφους εάν ήθελε, δηλαδή η εμπιστοσύνη δεν διαμοιραζόταν ανάμεσα σε διαφορετικές αρχές/οντότητες.

Η επίλυση όλων των παραπάνω προβλημάτων ήρθε με την ανάπτυξη της δεύτερης έκδοσης του Helios, η οποία και χρησιμοποιήθηκε στις εκλογές. Τα νέα βασικά χαρακτηριστικά της δεύτερης αυτής έκδοσης ήταν ότι χρησιμοποιούσε ομομορφική καταμέτρηση αντί για δίκτυο μίξης, ένα διαμοιρασμένο σχήμα αποκρυπτογράφησης και ότι ήταν

συμβατό με το σύστημα ταυτοποίησης των χρηστών του πανεπιστημίου. Αυτό ήταν μια σημαντική προσθήκη στο πρόγραμμα καθώς αντί το Helios να δημιουργεί στοιχεία σύνδεσης για κάθε έναν ψηφοφόρο και να τα στέλνει μέσω ηλεκτρονικού ταχυδρομείου, οι ψηφοφόροι μπορούσαν να συνδεθούν για να ψηφίσουν μέσω του συστήματος ταυτοποίησης που είχε ήδη το πανεπιστήμιο.

Καθώς για τις εκλογές χρησιμοποιήθηκε ομομορφική κρυπτογράφηση έπρεπε να δημιουργηθούν τα διαμοιρασμένα κλειδιά με τρόπο τέτοιο ώστε οι διάφοροι έφοροι να είναι σίγουροι ότι δεν έχει κρατηθεί κάποιο αντίγραφο των κλειδιών τους από το σύστημα, ότι τα κλειδιά που δημιουργήθηκαν είναι όντως τυχαία και ότι η πληροφορία για τα κλειδιά δεν διαρρέει με κανέναν τρόπο από το σύστημα (για παράδειγμα μέσω των αποδείξεων). Για τον σκοπό αυτό διοργανώθηκε μια συνάντηση στην οποία συμμετείχαν όλοι οι έφοροι οι οποίοι θα λάμβαναν τα κλειδιά καθώς και εξωτερικοί επιστήμονες οι οποίοι θα επιτηρούσαν την ορθότητα της διαδικασίας. Για την δημιουργία των κλειδιών χρησιμοποιήθηκαν φορητοί υπολογιστές από τους οποίους αφαιρέθηκαν οι σκληροί δίσκοι και το λειτουργικό σύστημα έτρεχε μέσω οπτικού δίσκου. Οι αρχές χρησιμοποίησαν USB μέσα αποθήκευσης για να αποθηκεύσουν τα κλειδιά. Μετά την διαδικασία οι οπτικοί δίσκοι με το λειτουργικό καταστράφηκαν.

Μετά την δημιουργία των κλειδιών ακολούθησε η δημοσιοποίηση των στοιχείων των εκλογών: το δημόσιο κλειδί το οποίο θα χρησιμοποιούνταν για την κρυπτογράφηση των ψήφων, το αναγνωριστικό των εκλογών, οι ερωτήσεις των εκλογών και ο ελάχιστος και ο μέγιστος αριθμός σταυρών. Οι πληροφορίες αυτές έγιναν διαθέσιμες μέσω ενός υπογεγραμμένου PDF.

Πριν την ψηφοφορία, υπήρξε μία περίοδος εγγραφής των ψηφοφόρων στο σύστημα. Τα μέλη του πανεπιστημίου έλαβαν ένα μήνυμα ηλεκτρονικού ταχυδρομείου το οποίο τους παρέπεμπε να συνδεθούν στο σύστημα του πανεπιστημίου και να εγγραφούν στις εκλογές. Με την εγγραφή τους δημιουργούταν ένα ανώνυμο αναγνωριστικό για κάθε ψηφοφόρο και ένας τυχαίος κωδικός. Οι ψηφοφόροι μπορούσαν να κατεβάσουν τα στοιχεία αυτά σε μορφή PDF. Κατά την διαδικασία αυτή εγγράφηκαν περίπου 5000 από τους 25000 χρήστες με δικαίωμα ψήφου.

Κατά την διοργάνωση των εκλογών προέκυψε ένας νέος κίνδυνος ο οποίος αυτή την φορά δεν είχε να κάνει με τις ιδιότητες ασφαλείας του συστήματος. Πρόκειται για την πιθανή διάκριση εις βάρος των ατόμων τα οποία δεν είναι εξοικειωμένα με την χρήση ηλεκτρονικών υπολογιστών. Για την αποφυγή τέτοιων περιστατικών λήφθηκαν τα

ακόλουθα μέτρα:

- Η εκλογική διαδικασία ανακοινώθηκε επανειλημμένα στο πανεπιστήμιο και δημοσιεύτηκε και σε μη ηλεκτρονικά μέσα.
- ΄Εγιναν διάφορες δημόσιες παρουσιάσεις του συστήματος.
- Ταυτόχρονα με την διαδικασία των εγγραφών των ψηφοφόρων διοργανώθηκαν δοκιμαστικές εκλογές. ΄Ετσι οι ψηφοφόροι μπορούσαν να χρησιμοποιήσουν την πλατφόρμα δοκιμαστικά και να εξοικειωθούν μαζί της.
- Δημιουργήθηκαν ειδικά γραφεία τα οποία βοηθούσαν τους ψηφοφόρους να εγγραφούν στο σύστημα και να ψηφίσουν.
- Τυπώθηκε οδηγός χρήσης της εφαρμογής και δημοσιεύτηκαν βίντεο τα οποία καθοδηγούσαν τους χρήστες για το πως να εγγραφούν και να ψηφίσουν.
- Επιτράπηκε η επαναψήφιση. ΄Ετσι εάν κάποιος ψηφοφόρος έκανε κάποιο λάθος μπορούσε να διορθώσει την ψήφο του. Επίσης εάν κάποιος είχε πρόβλημα να ψηφίσει μπορούσε να ζητήσει βοήθεια και με την καθοδήγηση ενός ειδικού να ρίξει μια τυχαία ψήφο. Στη συνέχεια έχοντας μάθει την διαδικασία μπορούσε να ψηφίσει ξανά μόνος του. Μόνο η τελευταία ψήφος κάθε ψηφοφόρου προσμετρώταν στο αποτέλεσμα και εμφανιζόταν στον πίνακα ανακοινώσεων.

Οι εκλογές του πανεπιστημίου αποτελούνταν από δύο γύρους. Η ψηφοφορία για κάθε γύρο διήρκεσε δύο ημέρες. Και τις δύο ημέρες οι κάλπες άνοιγαν στις 7 το πρωί και έκλειναν στις 8 το βράδυ. Το ψηφοδέλτιο είχε 3 υποψήφιους και οι ψηφοφόροι καλούνταν να επιλέξουν δύο ή να ψηφίσουν λευκό.

Από τους 5000 εγγεγραμμένους ψηφοφόρους ψήφισαν περίπου 4000 σε κάθε γύρο. Περίπου 1% των ψηφοφόρων ψήφισε πάνω από μια φορά.

Για την εξυπηρέτηση των ψηφοφόρων εγκαταστάθηκαν θάλαμοι ψηφοφορίας (όπως και στις παραδοσιακές εκλογές) σε διάφορα σημεία του πανεπιστημίου στους οποίους οι ψηφοφόροι θα μπορούσαν να ψηφίσουν. Λιγότεροι από το 3% των ψηφοφόρων χρησιμοποίησε τους θαλάμους ψηφοφορίας για να ψηφίσει. Μάλιστα, εκτιμήθηκε πως οι περισσότεροι ψηφοφόροι που ψήφισαν σε θάλαμο ψηφοφορίας δεν είχαν επαρκείς γνώσεις χρήσης ηλεκτρονικών υπολογιστών.

Μετά το κλείσιμο των κάλπεων οι ψηφοφόροι είχαν μία ημέρα για να ελέγξουν τις ψήφους τους στον πίνακα ανακοινώσεων και να υποβάλουν τυχόν ενστάσεις.

Ο πίνακας ανακοινώσεων φιλοξενήθηκε σε ιστοσελίδα στο διαδίκτυο. Για την εξασφάλιση της ακεραιότητας των δεδομένων χρησιμοποιήθηκαν ψηφιακές υπογραφές. Μια υπογεγραμμένη απόδειξη δημοσιεύτηκε για κάθε ψήφο, μαζί με μια υπογεγραμμένη έκδοση όλου του περιεχομένου του πίνακα ανακοινώσεων. Οι ατομικές υπογραφές έγιναν διαθέσιμες για να διευκολύνουν τους ψηφοφόρους ενώ ο πλήρης πίνακας ανακοινώσεων δόθηκε σε ένα αρχείο για να γίνει σίγουρο ότι οι διοργανωτές των εκλογών δεν μπορούσαν να αλλάξουν τις ψήφους των οποίων οι αποδείξεις δεν ελέγχθηκαν εκείνη την ημέρα (κάποιος με πρόσβαση στον εξυπηρετητή του Helios μπορούσε να γνωρίζει την πληροφορία με το να διαβάσει τα αρχεία καταγραφής του συστήματος).

Στην περίπτωση που ένας χρήστης έκανε ένσταση ότι η ψήφος του αλλάχτηκε ή χάθηκε και η ένσταση αυτή κρινόταν σωστή και βάσιμη τότε δύο πράγματα μπορούσαν να έχουν συμβεί:

1. Ο εξυπηρετητής των εκλογών είχε παραβιαστεί (ή οι διοργανωτές των εκλογών έκλεψαν) και η υπογεγραμμένη ψήφος ήταν όντως λάθος

2. Ο ψηφοφόρος δεν κράτησε τα στοιχεία σύνδεσής του κρυφά με αποτέλεσμα κάποιος τρίτος να τα κλέψει και να ψηφίσει εκ μέρους του.

Μια ιδιαιτερότητα της διαδικασία επαλήθευσης ήταν ότι οι ψηφοφόροι που υπέβαλλαν κάποια ένσταση είχαν την δυνατότητα να ψηφίσουν ξανά, χρησιμοποιώντας το ίδιο περιβάλλον ψηφοφορίας με αυτό κατά την διάρκεια των εκλογών. Η βασική διαφοροποίηση ήταν ότι οι ψήφοι αυτές δεν αναρτώνταν στον πίνακα ανακοινώσεων, αντίθετα, αποθηκευόντουσαν σε ένα ειδικό και ελεγχόμενο μέρος της κάλπης. Παράλληλα οι ψηφοφόροι που ξαναψήφιζαν την περίοδο της επαλήθευσης λάμβαναν μια ψηφιακά υπογεγραμμένη απόδειξη από το σύστημα, η οποία περιείχε τον κατακερματισμό της ψήφου.

Για να θεωρηθεί έγκυρη η ένσταση και να γίνει αποδεκτή η νέα ψήφος, ο ψηφοφόρος έπρεπε στη συνέχεια να τυπώσει την απόδειξη, να την υπογράψει με το χέρι και να την παραδώσει ο ίδιος ή να την στείλει με φαξ στην επιτροπή των εκλογών. Οι λόγοι που επιλέχθηκε αυτή η διαδικασία ήταν οι ακόλουθοι:

- Με το να υπογράφει το σύστημα ψηφιακά την απόδειξη που δίνει στον ψηφοφόρο, η επιτροπή των εκλογών μπορούσε να είναι σίγουρη ότι η απόδειξη που στέλνει ο χρήστης δημιουργήθηκε όντως από το σύστημα κατά την διάρκεια της επαλήθευσης και αφορά τη συγκεκριμένη ψήφο.

- Η χειρόγραφη υπογραφή του ψηφοφόρου ήταν ένα μέσο πιστοποίησης της ταυτότητας του ψηφοφόρου και της γνησιότητας της ένστασης.
- Η χρήση του φαξ ως μέσο αποστολής (ή της προσωπικής παράδοσης της ψήφου στην εφορευτική επιτροπή) δέσμευε την εφορευτική επιτροπή στο να μην μπορεί να αρνηθεί την ύπαρξη της ένστασης και της νέας ψήφου.

Περίπου το 30% των ψηφοφόρων έλεγξε τις ψήφους του στον πίνακα ανακοινώσεων και 7 ψηφοφόροι υπέβαλαν ενστάσεις συνολικά και στους δύο γύρους. Καμία από τις ενστάσεις δεν έδειξε κάποια δυσλειτουργία του συστήματος, καθώς οι ενστάσεις έγιναν από χρήστες οι οποίοι προσπάθησαν να ψηφίσουν μετά την λήξη των εκλογών και συνεπώς οι ψήφοι τους δεν εμφανίστηκαν στον πίνακα ανακοινώσεων, από ψηφοφόρους οι οποίοι απλά ήθελαν να ελέγξουν το σύστημα από περιέργεια και από ψηφοφόρους οι οποίοι ακούσια είχαν ανταλλάξει τις αποδείξεις τους.

Μετά την επίλυση των ενστάσεων δημοσιεύτηκε ξανά ο πίνακας ανακοινώσεων με την τελική μορφή της κάλπης.

Πέρα από τις εκλογές του Universite Catholique de Louvain, το Helios χρησιμοποιήθηκε από άλλους οργανισμούς όπως από το Princeton για τις μαθητικές εκλογές του[27], από το Association for Computing Machinery (ACM) για τις εσωτερικές εκλογές του[28] και από το International Association for Cryptologic Research (IACR)[29].

Σχετικά με τον τελευταίο οργανισμό, πριν την διεξαγωγή των πραγματικών εκλογών πραγματοποιήθηκε μια εικονική ηλεκτρονική διαδικασία στις αρχές του 2010. Σε αυτήν συμμετείχαν 379 μέλη του οργανισμού. Τα αποτελέσματα και τα σχόλια που προέκυψαν από τις εκλογές αυτές ήταν ιδιαίτερα ενδιαφέροντα καθώς δείχνουν ότι πέρα από τις ανάγκες που καλύπτει θεωρητικά ένα πρωτόκολλο εκλογών υπάρχουν και πρακτικά προβλήματα που πρέπει να επιλυθούν.

Το σημαντικότερο πρόβλημα που προέκυψε ήταν ότι για να ψηφίσει ένας ψηφοφόρος με το Helios έπρεπε να έχει εγκατεστημένη την Java[30] στον υπολογιστή του. Αρκετά μέλη του οργανισμού δεν επιθυμούσαν να εγκαταστήσουν την Java στον υπολογιστή τους ή να χρησιμοποιήσουν κάποιον άλλο υπολογιστή που είχε εγκατεστημένη την Java. Για να λυθεί το πρόβλημα αυτό, μια πρόσθετη λειτουργία προστέθηκε στο Helios η οποία ήταν η δυνατότητα κρυπτογράφησης του ψηφοδελτίου στον εξυπηρετητή του Helios. Προφανώς, η λύση αυτή είχε το μεγάλο μειονέκτημα ότι έδινε στο Helios πλήρη πρόσβαση στο περιεχόμενο της ψήφου και συνεπώς ένα διεφθαρμένο Helios θα μπορούσε να παραβιάσει την μυστικότητα των ψήφων. Παρόλα αυτά

ο οργανισμός θεώρησε πως η πρακτική διευκόλυνση που προσέφερε λύση αυτή αντιστάθμιζε τους κινδύνους που προκύπτουν και προτιμήθηκε.

Μια άλλη λειτουργία που ζητήθηκε από το Helios ήταν να υποστηρίζεται ένα διαμοιρασμένο σχήμα αποκρυπτογράφησης στο οποίο όμως να μην απαιτούνται όλα τα κλειδιά για την αποκρυπτογράφηση των ψήφων. Αυτό γιατί εάν κάποιο μέλος της εφορευτικής επιτροπής έχανε το κλειδί του, η κάλπη δεν θα μπορούσε να αποκρυπτογραφηθεί. Ως προσωρινή λύση προτάθηκε η διατήρηση αντιγράφων ασφαλείας όλων των κλειδιών της εφορευτικής επιτροπής.

Τέλος, μια ακόμα λειτουργία που ζητήθηκε από το Helios ήταν η δυνατότητα ύπαρξης πολλαπλών διαχειριστών στην εφαρμογή καθώς στην δεύτερη έκδοση του Helios, υπήρχε μόνο ένας διαχειριστής ο οποίος θα μπορούσε να επεξεργαστεί τις εκλογές.

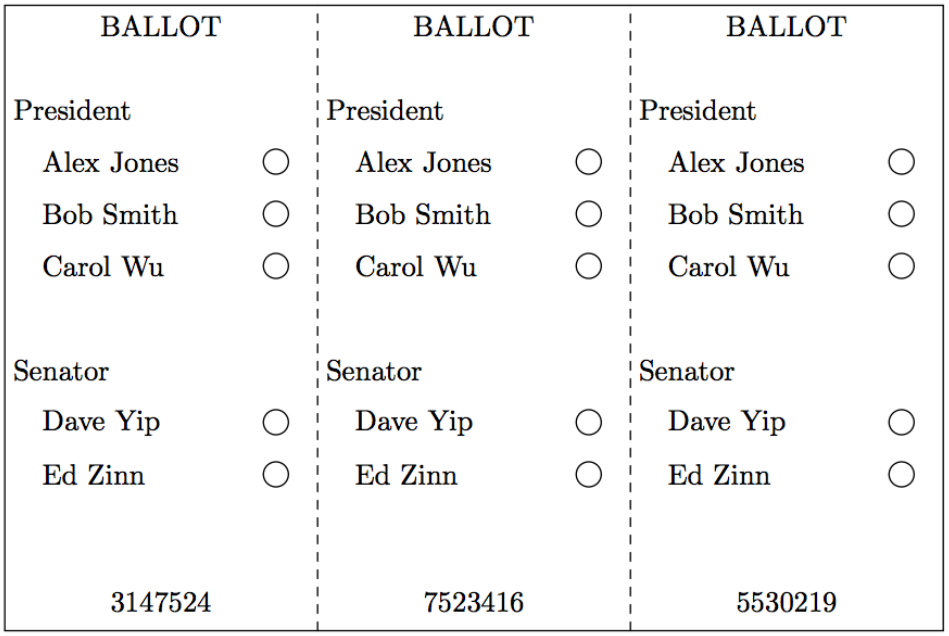
Το αποτέλεσμα μετά από αυτή την διαδικασία ήταν η κατασκευή της τρίτης έκδοσης του Helios η οποία έλυνε τα παραπάνω προβλήματα.

3.4 Ακραίως επαληθεύσιμα συστήματα εκλογών τα οποία δεν χρησιμοποιούν κρυπτογραφικές μεθόδους

Τα συστήματα αυτά αποτελούν ένα ενδιαφέρον πείραμα στην έρευνα για τα ακραίως επαληθεύσιμα συστήματα εκλογών. Τέτοια συστήματα όπως το ThreeBallot, το VAV, το Twin[31] και το Aperio [32] μιμούνται τις ιδιότητες της ακραίας επαληθευσιμότητας χρησιμοποιώντας φυσικό χώρο εκλογών και χάρτινο ψηφοδέλτιο, χωρίς όμως να βασίζονται στην κρυπτογράφηση των δεδομένων. Παρόλο που δεν υπάρχουν πολλά τέτοια συστήματα που να λειτουργούν στην πράξη, η μελέτη αυτών των συστημάτων έδωσε χρήσιμες ιδέες για τα ακραίως επαληθεύσιμα συστήματα. Επίσης, χάρη στην απουσία των σύνθετων κρυπτογραφικών πρωτοκόλλων και πράξεων, τα συστήματα αυτά βοηθούν στην επεξήγηση των βασικών αρχών της από άκρη σε άκρη επαληθευσιμότητας σε ανθρώπους χωρίς καμία τεχνική γνώση.

3.4.1 ThreeBallot, VAV, Twin

Το ThreeBallot προτάθηκε από τους Rivest και Smith το 2007 και πήρε το όνομά του από τον ιδιαίτερο σχεδιασμό του ψηφοδελτίου του, το οποίο αποτελείται από τρία αποσπώμενα ψηφοδέλτια, όπως παρουσιάζονται στο Σχήμα 3.4.



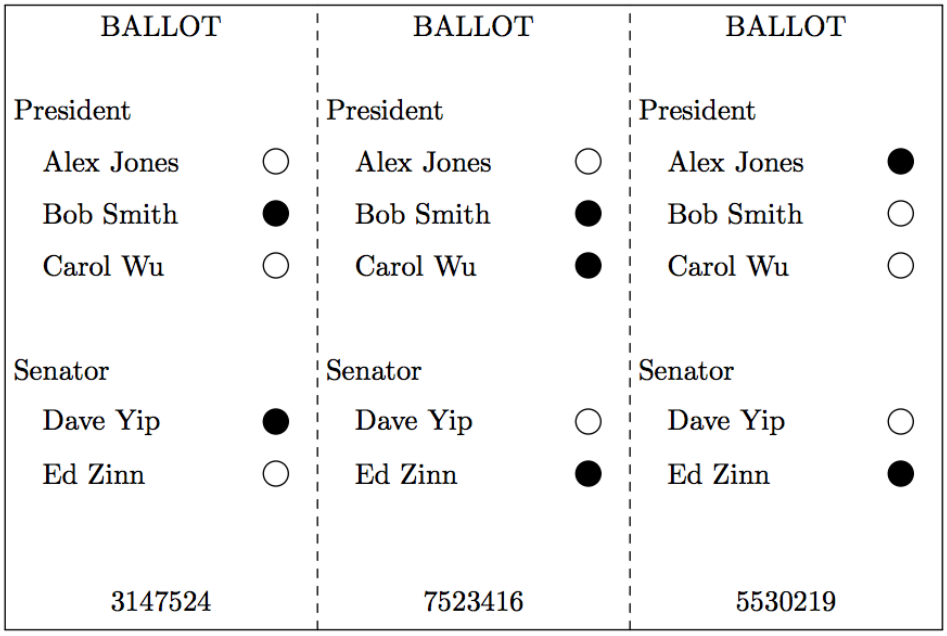
Σχήμα 3.4: Το ψηφοδελτίο του ThreeBallot

Κάθε ψηφοδέλτιο έχει έναν μοναδικό σειριακό αριθμό τυπωμένο στο κάτω μέρος του. Στον θάλαμο ψηφοφορίας ο ψηφοφόρος σημειώνει τα ψηφοδέλτια με τρόπο τέτοιο ώστε κάθε υποψήφιος τον οποίο θέλει να ψηφίσει σημειώνεται δύο φορές ενώ όλοι οι άλλοι σημειώνονται μία φορά. Το Σχήμα 3.5 μία ψήφο στον υποψήφιο Bob Smith για πρόεδρο και τον Ed Zinn για γερουσιαστή.

Μετά την συμπλήρωση και των τριών ψηφοδελτίων, τα ψηφοδέλτια αποσπώνται. Ο ψηφοφόρος διαλέγει τυχαία ένα από τα τρία ψηφοδέλτια, το φωτοτυπεί και παίρνει ένα αντίγραφό του σαν απόδειξη. Στη συνέχεια ρίχνει και τα τρία ψηφοδέλτια στην κάλπη.

Μετά το κλείσιμο των κάλπεων, όλα τα ψηφοδέλτια δημοσιοποιούνται σε έναν πίνακα ανακοινώσεων. Ο ψηφοφόρος χρησιμοποιεί την απόδειξη για να επαληθεύσει ότι το ψηφοδέλτιό του καταγράφηκε σωστά. Το αποτέλεσμα προκύπτει από την πρόσθεση των όλων ψήφων που βρίσκονται στον πίνακα ανακοινώσεων. Αφού κάθε υποψήφιος μπορεί να λάβει μία μόνο ψήφο από κάθε ψηφοφόρο, το αποτέλεσμα είναι αυξημένο κατά τον αριθμό των ψηφοφόρων, ο οποίος αφαιρείται από το τελικό αποτέλεσμα. Οποιοσδήποτε παρατηρητής μπορεί να επαναλάβει την καταμέτρηση και να επαληθεύσει το αποτέλεσμα.

Στο σημείο αυτό πρέπει να γίνει κατανοητό ότι η απόδειξη που λαμβάνει ο ψηφοφόρος δεν είναι μια κρυπτογράφηση της ψήφου του.

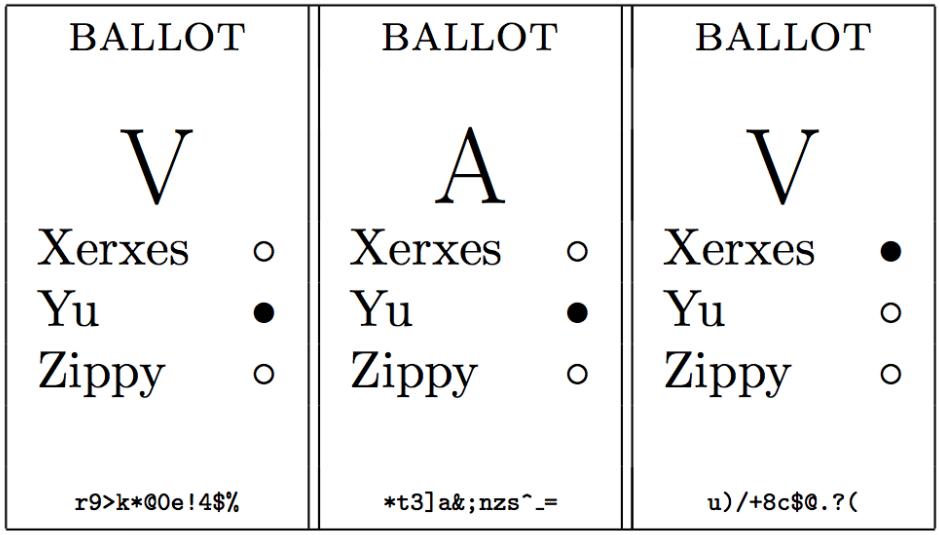


Σχήμα 3.5: Παράδειγμα συμπλήρωσης του ψηφοδελτίου του Threeballot

Αντίθετα, η απόδειξη μαρτυρά ένα το ένα από τα τρία μέρη της ψήφου, το οποίο έχει αποσυνδεθεί, όμως, από τα υπόλοιπα μέρη του ψηφοδελτίου. Η μυστικότητα της ψήφου του ψηφοφόρου διατηρείται καθώς η απόδειξη δεν αποκαλύπτει τίποτα για την πραγματική ψήφου του, εκτός και αν εξεταστεί σε συνδυασμό με τα άλλα δύο ψηφοδέλτια τα οποία έριξε στην κάλπη. Αυτά, όμως, μπορεί να είναι οποιαδήποτε στον πίνακα ανακοινώσεων. Επίσης εάν κάποιος αλλάξει το ψηφοδέλτιο του ψηφοφόρου, ο ψηφοφόρος έχει μία στις τρεις πιθανότητα να το εντοπίσει στον πίνακα ανακοινώσεων. Μάλιστα, εάν κάποιος αλλάξει πολλά ψηφοδέλτια, τότε αυτή η πιθανότητα γίνεται ακόμα μεγαλύτερη.

Παρά την απλότητά του, το ψηφοδέλτιο του ThreeBallot δεν είναι εύχρηστο. Σε μια δοκιμαστική ψηφοφορία, ένας μεγάλος αριθμός ψηφοφόρων είχε δυσκολία να χρησιμοποιήσει το ThreeBallot και περισσότεροι από το 30% των αρχικών ψήφων που ρίχθηκαν στην κάλπη αποδείχθηκαν άκυρες[33]. Επίσης, το ThreeBallot έχει και προβλήματα ασφαλείας. Υπάρχει ο κίνδυνος εξαναγκασμού του ψηφοφόρου να σημειώσει τα ψηφοδέλτια με τέτοιο τρόπο έτσι ώστε να μπορούν να εντοπιστούν στον πίνακα ανακοινώσεων.

Οι Rivest και Smith επίσης πρότειναν και δύο παραλλαγές του ThreeBallot, το VAV (Vote/AntiVote/Vote) και το Twin. Το ψηφοδέλτιο του VAV αποτελείται από δύο ψηφοδέλτια θετικής ψήφου και ένα ψηφο-



Σχήμα 3.6: Το ψηφοδελτίο του VAV

δέλτιο αρνητικής ψήφου, όπως φαίνεται στο Σχήμα 3.6

Η διαδικασία συμπλήρωσης του ψηφοδελτίου διαφέρει από αυτή του ThreeBallot καθώς μόνο ένας υποψήφιος σημειώνεται σε κάθε ψηφοδέλτιο. Το ψηφοδέλτιο αρνητικής ψήφου ακυρώνει ένα ψηφοδέλτιο θετικής ψήφου. Αυτό σημαίνει ότι το ψηφοδέλτιο αρνητικής ψήφου πρέπει να είναι ίδιο με ένα από τα δύο ψηφοδέλτια θετικής ψήφου. Το εναπομείναν θετικό ψηφοδέλτιο αποτελεί και την πραγματική ψήφο του ψηφοφόρου.

Πριν ρίξει τα ψηφοδέλτια στην κάλπη, ο ψηφοφόρος φωτοτυπεί ένα από τα τρία και το κρατάει το αντίγραφο ως απόδειξη. Η διαδικασία καταμέτρησης και επαλήθευσης στο VAV είναι παρόμοιες με αυτές του ThreeBallot.

Το Twin έρχεται να διαφοροποιηθεί λίγο από τα προηγούμενα συστήματα καθώς βασίζεται στην λογική των παραδοσιακών συστημάτων εκλογών όπου ο ψηφοφόρος ρίχνει μόνο ένα ψηφοδέλτιο στην κάλπη. Η καινοτομία στο Twin είναι ότι ο ψηφοφόρος δεν παίρνει πίσω την απόδειξη για την δικιά του ψήφο, αλλά μια απόδειξη της ψήφου ενός άλλου ψηφοφόρου.

Στο εκλογικό κέντρο, υπάρχει ένα μεγάλο καλάθι το οποίο γεμίζεται περιοδικά με έγκυρες αποδείξεις ψηφοφόρων. Ο κάθε ψηφοφόρος αφού ρίξει την ψήφο του στην κάλπη, παίρνει μια απόδειξη από το καλάθι στην τύχη, την φωτοτυπεί και κρατά το αντίγραφο της. Οι αποδείξεις αυτές ονομάζονται κυμαινόμενες αποδείξεις. Στη συνέχεια

μπορεί να επαληθεύσει ότι η ψήφος της οποίας την απόδειξη φωτοτύπησε υπάρχει στον πίνακα ανακοινώσεων. Το σύστημα αυτό είναι πολύ απλό και εύκολο στην χρήση.

Οι κυμαινόμενες αποτελούν ένα αρκετά καινοτόμο τρόπο επαλήθευσης καθώς εξασφαλίζουν:

- Ανωνυμία: Κανείς δεν μπορεί να γνωρίζει ποιος ψηφοφόρος έριξε το ψηφοδέλτιο το οποίο αντιστοιχεί σε ένα αντίγραφο απόδειξης
- Ανταλλαγή απόδειξης: Η ανταλλαγή αποδείξεων μεταξύ ψηφοφόρων είναι ανούσια καθώς κανένας ψηφοφόρος δεν παίρνει μαζί του την απόδειξη για την δικιά του ψήφο.
- Κάλυψη: ΄Ενα μέρος των πρωτότυπων αποδείξεων αντιγράφονται με μεγάλη πιθανότητα (και δεν είναι εφικτό κάποιος να γνωρίζει ποιο υποσύνολο των αποδείξεων έχει αντιγραφεί).
- Αντίσταση σύγκρουσης: ΄Ενας αντίπαλος δεν έχει αποτελεσματική μέθοδο για να αποκτήσει όλες τα αντίγραφα μίας απόδειξης (στην περίπτωση που κάποιος αγοράζει τις αποδείξεις των ψηφοφόρων).

΄Ενα πρόβλημα που παρουσιάζεται στο Twin είναι ότι αφού οι ψηφοφόροι δεν μπορούν να επαληθεύσουν τα ψηφοδέλτιά τους, μια μικρή παράταξη μπορεί να πιστεύει ότι μόνο ένα μικρό μέρος των ψηφοδελτίων της ελέγχθηκαν από έμπιστα μέλη της παράταξης (καθώς αποτελούν μικρό μέρος του εκλογικού συνόλου). Συνήθως, όμως, μια μεγάλη παράταξη έχει κίνητρο να αποτρέψει την απάτη απέναντι σε μια μικρή παράταξη στις περιπτώσεις που αυτό αλλάζει το αποτέλεσμα των εκλογών.

Κεφάλαιο 4

Μελέτη του συστήματος Ζευς

4.1 Η ανάγκη για το Ζευς

Το καλοκαίρι του 2012, ζητήθηκε από το Εθνικό Δίκτυο ΄Ερευνας & Τεχνολογίας (ΕΔΕΤ) η πρόταση ενός συστήματος ηλεκτρονικής ψηφοφορίας με σκοπό την εκλογή των Συμβουλίων Διοίκησης για τα Ιδρύματα Ανώτατης Εκπαίδευσης στην Ελλάδα. Οι εκλογές των Συμβουλίων Διοίκησης των Πανεπιστημίων γίνονται με την χρήση Ενιαίου Ψηφοδελτίου, στο οποίο οι ψηφοφόροι δεν δηλώνουν μόνο ποιους υποψηφίους επιθυμούν να ψηφίσουν, αλλά τους ιεραρχούν με σειρά προτίμησης.

Η μελέτη για την υλοποίηση ενός τέτοιου συστήματος ηλεκτρονικών εκλογών ξεκίνησε αμέσως μετά την ψηφοφορία σχετικού διατάγματος το οποίο θεσμοθέτησε και επέτρεψε τις ηλεκτρονικές εκλογές για την εκλογή των Συμβουλίων Διοίκησης στα Ιδρύματα Ανώτατης Εκπαίδευσης.

Λόγω του περιορισμένου χρόνου μέχρι την διεξαγωγή της πρώτης ηλεκτρονικής ψηφοφορίας - η οποία θα γινόταν τρεις μήνες μετά - και της ιδιαίτερα ευαίσθητης φύσης μιας εκλογικής διαδικασίας, εξετάστηκε η δυνατότητα χρήσης κάποιου υπάρχοντος συστήματος ηλεκτρονικών εκλογών ανοιχτού κώδικα. ΄Ενα τέτοιο ώριμο σύστημα εκλογών, διαθέσιμο σε ανοιχτό κώδικα, ήταν το Helios το οποίο είχε καλή επίδοση και είχε χρησιμοποιηθεί επιτυχώς σε διάφορες πραγματικές εκλογές.

΄Οπως περιγράφηκε στην προηγούμενη ενότητα, η τρέχουσα έκδοση του Helios (τρίτη έκδοση) υποστηρίζει διαδικτυακές εκλογές με από άκρη σε άκρη επαληθευσιμότητα, από την στιγμή που ο ψηφοφόρος ρίχνει το ψηφοδέλτιο στην κάλπη μέσω του πλοηγού του στο διαδίκτυο έως και την δημοσιοποίηση των αποτελεσμάτων. Αυτό το

πετυχαίνει με το να μην αποκρυπτογραφεί ποτέ τα ψηφοδέλτια αλλά με το να εφαρμόζει μια σειρά ομομορφικών υπολογισμών σε αυτά. Στο τέλος, τα αποτελέσματα των υπολογισμών αυτών αποκρυπτογραφούνται και δημοσιοποιούνται.

Παρόλο που η χρήση του Helios για όλη την διαδικασία των εκλογών των Ελληνικών Πανεπιστημίων ήταν ιδιαίτερα δελεαστική, η ομομορφική καταμέτρηση του Helios δεν μπορούσε να εφαρμοστεί στο εκλογικό σύστημα για την εκλογή των Συμβουλίων Διοίκησης, στο οποίο δεν παίζουν ρόλο μόνο οι ψήφοι στους διάφορος υποψηφίους αλλά και η σειρά προτίμησης με την οποία έχουν ψηφιστεί. Κάθε γύρος καταμέτρησης του συστήματος Ενιαίου Ψηφοδελτίου των εκλογών των Συμβουλίων Διοίκησης χρειάζεται ολόκληρα τα ψηφοδέλτια για τον υπολογισμό του αποτελέσματος. Έτσι, ακόμα και αν η ομομορφική καταμέτρηση του Helios περνούσε στον αλγόριθμο καταμέτρησης του Ενιαίου Ψηφοδελτίου την πληροφορία ότι ένας υποψήφιος επιλέχθηκε σε σειρά προτίμησης ρ από ν ψηφοφόρους, αυτό δεν θα ήταν αρκετό αφού ο αλγόριθμος θα χρειαζόταν ολόκληρα τα ψηφοδέλτια για να υπολογίσει το αποτέλεσμα.

Αυτό δεν σημαίνει ότι η ομομορφική καταμέτρηση δεν μπορεί να χρησιμοποιηθεί σε τέτοιου τύπου εκλογές Ενιαίου Ψηφοδελτίου. Πράγματι είναι εφικτό να γίνει ομομορφική καταμέτρηση των ψήφων χρησιμοποιώντας την μέθοδο Shuffle-Sum[34], όμως το Helios δεν προσφέρει αυτή την δυνατότητα μέχρι στιγμής.

Μη διαθέτωντας χρόνο να για την κατασκευή ενός νέου συστήματος ηλεκτρονικών εκλογών, και δίχως πρόθεση διεξαγωγής κρυπτογραφικής έρευνας έγινε προσπάθεια ανάπτυξης ενός συστήματος το οποίο να βασίζεται όσο το δυνατόν περισσότερο στο Helios, με όλες τις απαραίτητες τροποποιήσεις ώστε αυτό να ταιριάζει στις ανάγκες των εκλογών των Ελληνικών Πανεπιστημίων.

Έτσι αποφασίστηκε να χρησιμοποιηθεί το Helios για την καταμέτρηση των ψηφοδελτίων αλλά όχι για τον υπολογισμό του τελικού αποτελέσματος των εκλογών. Μετά την συλλογή και την επαλήθευση της ακεραιότητας των ψηφοδελτίων, τα ψηφοδέλτια μπορούν να ανωνυμοποιηθούν, να αποκρυπτογραφηθούν και να δοθούν ως είσοδο σε έναν οποιοδήποτε αλγόριθμο καταμέτρησης, όπως αυτού του Ενιαίου Ψηφοδελτίου. Μάλιστα, αφού τα ψηφοδέλτια και ο αλγόριθμος καταμέτρησης δημοσιοποιούνται, οποιαδήποτε τρίτη αρχή μπορεί να επαληθεύσει το αποτέλεσμα των εκλογών.

Όπως αναφέρθηκε στην προηγούμενη ενότητα, ενώ η από την δεύτερη έκδοση του Helios και μετά η καταμέτρηση γίνεται με ομομορφική κρυπτογράφηση, η πρώτη έκδοση του συστήματος χρησιμοποιούσε το Sako-Kilian δίκτυο μίξης για την ανωνυμοποίηση των ψηφοδελτίων. Παρόλο που το Helios δεν χρησιμοποιεί πια δίκτυα μίξης, υπάρ-

χει μια παραλλαγή του Helios η οποία χρησιμοποιεί δίκτυα μίξης[35]. Δυστυχώς, όμως, ο πηγαίος κώδικάς αυτής της υλοποίησης της δεν ήταν ανοιχτός και έτσι η έκδοση αυτή δεν μπόρεσε να χρησιμοποιηθεί.

Για τον λόγο αυτό αναπτύχθηκε από την αρχή το δίκτυο μίξης. Καθώς ο χρόνος ήταν περιορισμένος και καθώς υπήρχε αρκετή υπολογιστική ισχύς διαθέσιμη χρησιμοποιήθηκε το Sako-Kilian πρωτόκολλο μίξης, το οποίο όπως αναφέρθηκε και στο προηγούμενο κεφάλαιο δεν είναι το πιο αποδοτικό.

΄Ετσι αναπτύχθηκε το σύστημα ηλεκτρονικών εκλογών Ζευς, το οποίο έχει χρησιμοποιηθεί με αδιαμφισβήτητη επιτυχία σε πολλές εκλογές εδώ και αρκετούς μήνες. Η επιτυχία του Ζευς ήταν πολύ σημαντική δεδομένης της κριτικής που είχε δεχθεί.

Αν και το Ζευς μοιράζεται πολλά κοινά χαρακτηριστικά με το Helios, διατηρεί μόνο το 50% του αρχικού πηγαίου κώδικα του Helios, συμπεριλαμβανομένης της ομομορφικής καταμέτρησης η οποία δεν χρησιμοποιείται.

Μια σημαντική διαφοροποίηση από το Helios αποτελεί και το γραφικό περιβάλλον του Ζευς. Λαμβάνοντας υπόψη την ανάλυση χρηστικότητας του Helios από τον Karayumak[36] καθώς και την εμπειρία που αποκτήθηκε από τις εκλογές που διεξήχθησαν με το Ζευς, το γραφικό περιβάλλον του συστήματος ξανασχεδιάστηκε με σκοπό να είναι περισσότερο εύχρηστο και φιλικό στον χρήστη.

Μια άλλη διαφοροποίηση είναι ότι με τον καιρό διάφοροι ερευνητές έχουν εντοπίσει διάφορα τρωτά σημεία στις διάφορες εκδόσεις του Helios[37][38]. Οι επιθέσεις αυτές δεν έχουν επίδραση στο Ζευς.

Τέλος, τον τελευταίο καιρό έχει γίνει μελέτη σχετικά με την προσθήκη αιώνιας μυστικότητας[39] στο Helios. Αυτή τη στιγμή το Helios προσφέρει υπολογιστικά ασφαλή μυστικότητα, δηλαδή είναι υπολογιστικά δύσκολο (από την πλευρά των απαιτούμενων υπολογιστικών πόρων) να παραβιαστεί η ανωνυμία των ψηφοφόρων. Αυτό δεν σημαίνει παρόλα αυτά ότι το σπάσιμο της ανωνυμίας δεν θα είναι εφικτό σε μερικά χρόνια. Πρωτόκολλα για αιώνια μυστικότητα μπορούν να χρησιμοποιηθούν τόσο σε συστήματα που υλοποιούν ομομορφική καταμέτρηση όσο και σε συστήματα με δίκτυα μίξης. Το Ζευς, όπως και το Helios, δεν παρέχει αιώνια μυστικότητα.

Πέρα από τις παραπάνω διαφορές και επεκτάσεις του Helios, το Ζευς τροποποιεί και την χρήση των ψήφων ελέγχου του Helios, με σκοπό να εξυπηρετούν τόσο τον έλεγχο της ακεραιότητας της ψήφου όσο και να χρησιμεύουν ως ένας διαύλος πιστοποιημένης επικοινω-

νίας του Ζευς με τον ψηφοφόρο.

4.2 Τα στάδια εκλογών του Ζευς

Το Ζευς είναι μια διαδικτυακή εφαρμογή. Ο πυρήνας του Ζευς είναι ένα ανεξάρτητο λογισμικό το οποίο υλοποιεί όλες τις απαραίτητες κρυπτογραφικές συναρτήσεις και επαληθεύσεις. Μία εφαρμογή ιστού και ένα γραφικό περιβάλλον χρήστη έρχονται να επεκτείνουν το λογισμικό αυτό ώστε να δημιουργηθεί ένα εύχρηστο σύστημα εκλογών. Η εφαρμογή ιστού επεκτείνει το ανεξάρτητο λογισμικό και χτίζει ένα εύχρηστο σύστημα εκλογών πάνω σε μια βάση δεδομένων η οποία χειρίζεται την πιστοποίηση της ταυτότητας των χρηστών, την ρύθμιση των εκλογών, την υποβολή των ψήφων και την αλληλεπίδραση των μελών της εφορευτικής επιτροπής για την δημιουργία των κλειδιών και την αποκρυπτογράφηση των ψήφων. ΄Ολες αυτές οι ενέργειες θα παρουσιαστούν στη συνέχεια. Τόσο οι ψηφοφόροι όσο οι διαχειριστές και τα μέλη της εφορευτικής επιτροπής χρησιμοποιούν τον περιηγητή τους στο διαδίκτυο για να χρησιμοποιήσουν το Ζευς.

΄Οπως και στο Helios, κάθε εκλογική διαδικασία με το σύστημα Ζευς αποτελείται από τις ακόλουθες φάσεις: την προετοιμασία των εκλογών, την ψηφοφορία, την επεξεργασία των ψηφοδελτίων (μίξη και αποκρυπτογράφηση) και την καταμέτρηση των ψήφων. ΄Ολα τα δεδομένα που σχετίζονται με τις παραπάνω φάσεις των εκλογών αποθηκεύονται σε ένα ενιαίο έγγραφο στην μνήμη του εξυπηρετητή του Ζευς. Ο χειρισμός αυτού του εγγράφου γίνεται από το ανεξάρτητο λογισμικό που αναφέρθηκε προηγουμένως.

Το γεγονός ότι το λογισμικό αυτό είναι πλήρως ανεξάρτητο από όλα τα άλλα μέρη του συστήματος διευκολύνει και απλοποιεί την διαδικασία επαλήθευσης του από τρίτες αρχές.

4.2.1 Προετοιμασία των εκλογών

Ρύθμιση παραμέτρων των εκλογών

Κάθε εκλογική διαδικασία με το Ζευς ξεκινάει με την προετοιμασία των εκλογών. Αρχικά δημιουργείται ένας λογαριασμού στο Ζευς από τους διαχειριστές του συστήματος. Μέσω αυτού του λογαριασμού, ο εκάστοτε οργανισμός μπορεί να συνδεθεί στο σύστημα και να διοργανώσει τις εκλογές του. Ο διαχειριστής των εκλογών θέτει τον τίτλο και την περιγραφή των εκλογών, την ημερομηνία έναρξης και λήξης της εκλογικής διαδικασίας και καθορίζει την εφορευτική επιτροπή. Στη

συνέχεια, επιλέγει τον τύπο των εκλογών και ορίζει το ψηφοδέλτιο. Ανάλογα τον τύπο των εκλογών, το ψηφοδέλτιο μπορεί να αποτελείται από μια λίστα με υποψηφίους ή από πολλές λίστες υποψηφίων διαφορετικών παρατάξεων. Αφού καταρτίσει το ψηφοδέλτιο, ο διαχειριστής των εκλογών ανεβάζει στο σύστημα την λίστα με όλους τους ψηφοφόρους σε μορφή CSV αρχείου.

Δημιουργία των κλειδιών της εφορευτικής επιτροπής

Μετά τον ορισμό τους, τα μέλη της εφορευτικής επιτροπής λαμβάνουν ένα μήνυμα ηλεκτρονικού ταχυδρομείου το οποίο περιέχει έναν μυστικο σύνδεσμο με τον οποίο μπορούν να συνδεθούν στο σύστημα και να δημιουργήσουν τα κλειδιά κρυπτογράφησης τους για τις εκλογές. ΄Ετσι τα μέλη της εφορευτικής επιτροπής δεν χρειάζεται να έχουν κάποιο λογαριασμό ή να θυμούνται κάποιον κωδικό για την είσοδό τους στο σύστημα, απλά χρησιμοποιούν τον μυστικό συνδέσμο.

Η μέθοδος ταυτοποίησης και σύνδεσης των μελών της εφορευτικής επιτροπής στο σύστημα μπορεί εύκολα να τροποποιηθεί και να προσαρμοστεί στις ανάγκες τις εκάστοτε ψηφοφορίας. Για παράδειγμα σε μία από τις εκλογές που έγιναν με το Ζευς οι σύνδεσμοι σύνδεσης των μελών της εφορευτικής επιτροπής στάλθηκαν μέσω SMS αντί μέσω email. Βέβαια, αυτή η διαδικασία χρησιμοποιήθηκε μόνο μία φορά και δεν έχει ενσωματωθεί στον κώδικα του Ζευς ακόμα.

Ακολουθώντας τον σύνδεσμο στο μήνυμα που λαμβάνουν, οι έφοροι δημιουργούν το ζεύγος κλειδιών τους. Ολοκληρη η διαδικασια δημιουργίας των κλειδιών γίνεται εξολοκλήρου στο πρόγραμμα πλοήγησης των χρηστών, υποβοηθούμενη με τυχαιότητα η οποία φορτώνεται από τον εξυπηρετητή του Ζευς. Αυτο γινεται λόγω της κακής τυχαιότητας των προγραμμάτων περιήγησης στο διαδίκτυο και ειναι μια πρακτική η οποία κληρονομήθηκε από το Helios.

Μετά την δημιουργία των κλειδιών, τα μέλη της εφορευτικής επιτροπής πρέπει να αποθηκεύσουν σε ασφαλές μέρος το ιδιωτικό κλειδί τους. Μόλις γίνει αυτό, το σύστημα αποσυνδέει τους χρήστες. Το Ζευς στέλνει τότε ένα νέο μήνυμα ηλεκτρονικού ταχυδρομείου στα μέλη της εφορευτικής επιτροπής με σκοπό να επαληθεύσουν ότι όντως έχουν στην κατοχή τους το ιδιωτικό κλειδί. Κάθε μέλος της εφορευτικής επιτροπής ακολουθώντας έναν μυστικό σύνδεσμο στο μήνυμα που έλαβε, μεταβαίνει σε μία σελίδα του Ζευς στην οποία βλέπει τον κατακερματισμό του δημοσίου κλειδιού του και στην οποία ανεβάζει το ιδιωτικό κλειδί που αποθήκευσε προηγουμένως με σκοπό να το επαληθεύσει. Η επαλήθευση γίνεται τοπικά συγκρίνοντας τον κατακερματισμό του κλειδιού με αυτόν που έχει αποθηκευτεί στον εξυπηρετητή. Η όλη διαδικασία είναι αντίστοιχη αυτής στην οποία ο χρήστης εισάγει τον κωδικό του δύο φορές, αφού η σωστή αποθήκευση των ιδιωτικών κλειδι-

ών των χρηστών είναι κρίσιμης σημασίας για την αποκρυπτογράφηση των αποτελεσμάτων.

Πέρα από τα μέλη της εφορευτικής επιτροπής που ορίζονται από τον διαχειριστή των εκλογών, μέλος της εφορευτικής επιτροπής κάθε εκλογικής διαδικασίας είναι και το ίδιο το Ζευς. ΄Ετσι υπάρχει μια πρόσθετη εγγύηση της μυστικότητας των ψήφων των ψηφοφόρων πέρα από αυτήν που παρέχει η διορισμένη εφορευτική επιτροπή.

Οριστικοποίηση των εκλογών και πρόσκληση των ψηφοφόρων

Οι διαχειριστές μπορούν να αλλάξουν τις παραμέτρους των εκλογών μέχρι και την στιγμή που επιλέγουν να οριστικοποιήσουν τις εκλογές. Μετά από αυτή την στιγμή επιτρέπεται επεξεργασία μόνο συγκεκριμένων πληροφοριών για τις εκλογές.

Με την οριστικοποίηση των εκλογών όλοι οι εγγεγραμμένοι ψηφοφόροι λαμβάνουν ένα μήνυμα ηλεκτρονικού ταχυδρομείου το οποίο περιέχει όλη την απαιτούμενη πληροφορία για να συνδεθούν στο σύστημα και να ψηφίσουν. ΄Οπως στην περίπτωση των μελών της εφορευτικής επιτροπής, οι ψηφοφόροι δεν χρειάζονται κάποιο λογαριασμό για να εισέλθουν στο σύστημα. Χρησιμοποιούν έναν μυστικό σύνδεσμο που περιέχεται στο μήνυμα που έλαβαν.

Στην περίπτωση που οι ψηφοφόροι ακολουθήσουν τον σύνδεσμο πριν την έναρξη των εκλογών, με την σύνδεσή τους στο σύστημα μπορούν να δουν πληροφορίες για τις εκλογές, στοιχεία επικοινωνίας με το τμήμα εξυπηρέτησης του Ζευς καθώς και τις ημερομηνίες διεξαγωγής των εκλογών. Μετά την έναρξη των εκλογών, οι σύνδεσμοι αυτοί στέλνουν τους ψηφοφόρους απευθείας στον ψηφιακό θάλαμο ψηφοφορίας.

΄Οπως και στην περίπτωση της εφορευτικής επιτροπής, ο λόγος που επιλέχθηκε η σύνδεση των ψηφοφόρων στο σύστημα να γίνεται μέσω του μυστικού συνδέσμου είναι για να μην χρειάζεται οι ψηφοφόροι να έχουν λογαριασμό στο σύστημα και να θυμούνται κάποιον κωδικό. Επίσης αυτό απλοποιεί και την διαδικασία από την πλευρά του Ζευς καθώς με τον τρόπο αυτό δεν καλείται το Ζευς να διαχειριστεί τις περιπτώσεις που οι χρήστες έχασαν τον κωδικό τους.

Αυτό φυσικά απαιτεί οι χρήστες να έχουν πρόσβαση στο ηλεκτρονικό ταχυδρομείο τους αφού σε αντίθετη περίπτωση δεν μπορούν να έχουν πρόσβαση στον μυστικό σύνδεσμο. Μια τέτοια επίθεση έλαβε χώρα σε μια από τις εκλογές που διεξήχθησαν με το Ζευς, αντιμετωπίστηκε όμως παρατείνοντας την διάρκεια των εκλογών και αποστέλλοντας τις προσκλήσεις ψηφοφορίας μέσω SMS μηνυμάτων.

΄Ολες οι πληροφορίες αυτού του σταδίου εκλογών (υποψήφιοι, ψηφοφόροι, μέλη της εφορευτικής επιτροπής) καταγράφονται στο έγγραφο των εκλογών.

Στο σημείο αυτό, μπορεί να γίνει έναρξη της ψηφοφορίας. Με το άνοιγμα των καλπών γίνεται και ο συνδυασμός των δημοσίων κλειδιών των μελών της εφορευτικής επιτροπής (μέσω ενός πολλαπλασιασμού) και παράγεται ένα κοινό δημόσιο κλειδί εκλογών, το οποίο οι ψηφοφόροι θα χρησιμοποιήσουν για την κρυπτογράφηση της ψήφου τους. Μετά την δημιουργία του κλειδιού αυτού δεν μπορεί να γίνει καμία αλλαγή στην λίστα των μελών της εφορευτικής επιτροπής, στον εκλογικό κατάλογο ή στο ψηφοδέλτιο.

4.2.2 Ψηφοφορία

΄Οπως αναφέρθηκε προηγουμένως, οι ψηφοφόροι μπορούν να εισέλθουν στον ψηφιακό θάλαμο ψηφοφορίας μέσω του προγράμματος περιήγησης τους στο διαδίκτυο ακολουθώντας τον σύνδεσμο που έλαβαν στο email τους.

Αφού φορτωθεί ο θάλαμος ψηφοφορίας λειτουργεί τοπικά, χωρίς καμία αλληλεπίδραση με τον εξυπηρετητή του Ζευς ή κάποια άλλη ιστοσελίδα. Ο ψηφοφόρος μπορεί εάν το επιθυμεί να αποσυνδεθεί από το διαδίκτυο όσο είναι μέσα στον ψηφιακό θάλαμο.

Μετά την είσοδο στον θάλαμο ψηφοφορίας, το ψηφιακό ψηφοδέλτιο εμφανίζεται στην οθόνη και ο ψηφοφόρος επιλέγει τους υποψηφίους της επιλογής του. Πριν την υποβολή της ψήφου ζητείται επιβεβαίωση από τον ψηφοφόρο.

Στη συνέχεια η ψήφος του ψηφοφόρου κρυπτογραφείται με το κοινό δημόσιο κλειδί των εκλογών και αποστέλλεται στον εξυπηρετητή του Ζευς. Πέρα από το κρυπτοκείμενο της ψήφου του, ο ψηφοφόρος υποβάλει επίσης στον εξυπηρετητή μία απόδειξη διακριτού λογαρίθμου[40] ότι κατέχει την τυχαιότητα που χρησιμοποιήθηκε για την κρυπτογράφηση του ψηφοδελτίου και προαιρετικά ένα κωδικό ελέγχου, με τον οποίο μπορεί να επαληθεύσει ότι το τοπικό σύστημα πραγματικά υποβάλει την ψήφο που ο ψηφοφόρος επέλεξε και ότι δεν θα την αλλάξει εν αγνοία του. Περισσότερες πληροφορίες σχετικά με τους κωδικούς ελέγχου και την χρήση τους θα παρουσιαστούν σε επόμενη ενότητα.

Η παρούσα έκδοση του Ζευς επιτρέπει την υποβολή σχετικών κρυπτοκειμένων. Αυτό δεν αποτελεί πρόβλημα για το Ζευς καθώς και στις πραγματικές εκλογές δεν απαγορεύεται οι παρατάξεις να δίνουν προσυμπληρωμένα ψηφοδέλτια στους ψηφοφόρους τα οποία αυτοί να ρίξουν στην κάλπη.

Για κάθε μία υποβληθείσα ψήφο, το Ζευς δημιουργεί και στέλνει στον ψηφοφόρο μια κρυπτογραφικά υπογεγραμμένη απόδειξη, την οποία ο ψηφοφόρος μπορεί να επιλέξει να αποθηκεύσει στον υπολογιστή του. Η ίδια απόδειξη επίσης αποστέλλεται και μέσω μηνύματος ηλεκτρονικού ταχυδρομείου στον ψηφοφόρο. Με αυτή την απόδειξη ο ψηφοφόρος μπορεί να επαληθεύσει ότι η ψήφος του υποβλήθηκε και αποθηκεύτηκε σωστά. Είναι σημαντικό να σημειωθεί ότι η απόδειξη δεν περιέχει προσωπικές πληροφορίες όπως το όνομα του ψηφοφόρου, η διεύθυνση IP και οι χρόνοι ψηφοφορίας (παρόλο που οι πληροφορίες αυτές καταγράφονται στον εξυπηρετητή του Ζευς). Ο λόγος είναι για να είναι δυνατή η δημοσιοποίηση του εγγράφου των εκλογών χωρίς να υπάρχει ο κίνδυνος της δημοσιοποίησης προσωπικών δεδομένων των ψηφοφόρων.

Κάθε ψηφοφόρος μπορεί να ψηφίσει πολλές φορές. Κάθε φορά η νέα ψήφος αντικαθιστά την προηγούμενη και μια νέα απόδειξη δημιουργείται, η οποία ρητώς αναφέρει ποια ψήφο αντικαθιστά η νέα. Καμία ψήφος δεν μπορεί να αντικατασταθεί πάνω από μία φορά.

Η απόδειξη που λαμβάνει ο ψηφοφόρος καταγράφεται επίσης στο έγγραφο των εκλογών. Η απόδειξη είναι ένα αρχείο κειμένου με απλή δομή το οποίο περιέχει το μοναδικό αναγνωριστικό της ψήφου που ρίχθηκε στην κάλπη, το μοναδικό αναγνωριστικό της ψήφου που αντικαθιστά (στην περίπτωση που αντικαθιστά κάποια ψήφο), του κρυπτοσυστήματος που χρησιμοποιήθηκε, το δημόσιο κλειδί των εκλογών, τα δημόσια κλειδιά όλων των μελών της εφορευτικής επιτροπής, και την λίστα με όλους τους ψηφοφόρους.

Το κείμενο της απόδειξης υπογράφεται με το ιδιωτικό κλειδί του Ζευς για την ψηφοφορία (το οποίο είναι εφικτό καθώς όπως έχει αναφερθεί το Ζευς είναι και αυτό μέλος της εφορευτικής επιτροπής για κάθε εκλογική διαδικασία) και η υπογραφή προστίθεται και αυτή στα περιεχόμενα της απόδειξης. Για την υλοποίηση της ψηφιακής υπογραφής χρησιμοποιείται το πρωτόκολλο ψηφιακής υπογραφής ElGamal σύμφωνα με τον Schneier[41].

Είναι σημαντικό να αναφερθεί ότι οι αποδείξεις υποβολής της ψήφου δεν είναι αρκετές για να εγγυηθούν ότι ένας διεφθαρμένος εξυπηρετητής δεν θα υποβάλει μια ψήφο εκ μέρους ενός χρήστη και στη συνέχεια θα ισχυριστεί ότι απλά ο χρήστης έχασε την απόδειξή του, ή ότι ένας χρήστης ο οποίος φρόντισε να διαγράψει την απόδειξή του δεν θα ισχυριστεί ότι η τελευταία ψήφος του στον εξυπηρετητή είναι ψεύτικη. Το πρόβλημα αυτό θα μπορούσε να λυθεί με την δημοσιοποίηση των κρυπτογραφημένων ψηφοδελτίων σε έναν δημόσιο πίνακα ανακοινώσεων μετά το κλείσιμο των καλπών και πριν την έναρξη της καταμέτρησης (όπως γίνεται στα συστήματα εκλογών που περιγράφηκαν στην προηγούμενη ενότητα). Παρόλα αυτά αυτό δεν ήταν

εφικτό στις εκλογές που διεξήχθησαν με το Ζευς καθώς θα απαιτούσε οι χρήστες να αλληλεπιδράσουν ακόμα μια φορά με το Ζευς και κάτι τέτοιο θα καθυστερούσε την διαδικασία της καταμέτρησης. Στις εκλογές που χρησιμοποιήθηκε το Ζευς η ταχεία ανακοίνωση του αποτελέσματος ήταν κρίσιμης σημασίας, ειδικά καθώς υπήρχαν ημέρες τις οποίες πάνω από μια εκλογική διαδικασία λάμβανε χώρε σε διάφορα ιδρύματα.

Κατά την διάρκεια της ψηφοφορίας οι διαχειριστές των εκλογών μπορούν να δουν τον αριθμό των ψηφοφόρων που έχουν ψηφίσει, και την λίστα των ψηφοφόρων. Για κάθε ψηφοφόρο μπορούν να δουν το όνομά του, το email του, εάν ψήφισε ή όχι, ποιο ήταν το τελευταίο email που στάλθηκε στον ψηφοφόρο και πότε ήταν η τελευταία φορά που ο ψηφοφόρος επισκέφθηκε τον θάλαμο ψηφοφορίας.

4.2.3 Επεξεργασία και καταμέτρηση

Μετά την καθορισμένη ώρα λήξης, η κάλπη κλείνει αυτόματα. ΄Ομως, οι διαχειριστές μπορούν να επιλέξουν να παρατείνουν την ψηφοφορία ακόμα και μετά την λήξη των εκλογών. ΄Οταν οι διαχειριστές το επιθυμούν, μπορούν να λήξουν οριστικά τις εκλογές.

Μίξη

Μετά το κλείσιμο των κάλπεων, η εκλογική διαδικασία μεταβαίνει στο στάδιο μίξης όπου τα κρυπτογραφημένα ψηφοδέλτια ανωνυμοποιούνται. Από το σύνολο των ψηφοδελτίων αφαιρούνται τα ψηφοδέλτια τα οποία αποτελούν ψήφους ελέγχου, όλα τα ψηφοδέλτια τα οποία αντικαταστάθηκαν από κάποιο άλλο νεότερο καθώς και τα ψηφοδέλτια τα οποία ρίχθηκαν από ψηφοφόρους που αποκλείστηκαν από τις εκλογές κατά την διάρκεια της ψηφοφορίας. Ο αποκλεισμός ενός ψηφοφόρου είναι μια διευκόλυνση που παρέχει το Ζευς η οποία οφείλεται στο γεγονός ότι η ταυτότητα του ψηφοφόρου είναι γνωστή ακόμα και μετά το ρίξιμο του ψηφοδελτίου στην κάλπη (σε αντίθεση με τις πραγματικές εκλογές όπου το ψηφοδέλτιο ρίχνεται ανώνυμα στην κάλπη). Οι διαχειριστές των εκλογών μπορεί να επιλέξουν να αφαιρέσουν το δικαίωμα ψήφου από ψηφοφόρους που λανθασμένα προστέθηκαν στον εκλογικό κατάλογο, ή από ψηφοφόρους των οποίων η συμπεριφορά κατά την διάρκεια των εκλογών παραβίασε τους κανονισμούς των εκλογών.

Είναι σημαντικό να σημειωθεί ότι ούτε οι αποκλεισμένοι ψηφοφόροι ούτε οι ψήφοι τους διαγράφονται από το έγγραφο των εκλογών. Αντίθετα οι ψηφοφόροι αυτοί προστίθενται σε μια λίστα αποκλεισμού μαζί με κάποια σημείωση η οποία δικαιολογεί τον αποκλεισμού

τους. Τα ψηφοδέλτια που απομένουν ανωνυμοποιούνται πρώτα με το δίκτυο μίξης του Ζευς, το οποίο είναι ένα Sako-Kilian δίκτυο μίξης. Ο μεγαλύτερος υπολογιστικός φόρτος της διαδικασίας της μίξης είναι για την παραγωγή αρκετών γύρων πιθανοτήτων αποδείξεων. Η εργασία αυτή διαμοιράζεται σε μία ομάδα παράλληλων εργατών, ένας γύρος κάθε φορά. Η υλοποίηση του Ζευς χρησιμοποιεί 128 γύρους και 16 εργάτες.

Η επαλήθευση των μίξεων μπορεί και αυτή να παραλληλοποιηθεί. Μόλις η πρώτη μίξη ολοκληρωθεί, επιπλέον μίξεις από εξωτερικούς δράστες μπορούν να προστεθούν μια προς μία χρησιμοποιώντας μυστικούς συνδέσμους που δημιουργούνται για τον σκοπό αυτό. Το Ζευς παρέχει ένα εργαλείο γραμμής εντολών το οποίο μεταξύ άλλων μπορεί να εκτελέσει μίξη των ψηφοδελτίων που παρέχονται από τους μυστικούς συνδέσμους.

Αποκρυπτογράφηση

Μετά την ολοκλήρωση όλων των μίξεων, ο διαχειριστής λήγει την διαδικασία μίξης και οι έφοροι ειδοποιούνται ξανά για την διαδικασία της αποκρυπτογράφησης. Κάθε μέλος της εφορευτικής λαμβάνει ένα μήνυμα ηλεκτρονικού ταχυδρομείου το οποίο περιέχει έναν νέο μυστικό σύνδεσμο με τον οποίο μπορεί να συνδεθεί στο Ζευς. Με την σύνδεση στο Ζευς, τα ανώνυμα πλέον κρυπτογραφημένα ψηφοδέλτια κατεβαίνουν στο πρόγραμμα περιήγησης του εκάστοτε μέλους. Στη συνέχεια το εκάστοτε μέλος της εφορευτικής επιτροπής εισάγει το ιδιωτικό κλειδί του και ξεκινάει η διαδικασία της μερικής αποκρυπτογράφησης των ψηφοδελτίων. Μόλις η διαδικασία ολοκληρωθεί, τα μερικώς αποκρυπτογραφημένα ψηφοδέλτια στέλνονται πίσω στο Ζευς. Τα αποτελέσματα κάθε μερικής αποκρυπτογράφησης αποθηκεύονται στο έγγραφο των εκλογών.

΄Οταν ολοκληρωθούν όλες οι μερικές αποκρυπτογραφήσεις των μελών της εφορευτικής επιτροπής, το Ζευς αποκρυπτογραφεί μερικώς και αυτό τα ψηφοδέλτια (είναι και αυτό μέλος της εφορευτικής επιτροπής). Στη συνέχεια, όλα τα μερικώς αποκρυπτογραφημένα ψηφοδέλτια διαμοιράζονται σε παράλληλους εργάτες με σκοπό να επαληθευτούν και να συνδυαστούν. ΄Ετσι παράγονται τα τελικά αποκρυπτογραφημένα ψηφοδέλτια. Τα αποκρυπτογραφημένα ψηφοδέλτια καταγράφονται στο έγγραφο των εκλογών και στην συνέχεια το έγγραφο εξάγεται σε μία κανονική αναπαράσταση με κείμενο. Αυτή η αναπαράσταση κειμένου κατακερματίζεται με σκοπό να δημιουργηθεί ένα κρυπτογραφικά ασφαλές αναγνωριστικό για αυτό, το οποίο μπορεί να δημοσιευτεί και να καταγραφεί στα πρακτικά.

Καταμέτρηση

Ανάλογα με τον τύπο των εκλογών, τα ψηφοδέλτια είτε στέλνονται σε κάποιο άλλο σύστημα για να καταμετρηθούν (στην περίπτωση που ο αλγόριθμος καταμέτρησης έχει υλοποιηθεί σε κάποιο άλλο σύστημα, όπως και έγινε στις περιπτώσεις των εκλογών που έχουν τρέξει μέχρι στιγμής με το Ζευς) είτε καταμετρώνται από το ίδιο το Ζευς. Μετά την δημοσιοποίηση του αποτελέσματος, ο διαχειριστής μπορεί να κατεβάσει ένα αρχείο με όλες τις αποδείξεις που έχουν δημιουργηθεί.

4.3 Ψήφοι ελέγχου και κωδικοί ελέγχου

΄Οπως αναφέρθηκε σε προηγούμενη ενότητα, ο ψηφοφόρος έχει την επιλογή να υποβάλλει μαζί με την ψήφο του και έναν κωδικό ελέγχου, να υποβάλει δηλαδή μία ψήφο ελέγχου. Οι κωδικοί ελέγχου περιέχονται και αυτοί στο μήνυμα ηλεκτρονικού ταχυδρομείου το οποίο περιλαμβάνει το μυστικό σύνδεσμο για την είσοδο των ψηφοφόρων στο σύστημα. Βέβαια, για πρόσθετη ασφάλεια, οι κωδικοί ελέγχου μπορούν να αποσταλούν και μέσω κάποιου άλλου καναλιού, όπως για παράδειγμα μέσω SMS μηνύματος. Οι κωδικοί ελέγχου είναι τυχαίοι αριθμοί ο οποίοι δημιουργούνται από το Ζευς.

Οι ψήφοι ελέγχου λειτουργούν με το να καταστρέφουν τα πλάνα ενός επιτιθέμενου ο οποίος μπορεί να έχει παραβιάσει τον υπολογιστή του ψηφοφόρου με σκοπό να αλλάξει την ψήφο που αυτός ρίχνει στην κάλπη. Για να καταστραφούν αυτά τα σχέδια εισάγεται αβεβαιότητα για το μέλλον της ψήφου: ο ψηφοφόρος μπορεί να υποβάλει απλά την κρυπτογραφημένη ψήφο του και αυτή να καταμετρηθεί ή να επιλέξει να την αποκαλύψει και να την δημοσιοποιήσει με σκοπό να δει το περιεχόμενό της. Εάν ο επιτιθέμενος δεν γνωρίζει ποια θα είναι η μοίρα της ψήφου, δεν μπορεί να αποφασίσει για το αν είναι ασφαλές να την αλλάξει ή όχι. Εάν αλλάξει την ψήφο και αυτή δημοσιοποιηθεί, τότε η επίθεση θα εντοπιστεί. Εάν δεν την αλλάξει και η ψήφος καταμετρηθεί, τότε η επίθεση απέτυχε.

΄Οπως παρουσιάστηκε στην προηγούμενη ενότητα, το Helios δημιουργεί την αβεβαιότητα αυτή με το να κρυπτογραφεί την ψήφο πριν ταυτοποιήσει τον ψηφοφόρο. ΄Ετσι δεν μπορεί να γνωρίζει εάν αυτός που συμπληρώνει το ψηφοδέλτιο είναι κάποιος ελεγκτής ή κάποιος απλός ψηφοφόρος. ΄Επειτα ζητάει από τους χρήστες να επιλέξουν εάν επιθυμούν να ελέγξουν την ψήφο τους ή να την ρίξουν στην κάλπη.

Το Ζευς, όμως, ταυτοποιεί τους ψηφοφόρους πριν την προβολή του ψηφοδελτίου και την δυνατότητα ελέγχου του, κάτι που καθιστά την μέθοδο του Helios μη εφαρμόσιμη.

Στο Ζευς, μια ψήφος μπορεί να υποβληθεί είτε με έναν συνοδευτικό κωδικό, είτε χωρίς κωδικό. Οι ψήφοι οι οποίες υποβάλλονται χωρίς κωδικό γίνονται αποδεκτές ως κανονικές ψήφοι προς καταμέτρηση και δεν γίνεται κάποιος έλεγχος σε αυτές. Εάν κάποιος ψηφοφόρος δεν εμπιστεύεται το τοπικό σύστημα και θέλει να το δοκιμάσει ώστε να είναι σίγουρος ότι υποβάλει την ψήφο του με ασφάλεια, τότε δεν πρέπει να υποβάλει ποτέ την ψήφο του χωρίς κωδικό επαλήθευσης.

Εάν η ψήφος υποβληθεί με έναν συνοδευτικό κωδικό τότε δύο πράγματα μπορεί να συμβούν. Εάν ο κωδικός δεν είναι μεταξύ αυτών που έλαβε ο ψηφοφόρος, ο εξυπηρετητής θεωρεί ότι είναι μια ψήφος ελέγχου. Εάν ο κωδικός είναι μεταξύ αυτών που έλαβε ο χρήστης η ψήφος ρίχνεται στην κάλπη σαν κανονική ψήφος.

Δεν πρέπει να υποβάλλονται ποτέ δύο διαφορετικές ψήφοι με τον ίδιο κωδικό γιατί την δεύτερη φορά ο επιτιθέμενος θα γνωρίζει τι να κάνει.

Η διαδικασία είναι η ακόλουθη:

1. Ο ψηφοφόρος εισάγει έναν από τους κωδικούς ελέγχου που έλαβε μέσω email

2. Ο ψηφοφόρος συνεχίζει και υποβάλλει το ψηφοδέλτιο στον εξυπηρετητή

3. Ο εξυπηρετητής λαμβάνει την κρυπτογραφημένη ψήφο. Εάν η κρυπτογραφημένη ψήφος συνοδεύεται από έναν σωστό κωδικό ελέγχου ή δεν συνοδεύεται από κωδικό ελέγχου η ψήφος αντιμετωπίζεται ως κανονική ψήφος. Αλλιώς, εάν η ψήφος συνοδεύεται από έναν κωδικό ελέγχου που δεν είναι σωστός, γίνονται τα ακόλουθα βήματα.

4. Το σύστημα αποθηκεύει το κρυπτοκείμενο σαν μία αίτηση ελέγχου της ψήφου

5. Το σύστημα ζητά από τον ψηφοφόρο να επιβεβαιώσει ότι έχει αποστείλει μια ψήφο ελέγχου

6. Εάν ο ψηφοφόρος απαντήσει αρνητικά, τότε η διαδικασία ελέγχου ακυρώνεται και ο ψηφοφόρος ανακατευθύνεται να στο αρχικό βήμα της ρίψης του ψηφοδελτίου. Η αίτηση ελέγχου παραμένει στο σύστημα αλλά δεν εμφανίζεται στους χρήστες.

7. Εάν ο ψηφοφόρος απαντήσει θετικά, ο πλοηγός στέλνει στο Ζευς το κρυπτοκείμενο της ψήφου μαζί με την τυχαιότητα Ελ Γαμαλ με την οποία η ψήφος κρυπτογραφήθηκε

8. Ο εξυπηρετητής του Ζευς προσπαθεί να αντιστοιχίσει το αποτύπωμα της ψήφου που στάλθηκε με αυτό που είχε αποσταλεί μαζί με τον κωδικό ελέγχου. Η αποτυχία να γίνει αυτό συνεπάγεται ότι το κρυπτοκείμενο που δημοσιεύτηκε αρχικά είναι αλλαγμένο και το σύστημα πληροφορεί τον χρήστη ότι η αίτηση ελέγχου δεν μπορεί να γίνει αποδεκτή. Αυτό προστατεύει τον ψηφοφόρο έναντι κακόβουλου λογισμικού το οποίο θα μπορούσε να υποβάλλει μια αλλαγμένη ψήφο και μετά αφού καταλάβει ότι η ψήφος είναι μια ψήφος ελέγχου να στείλει το πραγματικό κρυπτοκείμενο. Εάν η σύγκριση πετύχει, το σύστημα αποθηκεύει την ψήφο ελέγχου και επιστρέφει στον ψηφοφόρο ένα μοναδικό αναγνωριστικό της ψήφου ελέγχου.

9. Τα αποκρυπτογραφημένα περιεχόμενα κάθε ψήφου ελέγχου, βασισμένα στην τυχαιότητα η οποία στάλθηκε προηγουμένως από τον ψηφοφόρο, δημοσιεύονται σε έναν πίνακα ανακοινώσεων για τις ψήφους ελέγχου. Ο ψηφοφόρος μπορεί να πάει σε αυτόν τον πίνακα και να κοιτάξει για την ψήφο του χρησιμοποιώντας το αναγνωριστικό που έλαβε από τον εξυπηρετητή.

Το Ζευς καθιστά τον έλεγχο προεραιτικό, με το να δημιουργεί την απαιτούμενη αβαβαιότητα για έλεγχο χρησιμοποιώντας τους κωδικούς ελέγχου. Παρόλα αυτά το σύστημα μπορεί να τροποποιηθεί ώστε να απαιτεί έναν κωδικό για κάθε υποβολή ψήφου, στην περίπτωση αυτή οι κωδικοί ελέγχου παρέχουν μια δεύτερη λειτουργία, σαν ένα πρόσθετο παράγοντα πιστοποίησης της ταυτότητας των χρηστών.

Καθιστώντας τον κωδικό ελέγχου υποχρεωτικό θα αποτραπεί η επίθεση στην οποία ένας διεφθαρμένος περιηγητής στο διαδίκτυο εντοπίζει πότε ένα ψηφοδέλτιο αποστέλλεται χωρίς κωδικό ελέγχου και μόνο στην περίπτωση αυτή αλλάζει την ψήφο του ψηφοφόρου.

Η λειτουργία αυτή είναι πολύ χρήσιμη καθώς βοηθάει να συνδυαστεί ένα πολύ βολικό αλλά πιθανώς ανασφαλές μέσω, για παράδειγμα το email με ένα πιο ασφαλές και πιο προσωπικό όπως το κινητό τηλέφωνο. Οι προσκλήσεις, οι ειδοποιήσεις και οι περιγραφές σχετικές με την ψηφοφορία οι οποιες μπορεί να περιέχουν κείμενο μεγάλου μήκους καθώς και εικόνες μπορούν να σταλούν μέσω email ενώ οι κωδικοί ελέγχου οι οποίοι είναι μικροί σε μήκος μπορούν να σταλούν μέσω κινητού τηλεφώνου. Ο ψηφοφόρος θα χρειαστεί και το email και το μήνυμα στο κινητό του τηλέφωνο για να ψηφίσει επιτυχώς.

Παρόλο που η χρήση κωδικών ελέγχου βελτιώνει την εμπιστοσύνη στο σύστημα, δεν το κάθιστά άτρωτο σε επιθέσεις. Για παράδειγμα μια τέτοια επίθεση θα μπορούσε να είναι ένα κακόβουλο λογισμικό το οποίο σαρώνει το email του ψηφοφόρου, εντοπίζει το email που έστειλε το Ζευς και διαβάζει τους κωδικούς ελέγχου από εκεί. Έτσι το

κακόβουλο λογισμικό θα ξέρει πότε ο ψηφοφόρος στέλνει μια κανονική ψήφο και πότε μια ψήφο ελέγχου και θα συμπεριφερθεί ανάλογα. Αυτός ο κίνδυνος θα μπορούσε να μειωθεί με το να στέλνονται οι κωδικοί επαλήθευσης μέσω ενός άλλου καναλιού, όπως μέσω SMS. Παρόλα αυτά και το κανάλι των SMS να μπορούσε να παραβιαστεί, όπως έχει περιγραφεί στις επιθέσεις ενάντια στο σύστημα διαδικτυακών εκλογών της Νορβηγίας[42].

Κεφάλαιο 5

Επαληθεύσιμη καταγραφή της υποβληθείσας ψήφου

5.1 Μελέτη της ιδιότητας

΄Ολα τα συστήματα εκλογών που παρουσιάστηκαν, είτε πρόκειται για συστήματα τα οποία βασίζονται σε φυσικό θάλαμο ψηφοφορίας και χάρτινο ψηφοδέλτιο, είτε πρόκειται για εξολοκλήρου ψηφιακά συστήματα εκλογών, είτε για συστήματα χωρίς κρυπτογράφηση, έχουν ένα κοινό σημείο όσον αφορά την ιδιότητα της καταγραφής της υποβληθείσας επαληθευσιμότητας. ΄Ολα χρησιμοποιούν ένα δημόσιο πίνακα ανακοινώσεων στον οποίο δημοσιεύουν κάποια πληροφορία για την ψήφο που έριξε ο ψηφοφόρος στην κάλπη. ΄Επειτα, ορίζουν μια περίοδο στην οποία οι ψηφοφόροι καλούνται να επισκεφτούν τον πίνακα ανακοινώσεων και να επαληθεύσουν ότι η πληροφορία που εμφανίζεται για την ψήφο τους είναι σωστή και ταιριάζει με αυτή που έχουν λάβει ως απόδειξη από το σύστημα εκλογών ή έχουν καταγράψει οι ίδιοι (όπως στην περίπτωση του MarkPledge).

Προφανώς η μέθοδος αυτή δεν απαιτεί από όλους τους ψηφοφόρους να επαληθεύσουν την απόδειξή τους αλλά βασίζεται σε στατιστικό έλεγχο. Εάν ένα επαρκές, τυχαίο και ομοιόμορφα κατανεμημένο δείγμα ψηφοφόρων επαληθεύσει την ψήφο του, τότε η πιθανότητα κάποια προσπάθεια αλλοίωσης του αποτελέσματος των εκλογών να πιαστεί είναι αρκετά μεγάλη. ΄Ετσι πέρα από μέσο εντοπισμού τυχόν αλλοίωσης του αποτελέσματος των εκλογών, η μέθοδος αυτή λειτουργεί και αποτρεπτικά, καθώς ένας επιτιθέμενος γνωρίζει πως η πιθανότητα να εντοπιστεί η αλλοίωση είναι μεγάλη.

΄Ενα βασικό μειονέκτημα της μεθόδου αυτής είναι ότι εάν για κάποιο λόγο οι ψηφοφόροι δεν επαληθεύσουν την ψήφο τους ή το δείγμα δεν είναι επαρκές ή τυχαίο ή ομοιόμορφα κατανεμημένο, η εγγυήσεις ασφαλείας του συστήματος καταρρέουν και η καταγραφή της υποβλη-

θείσας ψήφου επαληθευσιμότητα δεν διασφαλίζεται. Συνεπώς, η ακραία επαληθευσιμότητα του συστήματος των εκλογών παύει να διασφαλίζεται πλήρως.

΄Οπως προέκυψε και από την παρουσίαση των εκλογικών συστημάτων της ενότητας 3, δεν είναι δεδομένο ότι αρκετοί ψηφοφόροι θα επαληθεύσουν την ψήφο τους. Υπάρχουν παραδείγματα όπου ο αριθμός των ψηφοφόρων που έλεγξε την απόδειξή του στον πίνακα ανακοινώσεων ήταν μεγάλος, όπως στις εκλογές που διεξήχθησαν με το Helios στο Universite Catholique de Louvain (30% των ψηφοφόρων) ή στις εκλογές του πανεπιστημίου της Ottawa που διεξήχθησαν με το Punchscan[43] (54% των ψηφοφόρων)[44]. Υπάρχουν όμως και παραδείγματα όπου ο αριθμός των ψηφοφόρων ήταν αρκετά μικρός, όπως στην περίπτωση των δημοτικών εκλογών στην Tahoma Park με το Scantegrity II (4% των ψηφοφόρων).

Στην κατεύθυνση αυτή είναι ιδιαίτερα ενδιαφέρον να μελετηθούν τα αποτελέσματα της μελέτης των Ester Moher, Jeremy Clark και Alexander Essex. Σκοπός της μελέτης ήταν να μετρηθεί πόσοι ψηφοφόροι τελικά υποβάλλουν κάποια ένσταση για την εκλογική διαδικασία, εφόσον ο έλεγχος της απόδειξης που έκαναν απέτυχε, σε σχέση με πόσοι ελέγχουν τις αποδείξεις τους μετά τις εκλογές. Επίσης μετρήθηκε το πως επηρεάζει το αποτέλεσμα των εκλογών (εάν είναι το αναμενόμενο ή όχι) τα ποσοστά αυτά.

Για την μέτρηση, διοργανώθηκαν δύο διαδικτυακές έρευνες στις οποίες κλήθηκαν να απαντήσουν χρήστες του διαδικτύου, μέσω της πλατφόρμας CrowdFlower (https://www.crowdflower.com/). Κάθε μία έρευνα ήταν δομημένη ως εξής: αρχικά οι συμμετέχοντες απαντούσαν ένα σύντομο ερωτηματολόγιο, έδιναν προεραιτικά το email τους και έπειτα ψήφιζαν. Στη συνέχεια λάμβαναν ένα email το οποίο είχε ένα σύνδεσμο στην σελίδα των αποτελεσμάτων καθώς και ένα αναγνωριστικό ψηφοδελτίου με το οποίο μπορούσαν να επαληθεύσουν την ψήφο τους (επίσης μέσω του προηγούμενου συνδέσμου). Το θέμα και των δύο ερευνών ήταν ότι κάποιοι ερευνητές ενδιαφερόντουσαν να μελετήσουν την συμπεριφορά των χρηστών αναφορικά με τις φιλανθρωπικές δωρεές. ΄Ετσι κλήθηκαν ψηφίσουν έναν φιλανθρωπικό οργανισμό στον οποίο θα προτιμούσαν να έκαναν δωρεά.

Στην πρώτη έρευνα ψήφισαν 841 χρήστες, εκ των οποίων οι 603 έδωσαν το email τους και έλαβαν το μήνυμα με τα στοιχεία της επαλήθευσης. Για την μελέτη του πως το αποτέλεσμα της ψηφοφορίας επηρεάζει το ποσοστό των χρηστών που επαληθεύουν τις ψήφους τους, επιλέχθηκε να ανακοινωθεί στους μισούς ψηφοφόρους το σωστό αποτέλεσμα (το οποίο συγκέντρωσε 58% των ψήφων και ήταν το αναμενόμενο αποτέλεσμα) ενώ στους άλλους μισούς ένα λάθος και μη αναμενόμενο αποτέλεσμα (συγκεκριμένα τον τελευταίο οργανισμό σε

ψήφους, ο οποίος συγκέντρωσε το 1.3% των ψήφων και δεν ήταν αναμενόμενος σαν πρώτο αποτέλεσμα). Από τους ψηφοφόρους που έλαβαν το email, μόνο οι 84 (13.9%) πάτησαν πάνω στον σύνδεσμο. 42 από αυτούς είδαν το σωστό και αναμενόμενο αποτέλεσμα ενώ 42 είδαν το λάθος και μη αναμενόμενο. Από αυτούς που είδαν το σωστό αποτέλεσμα, 22 έλεγξαν το ψηφοδέλτιο. Ο αριθμός αυτός ήταν μεγαλύτερος για αυτούς που δεν είδαν το σωστό αποτέλεσμα (32). Συνολικά από τους 54 που έλεγξαν το ψηφοδέλτιό τους, οι 26 πήραν λάθος απάντηση, δηλαδή ότι η ψήφος τους είχε αλλαχθεί. Από αυτούς μόνο 3 ξεκίνησαν την διαδικασία υποβολής ένστασης (3.6% των ψηφοφόρων που ακολούθησαν τον σύνδεσμο) ενώ μόνο ένας την ολοκλήρωσε και τελικά υπέβαλε την ένσταση (1.8% των ψηφοφόρων που επαλήθευσαν την ψήφο τους).

Στην δεύτερη έρευνα συμμετείχαν 755 χρήστες, εκ των οποίων 508 έδωσαν το email τους (το έλαβαν όμως μόνο οι 484). Από αυτούς οι 77 πάτησαν στον σύνδεσμο για να δουν τα αποτελέσματα. Στην έρευνα αυτή, όλοι οι ψηφοφόροι είδαν ως αποτέλεσμα μόνο το μη αναμενόμενο, δηλαδή τον οργανισμό που πήρε τους λιγότερους ψήφους (αυτή τη φορά 1.1% των ψήφων, έναντι του πρώτου οργανισμού ο οποίος πήρε το 60% των ψήφων). Από τους 77, οι 57 επαλήθευσαν το ψηφοδέλτιό τους. Από αυτούς 4 ξεκίνησαν και ολοκλήρωσαν την διαδικασία υποβολής ένστασης (7% των ψηφοφόρων που επαλήθευσαν την ψήφο τους).

Το προφανές συμπέρασμα που προκύπτει συγκρίνοντας τις δύο έρευνες είναι ότι όταν το αποτέλεσμα των εκλογών δεν είναι το αναμενόμενο, το ποσοστό των ψηφοφόρων που θα επαληθεύσουν την ψήφο τους είναι μεγαλύτερο. Συνδυάζοντας τα αποτελέσματα και των δύο ερευνών προκύπτει ότι το 7.5% έλεγξαν το ψηφοδέλτιό τους ενώ μόλις το 0.5% υπέβαλε κάποια ένσταση για το αποτέλεσμα των εκλογών. ΄Ενα ακόμα εύρημα της έρευνας ήταν ότι υπήρχε σημαντική συσχέτηση του αριθμού των διαδικτυακών λογαριασμών που είχαν οι χρήστες, με την πρόθεσή τους να υποβάλουν κάποια ένσταση για την διαδικασία (μετρήθηκε μέσω του ερωτηματολογίου που απάντησαν οι χρήστες). Χρήστες ο οποίοι δήλωσαν ότι έχουν περισσότερους διαδικτυακούς λογαριασμούς ήταν πιο πρόθυμοι να υποβάλουν κάποια ένσταση σε περίπτωση που η επαλήθευση αποτύχαινε. Μια ερμηνία αυτού θα μπορούσε να είναι ότι οι χρήστες ο οποίοι αλληλεπιδρούν με περισσότερες διαδικτυακές υπηρεσίες ίσως νιώθουν πιο σίγουροι να εντοπίσουν κάποιο σφάλμα στην διαδικασία και συνεπώς να υποβάλουν κάποια ένσταση.

Για να γίνει αντηληπτό πως θα μπορούσαν να επηρεάσουν τα μικρά αυτά ποσοστά μια εκλογική διαδικασία, χρησιμοποιήθηκαν ως παράδειγμα οι Γερουσιαστηκές εκλογές της πολιτείας της Minnesota

στις οποίες ο γερουσιαστής Al Franken βγήκε νικητής με διαφορά 225 ψήφων από τον δεύτερο, με τις συνολικές ψήφους των εκλογών να είναι 2,887,337. Εφαρμόζοντας τα ευρήματα της έρευνας, δηλαδή ότι ένα τυχαίο δείγμα μεγέθους 7.5% των ψηφοφόρων έλεγξε την εάν η απόδειξη της ψήφου του ήταν σωστή, τότε μια προσπάθεια αλλοίωσης του αποτελέσματος θα εντοπιζόταν με πιθανότητα 99.99%. Εάν, όμως, ληθφεί υπόψη ότι μόνο το 0.5% των ψηφοφόρων θα υποβέβαλε κάποια ένσταση τότε η πιθανότητα εντοπισμού κάποιας αλλοίωσης του αποτελέσματος μειώνεται στο 43.25%, δηλαδή είναι πιο πιθανό η αλλοίωση να μην εντοπιστεί.

Βέβαια, πρέπει να ληφθεί υπόψη ότι η ψηφοφορία πάνω στην οποία διεξήχθηκε στην έρευνα δεν ήταν μεγάλης σημασίας. Συνεπώς, αναμένεται ότι σε εκλογές στις οποίες διακυβέβονται σημαντικά ζητήματα το ποσοστό των ψηφοφόρων που θα επαληθεύσει την ψήφο του και θα υποβάλει κάποια ένσταση θα είναι μεγαλύτερο. Από την άλλη, όμως, πλευρά σε μια εκλογική διαδικασία μεγαλύτερης σημασίας είναι πιθανό η διαδικασία της επαλήθευσης και υποβολής ένστασης να είναι αρκετά πιο σύνθετη, γεγονός που δεν συμβάλει στην αύξηση των ποσοστών επαλήθευσης και υποβολής ενστάσεων. Επίσης, άλλος ένας παράγοντας που ίσως να επηρέασε τα αποτελέσματα της έρευνας είναι ότι όλοι οι συμμετέχοντες ήταν χρήστες του διαδικτύου. Αυτό δεν ισχύει για όλους τους ψηφοφόρους που συμμετέχουν στις πραγματικές εκλογές. Συνεπώς τα ποσοστά επαλήθευσης και υποβολής ενστάσεων σε πραγματικές εκλογές ενδέχεται να είναι μικρότερα λόγω της συμμετοχής χρηστών που δεν είναι εξοικειωμένοι με το διαδίκτυο. Αυτή είναι ίσως και μία ερμηνία για την μεγάλη διαφορά του ποσοστού των ψηφοφόρων που επαλήθευσε την ψήφο του στις δημοτικές εκλογές της Tahoma Park σε σχέση με τις εκλογές στο Universite Catholique de Louvain και του Πανεπιστημίου της Ottawa. Είναι πιθανό ότι το δείγμα των πολιτών που συμμετείχε στις δημοτικές εκλογές να περιήχε περισσότερους χρήστες οι οποίοι δεν ήταν εξοικειωμένοι με το διαδίκτυο και την τεχνολογία (να ήταν δηλαδή περισσότερο αντιπροσωπευτικό του συνολικού πληθυσμού) από ότι ήταν τα μέλη της Ακαδηματικής κοινώτητας και οι φοιτητές οι οποίοι συμμετείχαν στις εκλογές των πανεπιστημίων και για αυτό το ποσοστό των πολιτών που επαλήθευσαν την ψήφο τους στις δημοτικές εκλογές να ήταν τόσο μικρότερο.

Εάν ισχύει το παραπάνω τότε εισάγεται ένας νέος κίνδυνος ο οποίος μειώνει ακόμα περισσότερο την πιθανότητα εντοπισμού μιας προσπάθειας αλλοίωσης του εκλογικού αποτελέσματος. Εάν υποθέσουμε ότι συγκεκριμένες κοινωνικές ομάδες είναι λιγότερο πιθανό (λόγω χαμηλότερου μορφωτικού επιπέδου, μεγαλύτερης ηλικίας κ.α.) να επαληθεύσουν την ψήφο τους ή να υποβάλουν κάποια ένσταση, τότε

το δείγμα των ψηφοφόρων που ελέγχει τις αποδείξεις του και υποβάλλει ενστάσεις δεν είναι ούτε τυχαίο ούτε ομοιόμορφα κατανεμημένο. Αυτό σημαίνει ότι είναι εφικτό να στοχοποιηθούν συγκεκριμένοι ψηφοφόροι, οι οποίοι δεν είναι πιθανό να ελέγξουν την απόδειξή τους ή να υποβάλλουν κάποια ένσταση και η αλλοίωση να γίνει μόνο στα δικά τους ψηφοδέλτια (κάτι που είναι εφικτό αφού στα περισσότερα ακραίως επαληθεύσιμα συστήματα τα ψηφοδέλτια ρίχνονται επώνυμα στην κάλπη και ανωνυμοποιούνται μόνο πριν την καταμέτρηση).

Ο κίνδυνος αυτός είναι ακόμα μεγαλύτερος στην περίπτωση που κάποιος επιτηθέμενος αντί να αλλάξει τα ψηφοδέλτια των ψηφοφόρων που ψήφισαν, ψηφίσει εκ μέρους των ψηφοφόρων που απείχαν από τις εκλογές, δεδομένου ότι κάποιος που απείχε είναι λιγότερο πιθανό να επαληθεύσει ότι δεν υπάρχει ψήφος στο όνομά του από κάποιον που συμμετείχε στις εκλογές. ΄Οπως έχει ήδη αναφερθεί η επίθεση αυτή είναι εφικτή σε αρκετά συστήματα εκλογών, συμπεριλαμβανόμενων και των Helios και Ζευς, καθώς τα συστήματα αυτά γνωρίζουν τα στοιχεία σύνδεσης των ψηφοφόρων και μπορούν να ψηφίσουν εκ μέρους τους.

Τέλος, την ανησυχία για τα μικρά ποσοστά επαλήθευσης και υποβολής ενστάσεων έρχονται να ενισχύσουν τα αποτελέσματα δύο ακόμα μελετών. Η Maina Olembo[45] ανακάλυψε ότι οι ψηφοφόροι μπορεί αρχικά να επαληθεύσουν την ψήφο τους από περιέργεια, μετά, όμως, από συνεχή χρήση του συστήματος αυξάνεται η εμπιστοσύνη τους σε αυτό και η επαλήθευση δεν κρίνεται απαραίτητη. Επίσης, όπως ανακαλύφθηκε από τον Schneider[46], για πολλούς ψηφοφόρους η επαλήθευση της απόδειξης στον πίνακα ανακοινώσεων δεν αποτελεί κάποια εγγύηση της ασφάλειας και της ακεραιότητας του συστήματος και συνεπώς είναι πιθανό να κριθεί περιτή.

5.2 Μία ενδιαφέρουσα προσέγγιση

Προφανώς, το πρώτο στάδιο της αντιμετώπισης των προβλημάτων που περιγράφηκαν παραπάνω είναι η σωστή ενημέρωση των ψηφοφόρων για την αναγκαιότητα της επαλήθευσης και του ελέγχου καθώς και η άρτια εκπαίδευσή τους για την χρήση του συστήματος των εκλογών. Ιδιαίτερη έμφαση πρέπει να δοθεί σε κοινωνικές ομάδες οι οποίες δεν είναι εξοικειωμένες με την χρήση ηλεκτρονικών υπολογιστών.

΄Ενας άλλος τρόπος αντιμετώπισης του προβλήματος είναι η τροποποίηση της διαδικασίας επαλήθευσης έτσι ώστε να μην απαιτείται τόσο μεγάλο ή απόλυτα τυχαίο και ομοιόμορφα κατανεμημένο δείγμα

ψηφοφόρων που θα επαληθεύσουν τα ψηφοδέλτιά τους ώστε η πιθανότητα να εντοπιστεί κάποια προσπάθεια αλλοίωσης του αποτελέσματος να είναι μεγάλη. Μια ενδιαφέρουσα προσπάθεια έγινε από τους Jens-Matthias Bohli, Christian Henrich, Carmen Kempka, Jörn Müller-Quade και Stefan Röhrich[47], οι οποίοι τροποποίησαν τις αποδείξεις που λαμβάνουν οι ψηφοφόροι μετά την ψήφο τους. Η εργασία τους έγινε για συστήματα εκλογών με φυσικό θάλαμο ψηφοφορίας, και συγκεκριμένα το Bingo Voting. Χρησιμοποίησαν την ιδέα που προτάθηκε από τους Kiayias, Korman και Walluck η οποία χρησιμοποιήθηκε στο VoteBox, στην οποία αντί οι ψηφοφόροι να λαμβάνουν μία απόδειξη μόνο για την ψήφο τους, να λαμβάνουν μία απόδειξη η οποία να περιέχει και πληροφορία για τις προηγούμενες αποδείξεις.

Η υπόθεση είναι ότι μία απόδειξη περιέχει το αποτύπωμα κάποιας πληροφορίας σχετικής με την ψήφο, όπως για παράδειγμα το κρυπτοκείμενο της ψήφου. Η ιδέα είναι το αποτύπωμα αυτό να περιέχει επίσης και το αποτύπωμα της αμέσως προηγούμενης απόδειξης που δόθηκε από το σύστημα στον προηγούμενο ψηφοφόρο που ψήφισε. ΄Ετσι, δημιουργείται μια αλυσίδα αποτυπωμάτων. ΄Ετσι, όταν ένας ψηφοφόρος επαληθεύσει την απόδειξή του στον πίνακα ανακοινώσεων, επαληθεύει και όλες τις αποδείξεις των ψηφοφόρων που ψήφισαν πριν από αυτόν. Εάν έχει γίνει αλλοίωση στην ψήφο κάποιου ψηφοφόρου τότε το αποτύπωμα όλων των αποδείξεων μέχρι και αυτή της ψήφου του ψηφοφόρου που πραγματοποιεί τον έλεγχο θα είναι διαφορετικός και δεν θα ταιριάξει με αυτόν της απόδειξης. Με τον τρόπο αυτόν δεν απαιτείται μεγάλος αριθμός ψηφοφόρων να ελέγξει την απόδειξή του για να εντοπιστεί κάποια προσπάθεια αλλοίωσης του αποτελέσματος. Μάλιστα, αν η εφορευτική επιτροπή ψηφίζει τελευταία, τότε αρκεί αυτή να ελέγξει τις αποδείξεις της.

Η εφαρμογή, όμως, της μεθόδου αυτής δεν είναι προφανής σε συστήματα απομακρυσμένης ψηφοφορίας στα οποία ο θάλαμος ψηφοφορίας είναι ψηφιακός. Για παράδειγμα στην περίπτωση του Ζευς ή του Helios, η μέθοδος αυτή δεν προσφέρει κάποια πρόσθετη ασφάλεια αφού το σύστημα των εκλογών γνωρίζει τα στοιχεία σύνδεσης των ψηφοφόρων και μπορεί να ρίξει μία ψήφο εκ μέρους τους την ώρα που η κάλπη είναι ακόμα ανοιχτή, και έτσι να παραχθεί μία έγκυρη απόδειξη η οποία να προστεθεί στην αλυσίδα κατακερματισμών. Επίσης το σχήμα αυτό δεν μπορεί να εφαρμοστεί εύκολα σε συστήματα εκλογών στα οποία οι ψηφοφόροι μπορούν να ψηφίσουν πάνω από μία φορές.

Βέβαια και αυτή η μέθοδος, όπως η κλασσική μέθοδος επαλήθευσης των αποδείξεων απαιτεί να υπάρχει μια περίοδος πριν την έκδοση των αποτελεσμάτων στην οποία οι ψηφοφόροι μπορούν να επαληθεύσουν τις αποδείξεις τους και να υποβάλλουν ενστάσεις. ΄Οπως περιγράφηκε στο προηγούμενο κεφάλαιο, αυτός είναι και ο λόγος που το Ζευς δεν χρησιμοποιεί καθόλου τον πίνακα ανακοινώσεων για την

επαλήθευση των αποδείξεων. Συνεπώς, ακόμα και ένα σχήμα επαλήθευσης στο οποίο απαιτούνται λίγοι μόνο ψηφοφόροι να επαληθεύσουν τις αποδείξεις τους και να υποβάλλουν ενστάσεις δεν θα μπορούσε να εφαρμοστεί στο Ζευς.

Κεφάλαιο 6

Βελτίωση της επαληθευσιμότητας με την εισαγωγή μιας ελεγκτικής αρχής

Στόχος της παρούσας εργασίας είναι πρόταση ενός τρόπου εξασφάλισης της καταγραφής της υποβληθείσας επαληθευσιμότητας, ο οποίος να μπορεί να εφαρμοστεί σε διαδικτυακά συστήματα εκλογών απομακρυσμένης ψηφοφορίας και να καλύπτει τις ανάγκες του Ζευς.

Καθώς η καθυστέρηση του αποτελέσματος είναι ο βασικός λόγος για τον οποίο το Ζευς στερείται την επαληθεύσιμη καταγραφή της υποβληθείσας ψήφου, στόχος της εργασίας είναι η πρόταση ενός σχήματος επαλήθευσης το όποιο θα δεν απαιτεί από τους ψηφοφόρους να επαληθεύσουν οι ίδιοι τις αποδείξεις τους. Αντίθετα, θα υπάρχει μία ανεξάρτητη αρχή η οποία θα μπορεί να επαληθεύσει εκ μέρους των ψηφοφόρων ότι οι ψήφοι παρέμειναν ακέραιες. Αυτό σημαίνει ότι δεν θα υπάρχει η ανάγκη να οριστεί κάποια περίοδος επαλήθευσης και ενστάσεων αφού η ανεξάρτητη αρχή θα μπορεί να επαληθεύσει την ακεραιότητα των ψήφων αμέσως μετά το κλείσιμο των κάλπεων. Ο ψηφοφόρος δεν θα επαληθεύει ο ίδιος μεν την ψήφο του, αλλά θα εμπιστεύεται ότι τουλάχιστον ένας από τους δύο δράστες ήταν έντιμος και δεν έκλεψε. Έτσι διαμοιράζεται η εμπιστοσύνη που πρέπει να έχει ένας ψηφοφόρος για την ακεραιότητα της ψήφου του στους δύο αυτούς δράστες και η όποια προσπάθεια αλλοίωσης του αποτελέσματος για να μην γίνει αντιληπτή θα απαιτεί την συνεργασία και των δύο δραστών.

6.1 Το προτεινόμενο πρωτόκολλο

΄Οπως ήδη αναφέρθηκε, στόχος της εργασίας είναι η εισαγωγή μιας νέας ανεξάρτητης αρχή η οποία συμμετέχει στην διαδικασία με τη δική της υπηρεσία, με βασική αποστολή την αυτόματη επαλήθευση όλων των αποδείξεων.

Για να γίνει αυτό εφικτό, η αρχή πρέπει με κάποιο τρόπο να λάβει τις αποδείξεις των ψήφων των ψηφοφόρων. ΄Οπως συζητήθηκε στην προηγούμενη ενότητα, το σενάριο οι ψηφοφόροι να παραδίδουν τις αποδείξεις τους στην αρχή δεν είναι κάτι εύχρηστο και εφικτό στην περίπτωση της απομακρυσμένης ψηφοφορίας. Συνεπώς η αποστολή των αποδείξεων στην αρχή πρέπει να γίνεται αυτόματα. ΄Ενας τρόπος είναι να τις αποστέλλει το ίδιο το Ζευς.

΄Ετσι λοιπόν μετά την υποβολή μιας ψήφου από έναν ψηφοφόρο, το Ζευς δεν αποστέλλει την απόδειξη μόνο στον ψηφοφόρο αλλά την προωθεί και στην Ανεξάρτητη Αρχή. ΄Ετσι η Αρχή μπορεί να συγκεντρώσει όλες τις αποδείξεις.

Η μέθοδος αυτή αν και εύχρηστη δεν προσφέρει ουσιαστική ασφάλεια στο πρωτόκολλο. Αυτό γιατί ακόμα και αν η Αρχή είναι ο δράστης που πραγματοποιεί την επαλήθευση, το Ζευς εξακολουθεί να έχει τον έλεγχο όλης της διαδικασίας αφού αυτό στέλνει τις αποδείξεις στην Αρχή. Συνεπώς, θα μπορούσε εξαρχής να αλλοιώνει τις ψήφους και να δημιουργεί πλαστές αποδείξεις τις οποίες στη συνέχεια να προωθεί στην αρχή. Το αποτέλεσμα θα ήταν η αρχή να επαληθεύει επιτυχώς τις αποδείξεις που τις έστειλε το Ζευς, οι οποίες όμως δεν θα αντιστοιχούσαν στις πραγματικές ψήφους των πολιτών.

Ο λόγος που συμβαίνει αυτό είναι γιατί η αρχή έχει παθητικό χαρακτήρα στο πρωτόκολλο. Για να διαμοιραστεί πραγματικά η εμπιστοσύνη του ψηφοφόρου ανάμεσα στην Αρχή και το Ζευς, πρέπει η αρχή να συμμετέχει ενεργά στο πρωτόκολλο. Μια διαδικασία στην οποία η Αρχή μπορεί να διαδραματίσει ουσιαστικό ρόλο είναι η ψήφος ελέγχου που υποστηρίζει το Ζευς.

΄Οπως αναφέρθηκε στην ενότητα 4, ο ψηφοφόρος μπορεί να στείλει μαζί με την κρυπτογραφημένη ψήφο του έναν κωδικό ελέγχου. Εάν ο κωδικός ελέγχου είναι σωστός, τότε η ψήφος του υποβάλλεται κανονικά στην κάλπη. Εάν είναι λάθος, τότε το περιεχόμενο της ψήφου του αποκαλύπτεται. Η χρησιμότητα των ψήφων ελέγχου είναι για να προστατεύουν τον ψηφοφόρο από τυχόν κακόβουλο λογισμικό που έχει εγκατασταθεί στον υπολογιστή του και αλλοιώνει την ψήφο του. Χωρίς την γνώση του σωστού κωδικού ελέγχου το κακόβουλο λογισμικό δεν μπορεί να γνωρίζει εάν η ψήφος που στέλνει ο ψηφοφόρος θα καταμετρηθεί στο αποτέλεσμα ή θα είναι ψήφος ελέγχου και τα πε-

ριεχόμενά της θα αποκαλυφθούν. Συνεπώς, δεν μπορεί να γνωρίζει πότε να αλλοιώσει την ψήφο χωρίς να πιαστεί και πότε όχι.

Στο παρόν πρωτόκολλο του Ζευς, οι ψήφοι ελέγχου δημιουργούνται και αποστέλλονται στους ψηφοφόρος από το Ζευς. Επίσης, και ο έλεγχος εάν ο κωδικός είναι σωστός ή όχι γίνεται από το Ζευς. Στο προτεινόμενο πρωτόκολλο η δημιουργία και η αποστολή των κωδικών ελέγχου γίνεται από την Ανεξάρτητη Αρχή. Το Ζευς δεν έχει πρόσβαση στους κωδικούς.

΄Ετσι όταν ο ψηφοφόρος υποβάλει μία ψήφο με κωδικό ελέγχου, το Ζευς δεν μπορεί να αποφανθεί εάν πρόκειται για ψήφο ελέγχου ή κανονική. Για τον λόγο αυτό δημιουργεί την απόδειξη της ψήφου και την προωθεί στην Αρχή μαζί με τον κωδικό ελέγχου. Η Αρχή ελέγχει τον κωδικό ελέγχου και ενημερώνει το Ζευς. Εάν πρόκειται για ψήφου ελέγχου το Ζευς ζητάει από τον περιηγητή του ψηφοφόρου να του παραδώσει την τυχαιότητα με την οποία κρυπτογράφησε την ψήφο και στη συνέχεια την προωθεί στην Ανεξάρτητη Αρχή. Η Αρχή αποκρυπτογραφεί την ψήφο και στέλνει στον ψηφοφόρο τα περιεχόμενα της. Εάν δεν πρόκειται για ψήφο ελέγχου τότε η Αρχή ενημερώνει το Ζευς να καταμετρήσει την ψήφο και στέλνει η ίδια την απόδειξη στον ψηφοφόρο. Συνεπώς η Ανεξάρτητη αρχή ελέγχει και την αποστολή των αποδείξεων στους ψηφοφόρους.

Ο λόγος που πλέον η εμπιστοσύνη διαμοιράζεται μεταξύ της Αρχής και του Ζευς είναι γιατί πλέον οι κωδικοί ελέγχου δεν ελέγχουν μόνο τον περιηγητή αλλά και το Ζευς. Οι κωδικοί ελέγχου προστάτευαν τον χρήστη από κακόβουλο λογισμικό στον υπολογιστή του επειδή εισήγαγαν αβεβαιότητα για το μέλλον της ψήφου, ενώ ταυτόχρονα δέσμευαν το περιηγητή σε μία κρυπτογράφηση του ψηφοδελτίου - αυτή που έστελνε μαζί με τον κωδικό ελέγχου. Το ίδιο συμβαίνει τώρα και με το Ζευς. ΄Ενα “κακόβουλο” Ζευς μη γνωρίζοντας το μέλλον της ψήφου, δεν μπορεί να αποφασίσει αν είναι ασφαλές να την αλλοιώσει ή όχι ενώ ταυτόχρονα δεσμεύεται στο κρυπτοκείμενο της ψήφου που έστειλε ο χρήστης αφού το προωθεί υπογεγραμμένο στην Αρχή.

Από την άλλη πλευρά, η Αρχή δεν μπορεί από μόνη της να αλλοιώσει το αποτέλεσμα των εκλογών. Αυτό γιατί τα ψηφοδέλτια των ψηφοφόρων παραδίδονται πρώτα στο Ζευς και μετά στην Αρχή. ΄Ετσι η Αρχή δεν μπορεί να αλλοιώσει κάποιο ψηφοδέλτιο και να το στείλει στην ψηφιακή κάλπη.

6.2 Αναλυτική περιγραφή του πρωτοκόλλου

6.2.1 Προετοιμασία των εκλογών

Η προετοιμασία των εκλογών γίνεται όπως και στο αρχικό πρωτόκολλο του Ζευς. Η μόνη διαφοροποίηση του νέου πρωτοκόλλου είναι ότι το Ζευς δεν δημιουργεί κωδικούς ελέγχου για τους ψηφοφόρους.

1. Η Αρχή δημιουργεί ζεύγος δημοσίου και ιδιωτικού κλειδιού. Τα κλειδιά αυτά θα χρησιμοποιηθούν για την επαλήθευση και δημιουργία υπογραφών εκ μέρους της Αρχής.

2. Γίνεται ανταλλαγή του δημοσίου κλειδιού του Ζευς (με το οποίο μπορεί να γίνει επαλήθευση των υπογραφών που δημιουργεί του Ζευς) με το δημόσιο κλειδί της Αρχής. Επίσης το δημόσιο κλειδί της Αρχής δημοσιοποιείται.

3. Το Ζευς στέλνει στην Αρχή τις παραμέτρους των εκλογών (το όνομα της ψηφοφορίας, το αναγνωριστικό της και το ψηφοδέλτιο) καθώς και τον εκλογικό κατάλογο (μαζί με τα στοιχεία επικοινωνίας των ψηφοφόρων). ΄Ολα τα παραπάνω δεδομένα υπογράφονται με το ιδιωτικό κλειδί του Ζευς.

4. Η Αρχή δημιουργεί και υπογράφει τους κωδικούς ελέγχου και τους στέλνει στους ψηφοφόρους.

6.2.2 Η ψηφοφορία

Από την πλευρά του χρήστη δεν υπάρχει καμία διαφοροποίηση στον τρόπο ψηφοφορίας. Η διαφοροποίηση γίνεται ορατή μόνο από την πλευρά του Ζευς:

1. Ο ψηφοφόρος χρησιμοποιεί τον μυστικό σύνδεσμο που έλαβε από το Ζευς για να συνδεθεί και να ψηφίσει.

2. Επιλέγει τους υποψηφίους που επιθυμεί και προχωράει στην κρυπτογράφηση της ψήφου του.

3. Πριν την υποβολή της έχει την δυνατότητα να υποβάλει μαζί της και έναν κωδικό ελέγχου. Τους κωδικούς ελέγχου τους έχει λάβει σε ξεχωριστό μήνυμα ηλεκτρονικού ταχυδρομείου από την Αρχή.

Πρώτη περίπτωση: Ο ψηφοφόρος δεν υποβάλει κωδικό ελέγχου. Στην περίπτωση αυτή η ψήφος του πρέπει να καταμετρηθεί κανονικά.

1. Το Ζευς λαμβάνει την κρυπτογραφημένη ψήφο του ψηφοφόρου, την ρίχνει στην ψηφιακή κάλπη και δημιουργεί την απόδειξη (την οποία και υπογράφει).

2. Στέλνει την απόδειξη στην Αρχή.

3. Η Αρχή αφού δεν έλαβε κάποιον κωδικό ελέγχου απλά υπογράφει και προωθεί την απόδειξη στον ψηφοφόρο.

Δεύτερη περίπτωση: Ο ψηφοφόρος εισάγει έγκυρο κωδικό ελέγχου. Και σε αυτή την περίπτωση η ψήφος του πρέπει να καταμετρηθεί κανονικά.

1. Το Ζευς λαμβάνει την κρυπτογραφημένη ψήφο του ψηφοφόρου και τον κωδικό ελέγχου. Δεν ρίχνει την ψήφο στην ψηφιακή κάλπη καθώς δεν γνωρίζει εάν πρόκειται για ψήφο ελέγχου ή όχι.

2. Δημιουργεί την απόδειξη για την ψήφο και την προωθεί στην Αρχή μαζί με τον κωδικό ελέγχου (υπογράφοντας και τα δύο δεδομένα).

3. Η Αρχή ελέγχει τον κωδικό.

4. Αφού ο κωδικός ήταν σωστός ενημερώνει το Ζευς ότι πρόκειται για έγκυρη ψήφο. Το μήνυμα που στέλνει στο Ζευς είναι υπογεγραμμένο με το ιδιωτικό κλειδί της Αρχής.

5. Το Ζευς επαληθεύει την εγκυρότητα της υπογραφής του μηνύματος της Αρχής και καταμετρά την ψήφο.

6. Η Αρχή υπογράφει και προωθεί την απόδειξη στον ψηφοφόρο.

Τρίτη περίπτωση: Ο ψηφοφόρος εισάγει λανθασμένο κωδικό ελέγχου, δηλαδή υποβάλει μία ψήφο ελέγχου της οποίας τα περιεχόμενα πρέπει να αποκαλυφθούν.

1. Το Ζευς λαμβάνει την κρυπτογραφημένη ψήφο του ψηφοφόρου και τον κωδικό ελέγχου. Δεν ρίχνει την ψήφο στην ψηφιακή κάλπη καθώς δεν γνωρίζει εάν πρόκειται για ψήφο ελέγχου ή όχι.

2. Δημιουργεί την απόδειξη για την ψήφο και την προωθεί στην Αρχή μαζί με τον κωδικό ελέγχου (υπογράφοντας και τα δύο δεδομένα).

3. Η Αρχή ελέγχει τον κωδικό.

4. Αφού ο κωδικός είναι λάθος, ενημερώνει το Ζευς ότι πρόκειται για ψήφο ελέγχου. Το μήνυμα που στέλνει στο Ζευς είναι υπογεγραμμένο με το ιδιωτικό κλειδί της Αρχής.

5. Το Ζευς επαληθεύει την εγκυρότητα της υπογραφής του μηνύματος της Αρχής και ζητά από τον ψηφοφόρο να επιβεβαιώσει ότι όντως επιθυμεί να ρίξει μια ψήφο ελέγχου.

6. Εάν ο ψηφοφόρος απαντήσει θετικά, το Ζευς ζητά από τον περιηγητή του χρήστη να παραδώσει την τυχαιότητα με την οποία κρυπτογραφήθηκε η ψήφος. Εάν απαντήσει αρνητικά τότε η διαδικασία είναι όμοια με αυτή της πρώτης περίπτωσης.

7. Το Ζευς υπογράφει και προωθεί την τυχαιότητα στην Αρχή.

8. Η Αρχή αποκρυπτογραφεί την ψήφο, υπογράφει το περιεχόμενο της και το στέλνει στον ψηφοφόρο, μαζί με την απόδειξη της ψήφου.

6.2.3 Επαλήθευση μετά το κλείσιμο των καλπών

Μετά το κλείσιμο των καλπών και πριν ξεκινήσει η διαδικασία της μίξης πρέπει να γίνει η επαλήθευση της εγκυρότητας των αποδείξεων των ψηφοφόρων. Μόλις ο διαχειριστής των εκλογών λήξει τις εκλογές, εκτελούνται οι ακόλουθες λειτουργίες:

1. Το Ζευς ενημερώνει την αρχή ότι οι εκλογές έληξαν.

2. Το Ζευς δημιουργεί ένα συμπιεσμένο αρχείο με τις αποδείξεις όλων των ψήφων που υποβλήθηκαν στην ψηφιακή κάλπη. Στο αρχείο αυτό προσθέτει τα δεδομένα των παραμέτρων των εκλογών, το ψηφοδέλτιο και το αποτύπωμα του εκλογικού καταλόγου. Το αρχείο αυτό το υπογράφει με το ιδιωτικό του κλειδί.

3. Στέλνει το αρχείο αυτό στην Ανεξάρτητη Αρχή.

4. Η Αρχή επαληθεύει την εγκυρότητα της υπογραφής

5. Εάν η υπογραφή είναι έγκυρη, τότε αποσυμπιέζει το αρχείο.

6. Ελέγχει αρχικά ότι οι παράμετροι των εκλογών και το αποτύπωμα του εκλογικού καταλόγου ταιριάζουν με τα δεδομένα που έλαβε πριν τις εκλογές από το Ζευς.

7. Στη συνέχεια συγκρίνει όλες τις αποδείξεις που έλαβε κατά την διάρκεια των εκλογών με αυτές που περιέχονται στο συμπιεσμένο αρχείο.

8. Εάν η επαλήθευση επιτύχει, τότε η Αρχή δημιουργεί ένα αρχείο PDF το οποίο περιέχει τις παραμέτρους των εκλογών, τον αριθμό των αποδείξεων, το αποτύπωμα του εκλογικού καταλόγου και το αποτύπωμα της λίστας όλων των αποδείξεων.

9. Το αρχείο αυτό το υπογράφει και το στέλνει στο Ζευς.

10. Το Ζευς προσθέτει το αρχείο αυτό στα πρακτικά των εκλογών.

Ταυτόχρονα με την παραπάνω διαδικασία το Ζευς μπορεί να επαληθεύσει και αυτό την εγκυρότητα των αποδείξεων (κάτι που βέβαια είναι περιττό μετά την εισαγωγή της Αρχής). Αφού λάβει την πιστοποίηση από την Ανεξάρτητη Αρχή, μπορεί να συνεχίσει το αρχικό πρωτόκολλο λειτουργίας του και να ξεκινήσει την μίξη των ψηφοδελτίων.

6.3 Τεχνικές λεπτομέρειες

Οι βασικές λειτουργίες που εκτελεί η αρχή (δημιουργία των κωδικών ελέγχου, έλεγχος κωδικών, αποστολή email, επαλήθευση υπογραφών και υπογραφή δεδομένων) είναι λειτουργίες που στο αρχικό πρωτόκολλο εκτελούνταν από το Ζευς. Συνεπώς, ο κώδικας που υλοποιεί τις παραπάνω λειτουργίες υπάρχει ήδη στο Ζευς. Για την αξιοποίηση αυτών των έτοιμων μεθόδων είναι απαραίτητο το σύστημα της Ανεξάρτητης Αρχής να έχει παρόμοια αρχιτεκτονική με το Ζευς. ΄Ετσι, όπως και το Ζευς, η ανάπτυξη του συστήματος της Αρχής γίνεται σε γλώσσα Python[48] με χρήση του Django Framework[49].

Η χρήση της Python και του Django για την εκμετάλλευση των υπαρχόντων μεθόδων του Ζευς δεν υποβαθμίζει το πρωτόκολλο. Αντίθετα είναι μια ασφαλής επιλογή καθώς τόσο η Python όσο και το Django είναι ευρέως διαδεδομένα για την ανάπτυξη διαδικτυακών εφαρμογών.

Ως πρωτόκολλο επικοινωνίας μεταξύ του Ζευς επιλέχθηκε το ασφαλές HTTPS. Ο λόγος επιλογής του ήταν η ασφάλεια που παρέχει αλλά κυρίως η ευκολία της υλοποίησης και απλότητα της χρήσης του. Ο εξυπηρετητής του Ζευς ήδη χρησιμοποιεί το HTTPS για την επικοινωνία με τους ψηφοφόρους, τους διαχειριστές και την εφορευτική επιτροπή. ΄Ετσι δεν απαιτείται κάποια ιδιαίτερη ρύθμιση του εξυπηρετητή του Ζευς για την επικοινωνία του με την Ανεξάρτητη Αρχή. Από την άλλη πλευρά, είναι σημαντικό η υλοποίηση ενός εξυπηρετητή ο οποίος θα διαδραματίζει τον ρόλο της Ανεξάρτητης Αρχής να είναι εύκολη. Το HTTPS υποστηρίζεται από όλες τις εταιρίες που παρέχουν web hosting και συνεπώς ήταν η προτιμότερη επιλογή.

Παρόλο που το HTTPS κρυπτογραφεί τα δεδομένα και πιστοποιεί την ταυτότητα των χρηστών, επιλέχθηκε να υλοποιηθεί από άκρη σε άκρη κρυπτογράφηση των δεδομένων, πέρα από αυτή που χρησιμοποιεί το πρωτόκολλο. Αυτό σημαίνει ότι και το Ζευς και η Αρχή κρυπτογραφούν τα δεδομένα πριν τα στείλουν.

6.4 Οι απαραίτητες αλλαγές στο Ζευς

΄Ενα από τα πλεονεκτήματα αυτού του πρωτοκόλλου είναι ότι δεν απαιτεί καμία αλλαγή στον ψηφιακό θάλαμο εκλογών και στην εμπειρία του ψηφοφόρου κατά την διάρκεια της ψηφοφορίας. ΄Ολες οι αλλαγές γίνονται στο γραφικό περιβάλλον που βλέπει ο διαχειριστής του Ζευς.

6.4.1 Γραφικό περιβάλλον προετοιμασίας εκλογών

Υποθέτουμε ότι ο εξυπηρετητής της Ανεξάρτητης Αρχής έχει δημιουργηθεί και ρυθμιστεί κατάλληλα. Αυτό σημαίνει ότι η αρχή έχει δημιουργήσει το ιδιωτικό και δημόσιο κλειδί της καθώς και έναν μοναδικό κωδικό μιας χρήσης. Ο κωδικός αυτός πρέπει να σταλεί χειροκίνητα από τον διαχειριστή της Αρχής στον διαχειριστή του Ζευς. Η αρχή επίσης έχει μία διεύθυνση URL.

Στο γραφικό περιβάλλον του διαχειριστή του Ζευς είναι απαραίτητη η προσθήκη μίας φόρμας στην οποία ο διαχειριστής εισάγει την διεύθυνση της Ανεξάρτητης Αρχής και τον μοναδικό κωδικό μίας χρήσης. Με την υποβολή της φόρμας το Ζευς επικοινωνεί με την Αρχή και την ενημερώνει ότι θα χρησιμοποιηθεί για την επαλήθευση των ψηφοδελτίων της συγκεκριμένης ψηφοφορίας (εφόσον ο κωδικός που έστειλε ήταν σωστός). Επίσης στέλνει στην αρχή το αναγνωριστικό της ψηφοφορίας και δημόσιο κλειδί υπογραφής του. Από την πλευρά της η Αρχή απαντάει με το δικό της δημόσιο κλειδί υπογραφής.

Ο διαχειριστής έχει και την επιλογή να αφήσει την φόρμα κενή. Σε αυτή την περίπτωση το Ζευς θα χρησιμοποιήσει μία τοπική έκδοση της Ανεξάρτητης Αρχής η οποία τρέχει στον δικό του εξυπηρετητή. Ο διαχειριστής του Ζευς έχει την δυνατότητα να αφαιρέσει την Ανεξάρτητη Αρχή και να προσθέσει κάποια άλλη. Κατά την αφαίρεση το Ζευς επικοινωνεί με την αρχή και την ενημερώνει ότι δεν θα συμμετέχει στις εκλογές αυτές.

΄Οταν ο διαχειριστής οριστικοποιήσει τις εκλογές, το Ζευς επικοινωνεί αυτόματα με την Ανεξάρτητη Αρχή και της στέλνει το όνομα των εκλογών, το ψηφοδέλτιο και τον εκλογικό κατάλογο. Η Αρχή αμέσως δημιουργεί τους κωδικούς ελέγχου και τους στέλνει στους ψηφοφόρους.

Μετά την έναρξη των εκλογών από τον διαχειριστή, το Ζευς επικοινωνεί αυτόματα με την Αρχή και την ενημερώνει ότι μπορεί να ξεκινήσει να δέχεται ψηφοδέλτια. Το Ζευς προωθεί αυτόματα τα ψηφοδέλτια και τους κωδικούς ελέγχου στην Αρχή.

6.4.2 Περιβάλλον λήξης εκλογών

΄Οταν ο διαχειριστής λήξει τις εκλογές, το Ζευς ενημερώνει αυτόματα την Ανεξάρτητη Αρχή. Η Αρχή περιμένει πλέον έναν μυστικό σύνδεσμο από το Ζευς με τον οποίο θα κατεβάσει όλα τα ψηφοδέλτια που περιέχει η ψηφιακή κάλπη του Ζευς. Μόλις το Ζευς δημιουργήσει το αρχείο αυτό το στέλνει αυτόματα στην Αρχή. Τότε η Αρχή εκτελεί αυτόματα την επαλήθευση.

Στο γραφικό περιβάλλον του διαχειριστή υπάρχει σχετική επισήμανση ότι το αρχείο στάλθηκε στην Αρχή και ότι το Ζευς αναμένει την απάντηση της. Μόλις η Αρχή ο ολοκληρώσει την επαλήθευση και στείλει το υπογεγραμμένο PDF στο Ζευς, τότε το Ζευς συνεχίζει το πρωτόκολλό του κανονικά. Ο διαχειριστής έχει την δυνατότητα να κατεβάσει το υπογεγραμμένο PDF και να το προσθέσει στα πρακτικά των εκλογών.

6.5 Προκλήσεις και επόμενα βήματα

Το προτεινόμενο πρωτόκολλο αντιμετωπίζει μεν αποτελεσματικά ένα σημαντικό ζήτημα για το Ζευς, όμως, αυξάνει σε ένα βαθμό την πολυπλοκότητα της εκλογικής διαδικασίας από την πλευρά του ψηφοφόρου. Ο βασικός λόγος που συμβαίνει αυτό είναι γιατί οι ψηφοφόροι λαμβάνουν πλέον δύο μηνύματα, ένα από το Ζευς και ένα από την Αρχή. Επιπρόσθετα, καθώς οι κωδικοί ελέγχου διαδραματίζουν καθοριστικό ρόλο για την λειτουργία του πρωτοκόλλου, απαιτείται η χρήση τους από περισσότερους ψηφοφόρους. ΄Ετσι, ενώ στο αρχικό πρωτόκολλο οι κωδικοί ελέγχου ήταν μια λειτουργία που απλά έλεγχε τον περιηγητή του ψηφοφόρου στο διαδίκτυο και μπορούσε να αγνοηθεί, τώρα αποτελούν ένα βασικό συστατικό της επαληθευσιμότητας του πρωτοκόλλου και είναι σημαντικό να χρησιμοποιούνται. Από την άλλη πλευρά βέβαια, η Αρχή στο ξεχωριστό μήνυμα που στέλνει στους ψηφοφόρους έχει την πολυτέλεια να μπορεί να επεξηγήσει την διαδικασία και να δώσει σαφείς οδηγίες για την σωστή χρήση των κωδικών.

Μία άλλη πρόκληση που αντιμετωπίζει το πρωτόκολλο είναι ότι απαιτεί την δημιουργία ενός εξυπηρετητή ο οποίος θα παίζει τον ρόλο της Ανεξάρτητης Αρχής. Αυτό σημαίνει ότι η Ανεξάρτητη Αρχή πρέπει να διαθέτει τεχνικές γνώσεις ή να έχει την οικονομική δυνατότητα να πληρώσει κάποιον μηχανικό για την δημιουργία του εξυπηρετητή. Επίσης, η Αρχή πρέπει να είναι σε θέση να διασφαλίσει ότι ο εξυπηρετητής της θα λειτουργεί σωστά καθ όλη την διάρκεια των εκλογών. Αυτό γιατί η εκλογική διαδικασία είναι πλέον άρρηκτα συνδεδεμένη με τον εξυπηρετητή της Αρχής. Εάν ο εξυπηρετητής της Αρχής δυσλειτουργήσει, τότε το Ζευς δεν θα μπορεί να διεξάγει τις εκλογές αφού

δεν θα είναι σε θέση να γνωρίζει εάν οι ψηφοφόροι υποβάλλουν κανονικές ψήφους ή ψήφους ελέγχου, ενώ από την άλλη θα δημιουργηθεί σύγχυση στους ψηφοφόρους καθώς δεν θα λαμβάνουν αποδείξεις για τις ψήφους τους.

Το προτεινόμενο πρωτόκολλο επιδέχεται επιπλέον μελέτη και επεκτάσεις. Μία μελλοντική επέκταση θα μπορούσε να είναι για παράδειγμα η δυνατότητα χρήσης πολλαπλών Ανεξάρτητων Αρχών ώστε εάν κάποια δυσλειτουργήσει να μπορούν να την καλύψουν οι υπόλοιπες. ΄Αλλη επέκταση θα μπορούσε να είναι η δυνατότητα χρήσης διαφορετικού καναλιού επικοινωνίας της αρχής με τους ψηφοφόρους, όπως για παράδειγμα τα SMS. Βέβαια αυτό θα αύξανε την πολυπλοκότητα δεδομένου του γεγονότος ότι η Αρχή θα έπρεπε να συνεργαστεί με κάποιο πάροχο υπηρεσιών SMS.

Μία άλλη κατεύθυνση προς την οποία θα μπορούσε να επεκταθεί το πρωτόκολλο είναι η συμμετοχή της Αρχής και σε άλλα σημεία της εκλογικής διαδικασίας, όπως για παράδειγμα η ταυτοποίηση των χρηστών στο Ζευς ή η υποστήριξη του ψηφιακού θαλάμου ψηφοφορίας. Μάλιστα θα μπορούσε σε κάθε ένα από τα παραπάνω σημεία να συμμετέχει και διαφορετική Ανεξάρτητη Αρχή, διαμοιράζοντας έτσι την εμπιστοσύνη σε ακόμα περισσότερους δράστες.

6.6 Υλοποίηση και επιπλέον υλικό

Η υλοποίηση, οι επόμενες προσθήκες του πρωτοκόλλου καθώς και οποιοδήποτε επιπλέον σχετικό υλικό θα δημοσιεύονται στον ακόλουθο σύνδεσμο: https://github.com/dimter/zeus-independent-verifier

Βιβλιογραφία

[1] David L. Chaum: *Untraceable electronic mail, return addresses, and digital pseudonyms*. Commun. ACM, 24(2):84–90, February 1981, ISSN 0001-0782. http://doi.acm.org/10.1145/358549.358563.

[2] L. F. Cranor and R. K. Cytron: *Sensus: a security-conscious electronic polling system for the internet*. In *System Sciences, 1997, Proceedings of the Thirtieth Hawaii International Conference on*, volume 3, pages 561–570 vol.3, Jan 1997.

[3] Wikipedia: *United States presidential election, 2000 — Wikipedia, the free encyclopedia*. http://en.wikipedia.org/w/index.php?title=United%20States%20presidential%20election%2C%202000&oldid=745848063, 2016. [Online; accessed 24-October-2016].

[4] Wikipedia: *Help America Vote Act — Wikipedia, the free encyclopedia*. http://en.wikipedia.org/w/index.php?title=Help%20America%20Vote%20Act&oldid=737163556, 2016. [Online; accessed 24-October-2016].

[5] Kevin J Coleman and Eric A Fischer: *The help america vote act and elections reform: Overview and issues*. Congressional research service, 2011.

[6] Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten: *Security analysis of the diebold accuvote-ts voting machine*. In *Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology*, EVT'07, pages 2–2, Berkeley, CA, USA, 2007. USENIX Association. http://dl.acm.org/citation.cfm?id=1323111.1323113.

[7] Scott Wolchok, Eric Wustrow, J. Alex Halderman, Hari K. Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati, and Rop Gonggrijp: *Security analysis of india's electronic voting machines*. In *Proceedings of the 17th ACM Conference on Computer and Communications Security*, CCS '10, pages 1–14, New York, NY, USA, 2010. ACM, ISBN 978-1-4503-0245-6. http://doi.acm.org/10.1145/1866307.1866309.

[8] Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J. Alex Halderman: *Security analysis of the estonian internet voting system*. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, pages 703–715, New York, NY, USA, 2014. ACM,

ISBN 978-1-4503-2957-6. http://doi.acm.org/10.1145/2660267.2660315.

[9] *Accurate voting*. http://accurate-voting.org/. Accessed: 2016-10-24.

[10] *Iavoss*. http://www.iavoss.org/. Accessed: 2016-10-24.

[11] Wikipedia: *Mix network — Wikipedia, the free encyclopedia*. http://en.wikipedia.org/w/index.php?title=Mix%20network&oldid=745085549, 2016. [Online; accessed 24-October-2016].

[12] *Cryptanalysis of a universally verifiable efficient re-encryption mixnet*. In *Presented as part of the 2012 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections*, Berkeley, CA, 2012. USENIX. https://www.usenix.org/conference/evtwote12/workshop-program/presentation/Khazaei.

[13] Wikipedia: *Zero-knowledge proof — Wikipedia, the free encyclopedia*. http://en.wikipedia.org/w/index.php?title=Zero-knowledge%20proof&oldid=741730558, 2016. [Online; accessed 24-October-2016].

[14] Wikipedia: *Commitment scheme — Wikipedia, the free encyclopedia*. http://en.wikipedia.org/w/index.php?title=Commitment%20scheme&oldid=744732618, 2016. [Online; accessed 24-October-2016].

[15] Wikipedia: *Hash function — Wikipedia, the free encyclopedia*. http://en.wikipedia.org/w/index.php?title=Hash%20function&oldid=745198457, 2016. [Online; accessed 24-October-2016].

[16] D. Chaum: *Secret-ballot receipts: True voter-verifiable elections*. IEEE Security Privacy, 2(1):38–47, Jan 2004, ISSN 1540-7993.

[17] D. Chaum, A. Essex, R. Carback, J. Clark, S. Popoveniuc, A. Sherman, and P. Vora: *Scantegrity: End-to-end voter-verifiable optical- scan voting*. IEEE Security Privacy, 6(3):40–46, May 2008, ISSN 1540-7993.

[18] D. Chaum, R. T. Carback, J. Clark, A. Essex, S. Popoveniuc, R. L. Rivest, P. Y. A. Ryan, E. Shen, A. T. Sherman, and P. L. Vora: *Scantegrity ii: End-to-end verifiability by voters of optical scan elections through confirmation codes*. IEEE Transactions on Information Forensics and Security, 4(4):611–627, Dec 2009, ISSN 1556-6013.

[19] Richard Carback, David Chaum, Jeremy Clark, John Conway, Aleksander Essex, Paul S. Herrnson, Travis Mayberry, Stefan Popoveniuc, Ronald L. Rivest, Emily Shen, Alan T. Sherman, and Poorvi L. Vora: *Scantegrity ii municipal election at takoma park: The first e2e binding governmental election with ballot privacy*. In *Presented as part of the 19th USENIX Security Symposium*. USENIX Association, 2010.

[20] Ben Adida and C Andrew Neff: *Ballot casting assurance.* EVT, 6:7, 2006.

[21] S. Neumann and M. Volkamer: *Civitas and the real world: Problems and solutions from a practical point of view*. In *Availability, Reliability and Security (ARES), 2012 Seventh International Conference on*, pages 180–185, Aug 2012.

[22] Ben Adida: *Helios: Web-based open-audit voting*. In *USENIX Security Symposium*, volume 17, pages 335–348, 2008.

[23] Ari Juels, Dario Catalano, and Markus Jakobsson: *Coercion-resistant electronic elections*. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, pages 61–70. ACM, 2005.

[24] Stephan Neumann, Christian Feier, Melanie Volkamer, and Reto E Koenig: *Towards a practical jcj/civitas implementation.* IACR Cryptology ePrint Archive, 2013:464, 2013.

[25] Josh Benaloh: *Simple verifiable elections.* EVT, 6:5–5, 2006.

[26] Ben Adida, Olivier De Marneffe, Olivier Pereira, Jean Jacques Quisquater, *et al.*: *Electing a university president using open-audit voting: Analysis of real-world use of helios*. EVT/WOTE, 9:10–10, 2009.

[27] Dan Morrell: *Secret ballots, verifiable votes*. `http://harvardmagazine.com/2010/05/secret-ballots-verifiable-votes`, 2010.

[28] Syed Taha Ali and Judy Murray: *An overview of end-to-end verifiable voting systems*. CoRR, abs/1605.08554, 2016. `http://arxiv.org/abs/1605.08554`.

[29] Stuart Haber, Josh Benaloh, and Shai Halevi: *The helios e-voting demo for the iacr*. IACR, May, 2010.

[30] Oracle Corporation: *Java programming language*. `https://www.java.com/en/`.

[31] Warren D. Smith: *Three voting protocols: Threeballot, vav, and twin*. In Ray Martinez and David Wagner (editors): *2007 USENIX/ACCURATE Electronic Voting Technology Workshop, EVT'07, Boston, MA, USA, August 6, 2007*. USENIX Association, 2007. `https://www.usenix.org/conference/evt-07/three-voting-protocols-threeballot-vav-and-twin`.

[32] Aleksander Essex, Jeremy Clark, and Carlisle Adams: *Aperio: High integrity elections for developing countries*. In David Chaum, Markus Jakobsson, Ronald L. Rivest, Peter Y. A. Ryan, Josh Benaloh, Miroslaw Kutylowski, and Ben Adida (editors): *Towards Trustworthy Elections, New Directions in Electronic Voting*, volume 6000 of *Lecture Notes in Computer Science*, pages 388–401. Springer, 2010, ISBN 978-3-642-12979-7. `http://dx.doi.org/10.1007/978-3-642-12980-3_24`.

[33] Harvey Jones, Jason Juang, and Greg Belote: *Threeballot in the field*. Term paper for MIT course, 6, 2006.

[34] J. Benaloh, T. Moran, L. Naish, K. Ramchen, and V. Teague: *Shufflesum: Coercion-resistant verifiable tallying for stv voting*. IEEE Transactions on Information Forensics and Security, 4(4):685–698, Dec 2009, ISSN 1556-6013.

[35] Philippe Bulens, Damien Giry, and Olivier Pereira: *Running mixnet-based elections with helios*. In Shacham, Hovav and Vanessa Teague [50]. https://www.usenix.org/conference/evtwote-11/running-mixnet-based-elections-helios.

[36] Fatih Karayumak, Maina M. Olembo, Michaela Kauer, and Melanie Volkamer: *Usability analysis of helios - an open source verifiable remote electronic voting system*. In Shacham, Hovav and Vanessa Teague [50]. https://www.usenix.org/conference/evtwote-11/usability-analysis-helios-%E2%80%94-open-source-verifiable-remote-electronic-voting.

[37] Saghar Estehghari and Yvo Desmedt: *Exploiting the client vulnerabilities in internet e-voting systems: Hacking helios 2.0 as an example*. In Douglas W. Jones, Jean-Jacques Quisquater, and Eric Rescorla (editors): *2010 Electronic Voting Technology Workshop / Workshop on Trustworthy Elections, EVT/WOTE '10, Washington, D.C., USA, August 9-10, 2010*. USENIX Association, 2010. https://www.usenix.org/conference/evtwote-10/exploiting-client-vulnerabilities-internet-e-voting-systems-hacking-helios-20.

[38] Mario Heiderich, Tilman Frosch, Marcus Niemietz, and Jörg Schwenk: *The bug that made me president a browser- and web-security case study on helios voting*. In Aggelos Kiayias and Helger Lipmaa (editors): *E-Voting and Identity - Third International Conference, VoteID 2011, Tallinn, Estonia, September 28-30, 2011, Revised Selected Papers*, volume 7187 of *Lecture Notes in Computer Science*, pages 89–103. Springer, 2011, ISBN 978-3-642-32746-9. http://dx.doi.org/10.1007/978-3-642-32747-6_6.

[39] Denise Demirel, Jeroen van de Graaf, and Roberto Samarone dos Santos Araújo: *Improving helios with everlasting privacy towards the public*. In J. Alex Halderman and Olivier Pereira (editors): *2012 Electronic Voting Technology Workshop / Workshop on Trustworthy Elections, EVT/WOTE '12, Bellevue, WA, USA, August 6-7, 2012*. USENIX Association, 2012. https://www.usenix.org/conference/evtwote12/workshop-program/presentation/demirel.

[40] Jan Camenisch and Markus Stadler: *Proof systems for general statements about discrete logarithms*. Technical report, ETH Zurich, 1997.

[41] Bruce Schneier: *Applied Cryptography, Second Edition: Protocols, Algorthms and Source Code in C*. John Wiley & Sons, Inc., 1995.

[42] Reto E. Koenig, Philipp Locher, and Rolf Haenni: *Attacking the verification code mechanism in the norwegian internet voting system*. In

James Heather, Steve A. Schneider, and Vanessa Teague (editors): *E-Voting and Identify - 4th International Conference, Vote-ID 2013, Guildford, UK, July 17-19, 2013. Proceedings*, volume 7985 of *Lecture Notes in Computer Science*, pages 76–92. Springer, 2013, ISBN 978-3-642-39184-2. http://dx.doi.org/10.1007/978-3-642-39185-9_5.

[43] Aleks Essex, Jeremy Clark, Richard Carback, and Stefan Popoveniuc: *The punchscan voting system: Vocomp competition submission*. Proceedings of the First University Voting Systems Competition (VoComp), 2007.

[44] Ester Moher, Jeremy Clark, and Aleksander Essex: *Diffusion of voter responsibility: Potential failings in e2e voter receipt checking*. USENIX Journal of Election Technology and Systems (JETS), 1(3):1–17, 2014, ISSN 2328-2797. https://www.usenix.org/jets/issues/0301/moher.

[45] Maina M. Olembo, Steffen Bartsch, and Melanie Volkamer: *Mental models of verifiability in voting*. In *Proceedings of the 4th International Conference on E-Voting and Identity*, Vote-ID'13, pages 142–155, Berlin, Heidelberg, 2013. Springer-Verlag, ISBN 978-3-642-39184-2. http://dx.doi.org/10.1007/978-3-642-39185-9_9.

[46] S. Schneider, M. Llewellyn, C. Culnane, J. Heather, S. Srinivasan, and Z. Xia: *Focus group views on pret a voter 1.0*. In *Requirements Engineering for Electronic Voting Systems (REVOTE), 2011 International Workshop on*, pages 56–65, Aug 2011.

[47] J. M. Bohli, C. Henrich, C. Kempka, J. Muller-Quade, and S. Rohrich: *Enhancing electronic voting machines on the example of bingo voting*. IEEE Transactions on Information Forensics and Security, 4(4):745–750, Dec 2009, ISSN 1556-6013.

[48] Python Software Foundation: *Python programming language*. https://www.python.org/.

[49] Django Software Foundation: *Django: The web framework for perfectionists with deadlines*. https://www.djangoproject.com/.

[50] Hovav Shacham and Vanessa Teague (editors): *2011 Electronic Voting Technology Workshop / Workshop on Trustworthy Elections, EVT/WOTE '11, San Francisco, CA, USA, August 8-9, 2011*. USENIX Association, 2011. https://www.usenix.org/publications/proceedings/?f[0]=im_group_audience%3A295.