ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ
ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ:

ΗΛΕΚΤΡΟΝΙΚΗ ΨΗΦΟΦΟΡΙΑ - E-VOTING

ΠΑΖΙΑΝΑΣ ΠΑΝΑΓΙΩΤΗΣ ΑΕΜ: 144

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΣΤΑΜΟΥΛΗΣ ΓΕΩΡΓΙΟΣ

Βόλος, Φεβρουάριος 2015

Οπισθόφυλλο

Περίληψη

Αρκετές φορές κατά την διάρκεια της ζωής μας θα χρειαστεί να ασκήσουμε το εκλογικό μας δικαίωμα. Όμως πόσες φορές θα πρέπει ορισμένοι από εμάς να διασχίσουμε ολόκληρη τη χώρα για να φτάσουμε στην εκλογική μας περιφέρεια; Πόσοι δεν έχουν την δυνατότητα, είτε την σωματική είτε την οικονομική, να πραγματοποιήσουν αυτή τη διαδρομή; Δεν θα ήταν πιο εύκολο για όλους μας να μπορούσαμε να ψηφίζουμε σε ειδικά διαμορφωμένα κέντρα ή ακόμα και από το σπίτι μας; Η διαδικασία της ψηφοφορίας είναι ίσως ο μοναδικός ελεγκτικός μηχανισμός που διαθέτουν οι πολίτες απέναντι στην εκάστοτε κυβέρνηση για αυτό και θα πρέπει να εκμεταλλευτούμε τη ραγδαία εξέλιξη της τεχνολογίας για να τη διευκολύνουμε. Λύση στα προβλήματα αυτά προσφέρει η Ηλεκτρονική Ψηφοφορία (E-voting), τεχνολογίες δηλαδή και πρωτόκολλα που επιτρέπουν την ασφαλή διεξαγωγή της εκλογικής διαδικασίας.

Το συγκεκριμένο θέμα πραγματεύεται η παρούσα διπλωματική, με τίτλο ***Ηλεκτρονική Ψηφοφορία E-Voting***. Στην διπλωματική επισημαίνονται, οι τεχνολογίες και τα πρωτόκολλα που υπάρχουν και εφαρμόζονται , τα οφέλη από τη χρήση αυτής της διαδικασίας είτε οικονομικά είτε κοινωνικά, οι απαραίτητες προϋποθέσεις για την ασφαλή διεξαγωγή της ,καθώς και οι κίνδυνοι και οι δυσκολίες που προκύπτουν τόσο σε τεχνικό όσο και σε κοινωνικό επίπεδο.

Abstract

Quite a few times during our life, we will have to exercise our voting right. However, how many times should some of us have to cross the entire county to reach our election district? How many are not able, either physically or economically, to make this trip? Would not be easier for all to be able to vote in specially designed centers or even form out house. The voting election process is probably the only control mechanism of the citizens in against the government, therefore we should take advantage of the rapid evolution of technology in order to facilitate it. Solution to these problems can provide new technologies and protocols which will allow the voting procedure to be securely performed.

The present study, entitled ***Electronic Voting E-Voting***, deals with this particular subject. This study highlights the existing technologies and protocols for E-Voting, the economic and social benefits, the requirements in order to protect and safeguard the process, as well as the threats and difficulties that arise in technical and social level.

Περιεχόμενα

Ευχαριστίες

Θα ήθελα να ευχαριστήσω όσους με βοήθησαν και στάθηκαν δίπλα μου κατά την διάρκεια αυτής της δύσκολης και επίπονης προσπάθειας. Ένα μεγάλο ευχαριστώ σε όλους μου τους καθηγητές ,που μου έδωσαν την δυνατότητα να αναπτύξω την μόρφωση και τους "ορίζοντές" μου και να πετύχω τους στόχους μου και ιδιαίτερα στον κ. Σταμούλη Γεώργιο και στον κ. Μποζάνη Παναγιώτη. Μεγάλο ευχαριστώ στους φίλους μου και τους συμφοιτητές μου για την αμέριστη βοήθειά τους σε όλα αυτά τα χρόνια. Τέλος, θα ήθελα να ευχαριστήσω ειλικρινά την οικογένεια μου που κατά την διάρκεια των σπουδών μου ήταν πάντα δίπλα μου να με στηρίζει και οικονομικά και ηθικά για να μπορέσω να αφοσιωθώ στις υποχρεώσεις μου.

1. Συστήματα ηλεκτρονικής ψηφοφορίας

1.1. Εισαγωγή

Η εκλογική διαδικασία έχει απασχολήσει την ανθρωπότητα από πολύ παλιά. Στην Αρχαία Ελλάδα έριχναν πέτρες και όστρακα σε πιθάρια για να καταθέσουν την ψήφο τους. Με την εξέλιξη της τεχνολογίας η διαδικασία των εκλογών αυτοματοποιήθηκε για να μπορεί να ανταπεξέλθει στην αύξηση του πληθυσμού των κοινοτήτων στις οποίες έπρεπε να διεξαχθούν οι εκλογές.

Τα τελευταία 20 χρόνια έχει παρατηρηθεί μεγάλη κινητικότητα γύρω από την ηλεκτρονική ψηφοφορία (e-voting). Αν και η αδιαφορία των πολιτικών είναι ένα μεγάλο πρόβλημα για των εκσυγχρονισμό των εκλογών, επίσης υφίσταται και το πρόβλημα της αποχής λόγω μεγάλων αποστάσεων ή θεμάτων υγείας. Στις μέρες μας υπάρχει η τεχνολογική ωριμότητα και οι κατάλληλες υποδομές για τον εκσυγχρονισμό των εκλογών. Η επίτευξη ενός ασφαλούς τρόπου διεξαγωγής ηλεκτρονικής ψηφοφορίας θα μειώσει κατά πολύ το κόστος των εκλογών και θα προσφέρει τη δυνατότητα στους ψηφοφόρους να ψηφίζουν από όπου θέλουν, για παράδειγμα από κάποιο θάλαμο σε ένα εμπορικό κέντρο ή ακόμη και από το σπίτι τους. Η επίδραση στη σύγχρονη κοινωνία θα είναι μεγάλη, καθώς θα μπορούν να διεξαχθούν εκλογές πιο συχνά, με μεγαλύτερη ευκολία, και η θέληση του κόσμου θα καθορίζει άμεσα περισσότερα ζητήματα. Επίσης, η ευκολία με την οποία θα μπορεί κάποιος να ψηφίσει θα συμβάλλει θετικά στην έλευση περισσότερων ψηφοφόρων στις εκλογές.

Οι πολίτες δεν εμπιστεύονται εύκολα τα ηλεκτρονικά συστήματα ψηφοφορίας αφού δεν έχουν ενεργή συμμετοχή και δεν αφήνουν φυσικές αποδείξεις. Όμως η ηλεκτρονική ψηφοφορία μπορεί να προσφέρει πολλές λύσεις στον σύγχρονο πολίτη και να του εξυψώσει το ενδιαφέρον. Η δυνατότητα ενός τυφλού ατόμου να ψηφίσει μυστικά και ανεξάρτητα είναι πολύ σημαντική. Άτομα με ειδικές ανάγκες μπορούν να συμμετέχουν στις εκλογές χωρίς να χρειαστεί να μετακινηθούν. Το σύστημα μπορεί να προσφέρει σε όλους τους ψηφοφόρους επιβεβαίωση για τη καταμέτρηση της ψήφου τους και να τους προειδοποιεί για πιθανά σφάλματα που έχουν κάνει. Οι τυφλοί θα λαμβάνουν εντολές για το τρόπο λειτουργίας του συστήματος και θα ειδοποιούνται κατά την ολοκλήρωση της διαδικασίας. Επιπρόσθετα οι ψηφοφόροι θα μπορούν να πλοηγούνται στους υποψηφίους και θα μπορούν να αναθεωρήσουν τη ψήφο τους. Οι εκλογές χρειάζονται τους ψηφοφόρους και πρέπει να δίνεται η δυνατότητα σε όλους να ψηφίζουν σωστά.

1.2. Ορισμός της ηλεκτρονικής ψηφοφορίας

Με τον όρο ηλεκτρονική ψηφοφορία (electronic voting), εννοούμε την άσκηση του εκλογικού δικαιώματος με τη χρήση ηλεκτρονικών μεθόδων [5].

Δυο είναι τα θεμελιώδη στοιχεία που συνθέτουν την ιδιαίτερη φύση της ηλεκτρονικής ψήφου και τη διαφοροποιούν σε μεγάλο βαθμό από τα υπάρχοντα συστήματα της εκλογικής διαδικασίας:

Η δυνατότητα άσκησης του εκλογικού δικαιώματος από απόσταση, χωρίς την

αυτοπρόσωπη, επομένως, παρουσία του ψηφοφόρου στο εκλογικό τμήμα.

Η χρήση υπολογιστικού συστήματος και κατά συνέπεια αυτοματοποιημένων μεθόδων, για την οργάνωση και διεξαγωγή της όλης εκλογικής διαδικασίας.

Η ρίψη μίας ηλεκτρονικής ψήφου μέσω του διαδικτύου πρέπει να συνοδεύεται από επαρκείς εγγυήσεις ασφάλειας ότι η ταυτότητα του ψηφοφόρου δεν θα αποκαλυφθεί κατά τη διάρκεια της μεταφοράς και της επεξεργασίας της ψήφου, όπως επίσης και ότι το περιεχόμενο της δεν θα μεταβληθεί, λόγω μη αποτελεσματικής λειτουργίας του συστήματος ή εξαιτίας εκλογικής λαθροχειρίας. Με βάση τα παραπάνω, Σύστημα Ηλεκτρονικής Ψηφοφορίας ορίζεται το σύστημα εκείνο που είναι προορισμένο να εξυπηρετήσει τις ανάγκες διεξαγωγής μίας ηλεκτρονικής ψηφοφορίας.

Ο κύριος στόχος των Συστημάτων Ηλεκτρονικής Ψηφοφορίας είναι η υποστήριξη της οργάνωσης και διεξαγωγής της εκλογικής διαδικασίας με απώτερο σκοπό την ενδυνάμωση της συμμετοχικής δημοκρατίας. Το Σύστημα υποστηρίζει τον καθορισμό των εκλογικών περιφερειών, την καταχώρηση των συνδυασμών και των υποψηφίων, τη δημιουργία ηλεκτρονικών ψηφοδελτίων, την εισαγωγή των στοιχείων των ψηφοφόρων για τη δημιουργία των εκλογικών καταλόγων, τη δημιουργία μέσων αυθεντικοποίησης για τους ψηφοφόρους και την αυτόματη καταμέτρηση των ψήφων μετά το πέρας της εκλογικής διαδικασίας.

Η χρήση τεχνολογιών ηλεκτρονικής ψηφοφορίας αναδιοργανώνει την παραδοσιακή εκλογική διαδικασία. Το χάρτινο ψηφοδέλτιο αντικαθίσταται από το ψηφιακό. Τα τοπικά συστήματα ηλεκτρονικής ψηφοφορίας (direct recording electronic (DRE) voting systems) αποτελούν το ηλεκτρονικό ισοδύναμο των mechanical-lever machines και είναι τα μόνα ηλεκτρονικά εκλογικά συστήματα που περιλαμβάνουν εκλογικά κέντρα. Σε όλα τα υπόλοιπα (internet-based), όλες οι διαδικασίες λαμβάνουν χώρα από απόσταση. Η πρώτη DRE μηχανή ψηφοφορίας (voting machine) χρησιμοποιήθηκε σε πραγματικές εκλογές το 1975 στο Streamwood και Woodstock Illinois.

1.3. Διάκριση ηλεκτρονικής ψηφοφορίας ανάλογα με το χώρο άσκησης του εκλογικού δικαιώματος

Η ηλεκτρονική ψηφοφορία είναι δυνατόν να πραγματοποιηθεί είτε στα παραδοσιακά εκλογικά τμήματα είτε, σε οποιοδήποτε άλλο χώρο από τον οποίο υπάρχει η δυνατότητα πρόσβασης στο διαδίκτυο. Σύμφωνα με τα παραπάνω, προκύπτει μια ουσιαστική διάκριση μεταξύ των μορφών που μπορεί να λάβει η ηλεκτρονική ψηφοφορία, η οποία συναρτάται με το χώρο από τον οποίο ο εκλογέας επιλέγει να ασκήσει το εκλογικό του δικαίωμα:

- **Ηλεκτρονική ψηφοφορία εντός των εκλογικών τμημάτων** (poll site e-voting): Στην περίπτωση αυτή, η ψηφοφορία γίνεται στα εκλογικά κέντρα, υπό την εποπτεία των αρμόδιων διοικητικών αρχών, οι οποίες έχουν την ευθύνη για τον έλεγχο της καλής λειτουργίας του υλικού και του λογισμικού του υπολογιστικού συστήματος, καθώς και την εποπτεία του περιβάλλοντος χώρου. Με την ύπαρξη εποπτείας, διαφυλάσσεται ο μυστικός χαρακτήρας

της διαδικασίας και αποτρέπονται φαινόμενα άσκησης πιέσεων επί των εκλογέων, όπως απειλές, εκφοβισμός, ή άσκηση βίας, προκειμένου να διαμορφώσουν την ψήφο τους κατά συγκεκριμένο τρόπο. Η εποπτεία των διοικητικών οργάνων καλείται να διασφαλίσει ότι οι πολίτες δεν θα συναντήσουν εμπόδια κατά την άσκηση του εκλογικού τους δικαιώματος, ενώ ταυτόχρονα μειώνει τον κίνδυνο ύπαρξης φαινομένων πλαστοπροσωπίας. Υποκατηγορία της άσκησης της ηλεκτρονικής ψηφοφορίας σε εποπτευόμενο από τις αρχές χώρο, αποτελεί η άσκηση του εκλογικού δικαιώματος σε κατάλληλα διαμορφωμένα περίπτερα (kiosk voting) ή θαλάμους, τα οποία είναι τοποθετημένα σε χώρους, όπου είναι εύκολη η προσέγγιση από το κοινό, όπως εμπορικά κέντρα και ταχυδρομεία. Όμως και αυτοί οι χώροι θα πρέπει να επιτηρούνται από τους αρμόδιους υπαλλήλους.

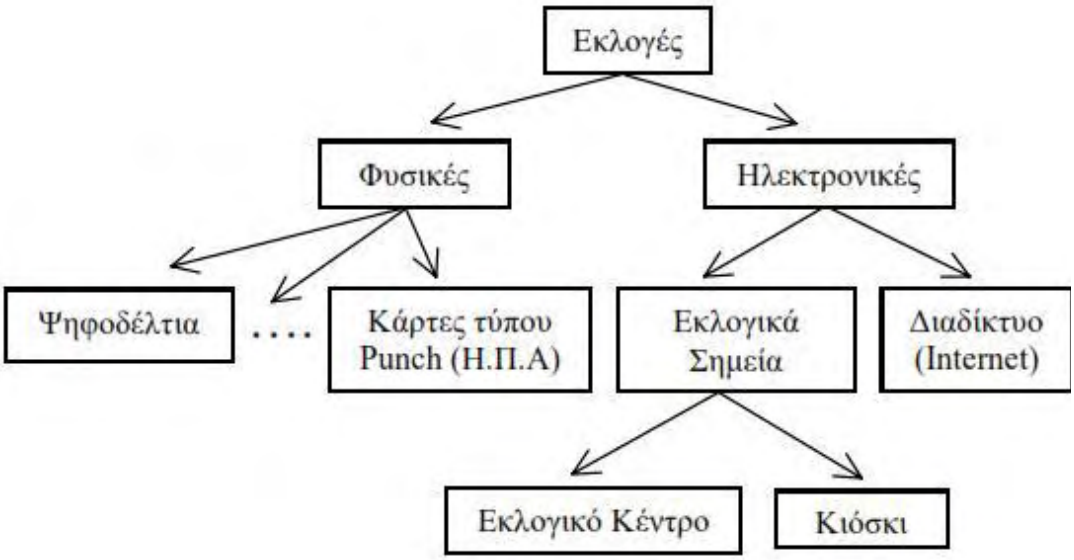
- **Ηλεκτρονική ψηφοφορία που πραγματοποιείται από απόσταση** (remote evoting): Η άσκηση του ηλεκτρονικού δικαιώματος γίνεται από οποιοδήποτε ιδιωτικό χώρο, όπου το μηχάνημα, μέσω του οποίου καταθέτει την ψήφο του ο εκλογέας, ελέγχεται από τον ίδιο ή κάποιον τρίτο. Ο χώρος αυτός μπορεί να είναι η οικία, ο επαγγελματικός χώρος του ψηφοφόρου ή κάποιος δημόσιος χώρος, όπως τα ‘‘internet cafe’’. Το σύστημα αυτό ψηφοφορίας είναι προφανές ότι μεγιστοποιεί την ευκολία συμμετοχής στην ψηφοφορία. Εγείρει, όμως, σημαντικές επιφυλάξεις για τις συνθήκες κάτω από τις οποίες ο ψηφοφόρος ασκεί το δικαίωμα του, καθώς και για το εάν οι δυνατότητες που παρέχει η σύγχρονη τεχνολογία, είναι σε θέση να διασφαλίσουν ότι το περιεχόμενο της ψήφου θα παραμείνει μυστικό και αναλλοίωτο.

Εν ολίγοις, η διάκριση μεταξύ της εποπτευόμενης και μη εποπτευόμενης ηλεκτρονικής ψήφου είναι ουσιαστική, διότι συνδέεται άμεσα με το επίπεδο ελέγχου που ασκούν στην όλη διαδικασία οι αρμόδιοι φορείς. Η απουσία εποπτείας είναι δυνατόν να επιτρέψει την παραβίαση της μυστικότητας και της ελευθερίας της ψήφου. Η ηλεκτρονική ψηφοφορία από απόσταση με τη χρήση του διαδικτύου, αποτελεί επιμέρους κατηγορία των λεγόμενων RVEM (Remote Voting by Electronic Means) δηλαδή ψηφοφορία από απόσταση με τη χρήση ηλεκτρονικών μέσων. Άλλα τέτοια μέσα μπορεί να αποτελούν:

Ψηφοφορία με τη χρήση τηλεφώνου. Αυτός ο τύπος του συστήματος μπορεί να λειτουργήσει είτε με τη χρήση των γραμμών της σταθερής τηλεφωνίας ή με τη χρήση κινητών τηλεφώνων.

Η ψήφος με την αποστολή μηνυμάτων μέσω κινητού τηλεφώνου (SMS - Short Message Service).

Χρήση της Ψηφιακής Διαδραστικής Τηλεόρασης (Interactive Digital Television). Η τεχνολογία αυτή αξιοποιεί τις δυνατότητες αλληλεπίδρασης των νέων τύπων τηλεόρασης (για παράδειγμα το SMART TV της Samsung) για να διευκολύνει τους ψηφοφόρους να καταθέσουν την ψήφο τους.



Εικόνα 1. Διάκριση Εκλογικών Διαδικασιών [14]

1.4. Μέρη ενός συστήματος Ηλεκτρονικής Ψηφοφορίας

Τα βασικά μέρη ενός συστήματος ηλεκτρονικής ψηφοφορίας είναι:

- **Ψηφοφόροι**: Τους συμβολίζουμε με ***M*** το πλήθος. Γενικά πρέπει η "δουλειά" που κάνουν να είναι ελάχιστη, δηλαδή αν είναι εφικτό, να ψηφίζουν και **να φεύγουν ("vote-and-go").**
- **Ψήφοι**: Στην αρχή η μόνη ψήφος που υποστηριζόταν από τα πρωτόκολλα ήταν της μορφής "ναι/ όχι". Πλέον η ψήφος μπορεί να πάρει διάφορες μορφές ανάλογα με τον τύπο εκλογών: "ναι/ όχι": συνήθως συμβολίζεται με "1" για ναι και "0" για όχι, και επιλέγουν 1 από αυτούς. Η μορφή της ψήφου συνήθως είναι ένας αριθμός από το {1,…,L}, με το L να είναι ο πληθάριθμός των υποψηφίων και επιλέγουν K από αυτούς, Η μορφή της ψήφου μπορεί να είναι ένα διάνυσμα μήκους L με άσους στις θέσεις των υποψηφίων που θέλουμε να ψηφίσουμε και μηδέν στις υπόλοιπες θέσεις.
- **Μηχανήματα Άμεσης Αυτόματης Εγγραφής (DRE):** Από τα πιο σημαντικά κομμάτια του συστήματος Ηλεκτρονικής Ψηφοφορίας. Ένα τέτοιο μηχάνημα θα πρέπει να είναι εύχρηστο, όσο το δυνατόν πιο απλό και ασφαλές. Με τα μηχανήματα αυτά ο εκλογέας δεν καταγράφει πλέον την επιλογή του, χρησιμοποιώντας ένα ξεχωριστό ψηφοδέλτιο, αλλά αντίθετα χρησιμοποιεί απευθείας την οθόνη του μηχανήματος, ενεργοποιώντας την ψήφο του με το άγγιγμα μίας συγκεκριμένης περιοχής. Με τη χρήση των μηχανημάτων αυτών, καταργείται η πιθανότητα διάπραξης λάθους κατά την άσκηση του δικαιώματος, καθώς είναι προγραμματισμένα να προβάλλουν ένα προειδοποιητικό μήνυμα στην περίπτωση που ο εκλογέας επιχειρήσει να ολοκληρώσει τη διαδικασία έχοντας ψηφίσει περισσότερους ή

λιγότερους υποψηφίους από ότι επιτρέπεται. Επίσης, είναι δυνατόν να χρησιμοποιηθούν και από άτομα με ειδικές ανάγκες (π.χ. ηχητικές εντολές, παροχή της μεθόδου braille σε περίπτωση ανθρώπων χωρίς όραση). Τέλος, μειώνουν σημαντικά το χρόνο και το κόστος της καταμέτρησης, εξαλείφοντας την πιθανότητα ανθρώπινου λάθους.

- **Μηχανήματα Συλλογής Ψήφων:** Ο τρόπος με τον οποίο τα ψηφοδέλτια συλλέγονται είναι πολλές φορές το ίδιο σημαντικός με το εκλογικό σύστημα που χρησιμοποιείται κατά την ψηφοφορία. Το σύστημα που χρησιμοποιείται για τη συλλογή των ψηφοδελτίων μπορεί να επηρεάσει το συνολικό αποτέλεσμα της ψηφοφορίας, την προσβασιμότητα των ψηφοφόρων στα αποτελέσματα, την πιθανότητα νοθείας, το οικονομικό κόστος της ψηφοφορίας, το ποσό της σκέψης και του χρόνου που δαπανούν οι ψηφοφόροι για να κάνουν τις επιλογές τους και την εμπιστοσύνη που τρέφει το εκλογικό σώμα για την ακρίβεια του εκλογικού αποτελέσματος.

1.5. Στάδια ενός Συστήματος Ηλεκτρονικής Ψηφοφορίας

Σε γενικές γραμμές, κάθε ηλεκτρονική ψηφοφορία αποτελείται από τέσσερα διακριτά στάδια:

- **Εγγραφή.** Πριν από τη διεξαγωγή των εκλογών, οι ψηφοφόροι αποδεικνύουν την αληθινή τους ταυτότητα και τη νομιμότητα του δικαιώματος τους να ψηφίσουν (π.χ. όριο ηλικίας). Όσοι πληρούν τις προϋποθέσεις εγγράφονται στον εκλογικό κατάλογο. Η Αρχή Αυθεντικοποίησης (Certification Authority, CA) δημιουργεί ένα ζεύγος δημόσιου- ιδιωτικού κλειδιού για κάθε νόμιμο ψηφοφόρο και δημοσιοποιεί το δημόσιο κλειδί του.
- **Επικύρωση.** Πριν την υποβολή της ψήφου ελέγχεται η ταυτότητα των ψηφοφόρων (ταυτοποίηση (identification) – αυθεντικοποίηση (authentication)).
- **Υποβολή Ψήφου.** Οι ψηφοφόροι υποβάλλουν την ψήφο τους. Μόνο μια ψήφος επιτρέπεται για κάθε ψηφοφόρο. Ο ψηφοφόρος "φτιάχνει" την ψήφο του ανάλογα με το πρωτόκολλο που χρησιμοποιείται και τη στέλνει στις αρχές μέσω του καναλιού που έχει δεσμευτεί για τη διαδικασία.
- **Καταμέτρηση Ψήφων.** Μόλις εκπνεύσει η προθεσμία υποβολής ψήφων, οι ψήφοι καταμετρούνται και ανακοινώνεται το εκλογικό αποτέλεσμα.

1.6. Θετικές Επιδράσεις ηλεκτρονικής ψηφοφορίας

Με την εισαγωγή της ηλεκτρονικής ψηφοφορίας στις διαδικασίες διενέργειας εκλογών σε τοπικό, εθνικό και ευρωπαϊκό επίπεδο, προσδοκάται να μειωθεί μια σημαντική μερίδα του εκλογικού σώματος το οποίο απέχει από τις πολιτικές διαδικασίες. Η αύξηση της συμμετοχής των ψηφοφόρων στις διαδικασίες ανάδειξης των αιρετών αντιπροσώπων, είναι σημαντική στο πλαίσιο μίας δημοκρατικής κοινωνίας, γιατί αυξάνει τη νομιμοποίηση των πολιτικών αποφάσεων που θα κληθεί

να λάβει η ηγεσία αυτή. Η άνοδος του ποσοστού των ψηφοφόρων που θα κινητοποιηθεί για να ασκήσει τα εκλογικά του δικαιώματα, οφείλεται κυρίως:

Τα συστήματα ηλεκτρονικής ψηφοφορίας υπόσχονται διευκόλυνση στην πρόσβαση σε ευπαθείς ομάδες ψηφοφόρων, καθώς και τη χρησιμοποίησή τους από άτομα με ειδικές ανάγκες. Επιπλέον, η καταμέτρηση των ψήφων και η δημοσίευση των αποτελεσμάτων θα γίνονται εύκολα, γρήγορα, με μικρότερο ποσοστό λάθους, αλλά και μικρότερο (μακροπρόθεσμα) οικονομικό κόστος, σε σχέση π.χ. με το κόστος εκτύπωσης ψηφοδελτίων στις παραδοσιακές εκλογές. Εκλογείς, οι οποίοι για διάφορους λόγους, όπως ασθένεια, απουσία στο εξωτερικό ή εγκατάσταση σε διαφορετική εκλογική περιφέρεια λόγω επαγγελματικών υποχρεώσεων, δεν είχαν τη δυνατότητα να προσέλθουν στα εκλογικά τμήματα, θα πάψουν πλέον να στερούνται τη δυνατότητα άσκησης του εκλογικού τους δικαιώματος.

Το μεγάλο ποσοστό διείσδυσης του Διαδικτύου, ιδιαίτερα στις ανεπτυγμένες χώρες, καθιστά επωφελή τη μετάβαση στα συστήματα ηλεκτρονικής ψηφοφορίας μέσω Διαδικτύου. Με τα συστήματα αυτά η διαδικασία υποβολής της ψήφου θα είναι φιλική προς τον χρήστη, με αποτέλεσμα να ευνοηθεί η αύξηση του ποσοστού συμμετοχής των πολιτών στις εκλογές. Ένας σημαντικός αριθμός υπολογιστών που είναι σήμερα διαθέσιμοι σε προσβάσιμους χώρους (π.χ. βιβλιοθήκες, σχολεία) μπορούν να τίθενται στην υπηρεσία του εκλογικού σώματος την ημέρα των εκλογών. Επίσης, η ψηφοφορία μέσω Διαδικτύου θα μπορούσε να διαδραματίσει σημαντικό ρόλο σε εκλογές μικρής κλίμακας, π.χ. φοιτητικές εκλογές. Αυτό θα δώσει σημαντική ώθηση στην εκλογική συμμετοχή των νέων που αποτελούν το μελλοντικό εκλογικό σώμα. Επιπλέον, λόγω του αυτοματοποιημένου χαρακτήρα του όλου εγχειρήματος, θα υπάρξει μείωση του μακροπρόθεσμου κόστους των εκλογών και ταυτόχρονη βελτίωση της διοικητικής αποτελεσματικότητας. Η καταμέτρηση των ψήφων θα πραγματοποιείται γρηγορότερα και με μεγαλύτερη ακρίβεια, μειώνοντας την πιθανότητα αμφισβητήσεως των εκλογικών αποτελεσμάτων και ανάγκης για επανάληψη της εκλογικής διαδικασίας. Μακροπρόθεσμα, η υποδομή αυτή θα δίνει τη δυνατότητα διενέργειας πολλαπλών εκλογικών αναμετρήσεων, εξασφαλίζοντας σημαντική εξοικονόμηση πόρων τόσο οικονομικών (μείωση του κόστους έκδοσης των παραδοσιακών έντυπων ψηφοδελτίων) όσο και σε ανθρώπινο δυναμικό, καθώς η απλοποίηση, σε μεγάλο βαθμό, της διαδικασίας και η εναπόθεση των περισσοτέρων ενεργειών στη λειτουργική ικανότητα των μηχανημάτων, θα περιορίσει τον αριθμό ατόμων και τις ώρες που δαπανώνται υπό τις σημερινές συνθήκες, ιδιαίτερα κατά τη φάση προετοιμασίας των εκλογών. Η ευκολία στην πρόσβαση που χαρακτηρίζει την ηλεκτρονική ψηφοφορία, αλλά και το ενδεχόμενο χρήσης της μεθόδου αυτής και σε άλλες διαδικασίες λήψης αποφάσεων, θεωρείται από πολλούς ότι μπορεί να οδηγήσει σε μια νέα μορφή άμεσης δημοκρατίας, τη δημοκρατία του κυβερνοχώρου (cyberdemocracy). Έτσι, η ηλεκτρονική ψηφοφορία δεν θα συμβάλλει μόνο σε μία ποσοτική αναβάθμιση του ποσοστού συμμετοχής των ψηφοφόρων, αλλά το κυριότερο σε μία ποιοτική βελτίωση της συμμετοχής αυτής (more votes, more informed voters) [5].

1.7. Αρνητικές Επιδράσεις ηλεκτρονικής ψηφοφορίας

Οι πρόσφατες τεχνολογικές εξελίξεις έχουν ανοίξει τη δυνατότητα της ηλεκτρονικής ψηφοφορίας και αυτό αποτελεί μεγάλη ευκαιρία αλλά και απειλή. Από τη μία πλευρά, η νέα τεχνολογία μπορεί να συμβάλει στην προσέλευση περισσότερων ψηφοφόρων ενώ από την άλλη μπορεί να επηρεάσει εκλογικές αξίες όπως, το απόρρητο της ψηφοφορίας. Επί του παρόντος διάφορες χώρες και διαφορετικά εκλογικά συστήματα αντιμετωπίζουν αυτές τις ευκαιρίες και τις απειλές και το ερώτημα είναι τι θα συμβεί. Αν και η ηλεκτρονική ψηφοφορία μπορεί να προσφέρει ενδιαφέρουσες υποσχέσεις, όπως χαμηλότερο κόστος, αναδιοργάνωση της εκλογικής διαδικασίας και αύξηση της ευκολίας των ψηφοφόρων, δεν είναι κάθε εμπλεκόμενος στην διαδικασία ψηφοφορίας ενθουσιώδης. Όπως πολλοί εμπειρογνώμονες επισημαίνουν, η εισαγωγή της ηλεκτρονικής ψήφου μπορεί να σχετίζεται με διάφορους κινδύνους.

Πρώτα απ 'όλα, τη λειτουργία των μηχανημάτων ψηφοφορίας από μεμονωμένους ψηφοφόρους μπορεί να θεωρηθεί ένας σχετικά νέος κίνδυνος. Όπως γνωρίζουμε από πολλές μελέτες, πολλοί άνθρωποι αντιμετωπίζουν δυσκολίες με τη λειτουργία σύγχρονων τεχνολογικών εργαλείων . Με την εισαγωγή των μηχανών στη διαδικασία της ψηφοφορίας, υπάρχει σαφής κίνδυνος να γίνει περιπλοκότερη αυτή η διαδικασία για τον μέσο ψηφοφόρο. Παρά το γεγονός ότι οι σχεδιαστές μπορούν να ισχυρίζονται ότι ένα ορισμένο σύστημα είναι φιλικό προς το χρήστη, η επάρκεια των χρηστών όσον αφορά στη χρήση των μηχανημάτων, ιδιαίτερα των ηλικιωμένων που δεν είναι εξοικειωμένοι με τεχνολογικές συσκευές αλλά και των ατόμων με ειδικές ανάγκες, δεν μπορεί να εξασφαλιστεί.

Δεύτερον, υπάρχουν λόγοι που συνδέονται με την αξιοπιστία και την ευρωστία των τεχνικών συστημάτων και ιδίως των ηλεκτρονικών μηχανών. Κάθε πολύπλοκη τεχνολογία μπορεί να καταρρεύσει και να προκαλέσει προβλήματα, τα οποία μπορεί να είναι δύσκολο να διορθωθούν. Στην περίπτωση της ηλεκτρονικής ψηφοφορίας, οι κίνδυνοι διατάραξης της παροχής ρεύματος και των αποτυχιών στην ηλεκτρονική αποθήκευση των ψήφων απαιτούν οπωσδήποτε ειδικά μέτρα, όπως η επαλήθευση και δυνατότητες backup για τον εντοπισμό λαθών και η διόρθωσή τους.

Τρίτον, τα συστήματα ηλεκτρονικής ψηφοφορίας μπορεί να είναι ευάλωτα σε επιθέσεις άντλησης εμπιστευτικών πληροφοριών που θίγουν την ακεραιότητα του συστήματος. Τη δυνατότητα επηρεασμού των συστημάτων θα μπορούσαν να την χρησιμοποιήσουν και οι ίδιες οι αρχές προκειμένου να βγει το εκλογικό αποτέλεσμα υπέρ τους. Σε περιπτώσεις που οι πολίτες ψηφίζουν από απόσταση μέσω του υπολογιστή τους, μπορεί να δεχθούν επίθεση από δούρειους ίππους και ιούς με στόχο να κατασκοπεύσουν τα ψηφοδέλτια ή και να τα τροποποιήσουν.

Για κάποιους ανθρώπους η ψήφος είναι απλώς μια μορφή δημόσιας υπηρεσίας . Για πολλούς είναι πολύ περισσότερα. Είναι ένα συστατικό στοιχείο της αντιπροσωπευτικής δημοκρατίας και μια τελετουργία συνάντησης των ενδιαφερομένων πολιτών. Σε αυτή τη χρονική στιγμή, όλοι οι πολίτες οι οποίοι εισέρχονται στο θάλαμο ψηφοφορίας είναι ισοδύναμης αξίας, κάθε ένας ρίχνει μία ψήφο, παρά τις διαφορές τους στη φυλή, την εκπαίδευση ή στην εργασία. Η

ψηφιοποίηση μιας διαδικασίας, η οποία αποτελεί τον κορυφαίο θεσμό της δημοκρατίας, χάριν ικανοποίησης ατομικιστικών επιδιώξεων (ευκολία συμμετοχής) υποβιβάζει την άσκηση ενός θεμελιώδους πολιτικού δικαιώματος στο επίπεδο των ηλεκτρονικών συναλλαγών στις οποίες προβαίνει καθημερινά ο πολίτης [5].

Πιο σημαντικό, όμως, είναι η απώλεια του ελέγχου από τις πιθανές απειλές κατά της μυστικότητας της ψηφοφορίας. Η Μυστικότητα της ψηφοφορίας θεωρείται ουσιώδης στα σύγχρονα φιλελεύθερα δημοκρατικά κράτη. Έχει υιοθετηθεί από ένα ευρύ φάσμα συμβάσεων και δηλώσεων , τα οποία πολλές δυτικές δημοκρατίες έχουν υπογράψει όπως η :

- Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου - άρθρο 21
- Διεθνής Σύμβαση για τα Ατομικά και Πολιτικά Δικαιώματα - άρθρο 25
- Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου - Πρωτόκολλο 1

Στην παραδοσιακή ψηφοφορία η μυστικότητα της ψηφοφορίας προστατεύεται μέσω της εποπτείας. Η εφορευτική επιτροπή στο εκλογικό κέντρο φροντίζει ώστε οι ψηφοφόροι να εισέρχονται στην κάλπη μόνοι τους και να ψηφίζουν χωρίς καμία αθέμιτη επιρροή. Η εποπτεία μειώνει τον κίνδυνο πλαστοπροσωπίας και διασφαλίζει το απόρρητο της ψηφοφορίας. Με την εισαγωγή της ηλεκτρονικής ψηφοφορίας, αυτού του είδους η εποπτεία θα χαθεί και αυτό θέτει σαφώς σε κίνδυνο τη μυστικότητα της ψηφοφορίας. Πολλοί πολιτικοί επιστήμονες υποστηρίζουν ότι η μορφή της αντιπροσωπευτικής δημοκρατίας κινδυνεύει με την ηλεκτρονική ψηφοφορία, καθώς εάν το κόστος της ψηφοφορίας είναι χαμηλό οι πολίτες θα απαιτούν διενέργεια εκλογών για οποιοδήποτε θέμα.

Όσον αφορά τα κύρια επιχειρήματα των υποστηρικτών της ηλεκτρονικής ψηφοφορίας, θα δούμε ότι οι κύριοι ισχυρισμοί της εξοικονόμησης κόστους, της ευκολίας στη χρήση και η μεγαλύτερη προσέλευση, δεν επαληθεύονται στην πραγματικότητα. Θα πρέπει να έχουμε κατά νου ότι εκτός από το βασικό κόστος εξοπλισμού θα υπάρξει και ένα πρόσθετο κόστος για γενικές υπηρεσίες που οι αρχές πρέπει να καλύψουν, όπως το κόστος της δωρεάν παροχής κλήσης και ότι οι ψηφοφόροι του Διαδικτύου πρέπει να διαθέτουν το δικό τους εξοπλισμό και πρόσβαση στο Διαδίκτυο [5].

2. Νομικό πλαίσιο και ιδιωτικότητα στην ηλεκτρονική ψηφοφορία

2.1. Ισχύον νομικό καθεστώς και νομικοί προβληματισμοί

Η ανάπτυξη της τεχνολογίας ηλεκτρονικής ψηφοφορίας και η διαμόρφωση του θεσμικού και νομικού πλαισίου βρίσκονται σε μία δυναμική διαδραστική σχέση. Η ανάπτυξη και εφαρμογή της τεχνολογίας προϋποθέτει τη διαμόρφωση του θεσμικού και νομικού πλαισίου και αντιστρόφως η διαμόρφωση του θεσμικού και νομικού πλαισίου προϋποθέτει τον εντοπισμό των προβλημάτων που ανακύπτουν από την εφαρμογή της σχετικής τεχνολογίας. Για να αποφευχθεί το προφανές αδιέξοδο απαιτείται μια παράλληλη πορεία, όπου οι βασικές θεσμικές παρεμβάσεις θα επιτρέψουν την αρχική εφαρμογή της τεχνολογίας και τα συμπεράσματα της αξιολόγησης της εφαρμογής της τεχνολογίας θα δώσουν τη δυνατότητα για επέκταση του νομικού και θεσμικού πλαισίου. Τα συστήματα ηλεκτρονικής ψηφοφορίας θα μπορούσαν, για παράδειγμα, αρχικά να εφαρμοστούν σε εσωτερικές εκλογικές διαδικασίες (σε συλλόγους, εταιρείες, επαγγελματικές ενώσεις κ.λπ.), καθώς και για την έκφραση της γνώμης των πολιτών σε επίπεδο τοπικής αυτοδιοίκησης. Οι απαιτούμενες θεσμικές και νομικές παρεμβάσεις αφορούν τρεις άξονες:

Προστασία των δικαιωμάτων του πολίτη. Οι πολιτικές πεποιθήσεις των πολιτών κατοχυρώνονται από την υφιστάμενη νομοθεσία ως ευαίσθητα προσωπικά δεδομένα. Η εισαγωγή, όμως, των τεχνολογιών ηλεκτρονικής ψηφοφορίας δημιουργεί νέες απειλές κατά της ιδιωτικότητας του πολίτη. Κατά συνέπεια το θεσμικό πλαίσιο θα πρέπει να επεκταθεί ώστε να καλύπτει και αυτές τις απειλές. Για παράδειγμα, είναι ανάγκη να αντιμετωπιστούν ζητήματα όπως η "οικογενειακή ψήφος", οι ψηφοφορίες στον εργασιακό χώρο, οι υποχρεώσεις των εταιρειών που παρέχουν υπηρεσίες τηλεπικοινωνιών και πρόσβασης στο διαδίκτυο, η διασφάλιση της μυστικότητας της ψήφου κατά τη διάρκεια της εκλογικής διαδικασίας και κατά την καταμέτρηση των ψήφων κ.ά. Είναι προφανές πως αυτά τα ζητήματα είναι ιδιαίτερα σύνθετα και απαιτείται περαιτέρω μελέτη και ανοικτός διάλογος για τη διαμόρφωση των απαιτούμενων ρυθμίσεων.

Διασφάλιση των δημοκρατικών αρχών. Οι θεμελιώδεις δημοκρατικές αρχές, αφορούν κάθε δημοκρατική διαδικασία ανεξάρτητα από την εμβέλειά της (εθνική, τοπική, κ.λπ.). Κατά συνέπεια θα πρέπει να αποφευχθεί η ανεξέλεγκτη χρήση τεχνολογιών ηλεκτρονικής ψηφοφορίας που δεν σέβονται τις θεμελιώδεις δημοκρατικές αρχές, καθώς ένα τέτοιο γεγονός, εκτός από τις προφανείς επιπτώσεις στην ποιότητα της Δημοκρατίας, θα αποτελούσε και δυσφήμιση για τις τεχνολογίες και τα συστήματα ηλεκτρονικής ψηφοφορίας, με αποτέλεσμα να υπονομεύσει την ανάπτυξη της σχετικής αγοράς. Συνεπώς, οι ρυθμιστικές παρεμβάσεις είναι απαραίτητες και μπορούν να λάβουν πολλές μορφές, όπως αυτορρύθμιση, πιστοποίηση συστημάτων και διαδικασιών, ρυθμιστικές παρεμβάσεις ανεξάρτητων διοικητικών αρχών κ.ά. Τα υφιστάμενα συστήματα δεν φαίνεται να έχουν τη δυνατότητα να υποστηρίξουν βουλευτικές εκλογές, εκτός εάν η ψηφοφορία

πραγματοποιείται αποκλειστικά σε εκλογικά κέντρα. Σε κάθε περίπτωση, τα συστήματα ηλεκτρονικής ψηφοφορίας θα πρέπει να ικανοποιούν τις εξής αρχές, που απορρέουν από το Ελληνικό και τα Ευρωπαϊκά Συντάγματα:

Αρχή της καθολικής ψηφοφορίας. Σύμφωνα με την αρχή της καθολικής ψηφοφορίας κάθε πολίτης, ο οποίος πληροί τις σύμφωνα με τον νόμο προϋποθέσεις εκλογιμότητας, μπορεί να συμμετέχει στην εκλογική διαδικασία.

Εκλογιμότητα και εγγραφή στους εκλογικούς καταλόγους και ταυτοποίηση. Η διαδικασία αυτή αποσκοπεί στο να διασφαλίσει ότι το εκλογικό δικαίωμα περιορίζεται σε αυτούς που πληρούν τις προϋποθέσεις για να το ασκήσουν, αλλά και ότι κάθε ψηφοφόρος ψηφίζει μόνο μία φορά.

Αρχή της ισότητας της ψήφου και της ψηφοφορίας. Με την αρχή της ισότητας επιδιώκεται η ίση συμμετοχή των πολιτών στην εκλογική διαδικασία. Αυτό συνεπάγεται ότι κάθε πολίτης έχει στη διάθεση του μόνο μία ψήφο και ότι όλες οι ψήφοι είναι μεταξύ τους ισοδύναμες.

Ισότητα των υποψηφίων που μετέχουν στις εκλογές. Αναφέρεται στην ανάγκη παροχής ίσων ευκαιριών σε όλους τους πολιτικούς σχηματισμούς και υποψηφίους που διαγωνίζονται στον πολιτικό στίβο.

Αρχή της μυστικότητας της ψήφου. Η αρχή της μυστικότητας της ψήφου έχει ως στόχο να προστατεύσει τη γνησιότητα και αυθεντικότητα της ψηφοφορίας, διασφαλίζοντας το απόρρητο των πολιτικών επιλογών του εκλογέα.

Αρχή της ελευθερίας της ψήφου και της ψηφοφορίας. Ελεύθερη είναι η εκλογική διαδικασία κατά την οποία η βούληση του λαού πραγματώνεται σε συνθήκες απουσίας εξαναγκασμών και πιέσεων, βίας, απόπειρας χειραγώγησης ή εκφοβισμού.

Αρχή της αμεσότητας της ψήφου και της ψηφοφορίας. Μεταξύ της άσκησης του εκλογικού δικαιώματος από τον ψηφοφόρο και της ανακοίνωσης του εκλογικού αποτελέσματος δεν πρέπει να παρεμβάλλεται καμία άλλη βούληση, διαδικασία ή όργανο, όπως στις περιπτώσεις της έμμεσης εκλογής.

Με βάση το παραπάνω πλαίσιο και το σύγχρονο τεχνολογικό περιβάλλον προσδιορίζονται και οι βασικές απαιτήσεις που θα πρέπει να πληροί ένα σύστημα ηλεκτρονικής ψηφοφορίας. Σε αυτές περιλαμβάνονται:

- Ορθότητα, ακρίβεια και επαληθευσιμότητα των αποτελεσμάτων.
- Ταυτοποίηση των ψηφοφόρων με βάση τους εκλογικούς καταλόγους και διασφάλιση της μοναδικότητας της ψήφου.
- Προστασία της ιδιωτικότητας του ψηφοφόρου και της μυστικότητας της ψήφου.
- Ανθεκτικότητα του συστήματος.
- Διασφάλιση της ελευθερίας της ψήφου (μη-εξαναγκασμός, uncoercibility).
- Αμεροληψία.
- Επαληθεύσιμη συμμετοχή.
- Ευκολία συμμετοχής των ψηφοφόρων.
- Ευελιξία και αποδοτικότητα.

Αλλαγές στις εκλογικές διαδικασίες. Η αξιοποίηση συστημάτων ηλεκτρονικής ψηφοφορίας απαιτούν αλλαγές στις εκλογικές διαδικασίες. Έτσι, ζητήματα όπως η αύξηση του χρόνου διεξαγωγής των εκλογών, ο έλεγχος της αξιοπιστίας των συστημάτων κ.λ.π. θα πρέπει να ρυθμιστούν νομοθετικά. Επιπλέον, είναι σημαντικό να ενθαρρυνθεί η συμμετοχή των πολιτών στο διάλογο για τη διαμόρφωση του σχετικού νομικού και θεσμικού πλαισίου, έτσι ώστε τόσο σημαντικές αποφάσεις να μη ληφθούν ερήμην των πολιτών.

2.2. Βασικές αρχές προστασίας δεδομένων

Η ανεξέλεγκτη καταγραφή και επεξεργασία προσωπικών δεδομένων πολλές φορές δημιουργεί προβλήματα στην ιδιωτική ζωή του πολίτη. Στην Ελλάδα, για τον σκοπό αυτό ιδρύθηκε με τον Νόμο 2472/97 ως ανεξάρτητος διοικητικός φορέας η "ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ". Ο σεβασμός και η προστασία της αξιοπρέπειας, της ιδιωτικής ζωής και της ελεύθερης ανάπτυξης της προσωπικότητας αποτελούν πρωταρχική επιδίωξη κάθε δημοκρατικής κοινωνίας άρα το θέμα αυτό χρήζει ιδιαίτερης σημασίας και στα συστήματα Ηλεκτρονικής Διακυβέρνησης. Αν και οι εθνικοί νόμοι για την προστασία δεδομένων έχουν ως κύριο σκοπό να προστατέψουν τα ίδια δικαιώματα, υφίστανται σημαντικές διαφορές. Οι διαφορές αυτές αποτελούν ένα πιθανό εμπόδιο για την ελεύθερη ροή της πληροφορίας και μια επιπρόσθετη επιβάρυνση για τους οικονομικούς διαχειριστές και πολίτες. Μερικές από αυτές τις διαφορές είναι: η ανάγκη να αναγνωρίζεσαι ή να επεξεργάζεσαι δεδομένα από τους οργανισμούς πολλών κρατών μελών, η ανάγκη για υπακοή σε διαφορετικά πρότυπα και η πιθανότητα περιορισμών κατά τη μεταφορά δεδομένων από άλλα κράτη μέλη της Ευρώπης. Τέλος, μερικά κράτη μέλη δεν έχουν νόμους για την προστασία δεδομένων. Γι' αυτές τις διαφορές δημιουργήθηκε η ανάγκη για ένα κοινό νομοσχέδιο της Ευρωπαϊκής Ένωσης με σκοπό τη προστασία δεδομένων.

Ο Ευρωπαϊκός νόμος για τη προστασία δεδομένων.

Με σκοπό την απομάκρυνση των εμποδίων για την ελεύθερη μεταφορά δεδομένων και χωρίς να μειωθεί η προστασία προσωπικών δεδομένων αναπτύχθηκαν οδηγίες ώστε να εναρμονιστούν οι εθνικές νομοθεσίες. Βάση αυτού, τα προσωπικά δεδομένα όλων των πολιτών θα έχουν ισότιμη προστασία σε όλη την Ευρώπη. Τα κράτη-μέλη κατάφεραν να εναρμονίσουν τις εθνικές τους νομοθεσίες με την κοινοτική οδηγία από τον Οκτώβριο του 1998. Οι οδηγίες είναι ένα κομμάτι του Ευρωπαϊκού νομοσχεδίου που κατευθύνεται από τα Κράτη Μέλη. Όταν το νομοσχέδιο περάσει σε Ευρωπαϊκό επίπεδο, κάθε κράτος μέλος πρέπει να διαβεβαιώσει ότι θα συμφωνήσει με το καθορισμένο νομικό σύστημα. Σε γενικές γραμμές, η οδηγία εφαρμόζεται μέσω της Εθνικής νομοθεσίας. Εντούτοις, είναι δυνατό μια οδηγία να έχει άμεση επίδραση στα άτομα και να μπορούν να την εφαρμόσουν χωρίς να χρειαστεί να περιμένουν την εθνική νομοθεσία. Επιπλέον αν τα άτομα θεωρήσουν ότι έχουν υποστεί ζημιά επειδή οι εθνικές αρχές απέτυχαν να αναπτύξουν την οδηγία, τότε μπορούν να απευθυνθούν σε εθνικά δικαστήρια. Η

προστασία προσωπικών δεδομένων εφαρμόζεται σε οποιαδήποτε λειτουργία ή ομάδα λειτουργιών που εκτελείται με προσωπικά δεδομένα. Αυτές οι λειτουργίες συμπεριλαμβάνουν τη συλλογή προσωπικών δεδομένων, την αποθήκευση τους, την διάδοση τους κ.α. Η οδηγία ισχύει για τα στοιχεία που υποβάλλονται σε επεξεργασία μέσω αυτοματοποιημένων μέσων (π.χ. βάση δεδομένων με πελάτες) αλλά και μη αυτοματοποιημένων συστημάτων. Η προστασία δεδομένων δεν εφαρμόζεται σε επεξεργασία δεδομένων για προσωπικούς σκοπούς όπως προσωπικό ημερολόγιο ή αρχεία με λεπτομέρειες για την οικογένεια και φίλους. Επίσης δεν εφαρμόζεται σε περιοχές όπως δημόσια ασφάλεια, επιβολή υπεράσπισης ή ποινικού δικαίου όπου είναι εκτός αρμοδιότητας του Ευρωπαϊκού συμβουλίου και παραμένει εθνικό δικαίωμα. Συγκεκριμένα υπάρχει μια χωριστή οδηγία (Οδηγία 97/66/EC) που έχει να κάνει με τη προστασία στις τηλεπικοινωνίες. Η οδηγία αυτή επιβάλει στα μέλη κράτη να εγγυηθούν για την προστασία δεδομένων μέσω εθνικών νόμων [4][6].

Πότε τα προσωπικά δεδομένα μπορούν να επεξεργαστούν?

Τα προσωπικά δεδομένα μπορούν να υπόκεινται σε επεξεργασία στις παρακάτω περιπτώσεις:

- Όταν το άτομο δώσει αναμφίβολα την συγκατάθεση του, π.χ. αν κάποιος/κάποια συμφωνήσει να παραχωρήσει τα προσωπικά του δεδομένα αφού έχει πρώτα ενημερωθεί για τον σκοπό επεξεργασίας τους.
- Αν η επεξεργασία δεδομένων είναι απαραίτητη για την εκτέλεση μιας εργασίας όπου τα στοιχεία αυτά είναι απαραίτητα. Για παράδειγμά η επεξεργασία δεδομένων για τη λήψη ενός δανείου ή για εξόφληση λογαριασμών.
- Όταν η επεξεργασία έχει να κάνει με νομικές υποχρεώσεις.
- Εάν η επεξεργασία δεδομένων είναι απαραίτητη για να προστατεύσει συμφέρον που είναι απαραίτητο για τη ζωή του ατόμου. Για παράδειγμα σε ένα τροχαίο ατύχημα όπου το άτομο είναι λιπόθυμο επιτρέπεται να δοθούν τα τεστ αίματος αν αυτό κρίνεται ουσιαστικό για να σωθεί.
- Αν η επεξεργασία είναι απαραίτητη για να επιτευχθούν δημόσια συμφέροντα.
- Τέλος τα δεδομένα μπορούν να επεξεργαστούν αν οι ελεγκτές ή ένα τρίτο πρόσωπο έχει νόμιμα συμφέροντα για να το κάνει. Εντούτοις, αυτά τα συμφέροντα δεν μπορούν να αγνοήσουν τα συμφέροντα ή τα θεμελιώδη δικαιώματα του αντικειμένου δεδομένων. Αποτέλεσμα είναι να βρεθεί μια λογική μέση κατάσταση για να υπάρχει ισορροπία ανάμεσα στα συμφέροντα τρίτων και στην εμπιστευτικότητα των δεδομένων. Τις τελικές αποφάσεις για τέτοιου είδους ζητήματα, της παίρνει το δικαστήριο.

Η οδηγία εφαρμόζεται σε μεταφορά δεδομένων στο δίκτυο;

Θα ήταν μάλλον παράλογο αν τέτοιες σημαντικές πληροφορίες που μεταφέρονται στο δίκτυο δεν είχαν θέση στη προστασία δεδομένων της οδηγίας. Για παράδειγμα, η οδηγία θεωρεί νόμιμη την αόρατη συλλογή δεδομένων που χρησιμοποιείται για διαδικασίες πρόσβασης (π.χ. cookies) αλλά από την άλλη

πλευρά αν τα δεδομένα συλλέγονται με ορατό τρόπο πρέπει το άτομο να έχει δώσει τη συγκατάθεση του και να έχει ενημερωθεί. Συνεπώς σε κάθε περίπτωση αφού τα περισσότερα συστήματα Ηλεκτρονικής Διακυβέρνησης έχουν να κάνουν με μεταφορά ευαίσθητων δεδομένων μέσω του διαδικτύου, πρέπει τα συστήματα αυτά να λαμβάνουν υπόψη όλες τις αρχές προστασίας προσωπικών δεδομένων όπως ορίζονται από την εθνική και ευρωπαϊκή νομοθεσία.

3. Τεχνικές απαιτήσεις και ασφάλεια συστημάτων ηλεκτρονικής ψηφοφορίας

3.1. Απαιτήσεις συστημάτων για την ηλεκτρονική ψηφοφορία

Απαιτήσεις σε υλικό

Αρχικά πολύ σημαντικό ζήτημα είναι η επιλογή και συντήρηση κατάλληλου υλικού εξοπλισμού (hardware). Στην υπάρχουσα εκλογική διαδικασία το κυριότερο, αν όχι το μοναδικό υλικό, που χρησιμοποιείται είναι οι κάλπες και τα παραβάν. Όπως είναι προφανές δεν έχει νόημα να αναφέρουμε αυτό το θέμα ως απαίτηση ασφαλείας της συμβατικής εκλογικής διαδικασίας. Στην ηλεκτρονική ψηφοφορία, όμως, το θέμα του υλικού εξοπλισμού είναι πολύ σημαντικό. Ο τρόπος λειτουργίας του, καθώς και η αξιοπιστία των τμημάτων που το αποτελούν, πρέπει να είναι όσο το δυνατόν καλύτερης ποιότητας.

Οι κίνδυνοι που μπορεί να προκύψουν από ελλιπές ή ελαττωματικό υλικό δεν προκύπτουν μόνο από ηθελημένη και κακόβουλη τροποποίηση του, αλλά και από ακούσια βλάβη. Όσον αφορά την κακόβουλη τροποποίηση του υλικού εξοπλισμού πρέπει να υπάρχουν εντατικοί έλεγχοι και κατά την κατασκευή του, αλλά και κατά το χρονικό διάστημα που θα ακολουθήσει μέχρι να χρησιμοποιηθούν. Πιθανή προσπάθεια τροποποίησης των μηχανημάτων, που χρησιμοποιούνται σε μια εκλογική διαδικασία, θα πρέπει να οδηγεί είτε σε αποτυχία της προσπάθειας είτε σε καταστροφή του μηχανήματος, έτσι ώστε ένα μηχάνημα που λειτουργεί να είναι σίγουρο πως δεν έχει υποστεί τροποποίηση.

Όσον αφορά τυχόν βλάβη κατά τη διάρκεια της εκλογικής διαδικασίας, πρέπει να υπάρχει ειδικευμένο και εξουσιοδοτημένο προσωπικό σε κάθε εκλογικό κέντρο, ώστε να μπορεί άμεσα να επιδιορθώνει το πρόβλημα και να αποκαθιστά την ορθή λειτουργία του υλικού. Μέχρι τώρα έχουν γίνει διάφορες προτάσεις για ειδικά μηχανήματα που μπορούν να χρησιμοποιηθούν για μια εκλογική διαδικασία με επικρατέστερα μέχρι στιγμής τα DREs. Να αναφέρουμε πως μέσα στις ανάγκες για κατάλληλο υλικό μπορεί να αναφερθεί τυχόν χρήση έξυπνων καρτών (smart cards) για αυθεντικοποίηση των χρηστών.

Απαιτήσεις σε λογισμικό

Εξίσου σημαντικό ζήτημα είναι και η ανάπτυξη και ο έλεγχος του λογισμικού που χρησιμοποιείται. Τα σημαντικότερα θέματα που φαίνεται να σχετίζονται με το λογισμικό έχουν να κάνουν με τους κρυπτογραφικούς αλγόριθμους και με τη διαφάνεια του κώδικα. Η κρυπτογραφία είναι, ίσως, το σημαντικότερο εργαλείο για την εξασφάλιση της ακεραιότητας και της εμπιστευτικότητας των ψήφων, αλλά και των μηχανισμών αυθεντικοποίησης των ψηφοφόρων.

Η διαφάνεια του κώδικα είναι, επίσης, πολύ σημαντικό θέμα. Αρχικά, ο κώδικας πρέπει να είναι όσο το δυνατόν πιο απλός και ευκολονόητος, χωρίς βέβαια αυτό να σημαίνει υποβάθμιση της ασφάλειας. Όσο πιο απλός είναι ο κώδικας, τόσο πιο ευκολονόητος θα είναι και τόσο πιο εύκολος θα είναι ο έλεγχός του. Το να είναι ευκολονόητος ο κώδικας είναι βασικό στοιχείο για τη διαφάνεια του. Αυτό δεν

σημαίνει βέβαια πως πρέπει οποιοσδήποτε, χωρίς κατάλληλο υπόβαθρο γνώσεων, να μπορεί να τον καταλάβει, αλλά δεν πρέπει ο κώδικας να είναι κατανοητός μόνο στην προγραμματιστική ομάδα που το δημιούργησε, όσο έμπιστη και κοινής αποδοχής και να είναι. Επίσης, ένας απλός και καλά δομημένος κώδικας μπορεί να οδηγήσει στην εύκολη και έγκαιρη ανίχνευση κάποιας προσθήκης μη-εξουσιοδοτημένων τμημάτων (δούρειοι ίπποι, ιοί, κ.λπ.) [5].

Απαιτήσεις διασύνδεσης υπολογιστικών συστημάτων

Ένα ακόμα πολύ σημαντικό ζήτημα, που μπορεί να θέσει σε κίνδυνο μια ηλεκτρονική ψηφοφορία είναι το θέμα τις διασύνδεσης των διαφόρων υπολογιστικών συστημάτων που μετέχουν στην διαδικασία. Όσο μεγαλύτερη είναι η χρήση δικτυακής τεχνολογίας, τόσο περισσότεροι είναι και οι κίνδυνοι που δημιουργούνται. Το κατά πόσο η διαδικασία της ηλεκτρονικής ψηφοφορίας θα προϋποθέτει χρήση δικτύου είναι κάτι που θα εξαρτηθεί από την ακριβή δομή της. Γεγονός είναι, πάντως, πως όσο μεγαλύτερη χρήση δικτυακών επικοινωνιών γίνεται, η διαδικασία γίνεται πιο λειτουργική, αλλά παράλληλα αυξάνονται και οι πιθανότητες για παραβίαση της ασφάλειάς της. Διάφορες προτάσεις που έχουν γίνει ανά διαστήματα προσεγγίζουν το ζήτημα με διαφορετικούς τρόπους. Το ότι σε κάθε εκλογικό κέντρο θα υπάρχουν ειδικά μηχανήματα που θα ψηφίζουν οι πολίτες δεν σημαίνει αυτόματα πως αυτά θα πρέπει να επικοινωνούν μεταξύ τους μέσω δικτύου. Η συγκέντρωση των αποτελεσμάτων θα μπορούσε να γίνει με την χρήση CDs, η ακόμα και με τη χρήση διαφόρων μορφών κινητής μνήμης. Με αυτόν τον τρόπο η διαδικασία γίνεται πολύ πιο χρονοβόρα και το θέμα της ασφάλειας μετατίθεται στη φερεγγυότητα των ανθρώπων και των διαδικασιών μεταφοράς.

3.2. Συλλογή ψηφοδελτίων

Υπάρχουν πολλές ιδιότητες που θεωρούνται επιθυμητές για ένα σύστημα συλλογής ψηφοδελτίων:

- **Ακρίβεια (Accuracy).** Ένα σύστημα συλλογής είναι *ακριβές* αν (1) δεν είναι δυνατή η αλλοίωση της ψήφου, (2) δεν είναι δυνατή η μη συμπερίληψη ενός εγκύρου ψηφοδελτίου στον τελικό υπολογισμό του αποτελέσματος και (3) δεν είναι δυνατή η συμπερίληψη ενός άκυρου ψηφοδελτίου στο τελικό αποτέλεσμα. Σε ένα *εντελώς ακριβές* σύστημα, όσες πιθανές ανακρίβειες μπορεί να εμφανιστούν κατά τη συλλογή ψηφοδελτίων, εντοπίζονται και διορθώνονται. Τα *μερικώς ακριβή* συστήματα εντοπίζουν τις ανακρίβειες αλλά δεν τις διορθώνουν. Ο *βαθμός ακρίβειας* του συστήματος μπορεί να μετρηθεί με βάση τον αριθμό των λαθών, την πιθανότητα λάθους ή τον αριθμό των ‘‘επίφοβων’’ σημείων του συστήματος συλλογής στα οποία είναι πιθανή η εμφάνιση λάθους.
- **Ευχρηστία (Convenience).** Ένα σύστημα είναι εύχρηστο αν επιτρέπει στους ψηφοφόρους να ψηφίζουν σύντομα, με μια και μόνη ενέργεια, με ελάχιστο εξοπλισμό και χωρίς ειδικά προσόντα. Η ευχρηστία ενός συστήματος συλλογής είναι κάπως υποκειμενική, και εξαρτάται όχι μόνο

από το ίδιο το σύστημα, αλλά και από τον πληθυσμό που το χρησιμοποιεί. Για παράδειγμα, υπάρχουν πληθυσμοί ψηφοφόρων που θεωρούν πιο βολικό να ψηφίζουν σε κεντρικά εκλογικά τμήματα με παραδοσιακούς τρόπους, ενώ άλλοι θεωρούν βολικότερο το να ψηφίζουν μέσω ηλεκτρονικού υπολογιστή από το σπίτι ή το γραφείο τους.

- **Ευελιξία (Flexibility).** Ένα σύστημα θεωρείται ευέλικτο αν επιτρέπει την ύπαρξη πληθώρας μορφών ερωτημάτων στα συλλεγόμενα ψηφοδέλτια, συμπεριλαμβανομένων ερωτημάτων ‘‘ανοικτής απάντησης’’, ώστε να είναι δυνατή η ‘‘δυναμική’’ εγγραφή υποψηφίων και η εξαγωγή στατιστικών αποτελεσμάτων.
- **Κινητικότητα (Mobility).** Ένα σύστημα επιδεικνύει κινητικότητα αν δεν υπάρχουν περιορισμοί ως προς το μέρος από το οποίο ένας ψηφοφόρος μπορεί να ψηφίσει. Τα συστήματα που απαιτούν την ψηφοφορία σε προκαθορισμένα εκλογικά κέντρα δεν διαθέτουν κινητικότητα, εκτός κι αν έχει ληφθεί πρόνοια για την έμμεση συλλογή των απόψεων των απόντων ψηφοφόρων.
- **Μυστικότητα (Privacy).** Ένα σύστημα συλλογής είναι ‘‘μυστικό’’ αν (1) ούτε οι εκλογικές αρχές ούτε κανείς άλλος μπορούν να συσχετίσουν ένα ψηφοδέλτιο με τον ψηφοφόρο που το χρησιμοποίησε και (2) κανείς ψηφοφόρος δεν μπορεί να αποδείξει ότι ψήφισε με ένα συγκεκριμένο τρόπο. Έτσι δυσχεραίνονται οι εκλογικοί εκβιασμοί και η εξαγορά ψήφων.
- **Επαληθευσιμότητα (Verifiability).** Ένα σύστημα συλλογής θεωρείται ‘‘επαληθεύσιμο’’ αν ο κάθε εμπλεκόμενος στην ψηφοφορία μπορεί να επαληθεύσει πως όλοι οι ψήφοι έχουν καταμετρηθεί σωστά. Ένας ελαστικότερος ορισμός της επαληθευσιμότητας δέχεται ως επαληθεύσιμο το σύστημα εκείνο που επιτρέπει στους ψηφοφόρους να επαληθεύσουν τις δικές τους ψήφους και ίσως να διορθώσουν πιθανά λάθη χωρίς να διακινδυνεύσουν την ιδιωτικότητα της ψήφου. Τα παραδοσιακά συστήματα συλλογής επιτρέπουν μόνο την μερική επαλήθευση του αποτελέσματος (μέσω της παρακολούθησης της διαδικασίας) από κομματικούς αντιπροσώπους [14].

3.3. Κύρια χαρακτηριστικά ενός Ηλεκτρονικού Συστήματος Ψηφοφορίας

Το σύστημα θα πρέπει να υποστηρίζει όλες εκείνες τις διαδικασίες που απαιτούνται για την ομαλή οργάνωση και διεξαγωγή των εκλογών. Ανάλογα του είδους των εκλογών οι υπηρεσίες που το σύστημα παρέχει ενδέχεται να περιλαμβάνουν την εγγραφή των ψηφοφόρων, την αυθεντικοποίηση τους, την ίδια τη ψήφο, τον υπολογισμό και την επιβεβαίωση του τελικού αποτελέσματος.

Το σύστημα θα πρέπει να υποστηρίζει όλες τις συμμετέχουσες οντότητες (ρόλους). Χαρακτηριστικά αναφέρονται οι οργανωτές των εκλογών, οι εκπρόσωποι των κομμάτων, οι υποψήφιοι, οι ψηφοφόροι .

Το σύστημα πρέπει να παρέχει ένα φιλικό στο χρήστη περιβάλλον, ώστε να

μπορεί να χρησιμοποιείται από οποιοδήποτε απλό φυλλομετρητή του Διαδικτύου (Web Browser).

Το σύστημα πρέπει να υποστηρίζει ένα σύνολο υπηρεσιών και ενεργειών, ώστε να μπορεί να διευκολύνει το χρήστη κατά την χρησιμοποίησή του.

Το σύστημα πρέπει να είναι σε θέση να υπολογίζει το τελικό αποτέλεσμα της καταμέτρησης των ψήφων [5].

3.4. Απαιτήσεις του συστήματος

Οι λειτουργικές απαιτήσεις ενός συστήματος ηλεκτρονικής ψηφοφορίας καθορίζουν κατά ελάχιστο ένα σύνολο υπηρεσιών (λειτουργιών) που το σύστημα πρέπει να υποστηρίζει διασφαλίζοντας ταυτόχρονα την ομαλή ροή αυτών, καθώς και τις ενδεχόμενες αλληλεπιδράσεις τους. Για παράδειγμα, ο αριθμός και ο τύπος των εκάστοτε εκλογικών διαδικασιών που υποστηρίζονται από ένα σύστημα ηλεκτρονικής ψηφοφορίας καθορίζονται από το σύνολο των λειτουργικών του απαιτήσεων. Επιπλέον, οι λειτουργικές απαιτήσεις σχετίζονται με πολλές από τις ιδιότητες χρήσης του συστήματος καθορίζοντας τις λειτουργίες και τα χαρακτηριστικά που αυτό πρέπει να παρέχει κατά τη χρήση του.

Από την άλλη, οι μη-λειτουργικές απαιτήσεις σχετίζονται με τη βασική υποδομή του συστήματος, δεν είναι άμεσα εμφανείς στους χρήστες και καθορίζουν πολλά από τα χαρακτηριστικά της αρχιτεκτονικής του συστήματος. Οι απαιτήσεις ασφάλειας ορίζουν διάφορες ιδιότητες που αφορούν το σύστημα στο σύνολό του, όπως η ευελιξία του, η αποδοτικότητά του κ.ά., και προέρχονται από το σύνολο των μη-λειτουργικών απαιτήσεων [5].

3.4.1. Απαιτήσεις Πρακτικότητας

Το σύστημα πρέπει να είναι εύκολα υλοποιήσιμο, συμβατό με τις διάφορες τεχνολογίες και πλατφόρμες (λειτουργικά συστήματα, αρχιτεκτονικές, εργαλεία πλοήγησης στο Web κ.λ.π), λειτουργικό, και να απευθύνεται σε όλες τις κατηγορίες πληθυσμού ανεξαρτήτως ηλικίας, γλώσσας, φυσικών ικανοτήτων, μόρφωσης, εξοικείωσης με τις τεχνολογίες του Internet κ.λ.π.. Επίσης, το σύστημα πρέπει να υποστηρίζει μια ποικιλία από format ψήφων, συμπεριλαμβανομένων και των λεγόμενων ‘‘λευκών’’ ή άκυρων ψήφων. Το σύστημα θα πρέπει να παρουσιάζει χαμηλή υπολογιστική πολυπλοκότητα και η αποδοτικότητα του να μην επηρεάζεται δραστικά από το μέγεθος του εκλεκτορικού σώματος ή των υποψηφίων (scalability), ενώ οι υπηρεσίες ασφάλειας που προσφέρει θα πρέπει να είναι διαφανείς (transparent) στον χρήστη [4].

3.4.2. Απαιτήσεις Ασφαλείας

Σε περίπτωση που πρόκειται να αντικατασταθεί η παραδοσιακή μορφή ψηφοφορίας με κάποιο σύστημα ηλεκτρονικής ψηφοφορίας πρέπει να διασφαλίζονται οι αντίστοιχες απαιτήσεις ασφάλειας.

Ορθότητα-Ακρίβεια (Accuracy)

Η ορθότητα απαιτεί ότι το τελικό ανακοινωθέν αποτέλεσμα της εκλογικής διαδικασίας είναι το ίδιο με το πραγματικό αποτέλεσμα των εκλογών, όπως αυτό προκύπτει από την καταμέτρηση των ψήφων. Αυτό κατ' επέκταση, σημαίνει ότι κανένας δεν είναι σε θέση να αλλάξει την ψήφο κάποιου άλλου ψηφοφόρου (inalterability), όλες οι έγκυρες ψήφοι συμπεριλαμβάνονται στο τελικό αποτέλεσμα (completeness) και καμία μη έγκυρη ψήφος δεν συμπεριλαμβάνεται στο τελικό αποτέλεσμα (soundness).

Δημοκρατία (Democracy)

Ένα σύστημα χαρακτηρίζεται δημοκρατικό αν και μόνο αν νόμιμοι χρήστες επιτρέπεται να ψηφίσουν και κάθε νόμιμος χρήστης μπορεί να ψηφήσει μόνο μία φορά. Ένα επιπλέον χαρακτηριστικό είναι ότι κανένας δεν είναι σε θέση να ψηφίσει εκ μέρους κάποιου άλλου.

Ιδιωτικότητα (Privacy)

Η συγκεκριμένη απαίτηση σχετίζεται με το γεγονός ότι κανένας δεν είναι σε θέση να συνδέσει την ταυτότητα ενός ψηφοφόρου με την εκάστοτε ψήφο του. Η υπολογιστική ιδιωτικότητα (computational privacy) αποτελεί μια ασθενή μορφή ιδιωτικότητας διασφαλίζοντας ότι η σχέση μεταξύ ψηφοδελτίου παραμένει μυστική για ένα μεγάλο χρονικό διάστημα, χρησιμοποιώντας ακόμα και τα πιο σύγχρονα και ισχυρά υπολογιστικά συστήματα. Η ιδιωτικότητα που βασίζεται στη θεωρία των πληροφοριών (information-theoretic privacy) αποτελεί μια πιο ισχυρή μορφή διατήρησης της ιδιωτικότητας, η οποία διασφαλίζει ότι κανένα ψηφοδέλτιο δεν μπορεί να συσχετισθεί με κάποιο ψηφοφόρο όσο χρονικό διάστημα η θεωρία των πληροφοριών παραμένει ισχυρή.

Ανθεκτικότητα (Robustness)

Η απαίτηση αυτή εγγυάται ότι δεν μπορεί να λάβει χώρα μια προσωρινή συνεργασία είτε ψηφοφόρων είτε αρχών (νόμιμη η κακόβουλη), η οποία θα μπορούσε να διακόψει την εκλογική διαδικασία. Η κατάσταση αυτή περιλαμβάνει τη δυνατότητα αποχής των ψηφοφόρων χωρίς την εμφάνιση προβλημάτων, καθώς επίσης, και την αποτροπή παράνομων ενεργειών οι οποίες ενδέχεται να ακυρώσουν το αποτέλεσμα των εκλογών. Η απαίτηση της ανθεκτικότητας (ρωμαλεότητα, robustness) αφορά επίσης και το ότι η ασφάλεια του συστήματος πρέπει να ικανοποιείται και σε σχέση με εξωτερικές απειλές και επιθέσεις π.χ. επιθέσεις άρνησης υπηρεσιών (DoS attacks).

Επαληθευσιμότητα (Verifiability)

Η επαληθευσιμότητα σχετίζεται με το ότι υπάρχουν μηχανισμοί για τον έλεγχο της εκλογικής διαδικασίας προκειμένου να διασφαλιστεί ότι αυτή διεξήχθη κανονικά. Η επαληθευσιμότητα μπορεί να επιτευχθεί σε τρεις (3) διαφορετικές μορφές:

Οικουμενική επαληθευσιμότητα, η οποία σχετίζεται με το ότι ο οποιοσδήποτε

(ψηφοφόροι, αρχές, εξωτερικοί ελεγκτές κ.ά.) είναι σε θέση να επιβεβαιώσουν το αποτέλεσμα μετά την καταμέτρηση των ψήφων,

Μεμονωμένη επαληθευσιμότητα με ανοικτή αντίρρηση στην καταμέτρηση, η οποία επιτρέπει σε κάθε ψηφοφόρο να επιβεβαιώσει ότι η ψήφος του όντως καταμετρήθηκε σωστά, χωρίς, όμως, να αποκαλυφθεί το περιεχόμενο αυτής,

Μεμονωμένη επαληθευσιμότητα, η οποία επιτρέπει την ατομική επιβεβαίωση της ψήφου για κάθε ψηφοφόρο, αλλά από την άλλη απαιτεί την αποκάλυψη του ψηφοδελτίου του ψηφοφόρου σε περίπτωση καταγγελίας.

Μη εξαναγκασμός (Uncoercibility)

Ένα σχήμα χωρίς απόδειξη (receipt-free scheme) είναι σε θέση να πείσει τους ψηφοφόρους ότι η ψήφος τους καταμετρήθηκε, χωρίς όμως να μπορεί να παρέχει απόδειξη για αυτό. Ένα σχήμα μη εξαναγκασμού (uncoercible scheme) δεν επιτρέπει στους ψηφοφόρους να πείσουν οποιονδήποτε για το τι έχουν ψηφίσει. Πιο συγκεκριμένα, στην περίπτωση αυτή ο ψηφοφόρος δεν κατέχει ούτε μπορεί να δημιουργήσει μια απόδειξη που να δείχνει το περιεχόμενο της ψήφου. Ενώ η έννοια του μη-εξαναγκασμού είναι πιο ισχυρή από το σχήμα χωρίς απόδειξη, η δεύτερη έννοια συνηθίζεται να χρησιμοποιείται στη βιβλιογραφία σαν το επικρατέστερο μέσο προκειμένου να διασφαλιστεί η ασφάλεια του συστήματος ηλεκτρονικής ψηφοφορίας.

Αμεροληψία (Fairness)

Η ιδιότητα αυτή διασφαλίζει ότι κανένας δεν είναι σε θέση να μάθει το αποτέλεσμα της εκλογικής διαδικασίας πριν την τελική καταμέτρηση των ψήφων. Συνεπώς, διασφαλίζει ότι δεν θα επηρεαστούν οι τελευταίοι χρονικά ψηφοφόροι μέσω της ανακοίνωσης μιας εκτίμησης του αποτελέσματος και ότι δεν παρέχεται ένα πλεονέκτημα σε ένα συγκεκριμένο σύνολο οντοτήτων.

Επαληθεύσιμη συμμετοχή (Verifiable participation)

Η συγκεκριμένη απαίτηση διασφαλίζει ότι υπάρχει δυνατότητα να βρεθεί αν ένας συγκεκριμένος ψηφοφόρος πήρε μέρος στην εκλογική διαδικασία ή όχι. Η συγκεκριμένη απαίτηση είναι αναγκαία στις περιπτώσεις όπου η συμμετοχή στη ψηφοφορία είναι υποχρεωτική (πχ. Ελλάδα, Αυστραλία, Βέλγιο κα) ή σε περιπτώσεις οργανισμών ή σωματείων που ακόμα και το μέγεθος της αποχής έχει κάποιο συγκεκριμένο νόημα. [4]

3.5. Απειλές και Μέθοδοι επίθεσης

Τα απομακρυσμένα ηλεκτρονικά συστήματα ψηφοφορίας (Remote Electronic Voting, REV) καταργούν τα γεωγραφικά εμπόδια και τα παραδοσιακά συστήματα εκλογών. Το σύστημα ψηφοφορίας δεν είναι πλέον περιορισμένο στον τοπικό σταθμό ψηφοφορίας. Είναι προσβάσιμο παγκοσμίως, αυξάνοντας δραματικά τον πιθανό αριθμό επιθέσεων. Από την ίδια τη φύση της, η διαδικασία της εκλογής είναι ένας ελκυστικός στόχος για κακόβουλες ενέργειες. Ένα online σύστημα πρέπει να

κερδίσει την δημόσια εμπιστοσύνη, η οποία εύκολα θα μπορούσε να υπονομευθεί από μια λάθος εκλογική ημέρα. Δύο είναι οι πιθανές πηγές επιθέσεων, οι εσωτερικές και οι εξωτερικές:

3.5.1. Εσωτερικές

Οι **νόμιμοι χρήστες** ενός REV συστήματος ίσως επιδιώξουν τη κακή χρήση ή ζημιά στο εκλογικό σύστημα και ίσως να έχουν τεχνικές ικανότητες για να υπονομεύσουν το σύστημα. Επειδή είναι νόμιμοι χρήστες υπόκεινται και σε νομικές κυρώσεις αν η επίθεση επικεντρώνεται σε αυτούς.

Οι **διαχειριστές** REV συστήματος πολύ συχνά εκμεταλλεύονται την προνομιούχο θέση τους. Μπορούν να συγκεντρώνουν πληροφορίες από κυβερνητικούς υπαλλήλους, υπαλλήλους οργανισμών αλλά και εξωτερικούς υπαλλήλους. Όλες αυτές οι πληροφορίες τους δίνουν γνώση για τα δικαιώματα προσβασιμότητας. Ίσως το κίνητρο τους είναι να εξαπατηθούν οι εκλογές για οικονομικό κέρδος, για προσωπική ικανοποίηση ή και για πολιτικούς λόγους. Οι διαχειριστές υπηρεσιών και οι κυβερνητικοί υπάλληλοι υπόκεινται εύκολα σε κυρώσεις αν η επίθεση επικεντρώνεται σε αυτούς. Οι υπόλοιποι κάτοχοι μυστικών πληροφοριών (κυβερνητικοί υπάλληλοι) που έχουν πρόσβαση στο REV σύστημα αλλά δεν συσχετίζονται με τη φροντίδα των εκλογικών υπηρεσιών ίσως καθοδηγήσουν εσωτερικές επιθέσεις. Αυτά τα άτομα ίσως έχουν οικονομικό, προσωπικό ή πολιτικό κίνητρο.

3.5.2. Εξωτερικές

Hackers ίσως προσπαθήσουν να δημιουργήσουν διακοπή ή αναστάτωση στο σύστημα λόγω προσωπικού φθόνου, επειδή πιστεύουν ότι η επίθεση σε ένα κυβερνητικό σύστημα είναι πρόκληση ή επειδή θέλουν να διαμαρτυρηθούν στη κυβέρνηση. Πολλοί εγκληματικοί οργανισμοί και άλλοι, όπως οικονομικοί μεσάζοντες ίσως θελήσουν να έχουν πρόσβαση στο σύστημα για να επωφεληθούν από προσωπικές πληροφορίες.

Ομάδες Διαμαρτυρίας ή ακτιβιστές επιδιώκουν να επιτεθούν στα συστήματα με σκοπό να δείξουν την αντίθεση τους με το REV, να διακόψουν τους ηλεκτρονικούς μηχανισμούς, να εκμεταλλευτούν πληροφορίες και για σκοπούς φθοράς. Επίσης ενδιαφέρονται πολλές φορές να διαπεράσουν το σύστημα για να αλλάξουν το αποτέλεσμα ενός διαγωνισμού ή μιας πολιτικής εκλογής.

Ξένες υπηρεσίες πληροφοριών θέλουν να αποκτήσουν προσωπικές πληροφορίες για γνώση και ανάλυση. Επιπρόσθετα θέλουν να έχουν πρόσβαση στα συστήματα για συλλογή πολιτικών πληροφοριών και την διαχείριση τους με σκοπό την αλλαγή έκβασης του αποτελέσματος.

Ερευνητές ή δημοσιογράφοι ενδιαφέρονται για σκόπιμη υπονόμευση του συστήματος εκλογών ώστε να αποδείξουν ότι τα συστήματα REV έχουν προβλήματα ασφάλειας.

Τρομοκρατικοί οργανισμοί που ενδιαφέρονται για συλλογή προσωπικών

πληροφοριών. Επίσης θέλουν να γνωρίζουν τις εκλογικές προθέσεις για να επηρεάσουν το αποτέλεσμα ή να διακόψουν τη διαδικασία.

Οι μέθοδοι που διακρίνονται ως οι πιο πιθανές για τέτοιου είδους επιθέσεις είναι οι παρακάτω:

- Ηλεκτρονικές Επιθέσεις
- Hacking

Η εισχώρηση στο REV σύστημα πρέπει να έχει πολλές διακλαδώσεις ώστε να παρέχει εμπιστοσύνη στο κοινό που ψηφίζει Online. Για να είναι αποτελεσματική μια τέτοια επίθεση δεν πρέπει καν να αλλάξει τα δεδομένα που αποθηκεύονται στο σύστημα. Η επίθεση δεν παίρνει μέρος κατά τη διάρκεια των εκλογών άλλα άλλη χρονική στιγμή ή μετά τις εκλογές. Μεγάλες ποσότητες προσωπικών δεδομένων που χρησιμοποιούνται από τους ψηφοφόρους για να επικυρώσουν τους εαυτούς τους στη φάση της καταχώρισης μπορούν να αποκαλυφθούν. Πληροφορίες μπορούν να χρησιμοποιηθούν για να συνδεθούν οι ψηφοφόροι με τις ψήφους και να υπονομευθεί η ανωνυμία. Λιγότερο σοβαρή απειλή θεωρείται η αλλαγή εμφάνισης του site που επίσης κλονίζει την εμπιστοσύνη του συστήματος. Αν οι υπερσύνδεσμοι του site αλλαχτούν, επηρεάζεται η πληρότητα και η εμπιστευτικότητα των ψήφων με αποτέλεσμα την ακύρωση της εκλογής. Οι μεμονωμένες πλατφόρμες δύσκολα αποτελούν στόχο για τους Hackers. Αντίθετα τα δημόσια τερματικά διαδικτύου είναι ένας ελκυστικός στόχος και πρέπει να ασφαλίζονται κατάλληλα.

Κακόβουλα προγράμματα (“malware”)

Υπάρχει πάντα ο κίνδυνος εισχώρησης ενός κακόβουλου προγράμματος στον REV server πριν ή κατά τη διάρκεια των εκλογών, μέσω ηλεκτρονικού ταχυδρομείου ή εξωτερικού συνδέσμου επικοινωνίας. Επιπλέον, ο τεράστιος αριθμός PCs που επικοινωνούν με το REV σύστημα μπορεί να αυξήσει τη πιθανότητα κινδύνου ενός κακόβουλου προγράμματος. Αυτό μπορεί να προκαλέσει ζημιά στο server και πιθανότατα να πολλαπλασιαστεί και σε άλλα PCs. Η κυβέρνηση πρέπει να είναι προετοιμασμένη για οποιαδήποτε ζημιά. Εάν ένα πρόγραμμα τύπου ‘‘Δούρειος Ίππος’’ εγκατασταθεί στο REV σύστημα, η εμπιστευτικότητα και η ακεραιότητα των ψήφων επηρεάζεται αρνητικά και μπορεί να ακυρωθεί η διαδικασία. Είναι πιθανό για έναν εισβολέα να εγκαταστήσει κακόβουλο πρόγραμμα που να παραμένει ανενεργό μέχρι τη στιγμή της εκλογής. Ένα πρόγραμμα όπως ο ‘‘Δούρειος Ίππος’’ είναι ικανό να μεταβιβάσει πληροφορίες σε τρίτους για το τρόπο με τον οποίο ένα άτομο ψήφισε ή να αλλάξει τη ψήφο ενός ατόμου. Άλλου τύπου κακόβουλα προγράμματα είναι τα worms που αναπαράγουν τον εαυτό τους εσωτερικά σε έναν υπολογιστή ή ακόμα και σε άλλους μέσω δικτύου. Τα προγράμματα αυτά εκμεταλλεύονται λάθη του συστήματος και μετά από κάποιο χρονικό διάστημα το κατακλύζουν ώστε να μην μπορεί να λειτουργήσει.

Πρόβλημα διαθεσιμότητας (DOS)

Με τη συνεχή και ταυτόχρονη χρήση του REV συστήματος ίσως δημιουργηθεί πρόβλημα και η εφαρμογή παραμείνει προσωρινά μη διαθέσιμη. Μια κακόβουλη επίθεση ή μια μαζική ακούσια κακή χρήση μπορεί να καταστήσει το σύστημα μη διαθέσιμο, είτε προσωρινά, είτε στη κατά τη διάρκεια της εκλογής.

Επιθέσεις στο DNS

Υπάρχει πάντα η πιθανότητα ένας επιτιθέμενος να αλλάξει μια εγγραφή στο DNS. Αυτό θα επέτρεπε στον κάτοχο του ψεύτικου site να υπονομεύσει τη ψηφοφορία του επαναπροσανατολιζόμενου ψηφοφόρου. Το ίδιο αποτέλεσμα μπορεί να επιτευχθεί από τον επιτιθέμενο αν εγκαταστήσει ένα πρόγραμμα που θα λέει στον browser να χρησιμοποιεί μια ιστοσελίδα σαν proxy, ουσιαστικά κάνοντας μια επίθεση "man-in-the-middle".

3.5.3. Άλλου είδους επιθέσεις

Εξαγορά ψήφων/ πώληση και εξαναγκασμός

Η εξαγορά ψήφων και οι δραστηριότητες πώλησης και εξαναγκασμού δημιουργούν σοβαρή απειλή για το σύστημα REV καθώς δεν υπάρχει φυσικός τρόπος για να παρατηρηθεί η ρίψη των ψήφων. Οι μηχανισμοί που υπάρχουν για να υπολογίσουν αυτές τις απειλές είναι σε πειραματική/ερευνητική μορφή.

Κλοπή ή παραποίηση ενός μέρους ψήφων

Η κλοπή και η παραποίηση ενός μέρους των ψήφων μπορεί να γίνει είτε ηλεκτρονικά είτε όχι. Αν γίνει χρήση κλεμμένων ή παραποιημένων ψήφων δημιουργείται πρόβλημα στο σύστημα REV που δεν μπορεί να υπολογίσει τη νομιμότητα των ψήφων. Οι μηχανισμοί που υπάρχουν για να υπολογίζουν αυτές τις απειλές είναι σε πειραματική/ερευνητική μορφή.

Σκόπιμη άρνηση της συναλλαγής

Κάποιος επιτιθέμενος μπορεί πιθανότατα να πάει στα μέσα ενημέρωσης και να παραπονεθεί ότι δήθεν δεν ψήφισε. Με αυτό το τρόπο θα μπορούσε αναμφισβήτητα να προκαλέσει πρόβλημα στο σύστημα.

3.5.4. Μη προβλέψιμες απειλές

Χρήστες

Οι νόμιμοι χρήστες μπορούν να προκαλέσουν ακούσια, κακή χρήση του REV ή πιθανή ζημιά του συστήματος. Μεγάλος αριθμός ψηφοφόρων χρησιμοποιεί το σύστημα λανθασμένα και μπορεί να οδηγήσει στην περιττή απώλεια απόδοσης ή ακόμα και στην καταστροφή.

Εξοπλισμός

Η λάθος επιλογή εξοπλισμού ή του προγράμματος μπορεί να οδηγήσει σε αναστολή της υπηρεσίας ή σε απώλεια δεδομένων.

Ανωτέρα Βία

Ένα ατύχημα ή ένα φυσικό φαινόμενο μπορεί να καταστρέψει τη παροχή υπηρεσιών ή τις αποθηκευμένες πληροφορίες.

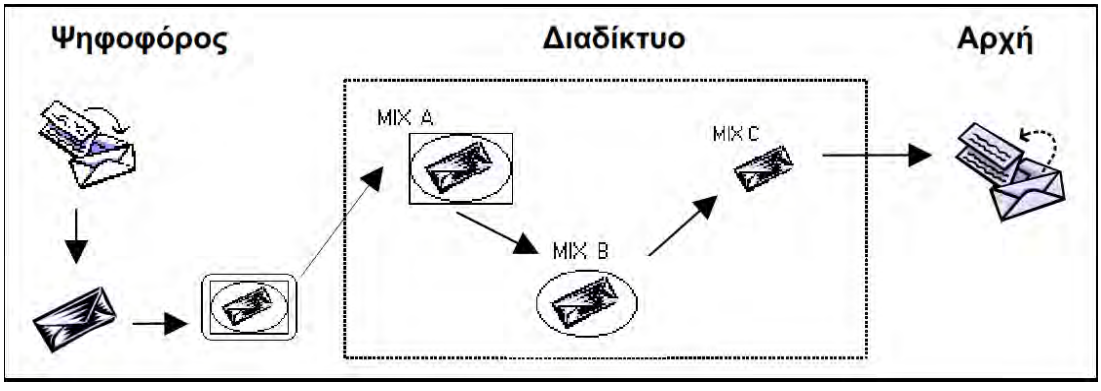
4. Μοντέλα – Πρωτόκολλα Κρυπτογραφίας

4.1. Mix-nets

Ο Chaum (όπως αναφέρεται στο βιβλίο Secure Electronic Voting) εισήγαγε την έννοια των μοντέλων MIX-net (MIX networks) τα οποία αποτελούν έναν κρυπτογραφικό μηχανισμό για την κατασκευή ανώνυμων καναλιών (anonymous channels) σε εφαρμογές υψηλής ασφάλειας. Ένα δίκτυο MIX-net αποτελείται από έναν αριθμό εξυπηρετητών, συνδεδεμένων μεταξύ τους, που καλούνται κόμβοι MIX. Κάθε κόμβος MIX λαμβάνει ως είσοδο (input) ένα σύνολο μηνυμάτων (π.χ. τις κρυπτογραφημένες ψήφους), κάνει κάποιους τυχαίους μετασχηματισμούς και επιστρέφει στην έξοδο (output) ένα διαφορετικό σύνολο μηνυμάτων, κατά τρόπο ώστε τα μηνύματα της εξόδου να μη μπορούν να συνδεθούν με τα εκείνα της εισόδου. Κατ' αυτόν τον τρόπο, καμία συνεργία οποιουδήποτε αριθμού κόμβων MIX (εκτός από την περίπτωση όπου συνεργούν όλοι μαζί) δε μπορεί να καθορίσει ποια ψήφος αντιστοιχεί σε ποιον ψηφοφόρο.

Στο δίκτυο MIX-net αποκρυπτογράφησης λειτουργούμε διαφορετικά, κάθε ψήφος κρυπτογραφείται διαδοχικά με τα δημόσια κλειδιά όλων των κόμβων MIX, με σειρά αντίστροφη της σειράς των κόμβων. Η ψήφος κρυπτογραφείται πρώτα με το δημόσιο κλειδί του MIX_C που θα παραλάβει τελευταίο τη λίστα με τις κρυπτογραφημένες ψήφους, στη συνέχεια με το κλειδί του προτελευταίου MIX_B και τέλος με το δημόσιο κλειδί του πρώτου τη τάξει MIX_A. Κάθε κόμβος MIX αποκρυπτογραφεί τη λίστα των ψήφων που του αποστέλλονται, τη μετασχηματίζει (π.χ. προσθέτοντας τυχαιότητα σε κάθε ψήφο και αναδιατάσσοντας τη λίστα με τις ψήφους που προκύπτει), και στη συνέχεια την προωθεί στον επόμενο κόμβο.

Ένας άλλος τύπος είναι το MIX-net επανακρυπτογράφησης, όπου όλες οι ψήφοι κρυπτογραφούνται με το δημόσιο κλειδί του πρώτου κόμβου MIX, και στη συνέχεια σε κάθε κόμβο MIX λαμβάνει χώρα ο μετασχηματισμός και η κρυπτογράφηση με το δημόσιο κλειδί του επόμενου κόμβου, με τρόπο επαληθεύσιμο μεταξύ των κόμβων ή για τους εξωτερικούς παρατηρητές.



Εικόνα 2. Παράδειγμα δικτύου MIX-net [14]

Οι πλέον χρήσιμες ιδιότητες των δικτύων MIX-net, ειδικά για εκλογές μεγάλης κλίμακας, είναι η οικουμενική επαληθευσιμότητα της ορθότητας των μετασχηματισμών και της αποκρυπτογράφησης που προσφέρουν, καθώς και η ανθεκτικότητα τους έναντι συνεργιών μεταξύ (έως) ενός ορισμένου αριθμού κακόβουλων ή δυσλειτουργικών κόμβων MIX που επιχειρούν να παρακωλύσουν την εκλογική διαδικασία ή να καταλύσουν τη μυστικότητα των ψήφων ή/και την ορθότητα των αποτελεσμάτων [44]. Επίσης, τα δίκτυα MIX-net θεωρούνται αποδοτικά:

Για τους εξωτερικούς παρατηρητές (που επιχειρούν να επαληθεύσουν την ορθότητα των πράξεων), αν και εφόσον ο υπολογιστικός φόρτος για τον παρατηρητή είναι σταθερός και ανεξάρτητος από τον αριθμό των κόμβων MIX που συμμετέχουν στη διαδικασία.

Για τους ψηφοφόρους, αν και εφόσον ο υπολογιστικός φόρτος για κάθε ψηφοφόρο είναι επίσης ανεξάρτητος του αριθμού των κόμβων MIX.

Για τους εξυπηρετητές (κόμβοι MIX), αν και εφόσον η υπολογιστική πολυπλοκότητα για κάθε κόμβο είναι ανεξάρτητη από τον αριθμό των υπολοίπων κόμβων που συμμετέχουν στη διαδικασία.

Έως σήμερα πάντως, κανένα σύστημα ηλεκτρονικής ψηφοφορίας δεν έχει υλοποιηθεί με χρήση τεχνικών MIX-net. Ωστόσο οι μηχανισμοί δικτύων MIX-net έχουν χρησιμοποιηθεί κατά καιρούς για την επίτευξη ανωνυμίας σε εφαρμογές ηλεκτρονικού εμπορίου.

Αυτό το ασφαλές ανώνυμο κανάλι επικοινωνίας που ονομάστηκε Mix-net, στηρίζεται στη χρήση κρυπτοσυστημάτων δημοσίου κλειδιού. Έστω Q το δημόσιο κλειδί ενός ψηφοφόρου και P το ιδιωτικό του. Θεωρούμε ότι ισχύει:

$D_P E_Q(X) = D_Q E_P(X)$ όπου X είναι το μήνυμα (ψήφος), D είναι η αποκρυπτογράφηση και E είναι η κρυπτογράφηση.

Έστω M το μήνυμα και C το αντίστοιχο κρυπτογράφημα. Αν και τα δυο είναι δημόσια γνωστά μπορούμε να κρύψουμε την αντιστοιχία μεταξύ τους κρυπτογραφώντας το M ως εξής:

$C = E_Q(M \circ R)$ και R τυχαίος αριθμός.

Η ψηφιακή υπογραφή ενός τυχαίου αριθμού R σχηματίζεται ως εξής:

$D = E_P(R \circ 0^l)$ όπου l ένα σχετικά μεγάλος αριθμός.

Δημιουργία ενός ανώνυμου καναλιού:

Έστω ότι υπάρχουν n αποστολείς $A_1,\ldots,A_n$ και κάθε ένας από αυτούς θέλει να στείλει ένα μήνυμα m_i σε ένα παραλήπτη B_i με τέτοιο τρόπο που να μην αποκαλύπτεται η επικοινωνία μεταξύ τους. Έστω ότι υπάρχουν K μίκτες S_i. Τα δημόσια κλειδιά των B_i και S_i είναι Q_{Bi} kai Q_{Si} αντίστοιχα.

Βήμα 1ο: Κάθε A_i επιλέγει τυχαίους αριθμούς $R_1,\ldots R_k$, (όσοι και οι μίκτες) και δημοσιεύει στον Πίνακα Ανακοινώσεων:

$$E_{Q_{S_1}}(R_1 \circ E_{Q_{S_2}}(R_2 \ldots E_{Q_{Si}}(R_k \circ B_i \circ E_{Q_{Bi}}(m_i))\ldots))$$

Δηλαδή ο A_i κρυπτογραφεί το μήνυμά του με το δημόσιο κλειδί του B_i. Μετά κρυπτογραφεί το αριθμό R_k την ταυτότητα του B_i και το κρυπτογραφημένο του μήνυμα με το δημόσιο κλειδί του κ-οστού μίκτη, κοκ.

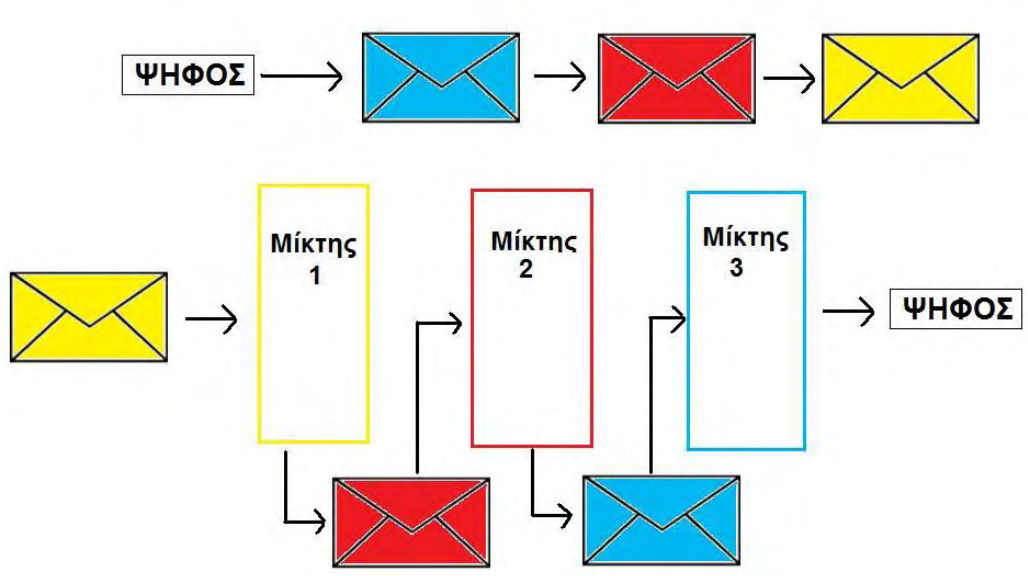
Βήμα 2ο: Ο S_1 λαμβάνοντας το μήνυμα αποκρυπτογραφεί με το ιδιωτικό του κλειδί και δημοσιεύει:

$$E_{Q_{S_2}}(R_2 \ldots E_{Q_{Si}}(R_k \circ B_i \circ E_{Q_{Bi}}(m_i))\ldots)$$

Βήμα 3ο: Οι $S_2 \ldots S_{k-1}$ μίκτες με τη σειρά τους επαναλαμβάνουν το βήμα 2, χρησιμοποιώντας ο κάθε ένας το ιδιωτικό του κλειδί.

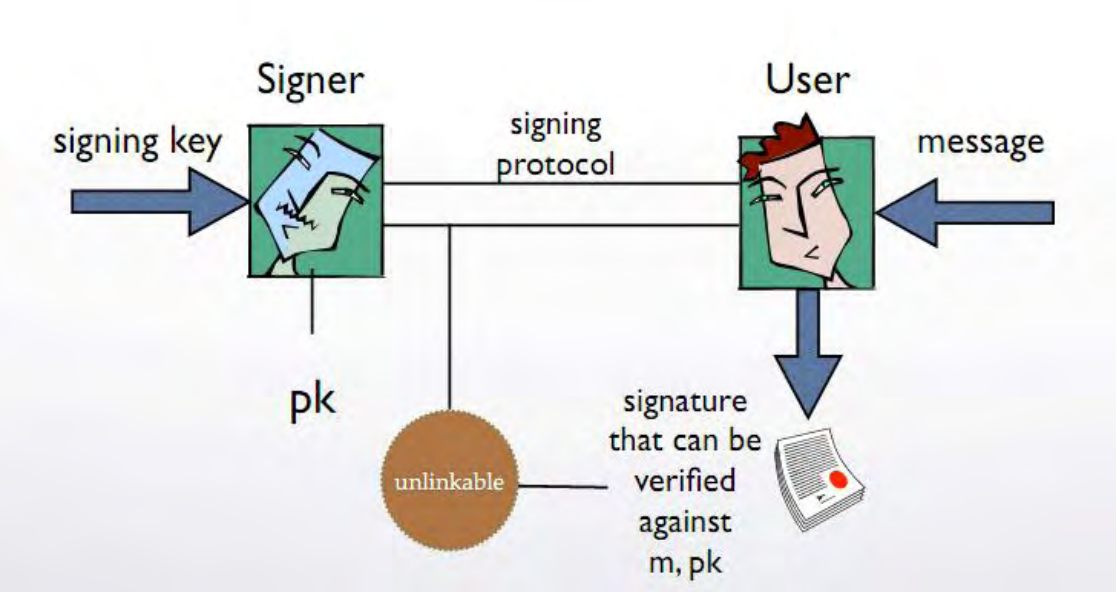
Βήμα 4ο: Στο τέλος ο Sk γράφει στον Πίνακα Ανακοινώσεων το: $Bi \circ E_{Q_{S_i}}(m_i)$

Αν ο S_k δεν είναι έντιμος, τότε μπορεί να γράψει στον Πίνακα κάτι διαφορετικό από το σωστό μήνυμα. Αν ο A_i παραπονεθεί, αφού έχει καταλάβει το λάθος, τότε θα μαθευτεί ότι εκείνος ήταν που ήθελε να στείλει ένα μήνυμα στο B_i. Κάτι τέτοιο όμως δεν είναι καλό για τη χρήση του ανώνυμου καναλιού σε εκλογική διαδικασία.



Εικόνα 3. Παράδειγμα Mix-net αποκρυπτογράφηση

4.2. Μοντέλο των ‘‘Τυφλών Υπογραφών’’ - Blind Signatures



Εικόνα 4. Μοντέλο ‘‘τυφλών υπογραφών’’

Η ‘‘τυφλή υπογραφή’’ (blind signature) σαν έννοια παρουσιάστηκε αρχικά από τον Chaum ως μια κρυπτογραφική μέθοδος που επιτρέπει σε έναν υπογράφοντα να ταυτοποιήσει ένα έγγραφο χωρίς να έχει κάποια πληροφορία για αυτό. Οι δύο βασικοί στόχοι μιας ‘‘τυφλής υπογραφής’’ είναι η μη πλαστογράφηση και η τυφλότητα (blindness), όπου η τυφλότητα αναφέρεται στην αδυναμία του υπογράφοντα να αντλήσει κάποια πληροφόρηση από το έγγραφο που υπογράφει. Επομένως το ιδιαίτερο χαρακτηριστικό των ‘‘τυφλών υπογραφών’’ είναι η μη συνδεσιμότητά τους (unlinkability) . [8]

4.2.1. Το μοντέλο του Chaum

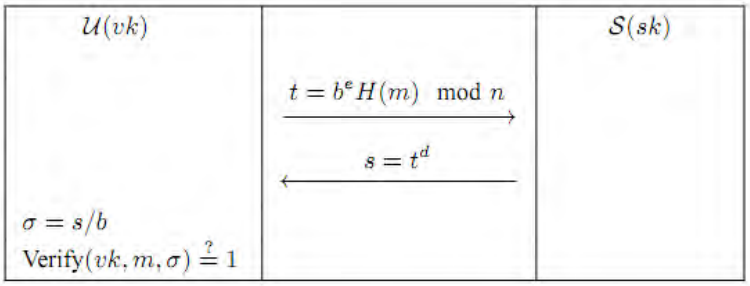
Η ‘‘τυφλή υπογραφή’’ Chaum βασίζεται στο σχήμα υπογραφών RSA με συναρτήσεις κατακερματισμού. Το μήνυμα M υπογράφεται με το H (M)d = σ και ένα ζευγάρι μηνύματος και υπογραφής (M, σ) επικυρώνεται ελέγχοντας αν σe ≡ H (M) mod n. Θα τροποποιήσουμε αυτό το σχήμα για να επιτύχουμε τυφλές υπογραφές [8,9]. Αναλυτικά:

Έστω e ένας πρώτος αριθμός, M μια ακολουθία συμβόλων, n ένα RSA modulus και H μια συνάρτηση κατακερματισμού. Ένα σχήμα τυφλών υπογραφών (blind signature scheme) είναι μια τριάδα (GGen, Sign, Verify) τέτοια ώστε :

- Ο αλγόριθμος GGen είναι ο αλγόριθμος παραγωγής κλειδιού: Επιλέγονται δύο πρώτοι αριθμοί p και q, τέτοιοι ώστε |p| = |q| = λ. Υπολογίζονται οι n = pq και φ(n) = (p − 1)(q − 1). Επιλέγεται ένας πρώτος e < φ(n) τέτοιος ώστε gcd(e, φ(n)) = 1 και υπολογίζεται ο d ≡ e−1 mod φ(n).

- Το Sign είναι ένα πρωτόκολλο υπογραφής, η λειτουργία του οποίου είναι η εξής:
  1. Ο U επιλέγει ένα b $\in Z*$ και θέτει t = be H (m) mod n. Στέλνει στον S το t.
  2. Ο S στέλνει στον U το $s = t^d \mod n$.
  3. Ο U θέτει σ = s/b mod n και επιστρέφει το σ ως την υπογραφή.
- Ο αλγόριθμος επαλήθευσης Verify: Για κάθε (M, σ), ελέγχει αν $\sigma^e = H(M) \mod n$. Σε περίπτωση που ισχύει η ισότητα, ο αλγόριθμος επιστρέφει True, αλλιώς επιστρέφει False.

Το σχήμα 2.1 περιγράφει τον γενικό τύπο των αλγορίθμων για έναν χρήστη U και έναν υπογράφοντα S στις τυφλές υπογραφές του Chaum.



Εικόνα 5. Η δημιουργία ‘‘τυφλής υπογραφής’’ Chaum [8]

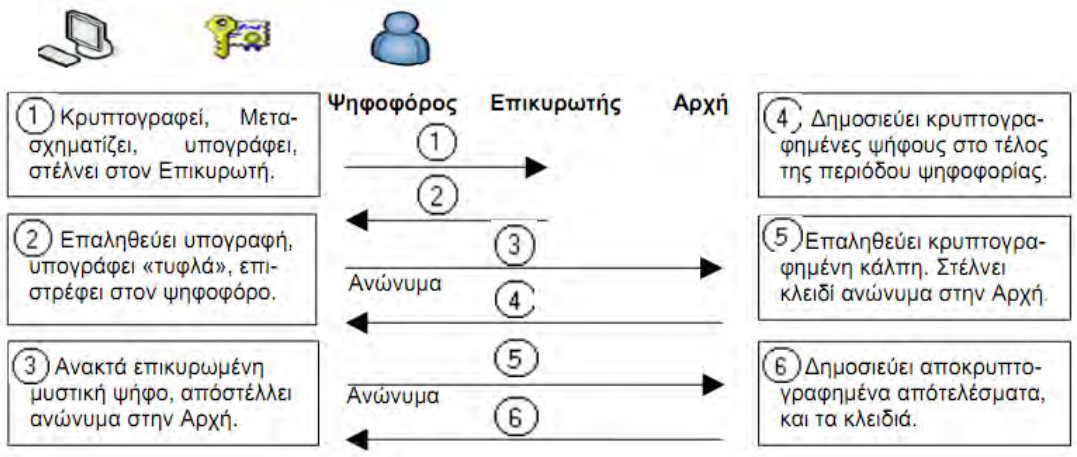
Υλοποίηση Ηλεκτρονικής Ψηφοφορίας

Η μέθοδος του Chaum , αν και εφαρμόστηκε αρχικά σε εφαρμογές ανώνυμου ηλεκτρονικού χρήματος (e-cash), χρησιμοποιήθηκε επίσης από τους Fujioka, Okamoto και Ohta για την επίλυση του προβλήματος της Επικύρωσης των ψήφων με παράλληλη προστασία της μυστικότητάς τους. Αναλυτικά : Κάθε ψηφοφόρος κρυπτογραφεί τη ψήφο του και στη συνέχεια την υποβάλλει σε έναν Επικυρωτή από τον οποίο λαμβάνει πίσω μια ‘‘τυφλή υπογραφή’’ στο κρυπτογράφημα της ψήφου (Εικόνα 6). Ο ψηφοφόρος στέλνει το επικυρωμένο κρυπτογράφημα σε μια Αρχή (μπορεί να είναι ο Επικυρωτής ή κάποια άλλη ανεξάρτητη οντότητα για επιπρόσθετη ασφάλεια) χρησιμοποιώντας ένα ανώνυμο κανάλι επικοινωνίας. Στο τέλος της περιόδου υποβολής ψήφων, η Αρχή δημοσιεύει τις κρυπτογραφημένες ψήφους σε έναν πίνακα ανακοινώσεων (bulletin board). Κάθε ψηφοφόρος ελέγχει εάν η ψήφος του είναι δημοσιευμένη στον πίνακα ανακοινώσεων (αν όχι, τότε μπορεί να καταγγείλει τη διαδικασία, επίσης ανώνυμα). [8,26,27]

Εάν η ψήφος του έχει δημοσιευτεί κανονικά, ο ψηφοφόρος υποβάλλει το κλειδί αποκρυπτογράφησης στην Αρχή, χρησιμοποιώντας ξανά το ανώνυμο κανάλι επικοινωνίας. Η Αρχή αποκρυπτογραφεί όλες τις ψήφους και δημοσιεύει τα αποτελέσματα στον πίνακα ανακοινώσεων.

Έως σήμερα έχουν προταθεί αρκετά σχήματα που βασίζονται στον μηχανισμό των ‘‘τυφλών υπογραφών’’. Επίσης, αρκετά τέτοια συστήματα έχουν υλοποιηθεί πιλοτικά σε εκλογές μικρής κλίμακας. Το σύστημα SENSUS ήταν το πρώτο

σύστημα ‘‘τυφλών υπογραφών’’ που υλοποιήθηκε σε ηλεκτρονικές εκλογές μέσω του διαδικτύου. Ακόμα το σύστημα των Davenport et al χρησιμοποιήθηκε στο παρελθόν για τη διενέργεια επίσημων φοιτητικών εκλογών. Τέλος, το σύστημα EVOX χρησιμοποιήθηκε στο MIT (Massachusetts Institute of Technology) σε εκλογές προπτυχιακών φοιτητών για την ανάδειξη των αντιπροσώπων τους. [28,29]



Εικόνα 6. Παράδειγμα ηλεκτρονικής ψηφοφορίας με ‘‘τυφλές υπογραφές’’

Πλεονεκτήματα και Μειονεκτήματα

Ένα πλεονέκτημα των συστημάτων που υιοθέτησαν το μοντέλο των ‘‘τυφλών υπογραφών’’ είναι η απαίτηση χαμηλού επικοινωνιακού φόρτου και υπολογιστικού κόστους, ακόμα και όταν ο αριθμός των ψηφοφόρων είναι μεγάλος (scalability). Επιπλέον, η μυστικότητα των ψήφων επαφίεται στους ψηφοφόρους, κάτι που ευνοεί την εύκολη και ασφαλή διαχείριση του συστήματος από την (συνήθως μια) Αρχή. Ακόμα, στο μοντέλο αυτό ο χρήστης αυθεντικοποιείται, κατά την εγγραφή του, με τέτοιον τρόπο ώστε να μην είναι δυνατή η σύνδεση της τελικής ψήφου του με την αληθινή ταυτότητα του, ενώ παράλληλα να αποτρέπεται η υποβολή διπλών ψήφων και η υποβολή ψήφων από μη εξουσιοδοτημένους χρήστες.

Τέλος, τα ανωτέρω σε συνδυασμό με την εγγενή υποστήριξη πολλαπλών υποψηφίων, καθιστούν τα συστήματα αυτά ιδιαίτερα ελκυστικά όχι μόνο για εκλογές μικρής ή μεγάλης κλίμακας, αλλά και για σφυγμομετρήσεις, δημοσκοπήσεις, κ.α.

Ένα σημαντικό μειονέκτημα των συστημάτων ‘‘τυφλής υπογραφής ’’ είναι ότι απαιτούν από τον ψηφοφόρο να είναι ενεργός (online) σε όλα τα στάδια της ψηφοφορίας. Από τη σκοπιά της ασφάλειας, τα συστήματα αυτά προσφέρουν μόνο ατομική επαληθευσιμότητα και είναι ιδιαίτερα ευάλωτα στο πρόβλημα των απεχόντων ψηφοφόρων. Έτσι εάν ένας εγγεγραμμένος ψηφοφόρος επικυρώσει τη ψήφο του (Βήματα 1,2 στην Εικόνα 6) αλλά στη συνέχεια απέχει από τη ψηφοφορία, τότε ένας κακόβουλος Επικυρωτής μπορεί να υποβάλλει μια πλαστή ψήφο εκ μέρους του ψηφοφόρου. [30]

Το Πρόβλημα των Απεχόντων Ψηφοφόρων

Το βασικότερο λοιπόν, μειονέκτημα του μοντέλου της ‘‘τυφλής υπογραφής’’ είναι το ότι εάν ένας ψηφοφόρος εγγράφεται στο σύστημα αλλά στη συνέχεια αποφασίζει (δικαιωματικά) να απέχει από τις εκλογές, δηλαδή να μην υποβάλλει ψήφο, τότε η Αρχή μπορεί να υποβάλλει μια πλαστή ψήφο για λογαριασμό του ψηφοφόρου, χωρίς μάλιστα αυτό να γίνει αντιληπτό από εξωτερικούς παρατηρητές ή/και από τους υπόλοιπους ψηφοφόρους. Προφανώς το γεγονός αυτό συνιστά άμεση παραβίαση και των δύο ιδιοτήτων της Δημοκρατικότητας του εκλογικού συστήματος.[9]

Από εδώ και πέρα, ως δέσμευση ψήφου (vote-tag) θα αποκαλούμε την κρυπτογραφημένη ψήφο σε συστήματα που βασίζονται στο μοντέλο των ‘‘τυφλών υπογραφών’’ . Όταν η δέσμευση ψήφου υπογραφεί ‘‘τυφλά’’ από την Αρχή κατά την περίοδο Εγγραφής, τότε και μόνον τότε θεωρείται ως έγκυρη. Πρόσφατα, για την αντιμετώπιση του προβλήματος των ψηφοφόρων που απέχουν, ο Riera [17] πρότεινε όλοι οι ψηφοφόροι να υποβάλλουν, μετά την εγγραφή τους και πριν υποβάλλουν την έγκυρη δέσμευση ψήφου τους, ένα ψηφιακά υπογεγραμμένο μήνυμα αναγνώρισης Μ το οποίο θα αναφέρει ότι κατέχουν μια έγκυρη δέσμευση ψήφου. Στη συνέχεια, και αφού αρχίσει η περίοδος υποβολής ψήφων, οι χρήστες θα υποβάλλουν ανώνυμα την έγκυρη δέσμευση ψήφου τους στην Αρχή. Η Αρχή θα δημοσιεύσει τη λίστα (έγκυρες δεσμεύσεις, μηνύματα αναγνώρισης) κατά το πρότυπο των δικτύων MIX-net, ώστε να μην υπάρχει συνδεσιμότητα των αποτελεσμάτων. Η λύση αυτή έχει το παρακάτω μειονέκτημα [14]: μετά τη δημοσίευση των αποτελεσμάτων, και εάν υπάρχουν περισσότερες ψήφοι από υπογραφές, αυτό μπορεί να σημαίνει :

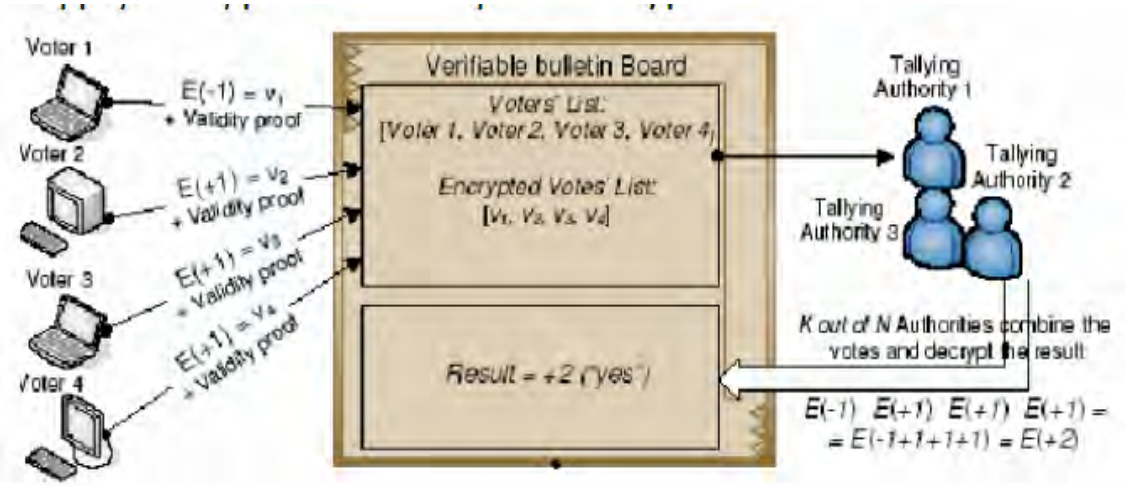
- Είτε ότι η Αρχή υπέβαλε πλαστές ψήφους
- Είτε ότι κάποιοι ψηφοφόροι υπέβαλαν (ανώνυμα) την έγκυρη δέσμευση ψήφου χωρίς να έχουν υποβάλλει νωρίτερα (επώνυμα) το μήνυμα αναγνώρισης Μ .

Αν πάλι υπάρχουν περισσότερες υπογραφές από ψήφοι, τότε αυτό μπορεί να σημαίνει:

- Είτε ότι η Αρχή διέγραψε κάποιες ψήφους από την τελική κάλπη,
- Είτε ότι κάποιοι ψηφοφόροι υπέβαλλαν το μήνυμα αναγνώρισης Μ στην Αρχή, αλλά στη συνέχεια αποφάσισαν να απέχουν, δηλαδή δεν υπέβαλαν την έγκυρη δέσμευση της ψήφου τους.

Όλα τα συστήματα που έχουν προταθεί και βασίζονται στο μοντέλο των ‘‘τυφλών υπογραφών’’ πάσχουν από το πρόβλημα της υποβολής πλαστών ψήφων από την Αρχή εκ μέρους των ψηφοφόρων που απέχουν. Σε τέτοια συστήματα, συχνά γίνονται μη πρακτικές υποθέσεις, π.χ. ότι όλοι οι εγγραφόμενοι ψηφοφόροι που αποφασίζουν να απέχουν θα υποβάλλουν μια λευκή ψήφο.

4.2.2. Ομομορφικό μοντέλο



Εικόνα 7. Παράδειγμα Ομομορφικού μοντέλου

Η χρήση ομομορφικών συναρτήσεων κρυπτογράφησης είναι ένας από τους τρεις τρόπους προσέγγισης του e-voting. Το μοντέλο αυτό χρησιμοποιεί τις ομομορφικές ιδιότητες ορισμένων αλγορίθμων κρυπτογράφησης για να εδραιώσει οικουμενική επαληθευσιμότητα σε εκλογές μεγάλης κλίμακας, διατηρώντας παράλληλα τη μυστικότητα των ατομικών ψήφων. Υπάρχει πληθώρα πρωτοκόλλων τα οποία χρησιμοποιούν την ομομορφική ιδιότητα, ανάμεσα τους τα :

Η **ομομορφική ιδιότητα** (Homomorphic property) θα μπορούσε να οριστεί σαν τη θεώρηση μιας συνάρτηση κρυπτογράφησης E και δύο επιλογές από το σύνολο των απλών μηνυμάτων v1 και v2. Η κρυπτογράφηση των μηνυμάτων είναι η e_1= $E(v_1)$ και $e_2 = E(v_2)$.Τότε η συνάρτηση E είναι $(\oplus,\otimes)$ ομομορφική αν ισχύει:

$$E(v_1) \otimes E(v_2) = E(v1 \oplus v_2)$$

Επομένως, κατά την ομομορφική κρυπτογράφηση υπάρχει μια πράξη ορισμένη στο σύνολο των μηνυμάτων και μια πράξη ορισμένη στο σύνολο των κρυπτογραφημάτων, τέτοιες ώστε το ‘‘γινόμενο’’ των κρυπτογραφήσεων οποιονδήποτε δύο ψήφων να ισούται με την κρυπτογράφηση του ‘‘αθροίσματος’’ των ψήφων.

Τα ομομορφικά συστήματα κρυπτογράφησης είναι πολύ σημαντικά για την κατασκευή εκλογικών πρωτοκόλλων διότι ο ομομορφισμός της κρυπτογραφικής συνάρτησης εγγυάται οικουμενική επαληθευσιμότητα στην τελική κάλπη, χωρίς την ανάγκη αποκρυπτογράφησης μεμονωμένων ψήφων, κάτι που θα παραβίαζε τη μυστικότητα τους. Δηλαδή, αν έχουμε ένα$(\oplus,\otimes)$ ομομορφικό σύστημα και ci είναι οι κρυπτογραφημένες ψήφοι ,τότε αποκρυπτογραφώντας το c = c1 ⊗ c2... ⊗ cn λαμβάνουμε το αποτέλεσμα της ψηφοφορίας χωρίς να αποκρυπτογραφήσουμε κάθε ψήφο ξεχωριστά.

Το τίμημα για τον ψηφοφόρο είναι ότι κάθε ψήφος θα πρέπει να συνοδεύεται από μια απόδειξη εγκυρότητας, ότι δηλαδή είναι της σωστής μορφής (π.χ. ‘‘Ναι’’ /

‘‘Όχι’’). Η απόδειξη αυτή πρέπει να είναι μηδενικής γνώσης και οικουμενικά επαληθεύσιμη. [12,13]

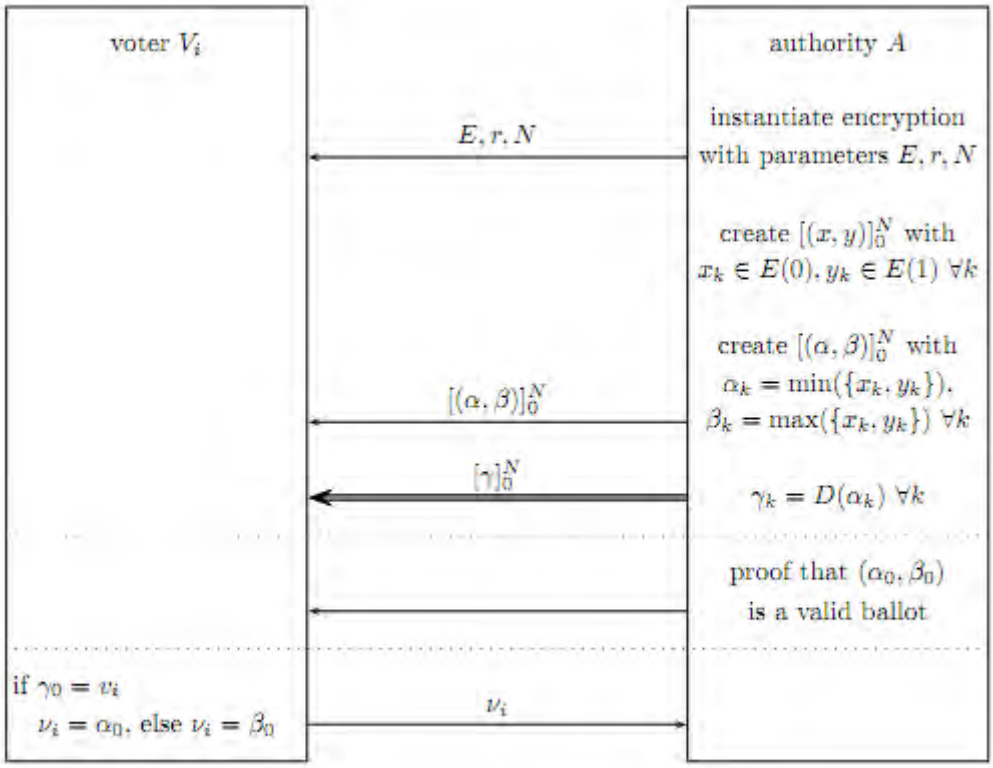
Ένα μειονέκτημα των συστημάτων που βασίζονται στο ομομορφικό μοντέλο είναι η περιορισμένη ευκαμψία τους (flexibility), καθώς οι ψήφοι συνήθως περιορίζονται σε δίτιμες ψήφους του τύπου ‘‘Ναι’’/ ‘‘Όχι’’. Για μεγάλο αριθμό υποψηφίων, οι υλοποιήσεις που βασίζονται στο μοντέλο αυτό συνεπάγονται υψηλό υπολογιστικό κόστος για τους εξυπηρετητές. Για παράδειγμα στην εργασία των Cramer et al, που αποτελεί τη χαρακτηριστικότερη και πλέον γνωστή υλοποίηση του μοντέλου, η πολυπλοκότητα των υπολογισμών στους εξυπηρετητές είναι εκθετική ως προς τον αριθμό των υποψηφίων. Πρόσφατα έχουν προταθεί εναλλακτικά ομομορφικά κρυπτογραφικά σχήματα ηλεκτρονικής ψηφοφορίας, των οποίων η υπολογιστική πολυπλοκότητα είναι είτε γραμμική (linear) είτε λογαριθμική (logarithmic). Τα σχήματα αυτά βασίζονται στο κρυπτοσύστημα του Pallier. Το σύστημα VoteHere, το οποίο ήδη χρησιμοποιείται πιλοτικά σε τοπικές εκλογές μικρής κλίμακας, αποτελεί μια υλοποίηση του ομομορφικού μοντέλου κρυπτογράφησης.

4.2.3. Το Μοντέλο του Benaloh

Ο πρώτος που ασχολήθηκε με την χρήση ομομορφικών συναρτήσεων σε συστήματα e-voting ήταν ο Josh Cohen Benaloh. Το μοντέλο του Benaloh χρησιμοποιεί ένα σχήμα ομομορφικού διαμοιρασμού μυστικών (homomorphic secret sharing). Ένα σχήμα Διαμοιρασμού Μυστικού επιτρέπει την κατάτμηση ενός μυστικού σε μερίδια (shares), τα οποία δίδονται σε ένα σύνολο *n* οντοτήτων, ούτως ώστε η συνεργασία και των *n* οντοτήτων να είναι απαραίτητη για την ανάκτηση του μυστικού. Σε ένα (*t*,*n*) threshold σχήμα Διαμοιρασμού Μυστικού, η ανάκτηση του μυστικού είναι εφικτή εφόσον συνεργαστεί μια ομάδα από τουλάχιστον *t* οντότητες, όπου $t \leq n$.Σε τέτοια ομομορφικά σχήματα υπάρχει μια πράξη ορισμένη στο σύνολο των μεριδίων, τέτοια ώστε το ‘‘άθροισμα’’ των μεριδίων οποιονδήποτε δυο μυστικών x_1 ,x_2 να ισούται με ένα μερίδιο του ‘‘αθροίσματος’’ $x_1 \oplus x_2$. [19,20]

Στο σχήμα του Benaloh κάθε ψηφοφόρος διαμοιράζει τη ψήφο του σε Αρχές, χρησιμοποιώντας ένα *threshold* σχήμα διαμοιρασμού μυστικού. [21,22] Τα μερίδια κρυπτογραφούνται με το δημόσιο κλειδί της κάθε Αρχής-παραλήπτη, υπογράφονται ψηφιακά και δημοσιεύονται σε έναν Πίνακα Ανακοινώσεων.

Μετά το τέλος της περιόδου υποβολής ψήφων κάθε Αρχή προσθέτει όλα τα μερίδια που έχει λάβει ώστε, βάσει της ομομορφικής ιδιότητας της συνάρτησης διαμοιρασμού, να αποκτήσει ένα μερίδιο του αθροίσματος των ψήφων της κάλπης. Τέλος, οι Αρχές συνδυάζουν τα μερίδια τους ώστε να σχηματίσουν την τελική κάλπη. Η ορθότητα της καταμέτρησης βασίζεται στην ιδιότητα των τεχνικών threshold: τουλάχιστον *t* από τις Αρχές πρέπει να συνδυάσουν τα μερίδια τους ώστε τα αποτελέσματα να είναι οικουμενικά επαληθεύσιμα. [21] Τα συστήματα αυτής της κατηγορίας, παρότι σχετικά απλά στη δομή τους, έχουν υψηλό επικοινωνιακό φόρτο: κάθε ψηφοφόρος πρέπει να υποβάλλει τη ψήφο του χρησιμοποιώντας κανάλια επικοινωνίας.



Εικόνα 8. Ομομορφικό μοντέλο [19]

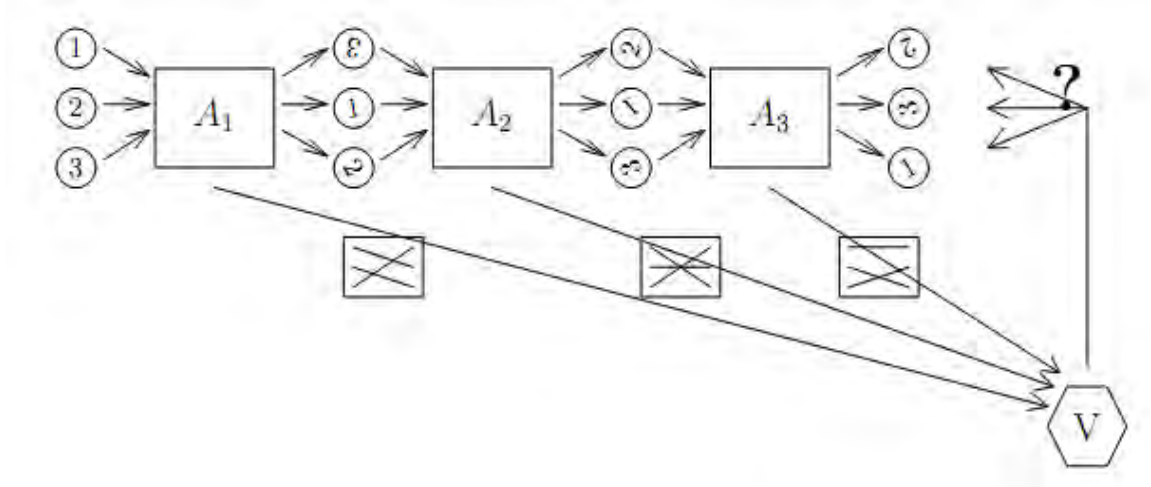
4.2.4. Το Μοντέλο Hirt-Sako

Το μοντέλο αυτό έχει παίξει σημαντικό ρόλο στην εξέλιξη της ηλεκτρονικής ψηφοφορίας, γιατί είναι το πρώτο εύχρηστο σύστημα ψηφοφορίας που δεν παρέχει απόδειξη. Μέχρι τότε, τα πρωτόκολλα ψηφοφορίας ζητούσαν από τους ψηφοφόρους να χρησιμοποιήσουν κάποια σειρά από τυχαία bits για να κρυπτογραφήσουν την ψήφο τους. Αυτά τα τυχαία bits αρκούν για να κατασκευαστεί μία απόδειξη, αν για παράδειγμα χρησιμοποιηθεί στη θέση τους μια συνάρτηση κατακερματισμού πάνω σε ένα προαποφασισμένο s. Στο συγκεκριμένο πρωτόκολλο, οι Αρχές παράγουν όλες μαζί την κρυπτογράφηση όλων των πιθανών ψήφων, και οι ψηφοφόροι απλά ‘‘δείχνουν’’ την κρυπτογράφηση της επιλογής τους [16].

Έστω ότι υπάρχουν M Αρχές και N ψηφοφόροι. Θεωρούμε ότι το σύστημα έχει κατώφλι t ,δηλαδή τουλάχιστον t Αρχές ,παραμένουν έντιμες κατά τη διάρκεια της εκτέλεσης του πρωτοκόλλου. Επίσης, θεωρούμε ότι υπάρχει ένας Πίνακας Ανακοινώσεων, καθώς και ένα ασφαλές κανάλι (untappable channel) από τις Αρχές στους ψηφοφόρους. Το κανάλι αυτό παρέχει ασφάλεια, έτσι ώστε κανείς να μην μπορεί να ακούσει ή να αλλάξει ότι μεταφέρεται από αυτό το κανάλι. Επιπλέον, ο ψηφοφόρος δεν μπορεί να αποδείξει ότι έλαβε κάτι συγκεκριμένο μέσω του καναλιού. Το σύστημα είναι 1-από-L, δηλαδή κάθε εγγεγραμμένος ψηφοφόρος διαλέγει και καταθέτει μία ψήφο από το σύνολο V των ορθών ψήφων, |V| = *L*.

Η βασική ιδέα του πρωτοκόλλου φαίνεται στην Εικόνα 9. Πρώτα κάθε ψήφος

που ανήκει στο V κρυπτογραφείται με ντετερμινιστικό τρόπο, π.χ. χρησιμοποιώντας ‘‘τυχαιότητα’’ 0. Η λίστα με τις κρυπτογραφημένες ψήφους δημοσιοποιείται στον Πίνακα Ανακοινώσεων. Η πρώτη Αρχή ‘‘ανακατεύει’’ τη λίστα και την παραδίδει στην επόμενη Αρχή. Μετά η δεύτερη Αρχή παίρνει τη λίστα και την ‘‘ανακατεύει’’ κ.ο.κ. Μαζί με το ανακάτεμα κάθε Αρχή αποκαλύπτει στον ψηφοφόρο την παρούσα διάταξη της λίστας, με ιδιωτικό επαληθεύσιμο τρόπο (privately verifiable), μέσω του ασφαλούς καναλιού. Όταν όλες οι Αρχές έχουν ‘‘ανακατώσει’’ τη λίστα, ο ψηφοφόρος ‘‘δείχνει’’ την ψήφο της επιλογής του.[42]



Εικόνα 9. Το μοντέλο Hirt-Sako με τρεις Αρχές και V ={1,2,3} [42]

4.2.5. Μοντέλο Cramer-Gennaro-Schoenmakers

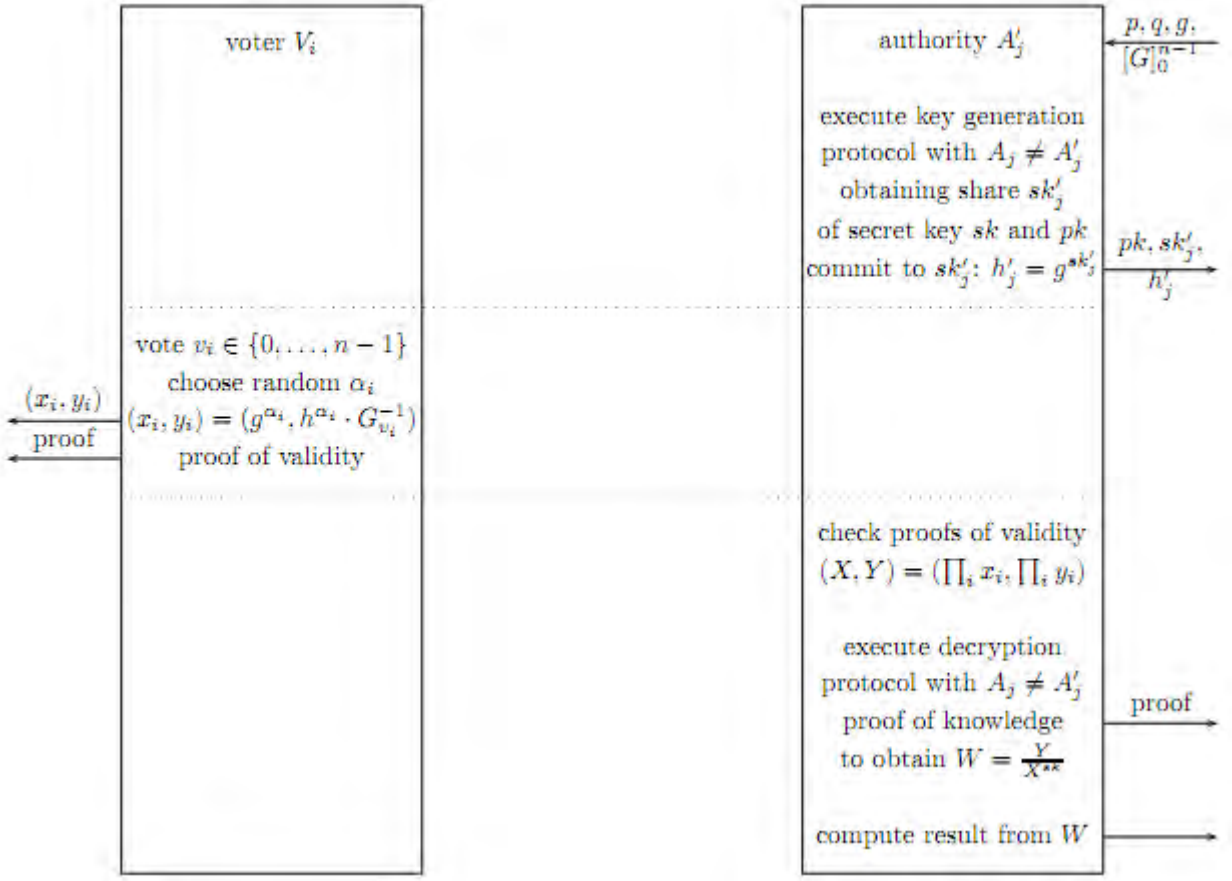
Το πρωτόκολλο αυτό είναι από τα πιο σημαντικά στην εξέλιξη της ηλεκτρονικής ψηφοφορίας. Εξασφαλίζει ιδιωτικότητα, παγκόσμια εξακριβωσιμότητα και ανθεκτικότητα, ενώ είναι βέλτιστο από άποψη πολυπλοκότητας χρόνου και επικοινωνίας για τους ψηφοφόρους αλλά και για τις Αρχές. Βασική ιδιότητα του συστήματος είναι ότι επιτυγχάνει σταθερή πολυπλοκότητα για τον ψηφοφόρο (χρονική και επικοινωνιακή) ανεξαρτήτως του αριθμού των Αρχών. Έτσι μπορούν να αυξάνουν οι Αρχές (και αντίστοιχα η ασφάλεια του συστήματος), χωρίς αυτό να έχει επίπτωση στον ψηφοφόρο.

Έστω ότι υπάρχουν n Αρχές και l ψηφοφόροι. Για να επιτευχθεί η παγκόσμια εξακριβωσιμότητα απαιτείται η χρήση ενός Πίνακα Ανακοινώσεων, στον οποίο θεωρούμε ότι δε γίνονται επιθέσεις τύπου ‘‘άρνησης παροχής υπηρεσίας’’. Επίσης θεωρούμε μία συνάρτηση κρυπτογράφησης με ομομορφική ιδιότητα, η οποία έχει την άθροιση ως πράξη στο χώρο των μηνυμάτων. Δηλαδή, δοθέντων των κρυπτογραφήσεων του μηνύματος m1 και m2 ,το γινόμενό τους είναι η κρυπτογράφηση του αθροίσματος m1+m2. Τέλος η ανθεκτικότητα επιτυγχάνεται με τη χρήση ενός κρυπτοσυστήματος κατωφλίου.

Το κρυπτοσύστημα που χρησιμοποιείται εδώ είναι το ανθεκτικό αθροιστικό El Gamal με κατώφλι. Το αποτέλεσμα είναι ότι κάθε αρχή Ai αποκτά ένα $\mathbf{s_i} \in G_q$ όπου q μεγάλος πρώτος και δημοσιεύει το $h_i = g^{si}$ **όπου g γεννήτορας του** *Gq*. Επίσης

κάθε συμμετέχοντας μαθαίνει το δημόσιο κλειδί του $h = g^s$ όπου s είναι το μυστικό που ανακατασκευάζεται από κάθε σύνολο Λ κατόχων των κομματιών $\mathbf{s_i}$.

Γενικά θα δουλεύουμε σε υποσύνολα Gq τάξης q του Zp*, όπου q,p είναι μεγάλοι πρώτοι και q | ρ — 1. θεωρούμε ότι οι πρώτοι p,q και ο γεννήτορας g του Gq (καθώς και οποιοσδήποτε άλλος γεννήτορας που θα εμφανιστεί στη συνέχεια), έχουν παραχθεί από ένα υποσύνολο Αρχών, η κάθε μία από τις οποίες εκτέλεσε ένα αντίγραφο ενός πιθανοτικού αλγορίθμου, όπου οι τυχαίες επιλογές προέρχονται από την ίδια τυχαία γεννήτρια. Τέλος θεωρούμε παράμετρο ασφαλείας k τέτοια ώστε το k να είναι ίσο με το μέγεθος των p,q και επίσης το μέγεθος του ψηφοδελτίου και των αποδείξεων ορθότητας να είναι ίσα με O(k). [13]



Εικόνα 10. Μοντέλο Cramer [13]

5. Συστήματα Ηλεκτρονικής Ψηφοφορίας

Η ηλεκτρονική ψηφοφορία αναφέρεται σε οποιαδήποτε διαδικασία ψηφοφορίας όπου ηλεκτρονικά μέσα χρησιμοποιούνται για τη ρίψη και μέτρηση ψηφοφοριών. Οι μέθοδοί της περιλαμβάνουν τα συστήματα ψηφοφορίας οπτικό-ανίχνευσης, τα ειδικευμένα συστήματα ψηφοφορίας όπως τα DRE ή τα άμεσα συστήματα ψηφοφορίας και ηλεκτρονικής καταγραφής όπως, τις κάρτες διατρήσεων, το εθνικό IDs, το Διαδίκτυο, τα δίκτυα υπολογιστών, και τα συστήματα τηλεφωνίας. Παρά τα εμπόδια που παρουσιάζουν τα συστήματα δημοσκοπήσεων και ηλεκτρονικής ψηφοφορίας, τα τελευταία χρόνια ένας αριθμός από πανεπιστήμια έχουν αρχίσει να αναπτύσσουν συστήματα ηλεκτρονικής ψηφοφορίας, συχνά για φοιτητικές εκλογές. Όλα όμως αυτά τα συστήματα έχουν σοβαρά μειονεκτήματα. Δύο από τα πιο γνωστά είναι το σύστημα Sensus και το E-Vox.

5.1. Σύστημα SENSUS

Το Sensus είναι ένα πρακτικό και ασφαλές σύστημα για διεξαγωγή δημοσκοπήσεων (ακόμη και εκλογών) μέσω δικτύων. Το Sensus επεκτείνοντας την εργασία των Fujioka, Okamoto και Ohta, χρησιμοποιεί blind signatures προκειμένου από τη μια μεριά να διασφαλίσει ότι μόνο εγγεγραμμένοι ψηφοφόροι μπορούν να ψηφίσουν και κάθε ψηφοφόρος ψηφίζει μόνο μια φορά και από την άλλη να διατηρήσει τη μυστικότητα του ψηφοφόρου.[26] Το Sensus επιτρέπει στο ψηφοφόρο να επαληθεύσει, ατομικά, ότι η ψήφος του μετρήθηκε σωστά και ανώνυμα να ελέγξει την ορθότητα των αποτελεσμάτων της ψηφοφορίας. Το πρωτόκολλο ψηφοφορίας του, απαιτεί την ύπαρξη ενός συστήματος επιβεβαιωτή (validator), ενός συστήματος καταμετρητή (tallier) και ενός συστήματος διεξαγωγής της δημοσκόπησης (pollster). Άλλα επιπρόσθετα συστήματα μπορούν να αυξήσουν την λειτουργικότητα του Sensus [30].

Το πρωτόκολλο Sensus χρησιμοποιεί blind signatures προκειμένου να παρέχει ασφάλεια ενώ ταυτόχρονα προστατεύει τη μυστικότητα του χρήστη [30]. Ο χρήστης πρέπει να ετοιμάσει την ψήφο του, να την κρυπτογραφήσει με ένα μυστικό κλειδί και να την αποκρύψει (blind). Στη συνέχεια ο ψηφοφόρος υπογράφει την ψήφο και την αποστέλλει στον επιβεβαιωτή (validator). Ο επιβεβαιωτής επικυρώνει ότι η υπογραφή (signature) ανήκει σε εξουσιοδοτημένο χρήστη ο οποίος δεν έχει ψηφίσει ακόμη. Εάν η ψήφος είναι έγκυρη, ο επιβεβαιωτής υπογράφει την ψήφο και την επιστρέφει στον ψηφοφόρο. Ο ψηφοφόρος αφαιρεί το στρώμα απόκρυψης (blinding layer) και αποκαλύπτει ένα κρυπτογραφημένο μήνυμα υπογεγραμμένο από τον επιβεβαιωτή, το οποίο αποστέλλει στον καταμετρητή (tallier). Ο καταμετρητής ελέγχει την υπογραφή πάνω στο κρυπτογραφημένο ψηφοδέλτιο. Εάν η ψήφος είναι έγκυρη ο καταμετρητής την τοποθετεί σε μια λίστα με έγκυρες ψήφους, η οποίο θα δημοσιευτεί μετά το τέλος της ψηφοφορίας. Στη συνέχεια ο καταμετρητής υπογράφει την κρυπτογραφημένη ψήφο και την επιστρέφει σαν απόδειξη στον ψηφοφόρο. Μόλις ο ψηφοφόρος λάβει την απόδειξη αποστέλλει στον καταμετρητή το κλειδί κρυπτογράφησης. Ο καταμετρητής

χρησιμοποιεί το κλειδί για να αποκρυπτογραφήσει την ψήφο και να προσθέσει την ψήφο στο τελικό αποτέλεσμα. [30]

5.2. Σύστημα EVOX

Το σύστημα αυτό συνδυάζει την ευελιξία ενός συστήματος VBM (Vote By Mail) με την ταχύτητα και την ισχύ των σύγχρονων υπολογιστών. Σχεδιάστηκε να είναι στο σύνολο του φιλικό προς το χρήστη. Με τον όρο φιλικό προς το χρήστη εννοούμε ότι ο εκάστοτε ψηφοφόρος χρειάζεται να εκτελέσει τον ελάχιστο αριθμό βημάτων που απαιτεί η εκλογική διαδικασία και τίποτα άλλο. Τα δύο απαραίτητα βήματα στην όλη διαδικασία είναι η εγγραφή και η ψηφοφορία. [43]

Από τη μεριά του ψηφοφόρου και τα δύο βήματα εκτελούνται εύκολα και γρήγορα. Η εγγραφή απαιτεί την προσέλευση του ψηφοφόρου στο κατάλληλο γραφείο εγγραφών, μαζί με τα απαραίτητα δικαιολογητικά. Η διαδικασία της ψηφοφορίας απαιτεί την ύπαρξη ενός υπολογιστή, την εισαγωγή των προσωπικών στοιχείων πρόσβασης και την επιλογή των απαντήσεων. Ο ψηφοφόρος μπορεί να φύγει όντας σίγουρος ότι η διαδικασία ολοκληρώθηκε με ασφάλεια και αξιοπιστία, όπως στα παραδοσιακά συστήματα.

Οι Fujioka, Okamoto και Ohta περιέγραψαν ένα θεωρητικό πυρήνα για ένα σύστημα ψηφοφορίας. Πολλές όμως από τις λεπτομέρειες που απαιτούνται για το κτίσιμο ενός πραγματικού συστήματος έμειναν έξω. [26] Το αναθεωρημένο πρωτόκολλο περιλαμβάνει τα παρακάτω βήματα :

1. Ο ψηφοφόρος επιλέγει τις απαντήσεις του και ‘‘δεσμεύεται’’ με την ψήφο του χρησιμοποιώντας HMAC-SHA hashing.

2. Η ψήφος αποκρύπτεται (blind) από τον ψηφοφόρο και αποστέλλεται στο διαχειριστή του συστήματος, μαζί με το όνομα και τον κωδικό πρόσβασης του ψηφοφόρου, μέσα από μια ασφαλή σύνδεση.

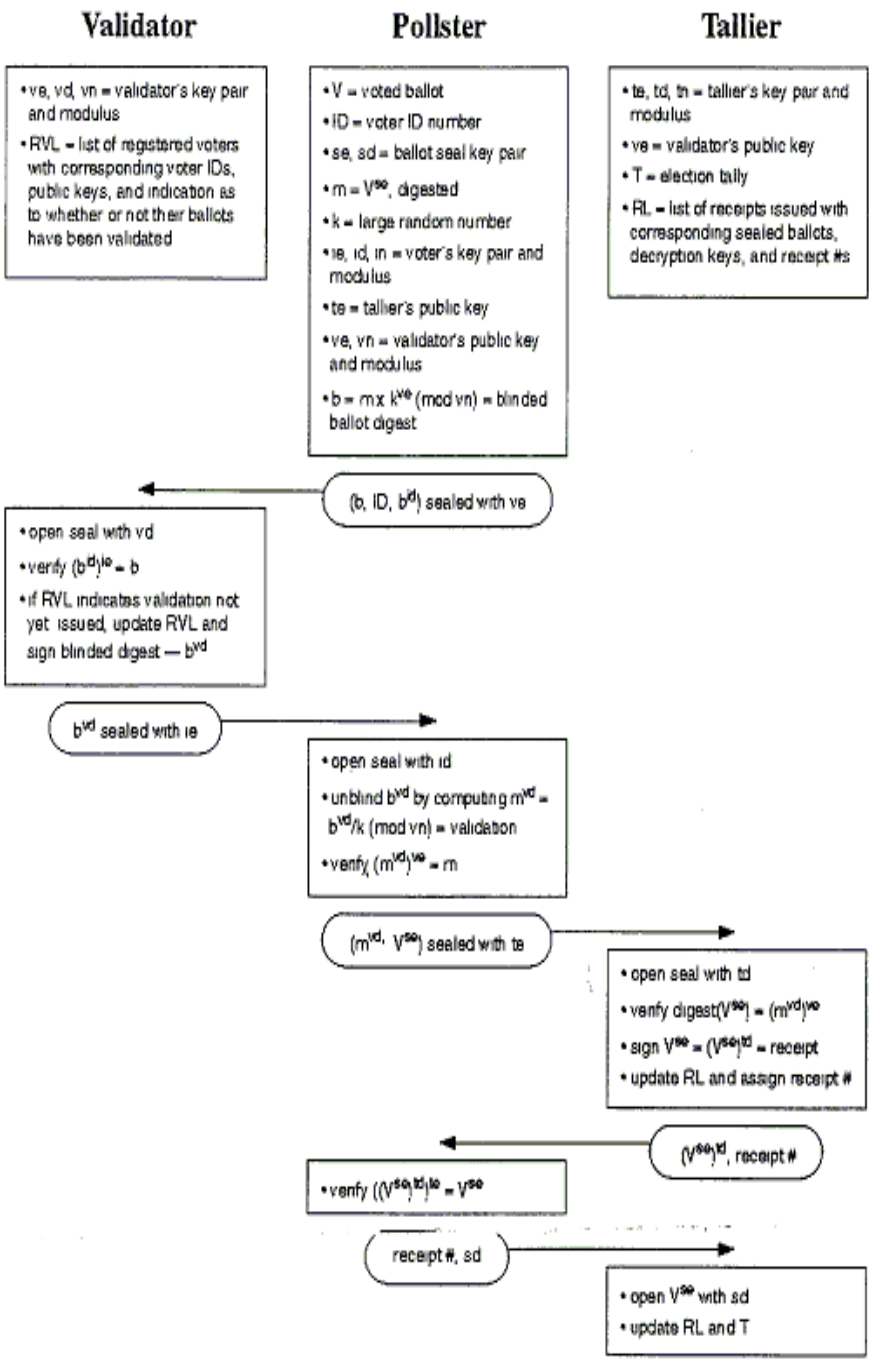
3. Ο διαχειριστής επιβεβαιώνει την εγκυρότητα του ψηφοφόρου να συμμετάσχει στη διαδικασία και υπογράφει την αποκρυμμένη (blinded) ψήφο. Στη συνέχεια επιστρέφει την ψήφο στον ψηφοφόρο. (Μετά το πέρας της ψηφοφορίας ο διαχειριστής δημοσιεύει μια λίστα με τα ονόματα των ψηφοφόρων, τις αποκρυμμένες ψήφους και τις υπογραφές τους)

4. Ο ψηφοφόρος επιβεβαιώνει την υπογραφή του διαχειριστή και αποκαλύπτει (unblinds) την ψήφο του.

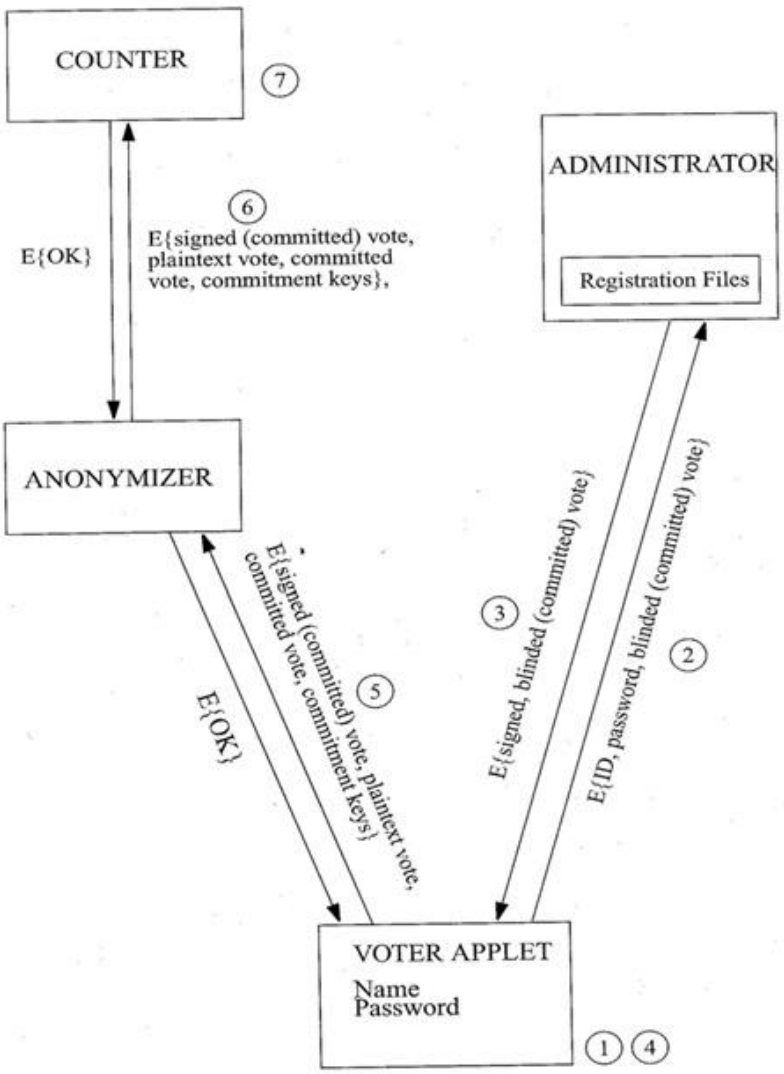
5. Η υπογεγραμμένη ψήφος μαζί με το απλό κείμενο και το κλειδί κρυπτογράφησης αποστέλλονται στον ανώνυμο εξυπηρετητή (server) μέσω μιας ασφαλούς σύνδεσης.

6. Όλες οι ψήφοι που λαμβάνονται από τον ανώνυμο εξυπηρετητή, πριν το πέρας της ψηφοφορίας ,αναδιατάσσονται τυχαία και προωθούνται στον καταμετρητή, αφού τελειώσει η ψηφοφορία. (Ο εξυπηρετητής δημοσιεύει μια ανακατεμένη λίστα με τα μηνύματα που έστειλε στον καταμετρητή).

7. Ο καταμετρητής επιβεβαιώνει τις υπογραφές του διαχειριστή και μετρά τις ψήφους. Ο καταμετρητής δημοσιεύει μια λίστα η οποία περιέχει το απλό κείμενο των ψήφων, τα κρυπτογραφημένα κλειδιά και τις υπογεγραμμένες ψήφους.



Εικόνα 11. [30] Σύστημα Sensus



Εικόνα 12. Σύστημα EVOX [43]

Τέλος παρατίθεται ένας συγκριτικός πίνακας με τα γνωστότερα Συστημάτων Ηλεκτρονικής Ψηφοφορίας.

	Πλεονεκτήματα	Καταλληλό-τερο για εφαρμογή	Μέθοδος Κρυπτογράφησης	Απαιτήσεις σε λογισμικό και υλικό	Γλώσσα προγραμματισμού
Sensus	• πρακτικό • ασφαλές • ευέλικτο	δημοσκοπή-σεις μέσω δικτύου	blind signatures	σύστημα επιβεβαιωτή (validator), σύστημα καταμετρητή (tallier) και σύστημα διεξαγωγής της δημοσκόπησης (pollster)	Τα βασικά υποσυστήματα έχουν υλοποιηθεί σε C και Unix και είναι εγκατεστημένα σε Web Server που υποστηρίζει CGI scripting
E-Vox	φιλικό προς το χρήστη	εκλογές στις οποίες συμμετέχουν δεκάδες χιλιάδες ψηφοφόροι	blind signatures, κρυπτογραφημένα μηνύματα	γρήγορο server, συνδέσεις δικτύου με πρωτόκολλο επικοινωνίας TCP/IP	ο web browser υποστηρίζει Java 1.1
DRE (Direct Recording System)	• ασφαλές, • αξιόπιστο, • μείωση ανθρώπινου δυναμικού, • ειδική καθοδήγηση για τυφλούς, ηλικιωμένους, ανάπηρους	ψηφοφορία από οποιονδήποτε σταθμό (δυνατή διεθνής ψηφοφορία)	συσκευή πινακοποίησης για την καταμέτρηση των ψήφων	οθόνη touch screen, εκτυπωτής (παράγει χάρτινα ψηφοδέλτια), κάρτες οπτικής σάρωσης, βάση δεδομένων νόμιμων ψηφοφόρων	οποιαδήποτε γλώσσα προγραμματισμού
Infopoll Software	• γρήγορο • οικονομικό • αξιόπιστο	οποιοδήποτε είδος έρευνας, δημοσκόπησης (π.χ. ερωτηματολόγια)		InfoPoll Σχεδιαστής – Designer InfoPoll Εξυπηρετητής – Server	HTML φόρμες, εργαλεία στατιστικής ανάλυσης
Pericles	δίκαιη εκλογική διαδικασία	φοιτητικές εκλογές στο MIT	σύστημα Kerberos	έναν εξυπηρετητή - server	γλώσσα C
Trueballot	ευέλικτη, ασφαλής και οικονομικά συμφέρουσα προσέγγιση	ψηφοφορίες σε οργανισμούς, σωματεία εργαζομένων και εταιρίες	πολλαπλά επίπεδα ασφάλειας (εξουσιοδοτημέ νοι χρήστες)	on line σύστημα ψηφοφορίας	
Ψήφος μέσω του Internet (VOI)	καλύτερη πρόσβαση σε ψηφοφόρους του εξωτερικού	ομοσπονδιακές, κρατικές και τοπικές εκλογές	Δυο συστήματα ανίχνευσης εισβολέων	FVAP server, Netscape Navigator	HTML

Πίνακας 1. Συγκριτικός πίνακας των Συστημάτων Ηλεκτρονικής Ψηφοφορίας

5.3. Εφαρμογές ηλεκτρονικής ψηφοφορίας

Η χρήση της ηλεκτρονικής ψηφοφορίας σε παγκόσμιο επίπεδο παραμένει μια σχετικά ασυνήθιστη πρακτική, αν και αυτό μεταβάλλεται με γοργό ρυθμό, καθώς οι χώρες πειραματίζονται με διάφορα ηλεκτρονικά μέσα ή επεκτείνουν την υφιστάμενη χρήση ηλεκτρονικής ψηφοφορίας. Επιπλέον, η ηλεκτρονική ψηφοφορία δεν

περιορίζεται στην Ευρώπη ή στη Βόρεια Αμερική, καθώς χώρες όπως η Βραζιλία και η Ινδία έχουν αντιμετωπίσει την ηλεκτρονική ψηφοφορία περισσότερο θετικά από ό, τι η Ευρώπη, οι Ηνωμένες Πολιτείες ή ο Καναδάς. Τα συστήματα ηλεκτρονικής ψηφοφορίας διαφέρουν σίγουρα σημαντικά από άποψη της τεχνολογίας και εφαρμογής. Κανένα σύστημα δεν είναι απαλλαγμένο από προβλήματα ή αντιπαραθέσεις, αλλά αυτό που είναι αρκετά αξιοσημείωτο είναι ότι, σε περιπτώσεις που η ηλεκτρονική ψηφοφορία εφαρμόστηκε σε εθνική κλίμακα, δεν υπήρξαν φαινόμενα σοβαρών σφαλμάτων ή αστοχιών του συστήματος.

5.3.1. Το παράδειγμα της Ελβετίας

Εικόνα 13. Οι Ελβετοί καλούνται συχνά να αποφασίσουν για το μέλλον τους με τοπικά δημοψηφίσματα.

Η Ελβετία είναι ένα από τα λίγα κράτη σε όλο τον κόσμο που ασχολούνται με τη ψηφοφορία μέσω Internet και την οργάνωση επίσημων on-line ψηφοφοριών σε τακτική βάση. Για πρώτη φορά οργανώθηκε τον Ιανουάριο του 2003. Το έργο του e-voting γεννήθηκε το έτος 2000, όταν άρχισε στη Γενεύη το θέμα της ηλεκτρονικής διακυβέρνησης.[32]

Η ψηφοφορία μέσω Internet είναι μια μέθοδος ψηφοφορίας δύο φάσεων: είναι τόσο ένας απομακρυσμένος τρόπος ψηφοφορίας όσο και μια ηλεκτρονική ψηφοφορία με κατακερματισμένη διαδικασία. Η απομακρυσμένη ψήφος έχει εφαρμοστεί ήδη από το 1995 και είναι ο πρώτος τρόπος ψηφοφορίας: το 95% των ψηφοδελτίων είναι μέσω ταχυδρομείου και η προσέλευση αυξήθηκε κατά 20 εκατοστιαίες μονάδες από την εισαγωγή της ταχυδρομικής ψήφου. Η ηλεκτρονική πλευρά της ψηφοφορίας μέσω Internet είναι ένα αποτέλεσμα των μηχανημάτων ψηφοφορίας που είναι ευρέως διαδεδομένα στην Ευρώπη.

Σε αντίθεση με τις μηχανές ψηφοφορίας, ωστόσο, και ιδιαίτερα σε αντίθεση με τα μηχανήματα που δεν είναι συνδεδεμένα με ένα δίκτυο, αλλά εργάζονται off-line,

η εφαρμογή της ηλεκτρονικής ψηφοφορίας στη Γενεύη δεν μπορεί να προσεγγιστεί ούτε σωματικά ούτε λογικά σε χρονικά διαστήματα κατά τη διάρκεια της ψηφοφορίας. Το κλείδωμα και άνοιγμα του κουτιού eBallot λαμβάνει χώρα με την παρουσία των ελεγκτών που διορίζονται από τα πολιτικά κόμματα και ενεργούν όπως μία εκλογική επιτροπή.

Θα μπορούσε να μας εκπλήσσει το γεγονός ότι σε μια χώρα όπου οι πολίτες σε ορισμένα σημεία ακόμα ψηφίζουν στην κεντρική πλατεία της πόλης με ανάταση των χεριών τους αναπτύσσεται μια εφαρμογή ψηφοφορίας μέσω Internet. Ωστόσο, υπάρχουν μια σειρά λόγοι για την υποστήριξη αυτού του έργου:

- Οι Ελβετοί πολίτες ψήφιζαν τέσσερις έως πέντε φορές το χρόνο, μερικές φορές περισσότερο. Άνεση είναι μια λέξη-κλειδί της διαδικασίας της ψηφοφορίας.

- Τα λεγόμενα συστήματα ‘‘άμεσης δημοκρατίας’’ είναι κατάλληλα για την ψηφοφορία στο Internet, όχι μόνο επειδή υποστηρίζουν πολλές ψηφοφορίες, αλλά και για τις πολλές αρμοδιότητες που αναλαμβάνουν οι πολίτες και την αντιπροσωπεία της περιορισμένης κυριαρχίας που δόθηκε στους βουλευτές.

- Σύμφωνα με την Ομοσπονδιακή Υπηρεσία για τις στατιστικές, το 65% του ελβετικού πληθυσμού είναι συνδεδεμένο στο Internet, είτε από το σπίτι ή το χώρο εργασίας. Ένας στους τρεις Ελβετούς κάνει πλοήγηση στο Διαδίκτυο σε καθημερινή βάση.

- 580,000 Ελβετοί πολίτες (περίπου ένας στους δέκα) ζουν στο εξωτερικό. Πρέπει να τους παρέχουν ένα απλό και αποτελεσματικό σύστημα ψηφοφορίας. Το ίδιο ισχύει και για τα άτομα με αναπηρία που ζουν στην Ελβετία.

- Η δημόσια υπηρεσία οφείλει να προσαρμοστεί στο νέο τρόπο ζωής και πρέπει να είναι όπου είναι οι άνθρωποι, συμπεριλαμβανομένου και του διαδικτύου.

Η ηλεκτρονική ψηφοφορία δεν θα αντικαταστήσει τους σημερινούς τρόπους ψηφοφορίας, τις ταχυδρομικές υπηρεσίες, τα δικαιώματα ψήφου και το εκλογικό κέντρο, θα είναι μια τρίτη δυνατότητα που δίνεται στους πολίτες.

Ο ρυθμός των τεχνολογικών εξελίξεων και οι αλλαγές που αυτό συνεπάγεται στην καθημερινή μας ζωή επιβάλλει ότι οι δημόσιες υπηρεσίες μένουν μπροστά από τις επικείμενες προσδοκίες των ανθρώπων. Αναμένοντας την ‘‘κατάλληλη στιγμή’’ για να επιβιβαστούν στο τρένο των νέων τεχνολογιών, θα περιμένουν πάρα πολύ καιρό. Πρέπει να προλάβουμε τις προσδοκίες του πληθυσμού, πρέπει ήδη να εργαστούμε πάνω στις νέες μορφές σχέσεων κράτους-πολίτη. Είναι αυτό που επέλεξε να κάνει η Γενεύη, με τη στήριξη της Συνομοσπονδίας.[36,33,39]

Τέλος παρατίθεται ένας συγκεντρωτικός πίνακας με τα Συστήματα Ηλεκτρονικής Ψηφοφορίας που έχουν χρησιμοποιηθεί σε διάφορες χώρες.

Country	E-voting electorate	Company	Type of elections	Electoral system	Year introduced	Year used	Software used	Hardware	Problems
India	668 million	Bharat electronic s limited & electronics corporation of India	State elections	FPP	2001	2004/2003/ 2001 by-election	Software Using EPROM (erasable program read- only memory)	EVM (electronic voting machine)	None
Belgium	3.2 million	Steria	General & municipal	Open PR-List	1994	1999	Digivote provided by Steria, Jites provided by Philips and Stesud by Favor	Digivote Electronic voting system	2003: 500 Power and compuer failures
Brazil	66 million	uniSys & Diebold	All Government levels		1996	1996/1998/ 2000/2002	Diebold Accuvote Using GEMS (global election Manageme nt system) using Windows CE	National's Geode GX-1 integrated Processor (Uma Electronica 2002)	none
Australia	218.000	Software improvement	ACT federal	PR-STV (hare-Clark)	2001	2001	Evacs operating On Debian/GN U Linux system	Standard PCs connected to an isolated LAN	NONE

Country	E-voting electorate	Company	Type of elections	Electoral system	Year introduced	Year used	Software used	Hardware	Problems
UK	1.5 million	Sequoia voting systems	Local gov1 (pilots)	FPP	2000	2000/2003	AVC Edge and AVC Advantage	Various forms. DRE (Direct recording electronic) used AVC Edge	Only with mobile e-voting e.g SMS text and internet. None related to stand -alone e-voting
Spain	130.000	Election systems & software	Mallorca local assembly	PR-List	2002	2003	ES & S Profile	iVotronic Touchscreen voting Machine	None
Spain	3.000	Indra & Demotek	Pilot municipal	PR-List	2002	2003	SIRE	SIRE system	None
Italy	66 million		Local, state, national			1998		Bull	None
Japan	15.000	Associati on of Electronic voting system	Municipal (Niimi)	Mixed member system	2001	2002	N/a	VT 25	None
Argentina	500.000	UniSys & Diebold	Gubematori al pilot	PR-List	2000	2003	ES&		

Πίνακας 2. Συστήματα ηλεκτρονικής ψηφοφορίας ανά χώρα [39]

5.4. Κατάσταση στην Ελλάδα

Δυστυχώς στην Ελλάδα, αν και το μοντέλο της ηλεκτρονικής ψηφοφορίας έχει συζητηθεί εκτενώς ,πραγματοποιούνται μόνο μικρής κλίμακας διαδικτυακές έρευνες.

Παρόλα αυτά υπάρχουν πρωτοβουλίες στον Ελλαδικό χώρο που δίνουν ελπίδες για περαιτέρω ανάπτυξη. Το σύστημα ηλεκτρονικής ψηφοφορίας e-Vote ήταν μια πρωτοβουλία της Ελληνικής Προεδρίας της Ευρωπαϊκής Ένωσης, η οποία είχε σκοπό, αξιοποιώντας το διαδίκτυο και τις νέες τεχνολογίες, τη συμμετοχή όσο το δυνατόν περισσοτέρων πολιτών στις συζητήσεις και στις διαδικασίες λήψης των αποφάσεων της Ευρωπαϊκής Ένωσης.[37,41]

Πιο συγκεκριμένα, οι δυνατότητες που παρέχονται μέσω του συγκεκριμένου συστήματος της Ελληνικής Προεδρίας, συγκρινόμενες με αυτές που παρέχει το σύστημα που αναπτύχθηκε στα πλαίσια του Ευρωπαϊκού Προγράμματος e-VOTE, παρουσιάζουν σημαντική υστέρηση. Το σύστημα της Ελληνικής Προεδρίας δεν προσφέρει τη δυνατότητα πλήρους εκλογικής διαδικασίας, αλλά παρέχει τη δυνατότητα έκφρασης της γνώμης των πολιτών.[35]

Στα πλαίσια του Ευρωπαϊκού Έργου e-VOTE χρησιμοποιήθηκε από το Δήμο του Αμαρουσίου ένα πρότυπο σύστημα ηλεκτρονικής ψηφοφορίας με στόχο αφενός να δοκιμαστεί το σύστημα σε πραγματικές συνθήκες, αλλά και για να ελεγχθεί η ανταπόκριση του απλού πολίτη σε θέματα και ζητήματα που άπτονται των συστημάτων ηλεκτρονικής ψηφοφορίας. Για το σκοπό αυτό πραγματοποιήθηκαν στο Δήμο του Αμαρουσίου πέντε (5) ψηφοφορίες, στις οποίες συμμετείχαν μόνο πολίτες του Δήμου και κάτοικοι της περιοχής, οι οποίοι καλούνταν να εκφράσουν τη γνώμη τους σχετικά με διάφορα θέματα που αφορούσαν το Δήμο.[34]

Τέλος το πρώτο βραβείο σε πανευρωπαϊκό επίπεδο απέσπασε το σύστημα ΠΝΥΚΑ του Τομέα Ηλεκτρονικής Διακυβέρνησης του ΕΑΙΤΥ, στη τελική φάση του διαγωνισμού e-voting που διοργάνωσε το Competence Center for Electronic Voting and Participation. [40] Το σύστημα υποστήριξης ηλεκτρονικών ψηφοφοριών ‘‘ΠΝΥΚΑ’’ υποστηρίζει όλα τα στάδια μιας διαδικτυακής ηλεκτρονικής ψηφοφορίας όπως εγγραφή/πιστοποίηση, υποβολή ψήφου, καταμέτρηση αποτελεσμάτων και επαλήθευση. Ενσωματώνει σημαντικές τεχνολογικές καινοτομίες όπως πλήρως κατανεμημένη αρχιτεκτονική, ομομορφική κρυπτογράφηση κατωφλίου, συσκευές υλικού για την αποθήκευση των κλειδιών κ.λ.π. και έχει αναπτυχθεί εξ’ ολοκλήρου με εργαλεία ανοικτού κώδικα. Μπορεί δε να παραμετροποιηθεί για να υποστηρίξει διαφορετικές μορφές ψηφοφορίας, από απλές διαδικασίες έκφρασης γνώμης μέχρι εκλογές και δημοψηφίσματα μεγάλης κλίμακας.

6. Η πρότασή μου για ένα σύστημα ασφαλούς Ηλεκτρονικής Ψηφοφορίας

Λαμβάνοντας υπόψη την πολύ μικρή διάχυση του διαδικτύου και γενικότερα την έλλειψη τεχνολογικής παιδείας στην Ελλάδα, το μοντέλο που θα παρουσιάσω συνδυάζει τεχνολογίες οι οποίες εφαρμόζονται στο συγκεντρωτικό μοντέλο ψηφοφορίας. Δηλαδή ψηφοφορία σε εκλογικό κέντρο.

Η μοντελοποίηση θα γίνει για σχολεία – εκλογικά κέντρα ενός μικρού δήμου ή κοινότητας. Ας υποθέσουμε ότι το σχολείο έχει σε κάθε όροφο μια ειδικά διαμορφωμένη αίθουσα για την εκλογική διαδικασία. Για να εισέλθει ο ψηφοφόρος στην αίθουσα πρέπει να αυθεντικοποιηθεί. Η αυθεντικοποίηση θα γίνεται με μια έξυπνη κάρτα (smart card) με ενσωματωμένο αναγνώστη δακτυλικού αποτυπώματος. Έτσι λοιπόν η ταυτοποίηση θα γίνεται με την εισαγωγή της κάρτας σε ειδικό αναγνώστη ο οποίος θα είναι συνδεδεμένος με tunnel mode (IPsec ESP) με τη βάση δεδομένων (εκλογικός κατάλογος) που θα περιέχονται τα ονόματα των εγγεγραμμένων ψηφοφόρων. Χρησιμοποιούμε αναγνώστη δακτυλικού αποτυπώματος για την αυθεντικοποίηση του χρήστη, γιατί εξασφαλίζει σε πολύ μεγάλο βαθμό μοναδικότητα και συνεπώς ασφάλεια. Επίσης λαμβάνεται υπόψη ο παράγοντας της ευκολίας για ανθρώπους μεγάλης ηλικίας ή ανθρώπους που δεν έχουν επαφή με την τεχνολογία. Είναι πολύ πιο εύκολο ο κάτοχος της κάρτας να την εισάγει στον αναγνώστη και απλά να ακουμπήσει το δάκτυλό του πάνω στην κάρτα, από το να θυμάται ακόμη ένα συνθηματικό (password). Το δακτυλικό αποτύπωμα χρησιμοποιείται σαν συνθηματικό – κλειδί για να αποκρυπτογραφηθεί το μυστικό που υπάρχει στην κάρτα και έχει τοποθετηθεί κατά τη διάρκεια της εγγραφής στο σύστημα.

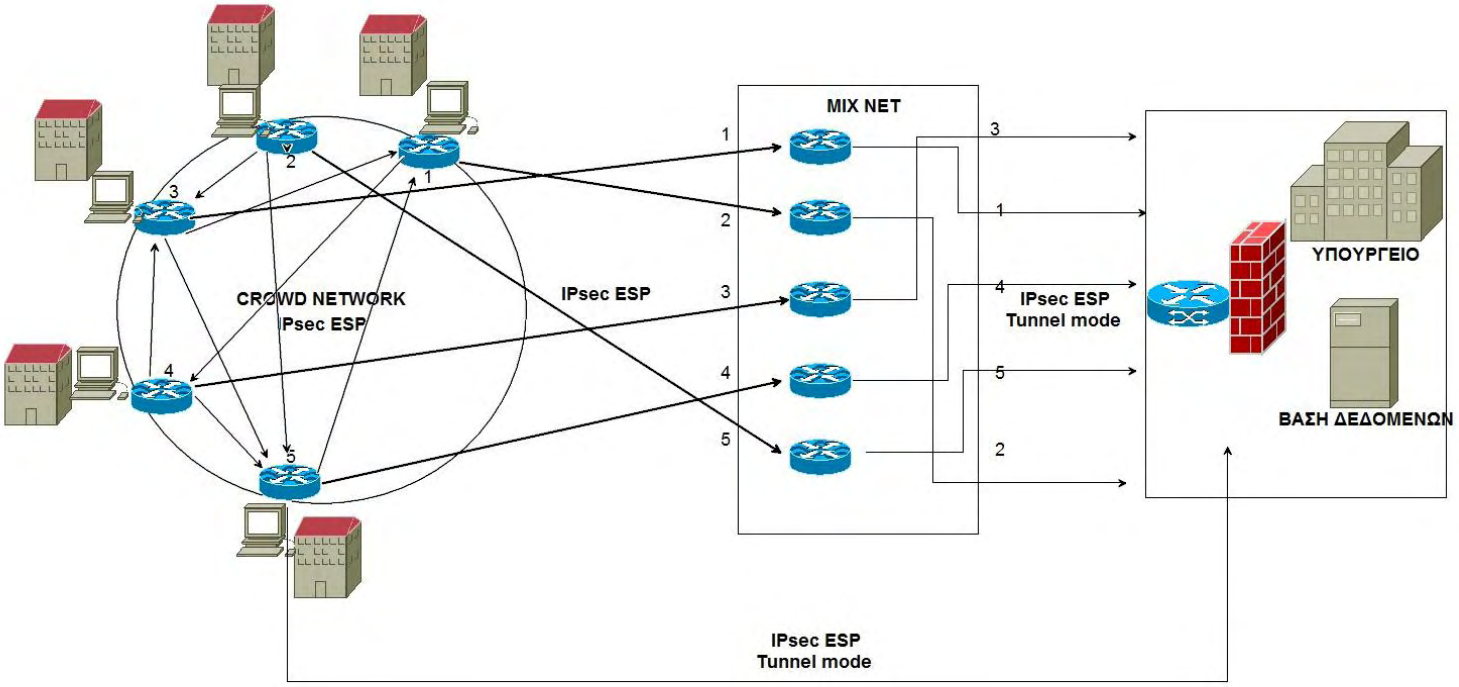
Μόλις ο χρήστης αυθεντικοποιηθεί και υπάρξει ταίριασμα με τους εκλογικούς καταλόγους, ότι δηλαδή έχει το δικαίωμα να ψηφίσει, τότε του επιτρέπεται η πρόσβαση. Μόλις ολοκληρωθεί η διαδικασία της ψηφοφορίας δημιουργείται ένα IP πακέτο όπου στην επικεφαλίδα υπάρχει η διεύθυνση προορισμού του συγκεντρωτικού server του Υπουργείου και σαν φορτίο θα έχει την ψήφο του ψηφοφόρου. Ο ψηφοφόρος αποχωρεί από την αίθουσα για να εισέλθει ο επόμενος. Έτσι εξασφαλίζουμε ότι δεν υπήρχε καταναγκασμός και τη μοναδικότητα της ψήφου. Η βάση δεδομένων ενημερώνεται ότι ο ψηφοφόρος εισήλθε στην αίθουσα ψηφοφορίας και δεν επιτρέπει την είσοδό του ξανά σε αυτήν.

Ο ψηφοφόρος από τη στιγμή που θα εισέλθει στην αίθουσα ψηφοφορίας έχει δυο επιλογές. Είτε να ψηφίσει είτε όχι. Και στις δυο περιπτώσεις για να ανοίξει η πόρτα της εξόδου και να του επιτραπεί να φύγει, θα πρέπει να πάρει ένα ticket στο οποίο αναγράφεται κρυπτογραφημένα με το δημόσιο κλειδί του, ένα αλφαριθμητικό (string) με δυο πεδία. Το πρώτο πεδίο θα είναι μηδέν (0) αν δεν ψήφισε ή ένα (1) αν ψήφισε. Το δεύτερο πεδίο, θα είναι ένα password με το οποίο θα αποκτά πρόσβαση στο σύστημα του Υπουργείου και θα μπορεί να επικυρώσει αν η ψήφος του καταχωρήθηκε επιτυχώς (bulletin board).

Το πακέτο αυτό που έχει δημιουργηθεί φτάνει με εσωτερική καλωδίωση στο server του εκλογικού κέντρου ο οποίος είναι συνδεδεμένος με ένα router.

Υποθέτουμε ότι το κτήριο φυλάσσεται οπότε δεν μπορεί κάποιος κακόβουλος χρήστης να παρεμβληθεί στο σύστημα. Κάθε εκλογικό κέντρο έχει από ένα server συνδεδεμένο με ένα router. Ας υποθέσουμε ότι ο δήμος ή η κοινότητα που εξετάζουμε έχει πέντε εκλογικά κέντρα. Οι πέντε αυτοί router συνδέονται μεταξύ τους με transport mode (IPsec, ESP Header) και δημιουργούν ένα δίκτυο crowd. Χρησιμοποιούμε στην υλοποίησή μας δίκτυο crowd γιατί προσφέρει ανωνυμία. Η βασική ιδέα σε ένα crowd πρωτόκολλο είναι ότι ένα πακέτο ακολουθεί μια τυχαία διαδρομή σε ένα δίκτυο ίδιων κόμβων. Έτσι κάποιος ωτακουστής (eavesdropper) δεν μπορεί ποτέ να είναι σίγουρος για το αν ο κόμβος που στέλνει ένα πακέτο είναι η πηγή ή απλά ένας ενδιάμεσος κόμβος.

Στη συνέχεια κάθε κόμβος του crowd δικτύου συνδέεται με ένα router με transport mode (IPsec ESP) σε ένα mix net. Ρυθμίζουμε τους κόμβους του δικτύου crowd να στέλνουν τα πακέτα ο ένας στον άλλον μέχρι να συγκεντρωθούν πέντε διαφορετικά πακέτα. Μόλις εισέλθει και το πέμπτο πακέτο στέλνονται στους κόμβους του mix net. Αυτό γίνεται γιατί θέλουμε να αποφύγουμε να δώσουμε πληροφορία στον επιτιθέμενο για το πώς δουλεύει το mix net που έχουμε. Για παράδειγμα αν φτάσει στο δίκτυο ένα πακέτο στην είσοδο ένα (1) και δρομολογηθεί από την έξοδο τέσσερα (4), αυτομάτως ο επιτιθέμενος γνωρίζει κάποια από τις αντιστοιχίες του mix net. Μετά και το ‘‘ανακάτεμα’’ των πακέτων στο mix net δίκτυο, στέλνονται με κρυπτογραφημένο τρόπο (tunnel mode, IPsec ESP) σε ένα κεντρικό κόμβο που τα οδηγεί στο συγκεντρωτικό server του Υπουργείου. Χρησιμοποιούμε tunnel mode γιατί το τμήμα του υπουργείου το οποίο είναι υπεύθυνο για τη διεξαγωγή των εκλογών, είναι ένα υποδίκτυο του δικτύου του υπουργείου. Οπότε θέλουμε η εσωτερική IP του υποδικτύου αυτού να είναι προστατευμένη κατά τη μεταφορά του IP πακέτου.



Εικόνα 14. Τοπολογία της προτεινόμενης λύσης

7. Συμπέρασμα

Είναι δεδομένο ότι όσο η επιστήμη των υπολογιστών εξελίσσεται, η είσοδός της στην ζωή μας θα γίνεται όλο και πιο συχνή. Η Ηλεκτρονική Ψηφοφορία είναι ένας κλάδος ο οποίος αναπτύσσεται ραγδαία το τελευταίο διάστημα με αρκετά ενθαρρυντικά αποτελέσματα. Έχει τη δυνατότητα να προσφέρει υπηρεσίες και ευκολία στους ίδιους τους ψηφοφόρους αλλά και στις κυβερνήσεις για την ασφαλή διεξαγωγή της εκλογικής διαδικασίας. Μένει μόνο να αναπτυχθεί η κατάλληλη υποδομή. Η υιοθέτηση της Ηλεκτρονικής Ψηφοφορίας από τις κυβερνήσεις φαίνεται πως θα πραγματοποιείται σε πολύ μεγαλύτερο βαθμό με την πάροδο των ετών.

Το γενικό συμπέρασμα λοιπόν που προκύπτει, είναι ότι η επιτυχία της Ηλεκτρονικής Ψηφοφορίας εξαρτάται από ένα πλήθος παραγόντων, όπως η:

- αξιοπιστία των συστημάτων,
- ευκολία χρήσης των συστημάτων,
- αποδοχή και η συμμετοχή των πολιτών,
- αποδοχή εκ μέρους του πολιτικού κόσμου,
- νομική και θεσμική κατοχύρωση της ηλεκτρονικής ψηφοφορίας,
- εξάπλωση της χρήσης των νέων τεχνολογιών και του διαδικτύου.

Επιπλέον, οι επιδράσεις που θα ασκήσει η εξάπλωση των τεχνολογιών της Ηλεκτρονικής Ψηφοφορίας στο πολιτικό σύστημα και στη λειτουργία του πολιτεύματος δεν είναι δυνατόν να εκτιμηθούν με ακρίβεια. Εύκολα, όμως, μπορεί κάποιος να διαπιστώσει ότι τα συστήματα αυτά αποτελούν ένα μέσο που οδηγεί σε αμεσότερη δημοκρατία, καθώς διευκολύνει τη διεξαγωγή τοπικών ή εθνικών δημοψηφισμάτων, καθώς και την άμεση έκφραση της γνώμης των πολιτών για κάθε πολιτικό και κοινωνικό ζήτημα.

Βέβαια θα πρέπει να τονιστεί ότι υπάρχουν ακόμη αρκετοί τομείς που θα πρέπει να διασφαλιστούν, είτε σε νομικό, είτε σε κοινωνικό είτε σε επίπεδο ασφάλειας, ούτως ώστε το εγχείρημα αυτό να πληροί όλες τις απαιτούμενες προϋποθέσεις για την επιτυχία και εξάπλωση των τεχνολογιών Ηλεκτρονική Ψηφοφορίας. Μόλις οι πολίτες πεισθούν ότι τα κυβερνητικά συστήματα είναι ασφαλή και εύχρηστα, οι ανησυχίες και οι προκαταλήψεις θα πάψουν να υφίστανται και έτσι θα διευκολυνθεί ακόμη περισσότερο η Ηλεκτρονική Ψηφοφορία.

Παράρτημα 1

Κρυπτογραφικά Εργαλεία

Πίνακες Ανακοινώσεων (Bulletin Boards).[23] Πρόκειται για *κανάλια δημόσιας εκπομπής* (public broadcast channels) που επιτρέπουν στους χρήστες (π.χ. ψηφοφόροι) να επικοινωνούν με τις Αρχές του συστήματος, με πλήρη διαφάνεια. Στα κανάλια αυτά η επικοινωνία αυθεντικοποιείται με τη χρήση ψηφιακών υπογραφών. Μια πρακτική και ασφαλής υλοποίηση των πινάκων ανακοινώσεων αποτελεί το κατανεμημένο σύστημα *Rampart*.

Ανώνυμα Κανάλια Επικοινωνίας (Anonymous Channels). Τα κανάλια αυτά εξασφαλίζουν την ανωνυμία των χρηστών του συστήματος. Εκτός από τα δίκτυα MIX-net, υπάρχουν και τα συστήματα ανωνυμίας με τη χρήση *διαμεσολαβητή* (proxy systems), όπως επίσης και τα *υβριδικά συστήματα* (hybrid systems) ανωνυμίας. [31]

Κρυπτογραφία τύπου Threshold (threshold cryptography).[21,22] Τα συστήματα κρυπτογράφησης τύπου threshold κατανέμουν τη λειτουργικότητα των κρυπτογραφικών πρωτοκόλλων ώστε να επιτύχουν ανθεκτικότητα (robustness). Για παράδειγμα, σε μια ψηφοφορία η διαδικασία της καταμέτρησης μπορεί να κατανεμηθεί μεταξύ Αρχών Ψηφοφορίας, με τη χρήση ενός threshold κρυπτογραφικού συστήματος δημοσίου κλειδιού (π.χ. threshold ElGamal). Σε αυτήν την περίπτωση υπάρχει μόνον ένα δημόσιο κλειδί, ενώ το ιδιωτικό κλειδί διαμοιράζεται στις Αρχές με τη χρήση τεχνικών διαμοιρασμού μυστικού. Κάθε ψηφοφόρος κρυπτογραφεί τη ψήφο του με το δημόσιο κλειδί των Αρχών, και η τελική κάλπη αποκρυπτογραφείται από κοινού με τη συνεργασία τουλάχιστον t Αρχών. Η μυστικότητα της ψήφου και η ακρίβεια των αποτελεσμάτων εξασφαλίζεται εφόσον δεν υπάρχουν περισσότερες από μια κακόβουλες ή απλά δυσλειτουργικές Αρχές. Ο αριθμός αποτελεί τη τιμή threshold του κρυπτογραφικού συστήματος. Τα συστήματα threshold μπορούν να ενισχυθούν, για προστασία από επιθέσεις υποκλοπής κλειδιού (key confiscation), με μηχανισμούς όπως προ-ενεργή ασφάλεια (proactive security) καθώς και με τεχνικές ισχυρής χρονικής ασφάλειας (strong forward security).

Αποδείξεις με Μηδενική Γνώση (Zero Knowledge Proofs).[10,11,25,8,18] Οι αποδείξεις αυτές χρησιμοποιούν πρωτόκολλα Απόδειξης/Επαλήθευσης με αλληλεπίδραση (interactive), στα οποία ο Αποδεικνύων (Prover) επιβεβαιώνει σε έναν Επαληθευτή (Verifier) την ορθότητα μιας δήλωσης, κατά τέτοιον τρόπο ώστε ο Επαληθευτής να μη μπορεί να μάθει τίποτε περισσότερο, εκτός από το γεγονός ότι η δήλωση είναι ορθή. Τα πρωτόκολλα απόδειξης με μηδενική γνώση χρησιμοποιούνται ευρέως σε ηλεκτρονικά πρωτόκολλα ψηφοφορίας.

Για παράδειγμα, τέτοια πρωτόκολλα χρησιμοποιούνται προκειμένου να αποδειχθεί η ορθότητα των μετασχηματισμών στα συστήματα ψηφοφορίας που χρησιμοποιούν δίκτυα MIX-net για την ανωνυμία των ψήφων, για να αποδειχτεί η εγκυρότητα των κρυπτογραφημένων ψήφων στις ομομορφικές εκλογές, για την ορθότητα των κρυπτογραφήσεων στα πρωτόκολλα προστασίας από καταναγκασμό, καθώς και για την ορθότητα των επικυρωμένων ψήφων στα συστήματα που

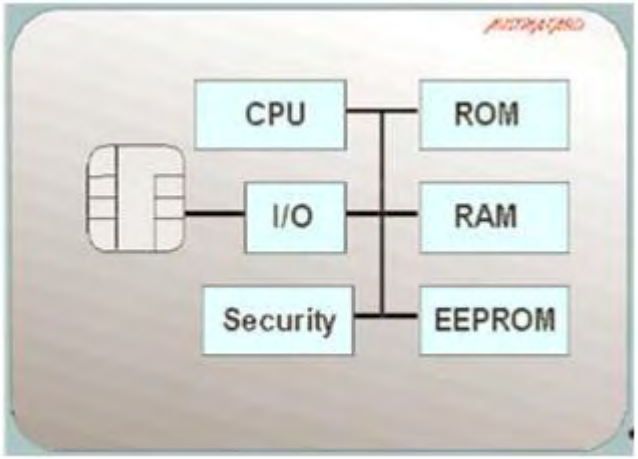
βασίζονται στο μοντέλο των ‘‘τυφλών υπογραφών’’. Οι αλληλεπιδραστικές αποδείξεις με μηδενική γνώση είναι μη μεταφέρσιμες (non transferable): ο Επαληθευτής δε μπορεί να αποδείξει σε κάποιον τρίτο την ορθότητα μιας δήλωσης. Εν τούτοις είναι δυνατόν αυτές οι αποδείξεις να μετασχηματιστούν σε αποδείξεις που είναι μεταφέρσιμες, επομένως οικουμενικά επαληθεύσιμες, με την ευριστική προσέγγιση των Fiat-Shamir [7]. Στην περίπτωση αυτή η ασφάλεια βασίζεται στο μοντέλο random oracle.

Παράρτημα 2

Έξυπνες Κάρτες (Smart Cards)

Μια smart card είναι μια κάρτα, κυρίως από πλαστικό (PVC), η οποία έχει ένα ενσωματωμένο ολοκληρωμένο κύκλωμα το οποίο μπορεί να επεξεργάζεται και να αποθηκεύει πληροφορίες. Ένας ενσωματωμένος μικροεπεξεργαστής ελέγχει τη λειτουργία των κύριων τμημάτων της κάρτας. Η RAM (μνήμη εργασίας) αξιοποιείται αποκλειστικά για προσωρινή αποθήκευση. Η ROM (μνήμη που δε διαγράφεται) αποθηκεύει το λειτουργικό σύστημα της κάρτας. Η EEPROM (μνήμη εφαρμογών) αποθηκεύει εφαρμογές και δεδομένα. Το μεγάλο μειονέκτημα αυτών των καρτών είναι ότι μπορεί να κλαπούν, να χαθούν ή να αντιγραφούν.

Εικόνες 15 και 16. Μια συνηθισμένη smart card. Μια smart card με ενσωματωμένο σύστημα αναγνώρισης δακτυλικού αποτυπώματος



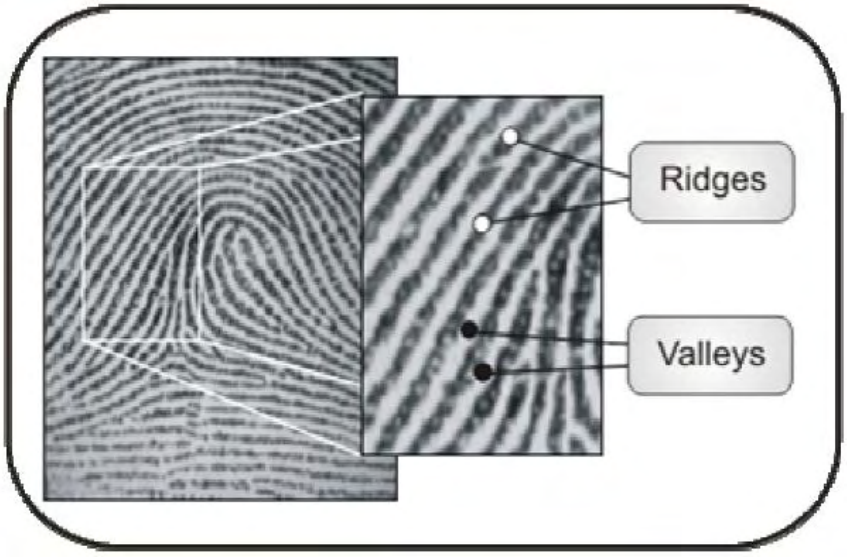
Εικόνα 17. Το ολοκληρωμένο σύστημα μιας smart card

Αναγνώριση Δακτυλικού Αποτυπώματος

Το ανθρώπινο δακτυλικό αποτύπωμα μπορεί να χρησιμοποιηθεί ως βιομετρικό χαρακτηριστικό μιας και το έχει κάθε άνθρωπος (καθολικότητα), είναι εμφανές διαχωρίσιμο μεταξύ δύο ατόμων (μοναδικότητα), είναι μόνιμο και αμετάβλητο κατά τη διάρκεια της ζωής του ατόμου (μονιμότητα) και μπορεί να μετρηθεί ποσοτικά (ικανότητα συλλογής).

Το 19^{ο} αιώνα έγινε αποδεκτή, από την επιστημονική κοινότητα, η πρόταση ότι δεν υπάρχουν δυο άνθρωποι με ίδια δακτυλικά αποτυπώματα και ότι τα δακτυλικά αποτυπώματα δεν αλλάζουν σημαντικά κατά τη διάρκεια της ζωής ενός ατόμου. Αυτό ακριβώς αποτέλεσε την απαρχή της χρησιμοποίησης των δακτυλικών αποτυπωμάτων στην επιβολή του νόμου για την αναγνώριση εγκληματιών.

Τα χαρακτηριστικά των δακτυλικών αποτυπωμάτων καθορίζουν την μοναδικότητα και με βάση την θέση τους, το σχήμα τους και το μέγεθός τους γίνεται η αναγνώριση του ατόμου. Τα βασικότερα χαρακτηριστικά είναι οι διαδοχικές κοιλάδες (valleys) και παρυφές (ridges) της επιδερμίδας που βρίσκεται στο δακτυλικό αποτύπωμα. Συνήθως σε μια εικόνα δακτυλικού αποτυπώματος οι κοιλάδες είναι άσπρες και οι παρυφές μαύρες. Οι παρυφές έχουν πάχος συνήθως 100-300μm και οι κοιλάδες 200μm.



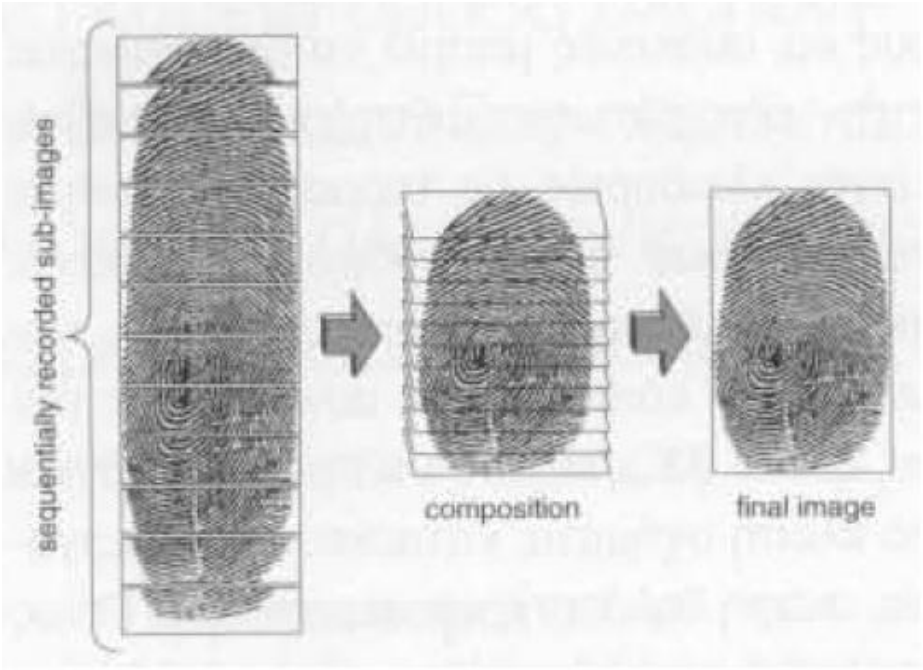
Εικόνα 18. Παρυφές και κοιλάδες δακτύλου

Συνήθως οι παρυφές και οι κοιλάδες βρίσκονται παράλληλα η μια στην άλλη μέχρι μια παρυφή να διακλαδωθεί σε δύο παρυφές ή να τερματίσει απότομα. Όταν αναλύουμε το δακτυλικό αποτύπωμα, μπορούμε να παρατηρήσουμε μία ή δύο περιοχές στις οποίες οι παρυφές και οι κοιλάδες έχουν συγκεκριμένα σχήματα. Αυτές οι περιοχές ονομάζονται ιδιαίτερες (singular regions) και διαχωρίζονται στις κατηγορίες: σημεία δέλτα (delta points) και σημεία πυρήνα (core points) και χαρακτηρίζονται από μεγάλη καμπυλότητα των παρυφών και των κοιλάδων και απότομων τερματισμών αυτών.

Τα δακτυλικά αποτυπώματα είναι πλήρη σχηματισμένα στον έβδομο μήνα ζωής

του εμβρύου και δεν αλλάζουν κατά την διάρκεια ζωής του ατόμου εκτός της περίπτωσης που συμβεί κάποιο σοβαρό ατύχημα όπως βαθύ κόψιμο, έγκαυμα, ακρωτηριασμός . Εάν τα εγκαύματα ή τα κοψίματα είναι στην επιφάνεια του δέρματος ,δεν επηρεάζεται η δομή των παρυφών και των κοιλάδων γιατί η δομή αυτή θα αναπαραχθεί ξανά στο καινούργιο δέρμα που μεγαλώνει. Υπάρχουν τόσες πολλές μεταβολές κατά τον σχηματισμό του δακτυλικού αποτυπώματος, οι οποίες καθιστούν απίθανη την ταύτιση δύο δακτυλικών αποτυπωμάτων από δύο άτομα. Ακόμα και τα δακτυλικά αποτυπώματα των ομόζυγων διδύμων διαφέρουν παρόλο που σχηματίζονται από το ίδιο γονίδιο.

Αισθητήρες δυναμικής εξόδου: Αντί το δάκτυλο να τοποθετείται απλά πάνω στον αισθητήρα, απαιτείται ένα αργό σύρσιμο του δακτύλου επάνω σε αυτόν. Ο αισθητήρας διαθέτει μια ευαίσθητη ζώνη αναγνώρισης η οποία είναι στενή και παράγει μια ολοκληρωμένη ακολουθία εικόνων, τις οποίες ο επεξεργαστής είναι σε θέση να ολοκληρώσει σε μια πλήρη εικόνα. Με τον τρόπο αυτό αυξάνεται σημαντικά η αξιοπιστία, ενώ οποιοδήποτε ίχνος βρωμιάς θα απομακρυνθεί. Αισθητήρες αυτής της μορφής κατασκευάζουν αρκετές εταιρείες, μεταξύ των οποίων και η UPEK.



Εικόνα 19. Ακολουθιακή καταγραφή εικόνων και σύνθεσή τους σε μια ολοκληρωμένη εικόνα

Εικόνα 20. Eikon-to-go. Αισθητήρας της UPEK

Βιβλιογραφία

[1] Burmester M, Gritzalis S ,Katsikas S and Chrissikopoulos V Συγχρονη Κρυπτογραφία ,θεωρια και Εφαρμογές ,εκδοσεις Παπασωτηρίου 2011

[2] D. Gritzalis (Ed.), Secure Electronic Voting: Trends and Perspectives, Capabilities and Limitations. Kluwer Academic Publishers, 2002.

[3] Mitrou L., Gritzalis D. and Katsikas S. (2002) Revisiting legal and regulatory requirements for secure e-voting. Proc. of the 16th IFIP International Information Security Conference (IFIP/SEC-2002) M. el Hadidi, et al. (Eds.), Egypt, 6-8 May 2002. Kluwer Academics Publishers.

[4] Ikonomopoulos S., Lambrinoudakis C., Gritzalis D., Kokolakis S. and Vassiliou K., "Functional Requirements for a Secure Electronic Voting System", Proc. of the 16th IFIP International Information Security Conference (IFIP/SEC-2002) M. el Hadidi, et al. (Eds.), Egypt, 6-8 May 2002. Kluwer Academics Publishers.

[5] Κάτσικας Σ., Μήτρου Λ. "Ομάδα εργασίας ΣΤ-4, Συστήματα ηλεκτρονικής ψηφοφορίας", Αθήνα Ιούλιος 2004.

[6] 1η Ανοιχτή Διαβούλευση "Νομικά και Θεσμικά Ζητήματα για Συστήματα Ηλεκτρονικής Ψηφοφορίας", Καθηγητής Σωκράτης Κάτσικας, 20-4-2004

[7] Fiat A., and Shamir A.: How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In: Advances in Cryptology – CRYPTO'86, Lecture Notes in Computer Science, Vol. 263, Springer-Verlag, pp. pp. 186-194, 1986.

[8] Chaum, D.: Blind Signatures for Untraceable Payments. In: CRYPT '82, Plenum Press, pp. 199-203, 1982

[9] Chaum, D., Damgard, I., and Graaf, J.: Multiparty Computations Ensuring Privacy of Each Party's Input and Correctness of the Result. In: Advances in Cryptology - CRYPTO '87, Lecture Notes in Computer Sciences, Vol. 293, Springer-Verlag, pp. 87-119, 1988.

[10] Burmester M., Magkos E., and Chrissikopoulos V. : Uncoercible e-bidding Games. In: Electronic Commerce Research Journal, Special Issue on Security Aspects in E-Commerce, Kluwer Academic Publishers. To be published, 2002.

[11] Burmester M., and Magkos E.: Towards Secure and Practical e- Elections in the New Era. In: Secure Electronic Voting, Kluwer Academic Publishers. To be published, 2002.

[12] Cohen J., and Fisher M.: A Robust and Verifiable Cryptographically Secure Election Scheme. In: Proceedings of the 26th IEEE Symposium on Foundations of Computer Science, IEEE Computer Society, pp. 372-382, 1985.

[13] Cramer R., Gennaro R., and Schoenmakers B.: A Secure and Optimally Efficient Multi-Authority Election Scheme. In: Advances in Cryptology - EUROCRYPT '97, Lecture Notes in Computer Science, Vol. 1233,

Springer-Verlag, pp. 103-118, 1997.

[14] Magkos E., and Chrissikopoulos V., Equitably Fair Internet Voting. In: Journal of Internet Technology, Vol. 3(3), Special Issue on Network Security, pp. 187-193, 2002.

[15] ElGamal T.: A Public-key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. In: IEEE Transactions on Information Theory, Vol. 31(4), pp. 469-472, 1985.

[16] Hirt M., and Sako K.: Efficient Receipt-Free Voting Based on Homomorphic Encryption. In: Advances in Cryptology - EUROCRYPT '2000, Lecture Notes in Computer Science, Vol. 1807, Springer-Verlag, pp. 539-556, 2000.

[17] Riera A.: An Introduction to Electronic Voting Schemes. University of Barcelona, Report PIRDI-9/98, Barcelona, Spain

[18] Abe M: Universally Verifiable Mix-net with Verification Work Independent of the Number of Mix-servers. In: Advances in Cryptology - EUROCRYPT '98, Lecture Notes in Computer Sciences, Vol. 1403, Springer-Verlag, pp. 437-447, 1998.

[19] Benaloh J.: Verifiable Secret-Ballot Elections. PhD Thesis, Yale University, 1987.

[20] Benaloh J. and Tuinstra D.: Receipt-Free Secret-Ballot Elections. In: Proceedings of the 26th Annual ACM Symposium on Theory of Computing, ACM Press, pp. 544-553, 1994.

[21] Desmedt Y. and Frankel Y.: Threshold Cryptosystems. In: Advances in Cryptology - CRYPTO '89, Lecture Notes in Computer Science, Vol. 435, Springer-Verlag, pp. 307-315, 1989.

[22] Desmedt, Y.: Threshold Cryptography. In: European Transactions on Telecommunications, Vol. 5(4), pp. 449-457, 1994.

[23] Schneier B.: Applied Cryptography, Second Edition - Protocols, Algorithm and Source Code in C. John Wiley and Sons, 1996.

[24] Davenport B., Newberger A. and Woodard J.: Creating a Secure Digital Voting Protocol for Campus Elections. Princeton University, 1996

[25] Cranor L., and Cytron R.: Sensus: A Security-Conscious Electronic Polling System for the Internet. In: Proceedings of the Hawaii International Conference on System Sciences, 1997

[26] Fujioka A., Okamoto T., and Ohta K.: A Practical Secret Voting Scheme for Large Scale Elections. In: Proceedings of AUSCRYPT '92, Lecture Notes in Computer Science, Vol. 718, Springer-Verlag, pp. 244-251, 1993.

[27] Okamoto T.: Receipt-Free Electronic Voting Schemes for Large Scale Elections. In: Proceedings of the 5th Security Protocols Workshop '97, Lecture Notes in Computer Science

[28] Okamoto T.: Threshold Key-Recovery Systems for RSA. In: Proceedings of the 5th Security Protocols Workshop, Lecture Notes in Computer Science, Vol. 1361, Springer-Verlag, pp. 191-200, 1997.

[29] Petersen, H., Horster, P., and Michels, M.: Blind Multisignature Schemes and their Relevance to Electronic Voting. In: Proceedings of the 11th Annual Computer Security Applications Conference, IEEE Press, pp. 149-155, 1995.
[30] Cranor L., and Cytron R.: Sensus: A Security-Conscious Electronic Polling System for the Internet. In: Proceedings of the Hawaii International Conference on System Sciences, 1997, at: http://lorrie.cranor.org/pubs/hicss/
[31] Reiter M., and Rubin A.: Crowds, Anonymity for Web Transactions. DIMACS Technical Report 97-15, April 1997
[32] E-voting, Welcome to the State of Geneva website
[33] "Εκλογές μέσω Διαδικτύου; Ίσως!" (21/1/2004) ,Συντάκτης: Δημήτρης Αλεξόπουλος
[34] "Ηλεκτρονική Ψηφοφορία (E-Vote): Μια Πολιτικη Προσεγγιση", http://policritos.blogspot.com/2006/12/e-vote.html
[35] e - vote:
[36] http://www.instore.gr/evote/evote_end/htm/3public/sort_project_description.htm
[37] Putting the 'E' in Elections: http://www.acm.org/technews/articles/2003-5/0203m.html#item18
[38] "Ηλεκτρονική Ψηφοφορία (E-Vote): http://policritos.blogspot.com/2006/07/e-vote.html,
[39] "Diebold Weighs Strategy for E-Voting," NewsFactor, 2007. http://www.newsfactor.com/story.xhtml?story_id=50483
[40] eEurope Initiative : http://europa.eu
[41] ΠΝΥΚΑ : http://www.pnyka.cti.gr
[42] Δράση eVote στο πλαίσιο της Ελληνικής Προεδρίας της ΕΕ : http://unpan1.un.org/intradoc/groups/public/documents/Other/UNPAN022022.pdf
[43] Hirt M. and Sako K. : Efficient Receipt-Free Voting Based on Homomorphic Encryption
[44] Herschberg M. A: Secure Electronic Voting Over the World Wide Web, 1997-05-27 Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonym," Communications of the ACM, 24:2, Feb. 1981