Κεφάλαιο 2

Ασφάλεια σε Συστήματα Ηλεκτρονικής Ψηφοφορίας

Στο Κεφάλαιο αυτό εξετάζουμε τους διάφορους τύπους συστημάτων ηλεκτρονικής ψηφοφορίας και περιγράφουμε τα κρυπτογραφικά μοντέλα ηλεκτρονικής ψηφοφορίας που έχουν προταθεί στη διεθνή βιβλιογραφία. Επίσης συζητούμε τρόπους αντιμετώπισης των προβλημάτων ασφάλειας στα συστήματα ηλεκτρονικής ψηφοφορίας και προτείνουμε δύο κρυπτογραφικά πρωτόκολλα για ασφαλή ηλεκτρονική ψηφοφορία μέσω Διαδικτύου. Το πρώτο πρωτόκολλο προσφέρει προστασία από καταναγκασμό για τους ψηφοφόρους, ενώ το δεύτερο επιλύει το πρόβλημα των απεχόντων ψηφοφόρων σε συστήματα ηλεκτρονικής ψηφοφορίας με κεντρική διαχείριση, και βασίζεται στο μοντέλο των «τυφλών» υπογραφών.

2.1 Εισαγωγή

Οι τεχνολογίες του Διαδικτύου έχουν παρεισφρήσει σε κάθε τομέα της οικονομικής και εκπαιδευτικής ζωής, κυρίως στις προηγμένες χώρες. Ο όρος *ηλεκτρονική δημοκρατία* (e-democracy) αναφέρεται στην χρήση των τεχνολογιών του Διαδικτύου για την επικοινωνία των πολιτών με την κυβέρνηση και τους πολιτικούς, την εξυπηρέτηση του πολίτη από τις δημόσιες υπηρεσίες, και τη συμμετοχή του στις αποφάσεις (π.χ. δημοψηφίσματα, συλλογή υπογραφών, δημοσκοπήσεις). Στα σημερινά αντιπροσωπευτικά δημοκρατικά καθεστώτα όπου οι πολίτες ψηφίζουν τους εκπροσώπους τους στην κυβέρνηση, επικρατεί ανησυχία για τα αυξανόμενα ποσοστά αποχής από τις εθνικές εκλογές, καθώς και γενικότερα για τη διαφαινόμενη τάση αποστασιοποίησης από τα πολιτικά δρώμενα. Για να αντιστραφεί το κλίμα αυτό αναζητούνται αλλαγές στον τρόπο συμμετοχής των πολιτών στα κοινά.

Ένα από τα μέτρα υπό συζήτηση είναι και η απλοποίηση της διαδικασίας των εκλογών, με τα συστήματα *ηλεκτρονικής ψηφοφορίας* (e-voting).

Η καθιέρωση της ηλεκτρονικής ψηφοφορίας, και μάλιστα της *ψηφοφορίας μέσω του Διαδικτύου* (Internet voting), αναμένεται να απλοποιήσει την διαδικασία υποβολής των ψήφων και να αυξήσει την εμπιστοσύνη των ψηφοφόρων στην ορθότητα των αποτελεσμάτων. Ωστόσο, οι επικριτές των συστημάτων ηλεκτρονικής ψηφοφορίας θεωρούν ότι οι υπάρχουσες τεχνολογίες δεν είναι ακόμα ώριμες να αντιμετωπίσουν τα προβλήματα ασφάλειας που προκύπτουν, να εξασφαλίσουν την ακρίβεια των αποτελεσμάτων και να επιλύσουν ζητήματα όπως αυτά του κοινωνικού αποκλεισμού των λεγόμενων «ψηφιακά αναλφάβητων» πολιτών και της αντιμετώπισης των «ευπαθών» κοινωνικών ομάδων [Dic00,Phi01].

Τα συστήματα ηλεκτρονικής ψηφοφορίας χρησιμοποιούν ψηφιακά δεδομένα για να αποτυπώσουν τις επιλογές του ψηφοφόρου. Στην ηλεκτρονική ψηφοφορία μέσω Διαδικτύου οι ψηφοφόροι έχουν την επιπλέον δυνατότητα χρησιμοποίησης του Διαδικτύου για την αποστολή των ψήφων τους στις Εκλογικές Αρχές. Έως σήμερα έχουν διεξαχθεί αρκετές εκλογές μέσω Διαδικτύου[1], αν και οι περισσότερες από αυτές είχαν ανεπίσημο χαρακτήρα, ενώ αρκετά συστήματα σχεδιάζονται και εφαρμόζονται πιλοτικά με σκοπό τη μελλοντική τους υλοποίηση σε συστήματα μεγάλης κλίμακας [Bur_Mag02b].

Σε γενικές γραμμές, κάθε ηλεκτρονική ψηφοφορία αποτελείται από τέσσερα (4) διακριτά στάδια:

- **Εγγραφή.** Πριν από τη διεξαγωγή των εκλογών, οι ψηφοφόροι αποδεικνύουν την αληθινή τους ταυτότητα και τη νομιμότητα του

[1] Παραδείγματα αποτελούν: οι εκλογές της παράταξης των Δημοκρατικών στην πολιτεία της Arizona των Η.Π.Α. (νομικά έγκυρες), Μάρτιος του 2000 [Moh01]; η αποστολή, μέσω Internet, των ψήφων του στρατιωτικού προσωπικού εντός και εκτός των Η.Π.Α (absentee ballots) στις Προεδρικές εκλογές των Η.Π.Α (νομικά έγκυρες), 2000 [Fed00]; Οι εκλογές της παράταξης των Ρεπουμπλικάνων στην πολιτεία της Alaska (ανεπίσημα αποτελέσματα), Ιανουάριος 2000 [May00]; Οι τοπικές και δημοτικές εκλογές στη Μεγ. Βρετανία (ανεπίσημα αποτελέσματα), Μάιος 2002 [Dtl02].

δικαιώματος τους να ψηφίσουν (π.χ. όριο ηλικίας). Όσοι πληρούν τις προϋποθέσεις εγγράφονται στον εκλογικό κατάλογο.

- **Επικύρωση.** Πριν την υποβολή της ψήφου ελέγχεται η ταυτότητα των ψηφοφόρων (ταυτοποίηση – identification).

- **Υποβολή Ψήφου.** Οι ψηφοφόροι υποβάλλουν την ψήφο τους. Μόνο μια ψήφος επιτρέπεται για κάθε ψηφοφόρο.

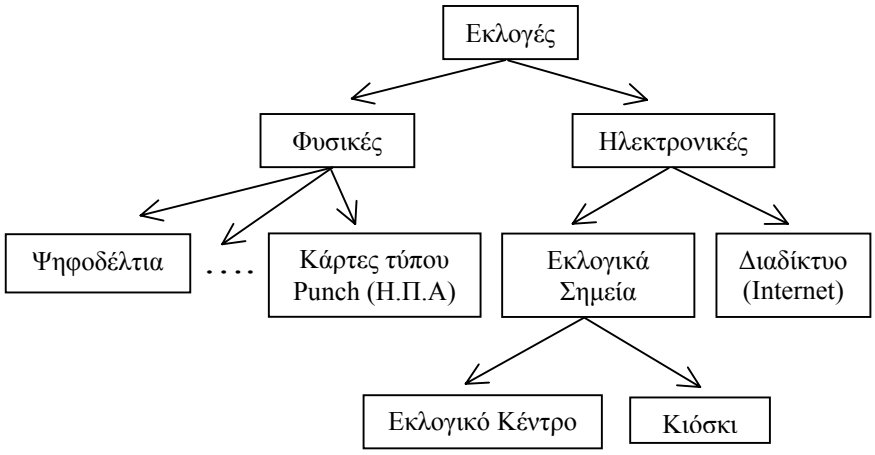
- **Καταμέτρηση Ψήφων.** Μόλις εκπνεύσει η προθεσμία υποβολής ψήφων, οι ψήφοι καταμετρούνται και ανακοινώνεται το αποτέλεσμα των εκλογών.

Κάθε ένα από τα παραπάνω στάδια μπορεί να εκτελεστεί με χρήση *φυσικών* ή *ηλεκτρονικών* διαδικασιών – Σχήμα 2. Η έρευνα μας επικεντρώθηκε στη διεξαγωγή ηλεκτρονικής ψηφοφορίας και συγκεκριμένα σε εκείνους τους τύπους ηλεκτρονικής ψηφοφορίας που περιλαμβάνουν τουλάχιστον μια απομακρυσμένη (remote) επικοινωνία μέσω ενός ανοικτού δικτύου όπως το Διαδίκτυο [Mag02,Bur_Mag02a,Bur_Mag02b,Mag01].

Διακρίνουμε δύο τύπους ηλεκτρονικής ψηφοφορίας: Την *Ηλεκτρονική Ψηφοφορία σε Εκλογικά Σημεία* (Polling Place E-Voting) και την *Ηλεκτρονική Ψηφοφορία μέσω Διαδικτύου* (Internet Voting) – Σχήμα 2.

Ηλεκτρονική Ψηφοφορία σε Εκλογικά Σημεία. Σε ένα εκλογικό σημείο, τόσο τα συστήματα-πελάτες (voting clients) που χρησιμοποιούν οι ψηφοφόροι για να υποβάλλουν ηλεκτρονικά την ψήφο τους, όσο και το φυσικό περιβάλλον στο οποίο διεξάγεται η ψηφοφορία, επιβλέπονται από εξουσιοδοτημένες οντότητες (π.χ. εκλογικοί υπάλληλοι, αντιπρόσωποι, αστυνομία). Ανάλογα με το είδος του εκλογικού σημείου, π.χ. *Εκλογικό Κέντρο* (Precinct) ή *Κιόσκι* (Kiosk) [Cal00], το στάδιο της Επικύρωσης μπορεί να γίνει είτε με φυσικές διαδικασίες (έλεγχος απ' ευθείας από τους εκλογικούς

υπευθύνους) είτε με ηλεκτρονικές (με κάποια ψηφιακή μέθοδο ταυτοποίησης). Τα στάδια της Υποβολής και της Καταμέτρησης ψήφου γίνονται εξ' ολοκλήρου με ηλεκτρονικές διαδικασίες: τα εκλογικά μηχανήματα (συστήματα-πελάτες) μπορεί να είναι Συσκευές Άμεσης Καταμέτρησης[2] (Direct Recording Equipment) [Cal01], που χρησιμοποιούνται ευρέως στις Η.Π.Α, ή επίσης ενδέχεται να στέλνουν την ηλεκτρονική κάλπη σε ένα κεντρικό εξυπηρετητή (server) μέσω μιας «ασφαλούς»[3] σύνδεσης Διαδικτύου ή μέσω του δικτύου ATM[4] [Int01].



Σχήμα 2. Μια ταξινομία των μεθόδων ψηφοφορίας [Bur_Mag02b]

Ψηφοφορία μέσω Διαδικτύου. Η ψήφος υποβάλλεται μέσω Διαδικτύου και τα συστήματα-πελάτες βρίσκονται υπό χαλαρή ή μηδαμινή επίβλεψη (τα συστήματα-πελάτες μπορεί να βρίσκονται στο σπίτι, στον χώρο εργασίας, σε βιβλιοθήκες, σχολεία, πανεπιστήμια). Η Εγγραφή μπορεί να γίνει με φυσικές

[2] Με τέτοιες συσκευές οι ψηφοφόροι κάνουν τις επιλογές τους σε έναν υπολογιστή (π.χ. αλληλεπιδρώντας με μια οθόνη αφής – touch screen). Οι ψήφοι τους καταμετρούνται τοπικά και αποθηκεύονται σε αποσπώμενα περιφερειακά μέσα αποθήκευσης (π.χ. σκληροί δίσκοι, μαγνητικές ταινίες).

[3] Μια «ασφαλής» (μυστική και αυθεντικοποιημένη) σύνδεση Internet μπορεί να επιτευχθεί είτε με φυσικό τρόπο (π.χ. μισθωμένες γραμμές οπτικών ινών) είτε ηλεκτρονικά με τεχνικές και εργαλεία όπως encrypting firewalls και ενδοδίκτυα VPN (Εικονικά Ιδιωτικά Δίκτυα).

[4] Τα δίκτυα ATM (Automated Teller Machines) έχουν ορισμένα επιθυμητά χαρακτηριστικά ασφάλειας (μυστικότητα του καναλιού επικοινωνίας, αξιόπιστος εξοπλισμός, ανθεκτικά τερματικά, υψηλό ποσοστό διείσδυσης). Ωστόσο συχνά διατυπώνονται αντιρρήσεις σχετικά με την καταλληλότητα τους για τη διενέργεια ηλεκτρονικών εκλογών [Jef00].

(π.χ. σε ένα εκλογικό γραφείο) ή με ηλεκτρονικές διαδικασίες (με κάποια ψηφιακή μέθοδο ταυτοποίησης). Τα στάδια της Επικύρωσης, της Υποβολής και της Καταμέτρησης γίνονται εξ' ολοκλήρου με ηλεκτρονικές διαδικασίες.

Η ψηφοφορία μέσω Διαδικτύου απαιτεί ένα μεγαλύτερο επίπεδο ασφάλειας από αυτό που απαιτείται σε συνήθεις συναλλαγές ηλεκτρονικού εμπορίου. Ενώ η ταυτοποίηση των ψηφοφόρων και η εξασφάλιση της μοναδικότητας της ψήφου ανά ψηφοφόρο, μπορούν να αντιμετωπιστούν με τεχνικές που ήδη χρησιμοποιούνται σε εφαρμογές ηλεκτρονικών συστημάτων πληρωμών (π.χ. ψηφιακές υπογραφές - ψηφιακά πιστοποιητικά), οι επιπλέον απαιτήσεις όπως η *μυστικότητα* (secrecy) και η *ανωνυμία* (anonymity) της ψήφου, η *οικουμενική επαληθευσιμότητα* (universal verifiability), καθώς και η *προστασία από καταναγκασμό* (uncoercibility), συνθέτουν ένα πολύπλοκο μοντέλο απαιτήσεων ασφάλειας το οποίο έως σήμερα δεν έχει αντιμετωπιστεί με μεθόδους που να είναι ασφαλείς και παράλληλα πρακτικές.

Συνεισφορά / Δομή του Κεφαλαίου

Στην Ενότητα 2.2 θεωρούμε τα συστήματα ηλεκτρονικής ψηφοφορίας, κατά πρώτο λόγο από τη σκοπιά της ασφάλειας και κατά δεύτερο λόγο από τη σκοπιά της πρακτικότητας στην υλοποίηση τους [Bur_Mag02b,Bur_Mag02a]. Στην Ενότητα 2.3 παραθέτουμε τις σημαντικότερες κρυπτογραφικές μεθόδους που έχουν προταθεί για την υλοποίηση των απαιτήσεων ασφάλειας στα συστήματα ηλεκτρονικής ψηφοφορίας, ενώ στις Ενότητες 2.4 και 2.5 περιγράφουμε δύο πρωτόκολλα [Mag01,Mag02] για την αντιμετώπιση συγκεκριμένων προβλημάτων ασφάλειας σε ηλεκτρονικές εκλογές μεγάλης κλίμακας. Στην Ενότητα 2.4 αναλύουμε πώς μπορεί να επιτευχθεί *προστασία από καταναγκασμό* με τη χρήση Έξυπνων Καρτών που συνεισφέρουν κάποια τυχαιότητα στην κρυπτογράφηση της ψήφου, κατά τρόπο που δεν αφήνει περιθώρια κακόβουλων ενεργειών στον χρήστη ή στην κάρτα, ενώ στην Ενότητα 2.5 αναλύουμε το πρόβλημα της *απόσυρσης ψήφου* στις ηλεκτρονικές

εκλογές κεντρικής διαχείρισης (central administration) και προτείνουμε μια μεθοδολογία αντιμετώπισης του προβλήματος. Το Κεφάλαιο ολοκληρώνεται με τη συζήτηση στην Ενότητα 2.6.

2.2 Θεώρηση Συστημάτων Ηλεκτρονικής Ψηφοφορίας

Στην Ενότητα αυτή συνοψίζουμε τις απαιτήσεις ασφάλειας και πρακτικότητας που πρέπει να εκπληρώνουν τα συστήματα ηλεκτρονικής ψηφοφορίας. Επίσης συζητούμε τα πλεονεκτήματα και μειονεκτήματα που συνεπάγεται η χρήση τέτοιων συστημάτων, και προτείνουμε μια σειρά από μέτρα που πρέπει να λαμβάνονται κατά τη διενέργεια ηλεκτρονικών εκλογών μέσω του Διαδικτύου.

2.2.1 Απαιτήσεις Ασφάλειας και Πρακτικότητας

Για τη σχεδίαση ενός συστήματος ηλεκτρονικής ψηφοφορίας που πρόκειται να χρησιμοποιηθεί σε εκλογές μεγάλης κλίμακας, είναι σημαντικό να καθορίσουμε τις απαιτήσεις ασφάλειας και πρακτικότητας. Οι απαιτήσεις αυτές πρέπει να είναι κοινώς αποδεκτές και τεχνολογικά ουδέτερες [Cran97,Int01,Sch96, Bur_Mag02b]. Ένα σύστημα ηλεκτρονικής ψηφοφορίας πρέπει λοιπόν να είναι:

α) Ασφαλές[5], δηλαδή:

- *Δημοκρατικό* (Democratic).
    - Μόνο εξουσιοδοτημένοι ψηφοφόροι δικαιούνται να υποβάλλουν ψήφους.

[5] Η ασφάλεια των συστημάτων ηλεκτρονικής ψηφοφορίας από τη σκοπιά της κρυπτογραφίας, συζητείται στην Ενότητα 2.3.

  - Κανένας ψηφοφόρος δε δικαιούται να υποβάλλει περισσότερες από μια ψήφους.

- *Ακριβές* (Accurate). Καμία ψήφος δεν είναι δυνατόν
  - να αλλοιωθεί,
  - να καταμετρηθεί περισσότερες από μια φορές,
  - να διαγραφεί από τις Εκλογικές Αρχές ή άλλους εσωτερικούς/εξωτερικούς εχθρούς.

- *Μυστικό* (Secret).
  - Όλες οι ψήφοι παραμένουν μυστικές για όσο διάστημα διαρκεί η περίοδος υποβολής ψήφων.
  - Καμία ψήφος δεν είναι δυνατόν να συνδεθεί με τον ψηφοφόρο που την υπέβαλλε.

- *Προστατευμένο από Καταναγκασμό* (Uncoercible). Κανένας χρήστης δεν έχει τη δυνατότητα να αποδείξει τη ψήφο του σε κάποιον τρίτο.

- *Οικουμενικά Επαληθεύσιμο* (Universally Verifiable). Κάθε εξωτερικός παρατηρητής μπορεί να πειστεί[6] ότι το σύστημα είναι ακριβές και ότι το αποτέλεσμα του υπολογισμού των ψήφων της κάλπης αντανακλά τη βούληση των ψηφοφόρων που τις υπέβαλλαν.

- *Ανθεκτικό* (Robust). Όλες οι απαιτήσεις ασφάλειας ικανοποιούνται πλήρως, παρά τα όποια τυχαία σφάλματα ή τις κακόβουλες

[6] Αντί για οικουμενική επαληθευσιμότητα, αρκετά συστήματα υποστηρίζουν μόνον *ατομική επαληθευσιμότητα* (atomic verifiability) [Rie98], σύμφωνα με την οποία οι ψηφοφόροι μπορούν να εντοπίζουν και να διορθώνουν τα λάθη που αφορούν μόνον τη δική τους ψήφο και που γίνονται κατά τη διάρκεια της ψηφοφορίας, κατά την καταμέτρηση των ψήφων ή την ανακοίνωση των αποτελεσμάτων. Ως λιγότερο ασφαλή, τα συστήματα που ενσωματώνουν ατομική επαληθευσιμότητα είναι κατάλληλα κυρίως για εκλογές μικρής κλίμακας (small-scale), όπου το κόστος της επίτευξης οικουμενικής επαληθευσιμότητας ξεπερνά τα προσδοκώμενα οφέλη.

συμπεριφορές κάποιων οντοτήτων (ψηφοφόροι, Αρχές, εσωτερικοί/εξωτερικοί εχθροί).

β) Πρακτικό, δηλαδή:

- Εύκολα υλοποιήσιμο, συμβατό με τις διάφορες τεχνολογίες και πλατφόρμες (λειτουργικά συστήματα, αρχιτεκτονικές, εργαλεία πλοήγησης στο Web κ.λ.π).

- Λειτουργικό για όλους τους ψηφοφόρους και ιδιαίτερα για τους ψηφοφόρους με ειδικές ανάγκες.

- Να υποστηρίζει μια ποικιλία από μορφοποιήσεις (format) ψήφων.

- Η αποδοτικότητα του να μην επηρεάζεται δραστικά από το μέγεθος του εκλογικού σώματος (scalability).

- Να υπόκειται σε ελέγχους αξιοπιστίας ώστε να εμπνέει εμπιστοσύνη.

2.2.2 Πλεονεκτήματα Συστημάτων Ηλεκτρονικής Ψηφοφορίας

α) Ηλεκτρονική Ψηφοφορία (Γενικά). Ορισμένα από τα πλεονεκτήματα των συστημάτων ηλεκτρονικής ψηφοφορίας προκύπτουν με βάση τη σύγκριση τους με παραδοσιακά εκλογικά συστήματα, τα οποία και ενέχουν σημαντικά προβλήματα αξιοπιστίας. Για παράδειγμα στις εκλογές του 2000 στις Η.Π.Α παρουσιάστηκε ένας αρκετά μεγάλος αριθμός *προβληματικών ψήφων* (residual votes), όπως αποκαλούνται οι ψήφοι με λιγότερες επιλογές υποψηφίων από τις προβλεπόμενες (under votes), οι αλλοιωμένες ψήφοι (spoiled votes), οι

ψήφοι που δε λήφθηκαν υπ' όψιν κατά την καταμέτρηση (uncounted votes) κ.λ.π. [Cal01]. Τα συστήματα ηλεκτρονικής ψηφοφορίας αναμένεται να μειώσουν σημαντικά τα ποσοστά λάθους στην υποβολή και καταμέτρηση των ψήφων [Moh01, Bur_Mag02b]. Επίσης υπόσχονται μεγαλύτερη προσβασιμότητα σε ευπαθείς ομάδες ψηφοφόρων. Επιπλέον, η καταμέτρηση των ψήφων και η δημοσίευση των αποτελεσμάτων θα γίνονται εύκολα, γρήγορα, με μικρότερη πιθανότητα λάθους, αλλά και μικρότερο (μακροπρόθεσμα) οικονομικό κόστος, σε σχέση π.χ. με το κόστος εκτύπωσης ψηφοδελτίων στις παραδοσιακές εκλογές.

β) Ψηφοφορία μέσω Διαδικτύου. 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 μεγάλος αριθμός υπολογιστών που είναι σήμερα διαθέσιμοι σε εύκολα προσβάσιμους χώρους (π.χ. βιβλιοθήκες, σχολεία, πανεπιστήμια) μπορούν να γίνονται διαθέσιμοι στο εκλογικό σώμα την ημέρα των εκλογών. Επίσης, η ψηφοφορία μέσω Διαδικτύου θα μπορούσε να διαδραματίσει σημαντικό ρόλο σε εκλογές μικρής κλίμακας, π.χ. φοιτητικές εκλογές, ανάδειξη αντιπροσώπων ή/και λήψη αποφάσεων σε συλλόγους, κοινότητες, οργανισμούς κ.λ.π. [Bur_Mag02b].

2.2.3 Μειονεκτήματα Συστημάτων Ηλεκτρονικής Ψηφοφορίας

Οι απειλές ασφάλειας που ελλοχεύουν στα συστήματα ηλεκτρονικής ψηφοφορίας είναι ιδιαίτερα σημαντικές [Cal00,Col02,Int01, Rub01,Bur_Mag02b,Phi01]:

α) Ηλεκτρονική Ψηφοφορία (Γενικά). Είναι γνωστό ότι τα ηλεκτρονικά δεδομένα αντιγράφονται, αλλοιώνονται και καταστρέφονται πολύ πιο εύκολα από ότι οι φυσικές ψήφοι. Επιπλέον, όλα τα ηλεκτρονικά συστήματα είναι ευάλωτα σε επιθέσεις από *εσωτερικούς εχθρούς* (insider attacks) καθώς και σε επιθέσεις *Άρνησης Εξυπηρέτησης* (Denial Of Service – DOS) [Rub01,Sch96] που έχουν ως στόχο τους υπολογιστικούς πόρους ενός ηλεκτρονικού υπολογιστή (σύστημα-πελάτης ή σύστημα-εξυπηρετητής).

Τα σημερινά ηλεκτρονικά συστήματα ψηφοφορίας διαθέτουν ανεπαρκή *στοιχεία ελέγχου* (audit trail) [Phi01] και δεν παρέχουν οικουμενική επαληθευσιμότητα, με συνέπεια τα αποτελέσματα της ψηφοφορίας να τίθενται υπό αμφισβήτηση. Επιπλέον, παρότι σήμερα υπάρχουν ασφαλείς κρυπτογραφικοί αλγόριθμοι, δεν υπάρχουν επαρκώς ασφαλή συστήματα (π.χ. πλατφόρμες, λειτουργικά συστήματα) στα οποία να μπορούμε να ενσωματώσουμε την κρυπτογραφία [Riv01].

β) Ψηφοφορία μέσω Διαδικτύου. Τα συστήματα ψηφοφορίας αυτού του τύπου θα γίνουν ευρέως αποδεκτά μόνον όταν σχεδόν όλοι οι ψηφοφόροι θα μπορούν να έχουν εύκολη και γρήγορη πρόσβαση στο Διαδίκτυο, κάτι που δεν ισχύει σήμερα. Επίσης, η μετάβαση σε εκλογές μέσω Διαδικτύου πιθανόν να συνεπάγεται υψηλό κόστος αγοράς και συντήρησης υπολογιστικών μηχανών, λογισμικού βάσεων δεδομένων και συστημάτων δρομολόγησης [Cal00]. Από τη σκοπιά της ασφάλειας, οι εκλογές μέσω Διαδικτύου είναι περισσότερο ευάλωτες σε *επιθέσεις καταναγκασμού* [Bur_Mag02a] όπου οι χρήστες αναγκάζονται ή συναλλάσσονται με κάποιον τρίτο για την υποβολή μιας προσυμφωνημένης ψήφου. Επιπρόσθετα, οι χρήστες πρέπει να δημιουργούν οι ίδιοι ένα ασφαλές περιβάλλον στις υπολογιστικές τους μηχανές (συστήματα πελάτες), προτού υποβάλλουν τη ψήφο τους. Οι έλεγχοι και η πιστοποίηση λογισμικού στα συστήματα ψηφοφορίας μέσω Διαδικτύου παρουσιάζουν επίσης ιδιαίτερες δυσκολίες, καθώς τα συστατικά μέρη των συστημάτων αυτών είναι συνήθως διαφορετικής προέλευσης και έχουν μυστικό (κλειστό) κώδικα, όπως για παράδειγμα τα σύγχρονα λειτουργικά

συστήματα Windows και τα προγράμματα πλοήγησης στο Web [Mer01]. Παράλληλα, τα συστήματα ψηφοφορίας μέσω Διαδικτύου είναι περισσότερο ευάλωτα, σε σχέση με τις υπόλοιπες κατηγορίες ηλεκτρονικής ψηφοφορίας, στα εξής σημεία:

- *Στα συστήματα-πελάτες* (clients): Ιοί τύπου «*σκουλήκια*» (worms) ή «*δούρειοι ίπποι*» (trojan horses) μπορούν να αλλοιώσουν τη ψήφο, πολύ πριν αυτή κρυπτογραφηθεί ή αυθεντικοποιηθεί. Επίσης, ο επιτιθέμενος μπορεί εξ' αποστάσεως να εκμεταλλευτεί «τρύπες» ή λάθη στο σχεδιασμό του λειτουργικού συστήματος ή του προγράμματος πλοήγησης [Rub01] στο Web.

- *Στο επίπεδο της επικοινωνίας*: Οι κυριότερες επιθέσεις στο επίπεδο της επικοινωνίας είναι οι επιθέσεις *πλαστοπροσωπίας* (spoofing) ονομάτων DNS ή διευθύνσεων IP, καθώς και οι *επιθέσεις ενδιάμεσης οντότητας* (man in the middle attacks) [Sch96]. Κατά τη διάρκεια μιας τέτοιας επίθεσης, για παράδειγμα, ο επιτιθέμενος στέλνει στο σύστημα-πελάτης μια φαινομενικά έγκυρη σελίδα Web. Ο χρήστης νομίζει ότι ο δικτυακός τόπος που εμφανίζεται στο πρόγραμμα πλοήγησης είναι ο επίσημος δικτυακός τόπος για την υποβολή της ψήφου. Αυτό μπορεί να είναι αρκετό για να μη ληφθεί καθόλου υπ' όψιν η ψήφος του χρήστη. Αργότερα ο επιτιθέμενος μπορεί να χρησιμοποιήσει τα ψηφιακά πιστοποιητικά που θα του έχει ήδη υποβάλλει ο ανυποψίαστος χρήστης, ώστε να ταυτοποιηθεί στον server του συστήματος και να υποβάλλει μια «πλαστή» ψήφο εκ μέρους του χρήστη.

  Η επικοινωνία μεταξύ client και server μπορεί επίσης να απειληθεί και από επιθέσεις τύπου TCP SYN/ACK στο επίπεδο δικτύου του μοντέλου TCP/IP, από επιθέσεις πλαστοπροσωπίας στο φυσικό επίπεδο του μοντέλου OSI (ARP spoofing) κ.λ.π. [Phi01].

- *Στα συστήματα-εξυπηρετητές* (servers): Οι επιθέσεις σε αυτό το επίπεδο είναι παρόμοιες με αυτές στα συστήματα-πελάτες. Εδώ βέβαια οι επιθέσεις Άρνησης Εξυπηρέτησης (DOS), όπως IP fragmentation ή υπερχείλιση καταχωρητών (buffer overflow), έχουν μεγάλη επικινδυνότητα, αφού μπορούν να υπονομεύσουν ολόκληρη την εκλογική διαδικασία [Phi01]. Το πρόβλημα της *συμφόρησης* (bottleneck) είναι παρόμοιο, ως προς τις συνέπειες που έχει, με μια επίθεση Άρνησης Εξυπηρέτησης, με τη διαφορά ότι η συμφόρηση προκαλείται από υπερβολικά μεγάλο αριθμό ταυτόχρονων νομίμων αιτήσεων για σύνδεση με τον server, και όχι απαραίτητα από κακόβουλη επίθεση [Dic00].

2.2.4 Συνιστώμενα Μέτρα Ασφάλειας

Τα πρώτα συστήματα ηλεκτρονικής ψηφοφορίας που αναμένεται να χρησιμοποιηθούν στο άμεσο μέλλον σε εφαρμογές μεγάλης κλίμακας, θα είναι αναμφισβήτητα συστήματα *ηλεκτρονικής ψηφοφορίας σε εκλογικά σημεία*, όπου τα συστήματα-πελάτες και το φυσικό περιβάλλον μπορούν να προστατεύονται επαρκώς. Στα συστήματα αυτά επίσης είναι δυνατή η προστασία του καναλιού επικοινωνίας μεταξύ πελατών και εξυπηρετητή, είτε με τη χρήση «ασφαλών» συνδέσεων (μισθωμένες γραμμές ή με τεχνικές δικτύων VPN) είτε με χρήση εξοπλισμού DRE [Cal00,Cha81,Int01] (Ενότητα 2.1).

Η δεύτερη κατηγορία ηλεκτρονικής ψηφοφορίας, η *ψηφοφορία μέσω Διαδικτύου*, όπως είδαμε στις προηγούμενες Ενότητες, παρουσιάζει τις μεγαλύτερες δυσκολίες υλοποίησης, κυρίως λόγω των προβλημάτων ασφάλειας που αναδεικνύει. Υπάρχουν αρκετές παράμετροι, συνυφασμένες τόσο με τεχνικά θέματα όσο και με θέματα σχεδιασμού *πολιτικής ασφάλειας* (security policy), οι οποίες πρέπει να επιλυθούν προτού οι ηλεκτρονικές

εκλογές μέσω Διαδικτύου αποτελέσουν μια πραγματικότητα για συστήματα μεγάλης κλίμακας. Συγκεκριμένα:

- Πρέπει να υιοθετηθούν ασφαλείς κρυπτογραφικές μέθοδοι καθώς και επαρκή *στοιχεία ελέγχου* με *οικουμενική επαληθευσιμότητα* ώστε τα ηλεκτρονικά συστήματα ψηφοφορίας να τύχουν ευρείας αποδοχής [Bur_Mag02b]. Οι ψηφοφόροι πρέπει να εκπαιδευτούν και να ενημερωθούν για όλες τις πτυχές (σχεδιασμός και υλοποίηση) ενός συστήματος ηλεκτρονικής ψηφοφορίας. Επίσης για λόγους αξιοπιστίας, το σύστημα πρέπει να έχει υλοποιηθεί με χρήση *ανοικτού λογισμικού* (open source) [Riv01_1].

- Οι εκλογές μέσω Διαδικτύου θα γίνουν πλήρως ηλεκτρονικές (από το στάδιο της Εγγραφής έως και το στάδιο της Καταμέτρησης) μόνον όταν υιοθετηθεί και υλοποιηθεί μια ενιαία και ασφαλής *Υποδομή Δημοσίου Κλειδιού* (Public Key Infrastructure – PKI) [Dic00], όπου οι απαιτήσεις της ακρίβειας και της μυστικότητας στην επικοινωνία μέσω Διαδικτύου θα υποστηρίζονται με ισχυρές ψηφιακές υπογραφές και τεχνολογίες κρυπτογράφησης. Επίσης, τα προγράμματα πλοήγησης στο Web θα πρέπει να υποστηρίζουν κρυπτογράφηση και ψηφιακές υπογραφές στο επίπεδο εφαρμογής του μοντέλου OSI. Επιπλέον, τεχνολογίες όπως *SSL/TLS* (Secure Socket Layer/Transport Layer Security) και *SSH* (Secure Shell) [Sta02] πρέπει να επανεκτιμηθούν και να αξιοποιηθούν για την αποτροπή των επιθέσεων πλαστοπροσωπίας και των επιθέσεων ενδιάμεσης οντότητας [Sch96].

- Συνίσταται η χρήση εφαρμογών όπως προγράμματα antivirus και εργαλεία *firewalls* στα συστήματα-πελάτες, καθώς και *Συστήματα Ελέγχου Εισβολής* (Intrusion Detection Systems) και *firewalls* στα συστήματα-εξυπηρετητές [Neu96]. Παράλληλα επιβάλλεται η χρήση διαδικασιών *πλεονασμού* (redundancy) [Rei95], ανάκαμψης από επίθεση ή

δυσλειτουργία στους εξυπηρετητές (π.χ. συστοιχίες δίσκων RAID, δυνατότητες hot swapping, τεχνικές clustering και load balancing για συστοιχίες εξυπηρετητών, αποθηκευτικές μονάδες DLT) στους εξυπηρετητές ή στο επίπεδο της επικοινωνίας (π.χ. ενσύρματα/ ασύρματα μέσα υψηλού ρυθμού διαμεταγωγής) καθώς και η υιοθέτηση αυστηρών ελέγχων στην αξιοπιστία του λογισμικού και του υλικού που χρησιμοποιείται.

- Τέλος, υπάρχει η ανάγκη για σχεδιασμό μιας αυστηρής *πολιτικής ασφάλειας* που θα προβλέπει διαδικασίες για την αντιμετώπιση απειλών και την ανάκαμψη από επιθέσεις [And01]. Επίσης, επιβάλλεται η ύπαρξη νομολογίας που θα κατοχυρώνει το δικαίωμα των ψηφοφόρων για μυστική ψήφο (π.χ. στον χώρο εργασίας) και θα αντιμετωπίζει επιθέσεις όπως καταναγκασμός του ψηφοφόρου [Mag01,Bur_Mag02a], ηλεκτρονική εισβολή (hacking) και αλλοίωση εκλογικών συστημάτων ή προσωπικών ψήφων, επιθέσεις πλαστοπροσωπίας, επιθέσεις άρνησης εξυπηρέτησης κ.λ.π. [Ell99].

2.3 Κρυπτογραφικά Μοντέλα Ασφάλειας

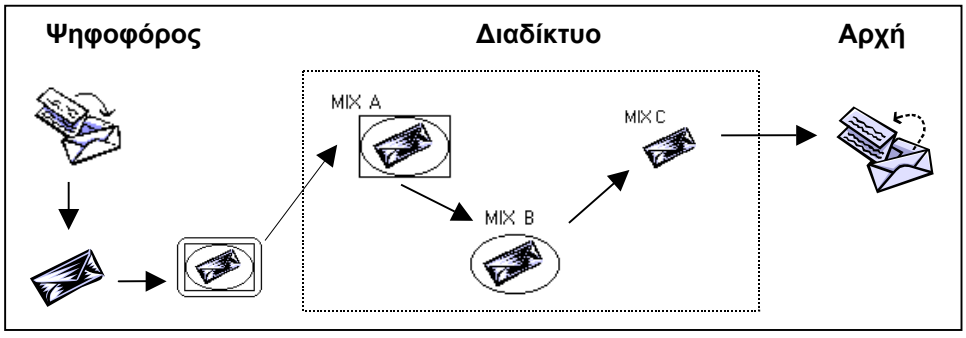
Τα βασικά κρυπτογραφικά μοντέλα ηλεκτρονικής ψηφοφορίας που έχουν προταθεί έως σήμερα είναι τέσσερα: το μοντέλο *MIX-net* [Cha81], το μοντέλο των «*τυφλών» υπογραφών* (blind signatures) [Fuj93], το *μοντέλο του Benaloh* [Ben87] και το *ομομορφικό μοντέλο* [Cra97].

2.3.1 Το Μοντέλο MIX-net

Ο Chaum [Cha81] εισήγαγε την έννοια των δικτύων 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 ορισμένους τυχαίους μετασχηματισμούς και επιστρέφει στην έξοδο (output) ένα διαφορετικό σύνολο (των ίδιων, μετασχηματισμένων) μηνυμάτων, κατά τρόπο ώστε τα μηνύματα της εξόδου να μη μπορούν να συνδεθούν με τα μηνύματα της εισόδου. Κατ' αυτόν τον τρόπο, καμία συνεργία οποιουδήποτε αριθμού κόμβων MIX (εκτός από την περίπτωση όπου συνεργούν όλοι οι κόμβοι) δε μπορεί να καθορίσει *ποια* ψήφος αντιστοιχεί σε *ποιόν* ψηφοφόρο

Στην [Cha81] κάθε ψήφος κρυπτογραφείται διαδοχικά με τα δημόσια κλειδιά όλων των κόμβων MIX, με σειρά αντίστροφη της σειράς των κόμβων – Σχήμα 3. 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. Αυτός ο τύπος δικτύου καλείται MIX-net *αποκρυπτογράφησης* [Cha81]. Εναλλακτικά, σε ένα παραπλήσιο μοντέλο, σε κάθε κόμβο MIX λαμβάνει χώρα μόνον ο μετασχηματισμός των ψήφων, και στη συνέχεια όλοι οι κόμβοι συνεργάζονται για την αποκρυπτογράφηση της τελικής λίστας των ψήφων [Abe98,Hirt00].



Σχήμα 3. Ένα παράδειγμα ενός δικτύου MIX-net με τρεις κόμβους MIX

Ένας άλλος τύπος είναι το MIX-net *επανακρυπτογράφησης* [Jak99], 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, κατά τρόπο επαληθεύσιμο (μεταξύ των κόμβων ή/και για τους εξωτερικούς παρατηρητές.

Οι πλέον χρήσιμες ιδιότητες των δικτύων MIX-net, ειδικά για εκλογές μεγάλης κλίμακας, είναι η *οικουμενική επαληθευσιμότητα* της ορθότητας των μετασχηματισμών και της αποκρυπτογράφησης [Sak95,Jak99] 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 [Jak98,Abe98,Jak02]. 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 [Abe98,Nef01].

- *Για τους ψηφοφόρους,* αν και εφόσον ο υπολογιστικός φόρτος για κάθε ψηφοφόρο είναι επίσης ανεξάρτητος του αριθμού των κόμβων MIX [Par94, Jak99].

- *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 [Abe98].

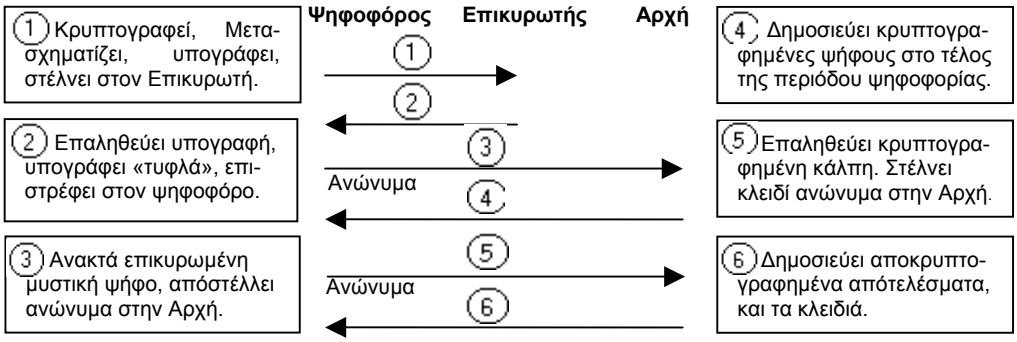
Έως σήμερα πάντως, κανένα σύστημα ηλεκτρονικής ψηφοφορίας δεν έχει υλοποιηθεί με χρήση τεχνικών MIX-net. Ωστόσο οι μηχανισμοί δικτύων MIX-net έχουν χρησιμοποιηθεί κατά καιρούς για την επίτευξη ανωνυμίας σε

εφαρμογές ηλεκτρονικού εμπορίου. Στο Κεφάλαιο 3, Ενότητα 3.6.1 θα χρησιμοποιήσουμε έναν τέτοιο μηχανισμό [Abe98] για την ανωνυμία των προσφορών που υποβάλλονται σε μια ηλεκτρονική δημοπρασία.

2.3.2 Το Μοντέλο των «Τυφλών» Υπογραφών

Η έννοια της «τυφλής» υπογραφής (blind signature) παρουσιάστηκε αρχικά από τον Chaum [Cha82] ως μια κρυπτογραφική μέθοδος για την υπογραφή ενός μηνύματος χωρίς τη γνώση του μηνύματος καθ' αυτού. Ένα ιδιαίτερο χαρακτηριστικό λοιπόν των «τυφλών» υπογραφών είναι η *μη συνδεσιμότητα* τους (unlinkability) [Cha82].

Αυτή η μέθοδος, αν και εφαρμόστηκε αρχικά σε εφαρμογές ανώνυμου *ηλεκτρονικού χρήματος* (e-cash), χρησιμοποιήθηκε επίσης από τους Fujioka, Okamoto και Ohta [Fuj93] για την επίλυση του προβλήματος της Επικύρωσης των ψήφων με παράλληλη προστασία της μυστικότητας τους: 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 (Σχήμα 4). 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 [Sak93]). 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.



Σχήμα 4. Ένα παράδειγμα ηλεκτρονικής ψηφοφορίας με «τυφλές» υπογραφές [Fuj93]

Έως σήμερα έχουν προταθεί αρκετά σχήματα που βασίζονται στον μηχανισμό των «τυφλών» υπογραφών (π.χ. [Oka97,Pet95]). Επίσης, αρκετά τέτοια συστήματα έχουν υλοποιηθεί πιλοτικά σε εκλογές μικρής κλίμακας[7].

Ένα πλεονέκτημα των συστημάτων που ακολουθούν το μοντέλο των «τυφλών» υπογραφών είναι ότι απαιτούν χαμηλό επικοινωνιακό φόρτο και υπολογιστικό κόστος, 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. Τέλος, τα ανωτέρω σε συνδυασμό με την εγγενή υποστήριξη πολλαπλών υποψηφίων, καθιστούν τα συστήματα αυτά ιδιαίτερα ελκυστικά όχι μόνο για εκλογές μικρής/μεγάλης κλίμακας, αλλά και για σφυγμομετρήσεις, δημοσκοπήσεις, κ.λ.π.

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*: εάν ένας εγγεγραμμένος ψηφοφόρος επικυρώσει τη ψήφο του (Βήματα 1,2 στο Σχήμα 4) αλλά στη συνέχεια απέχει

[7] Το σύστημα SENSUS [Cran97] ήταν το πρώτο σύστημα «τυφλών» υπογραφών που υλοποιήθηκε σε ηλεκτρονικές εκλογές μέσω του Διαδικτύου. Επίσης το σύστημα των Davenport et al [Dav96] χρησιμοποιήθηκε στο παρελθόν για τη διενέργεια επίσημων φοιτητικών εκλογών. Τέλος, το σύστημα EVOX [Hers97] χρησιμοποιήθηκε στο MIT (Massachusetts Institute of Technology) σε εκλογές προπτυχιακών φοιτητών για την ανάδειξη αντιπροσώπων τους.

από τη ψηφοφορία, τότε ένας κακόβουλος Επικυρωτής μπορεί να υποβάλλει μια πλαστή ψήφο εκ μέρους του ψηφοφόρου [Cran97]. Στην Ενότητα 2.5 θα προτείνουμε ένα «δίκαιο» πρωτόκολλο [Mag02] που αντιμετωπίζει το πρόβλημα. Πρόσφατα έχουν επίσης προταθεί πρωτόκολλα όπου η δύναμη του Επικυρωτή είναι κατανεμημένη (distributed), με τη χρήση κρυπτογραφικών τεχνικών τύπου *threshold* [Desm94] (Ενότητα 2.3.5). Μια υλοποίηση δίδεται στην εργασία [Dur99].

2.3.3 Το Μοντέλο του Benaloh

Το μοντέλο αυτό χρησιμοποιεί ένα σχήμα *ομομορφικού διαμοιρασμού μυστικών*[8] (homomorphic secret sharing). Σε τέτοια ομομορφικά σχήματα υπάρχει μια πράξη $\oplus$ ορισμένη στο σύνολο των μεριδίων, τέτοια ώστε το «άθροισμα» των μεριδίων οποιωνδήποτε δυο μυστικών x_1, x_2 να ισούται με ένα μερίδιο του «αθροίσματος» $x_1 \oplus x_2$.

Στο σχήμα του Benaloh [Ben87] κάθε ψηφοφόρος διαμοιράζει τη ψήφο του σε n Αρχές, χρησιμοποιώντας ένα (t,n) *threshold* σχήμα διαμοιρασμού μυστικού [Desm94]. 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 n Αρχές πρέπει να

[8] 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 [Desm94] σχήμα Διαμοιρασμού Μυστικού, η ανάκτηση του μυστικού είναι εφικτή εφόσον συνεργαστεί μια ομάδα από τουλάχιστον t οντότητες, όπου $t \leq n$.

συνδυάσουν τα μερίδια τους ώστε τα αποτελέσματα να είναι *οικουμενικά επαληθεύσιμα*.

Τα συστήματα αυτής της κατηγορίας (π.χ. [Sch99]), παρότι σχετικά απλά στη δομή τους, έχουν υψηλό επικοινωνιακό φόρτο: κάθε ψηφοφόρος πρέπει να υποβάλλει τη ψήφο του χρησιμοποιώντας n κανάλια επικοινωνίας.

2.3.4 Το Ομομορφικό Μοντέλο Κρυπτογράφησης

Το μοντέλο αυτό [Coh85,Cra96,Cra97] χρησιμοποιεί τις ομομορφικές ιδιότητες ορισμένων αλγορίθμων κρυπτογράφησης για να εδραιώσει οικουμενική επαληθευσιμότητα σε εκλογές μεγάλης κλίμακας, διατηρώντας παράλληλα τη μυστικότητα των ατομικών ψήφων. Κατά την ομομορφική κρυπτογράφηση υπάρχει μια πράξη $\oplus$ ορισμένη στο σύνολο των μηνυμάτων και μια πράξη $\otimes$ ορισμένη στο σύνολο των κρυπτογραφημάτων, τέτοιες ώστε το «γινόμενο» των κρυπτογραφήσεων οποιωνδήποτε δύο ψήφων $v_1, v_2 : E(v_1) \otimes E(v_2)$ να ισούται με την κρυπτογράφηση $E(v_1 \oplus v_2)$ του «αθροίσματος» των ψήφων. Ο ομομορφισμός της κρυπτογραφικής συνάρτησης εγγυάται οικουμενική επαληθευσιμότητα για την τελική κάλπη, χωρίς την ανάγκη αποκρυπτογράφησης μεμονωμένων ψήφων, κάτι που θα παραβίαζε τη μυστικότητα τους. 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* (Ενότητα 2.3.5) και οικουμενικά επαληθεύσιμη.

Στην Ενότητα 2.4 όπου και θα περιγράψουμε ένα πρωτόκολλο [Mag01] για ηλεκτρονικές εκλογές *Προστατευμένες από Καταναγκασμό* (uncoercible), θα βασιστούμε στο μοντέλο αυτό και θα αξιοποιήσουμε την ομομορφική ιδιότητα του αλγορίθμου κρυπτογράφησης ElGamal [ElG85].

Το σύστημα VoteHere [Adl00], το οποίο ήδη χρησιμοποιείται πιλοτικά σε τοπικές εκλογές μικρής κλίμακας, αποτελεί μια υλοποίηση του ομομορφικού μοντέλου κρυπτογράφησης.

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 συνεπάγονται υψηλό υπολογιστικό κόστος για τους εξυπηρετητές. Για παράδειγμα στην εργασία των Cramer et al [Cra97], 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) [Bau01] είτε *λογαριθμική* (logarithmic) [Dam01]. Τα σχήματα αυτά βασίζονται στο κρυπτοσύστημα του Pallier [Pal99].

2.3.5 Βασικά Κρυπτογραφικά Εργαλεία

Στη συνέχεια παρουσιάζουμε τα βασικά εργαλεία που χρησιμοποιούνται από τα περισσότερα κρυπτογραφικά πρωτόκολλα ηλεκτρονικής ψηφοφορίας. Τα εργαλεία αυτά θα χρησιμοποιηθούν και στα πρωτόκολλα που περιγράφουμε στις Ενότητες 2.4, 2.5.

Πίνακες Ανακοινώσεων (Bulletin Boards). 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 [Sch96]. Μια πρακτική και ασφαλής υλοποίηση των πινάκων ανακοινώσεων αποτελεί το κατανεμημένο σύστημα *Rampart* [Rei95].

Ανώνυμα Κανάλια Επικοινωνίας (Anonymous Channels). Τα κανάλια αυτά εξασφαλίζουν την ανωνυμία των χρηστών του συστήματος. Εκτός από τα

δίκτυα MIX-net, που γνωρίσαμε στην Ενότητα 2.3.1, υπάρχουν και τα συστήματα ανωνυμίας με τη χρήση *διαμεσολαβητή* (proxy systems) [Com02], όπως επίσης και τα *υβριδικά συστήματα* (hybrid systems) ανωνυμίας [Rei97]. Συζήτηση για εργαλεία ανώνυμης επικοινωνίας γίνεται επίσης στο Κεφάλαιο 3, Ενότητα 3.5.2.

Κρυπτογραφία τύπου Threshold (threshold cryptography). Τα συστήματα κρυπτογράφησης τύπου threshold [Desm94] κατανέμουν τη λειτουργικότητα των κρυπτογραφικών πρωτοκόλλων ώστε να επιτύχουν α*νθεκτικότητα* (robustness). Για παράδειγμα, σε μια ψηφοφορία η διαδικασία της καταμέτρησης μπορεί να κατανεμηθεί μεταξύ n Αρχών Ψηφοφορίας, με τη χρήση ενός (t,n) threshold κρυπτογραφικού συστήματος δημοσίου κλειδιού (π.χ. threshold ElGamal [Ped91]). Σε αυτήν την περίπτωση υπάρχει μόνον ένα δημόσιο κλειδί, ενώ το ιδιωτικό κλειδί διαμοιράζεται στις n Αρχές με τη χρήση τεχνικών *διαμοιρασμού μυστικού*[9] [Sha79]. 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 [Desm94]. Η μυστικότητα της ψήφου και η ακρίβεια των αποτελεσμάτων εξασφαλίζεται εφόσον δεν υπάρχουν περισσότερες από $t-1$ κακόβουλες ή απλά δυσλειτουργικές Αρχές. Ο αριθμός t 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*[9] (proactive security) [Herz97] καθώς και με τεχνικές *ισχυρής χρονικής ασφάλειας* (strong forward security – Ενότητα 5.4.1) [Bur_Mag01].

[9] Στα κατανεμημένα συστήματα με προ-ενεργή ασφάλεια, οι Αρχές ανανεώνουν περιοδικά τα μερίδια τους κατά τρόπο ώστε η γνώση της τιμής ενός μεριδίου να μη μπορεί να οδηγήσει στην γνώση της τιμής που θα έχει το μερίδιο μετά την ανανέωση. Η τεχνική αυτή αυξάνει την ασφάλεια των συστημάτων τύπου threshold έναντι επιθέσεων όπου ο επιτιθέμενος κατορθώνει να ανακτήσει έναν αριθμό μυστικών μεριδίων που είναι μικρότερος από την τιμή threshold του κρυπτογραφικού συστήματος [Herz97].

Αποδείξεις με Μηδενική Γνώση (Zero Knowledge Proofs). 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 [Gol85]. 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 (π.χ. [Hirt00]), για να αποδειχτεί η εγκυρότητα των κρυπτογραφημένων ψήφων στις ομομορφικές εκλογές (π.χ. [Cra97]), για την ορθότητα των κρυπτογραφήσεων στα πρωτόκολλα προστασίας από καταναγκασμό [Mag01], καθώς και για την ορθότητα των επικυρωμένων ψήφων [Sch96] στα συστήματα που βασίζονται στο μοντέλο των «τυφλών» υπογραφών [Cha81]. 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 [Fia86]. Στην περίπτωση αυτή η ασφάλεια βασίζεται στο μοντέλο *random oracle*[10] [Bel93]

[10] Το μοντέλο *random oracle* είναι ένα τυπικό μοντέλο απόδειξης ασφάλειας στο οποίο οι συναρτήσεις κατακερματισμού (hash functions) αντιμετωπίζονται ως συναρτήσεις τυχαιότητας [Bel93].

2.4 Προστασία Από Καταναγκασμό

Στις παραδοσιακές εκλογές, ο ρόλος του *εκλογικού παραβάν* (voting booth) δεν περιορίζεται απλώς στο να επιτρέπει στους ψηφοφόρους να επιλέξουν με απόλυτη μυστικότητα τη ψήφο τους: ουσιαστικά η ύπαρξη του παραβάν αποτρέπει γεγονότα όπως η *πώληση της ψήφου* (vote selling) και ο *καταναγκασμός* (coercion) των ψηφοφόρων. Η αποτροπή τέτοιων επιθέσεων αποτελεί σημαντικό κομμάτι της έρευνας για ασφαλή συστήματα ηλεκτρονικής ψηφοφορίας μέσω Διαδικτύου.

2.4.1 Ελευθερία από Απόδειξη και Προστασία από Καταναγκασμό

Η έννοιες «*ελευθερία από απόδειξη*» (receipt-freeness) και «*προστασία από καταναγκασμό*» (uncoercibility) στις ηλεκτρονικές εκλογές καθιερώθηκαν από τον Benaloh [Ben94]. Αυτές οι έννοιες σχετίζονται μεταξύ τους, όμως υπάρχουν λεπτές διαφορές που πρέπει να αποσαφηνιστούν [Bur_Mag02a].

Στην προσέγγιση της «Ελευθερίας από Απόδειξη» ο ψηφοφόρος είναι ο εν δυνάμει εχθρός: ο ψηφοφόρος δεν πρέπει να είναι ικανός καθ' οποιονδήποτε τρόπο να πείσει έναν τρίτο για το αληθινό περιεχόμενο της ψήφου του, ακόμα και αν ο ψηφοφόρος *επιθυμεί* κάτι τέτοιο (π.χ. για αμοιβή).

Στην «Προστασία από Καταναγκασμό» ο εχθρός είναι ένας εξωτερικός Καταναγκαστής: ο Καταναγκαστής δε θα πρέπει να είναι ικανός καθ' οποιονδήποτε τρόπο να μάθει από τον ψηφοφόρο (και να είναι σίγουρος για τη γνώση του) το αληθινό περιεχόμενο της ψήφου του, ακόμα και αν ασκήσει καταναγκασμό στον ψηφοφόρο (π.χ. απειλή, εκβιασμό).

Κατ' ουσίαν η Ελευθερία από Απόδειξη είναι περισσότερο ισχυρή ιδιότητα ασφάλειας από την Προστασία από Καταναγκασμό, δεδομένου ότι υπάρχουν ηλεκτρονικά συστήματα που προσφέρουν Προστασία από Καταναγκασμό, αλλά όχι Ελευθερία από Απόδειξη (π.χ. [Ben94,Can97,Can96]). Αυτό συμβαίνει επειδή στα συστήματα αυτά, παρότι ο

ψηφοφόρος μπορεί να επιτύχει να εξαπατήσει τον Καταναγκαστή, ο ψηφοφόρος μπορεί επίσης εάν το επιθυμεί να πουλήσει τη ψήφο του, έχοντας *εκ των προτέρων* δεσμευτεί στους τυχαίους μετασχηματισμούς που κάνει κατά την κρυπτογράφηση της ψήφου του [Hirt00].

Εντούτοις συχνά στη διεθνή βιβλιογραφία οι έννοιες «Προστασία από Καταναγκασμό» και «Ελευθερία από Απόδειξη» χρησιμοποιούνται αμφότερες για να δηλώσουν την προστασία και από τις δυο μορφές επίθεσης (π.χ. πώληση ψήφου ή/και εξωτερικός καταναγκασμός). Για λόγους απλότητας, σε αυτήν τη Διατριβή θεωρούμε ότι η έννοια της «Προστασίας από Καταναγκασμό» περιλαμβάνει τις ιδιότητες ασφάλειας της «Ελευθερίας από Απόδειξη». Πιστεύουμε ότι κάτι τέτοιο είναι και *σημειολογικά ορθό*, αφού η πώληση της ψήφου (ψηφοφόρος = εχθρός) μπορεί να εκληφθεί και ως *αυτό-καταναγκασμός* (self-coercing) [Bur_Mag02a].

2.4.2 Υποθέσεις για Επίτευξη Προστασίας από Καταναγκασμό

Αρκετά σχήματα ηλεκτρονικής ψηφοφορίας «θυσιάζουν» την Προστασία από Καταναγκασμό στο βωμό της ορθότητας των εκλογικών αποτελεσμάτων. Για παράδειγμα, σε μερικά πρωτόκολλα οι ψηφοφόροι λαμβάνουν από το σύστημα (ή, μπορούν να κατασκευάσουν) μια απόδειξη για την ψήφο που υπέβαλαν, ώστε αργότερα, σε περίπτωση που η ψήφος τους δεν έχει ληφθεί υπ' όψιν, να χρησιμοποιήσουν την απόδειξη αυτή για να καταγγείλουν τη διαδικασία. Ή, η απόδειξη αυτή μπορεί να χρησιμοποιηθεί από το ίδιο το σύστημα για τις ανάγκες μιας δεύτερης καταμέτρησης. Τα τελευταία βέβαια χρόνια έχουν προταθεί αρκετά κρυπτογραφικά σχήματα [Ben94,Sak95,Hirt00, Alp98,Oka97,Oka96,Nie94] τα οποία επιτυγχάνουν τόσο Προστασία από Καταναγκασμό όσο και ορθότητα των εκλογικών αποτελεσμάτων, σε αρκετές περιπτώσεις μάλιστα με *οικουμενική επαληθευσιμότητα* των αποτελεσμάτων, ανάλογα με το ποιο από τα τέσσερα μοντέλα ηλεκτρονικής ψηφοφορίας (Ενότητα 2.3) χρησιμοποιείται. Ωστόσο, σε όλα τα σχήματα γίνονται

ορισμένες βασικές υποθέσεις για τη φύση του καναλιού επικοινωνίας μεταξύ του ψηφοφόρου και της Αρχής του συστήματος. Συγκεκριμένα, θεωρείται η ύπαρξη:

- **Ενός «φυσικά» προστατευμένου καναλιού** (physically untappable channel) *από τον Ψηφοφόρο προς την Αρχή* [Oka97,Oka96]. Πρόκειται για ένα φυσικό κανάλι *μονής* κατεύθυνσης, που χρησιμοποιεί ο ψηφοφόρος για να στείλει μηνύματα στην Αρχή, τα οποία δεν είναι δυνατόν να υποκλαπούν.

- **Ενός «φυσικά» προστατευμένου καναλιού** *από την Αρχή προς τον Ψηφοφόρο* [Hirt00,Sak95,Alp98]. Πρόκειται για ένα φυσικό κανάλι *μονής* κατεύθυνσης, που χρησιμοποιεί η Αρχή για να στείλει μηνύματα στον ψηφοφόρο, τα οποία δεν είναι δυνατόν να υποκλαπούν.

- **Ενός «φυσικού» παραβάν** (physical voting booth) [Ben94,Nie94]. Πρόκειται για ένα φυσικό κανάλι *διπλής* κατεύθυνσης, το οποίο ουσιαστικά προσομοιώνει το παραβάν στις παραδοσιακές εκλογές. Η Αρχή και ο ψηφοφόρος μπορούν να χρησιμοποιήσουν από κοινού το κανάλι αυτό για να ανταλλάξουν μηνύματα, τα οποία δεν είναι δυνατόν να υποκλαπούν.

- **Ενός «εικονικού» παραβάν** (virtual booth). Η υπόθεση ύπαρξης ενός «εικονικά» προστατευμένου περιβάλλοντος γίνεται από *όλα* τα πρωτόκολλα Προστασίας από Καταναγκασμό. Ουσιαστικά σημαίνει ότι τη στιγμή που ο ψηφοφόρος χρησιμοποιεί π.χ. τον ηλεκτρονικό υπολογιστή του για να υποβάλλει την ψήφο του στην Αρχή, η οθόνη του υπολογιστή δεν παρακολουθείται από κανέναν εξωτερικό παρατηρητή (π.χ. όταν ο Καταναγκαστής στέκεται δίπλα στον ψηφοφόρο, ή όταν γίνεται χρήση ειδικών αισθητήρων για την καταγραφή και επεξεργασία της ηλεκτρομαγνητικής ακτινοβολίας που εκπέμπεται από την οθόνη -

τεχνικές TEMPEST [Tem02,Sta02]). Μια τέτοια επίθεση άμεσης παρακολούθησης δε μπορεί να αποτραπεί από κανένα κρυπτογραφικό πρωτόκολλο, παρά μόνον με μεθόδους φυσικής προστασίας (π.χ. το «*κλουβί*» του Faraday [Tem02]). Ο στόχος της έρευνας μας δεν είναι η αποτροπή τέτοιων επιθέσεων, αλλά η αντιμετώπιση σεναρίων *μαζικού καταναγκασμού* ή *μαζικού αυτό-καταναγκασμού*, όπου ένας μεγάλος αριθμός ψηφοφόρων έχουν τη δυνατότητα να κατασκευάσουν και να αποστείλουν μαζικά σε μια τρίτη οντότητα αποδείξεις με το περιεχόμενο της ψήφου τους, αλλοιώνοντας έτσι το εκλογικό αποτέλεσμα [Mag01,Mag02,Bur_Mag02a, Bur_Mag02b].

Στη διεθνή βιβλιογραφία έχει καταδειχθεί η δυσκολία υλοποίησης συστημάτων που κάνουν υποθέσεις για τη «φυσική» προστασία του καναλιού επικοινωνίας μεταξύ του ψηφοφόρου και της Αρχής [Mag01,Bur_Mag02a]. Τα συστήματα αυτά θα μπορούσαν να χρησιμοποιηθούν μόνο για ηλεκτρονική ψηφοφορία σε *Εκλογικά Σημεία*, όπου μισθωμένες γραμμές θα προσομοίωναν τα «φυσικά» προστατευμένα κανάλια επικοινωνίας. Βέβαια, κάτι τέτοιο δε συνάδει με τον απώτερο σκοπό της έρευνας για ασφαλή συστήματα ηλεκτρονικής ψηφοφορίας, που είναι η διεκπεραίωση ηλεκτρονικών εκλογών μεγάλης κλίμακας *μέσω Διαδικτύου*, όπου οι ψηφοφόροι μπορεί να είναι γεωγραφικά διάσπαρτοι ανά την επικράτεια ή τον κόσμο. Το γεγονός αυτό κατατάσσει τις υποθέσεις αυτές στην κατηγορία των *μη πρακτικών* υποθέσεων.

Η Συμβολή μας. Οι Sako και Hirt [Hirt00] παρατήρησαν πρόσφατα πως

«Τα φυσικά προστατευμένα κανάλια από την Αρχή προς το Ψηφοφόρο αποτελούν ελάχιστη προϋπόθεση για την επίτευξη προστασίας από καταναγκασμό.»

Ωστόσο στη συνέχεια θα περιγράψουμε ένα μοντέλο ηλεκτρονικής ψηφοφορίας, προστατευμένης από καταναγκασμό, στο οποίο υποθέτουμε ότι

Ο Καταναγκαστής μπορεί παράλληλα να είναι και ωτακουστής (eavesdropper) στο αμφίδρομο κανάλι επικοινωνίας μεταξύ του ψηφοφόρου και της Αρχής [Mag01].

Στη συνέχεια θα παρουσιάσουμε τις ελάχιστες απαιτήσεις ασφάλειας για προστασία από καταναγκασμό, και θα δείξουμε πως η προστασία από καταναγκασμό μπορεί να επιτευχθεί εφόσον ο χρήστης συνεργάζεται, κατά τη διάρκεια κατασκευής της κρυπτογραφημένης ψήφου του, με μια *Κάρτα Ανθεκτική σε Παραβιάσεις* (tamper-resistant token), π.χ. μια *«Έξυπνη» Κάρτα*[11] (smartcard), κατά τρόπο οικουμενικά επαληθεύσιμο. Η υλοποίηση του μοντέλου ασφάλειας θα βασιστεί στο ομομορφικό μοντέλο (Ενότητα 2.3.4) και είναι κατάλληλη για τη διενέργεια ηλεκτρονικών εκλογών μεγάλης κλίμακας μέσω Διαδικτύου.

2.4.3 Ελάχιστες Απαιτήσεις Ασφάλειας

Οι συμμετέχοντες στο μοντέλο μας είναι οι Ψηφοφόροι, οι Αρχές, και ο Καταναγκαστής. Υπάρχει επίσης μία λίστα (πιθανών) Ψήφων V και ένα σύνολο κανόνων R. Ένας Πίνακας Ανακοινώσεων χρησιμοποιείται για την αμφίδρομη επικοινωνία μεταξύ των ψηφοφόρων και των Αρχών [Rei95]. Η ψηφοφορία διενεργείται σε τρία στάδια:

- **Κρυπτογράφηση:** Ο ψηφοφόρος επιλέγει μια ψήφο από τη λίστα V και στη συνέχεια την κρυπτογραφεί.

- **Δημοσίευση:** Οι κρυπτογραφημένες ψήφοι δημοσιεύονται στον Πίνακα Ανακοινώσεων.

[11] Οι «έξυπνες» κάρτες διαθέτουν ένα ολοκληρωμένο κύκλωμα (chip) που αποτελείται από έναν μικρο-επεξεργαστή με εσωτερική μνήμη. Κατ' αυτόν τον τρόπο η κάρτα έχει δυνατότητα αποθήκευσης δεδομένων καθώς και δυνατότητα εκτέλεσης υπολογιστικών πράξεων (π.χ. κρυπτογράφηση, ψηφιακές υπογραφές) και αλληλεπίδρασης με έναν αναγνώστη έξυπνων καρτών. Οι σύγχρονες κάρτες διαθέτουν εσωτερικούς μηχανισμούς ασφάλειας οι οποίοι, σε περίπτωση απόπειρας υποκλοπής των δεδομένων της κάρτας, διαγράφουν αυτόματα τα περιεχόμενα της μνήμης της κάρτας.

- **Καταμέτρηση:** Οι Αρχές αποκρυπτογραφούν τις ψήφους και δημοσιεύουν τα αποτελέσματα στον Πίνακα Ανακοινώσεων για επαλήθευση. Ο νικητής καθορίζεται με βάση το σύνολο R των κανόνων της ψηφοφορίας.

Ο Καταναγκαστής είναι ο εχθρός του συστήματος και επιθυμεί να μάθει την τιμή μιας δεδομένης ψήφου. Οι δυνατότητες που έχει, είναι:

- Να καταναγκάσει τον ψηφοφόρο, *πριν* ή/και *μετά* την κρυπτογράφηση, αλλά όχι *κατά τη διάρκεια* της κρυπτογράφησης (βάσει της υπόθεσης για την ύπαρξη ενός «εικονικού» παραβάν τη στιγμή της υποβολής της ψήφου).

- Να γίνει ωτακουστής στο κανάλι επικοινωνίας που συνδέει τον ψηφοφόρο με τις Αρχές.

- Να συνεργαστεί με ορισμένες από τις Αρχές, αλλά όχι με περισσότερες από έναν προκαθορισμένο αριθμό (threshold).

Ο ψηφοφόρος αναμένεται να αποκαλύψει στον Καταναγκαστή οποιαδήποτε πληροφορία του ζητηθεί. Ο ψηφοφόρος μπορεί επίσης να δώσει ψευδείς πληροφορίες στον Καταναγκαστή, και να μην υποστεί συνέπειες, αρκεί ο Καταναγκαστής να μην μπορεί να αποδείξει ότι αυτές είναι ψευδείς. Δεν αποκλείουμε επίσης το ενδεχόμενο ο Καταναγκαστής να είναι ο ίδιος ο ψηφοφόρος (αυτό-καταναγκασμός). Σε αυτήν την περίπτωση, ο ψηφοφόρος δεν επιθυμεί μόνο να μάθει την τιμή της ψήφου του, αλλά επιπλέον να είναι ικανός να αποδείξει την τιμή αυτή σε έναν τρίτο, κατά τρόπο αδιαμφισβήτητο.

Για Προστασία από Καταναγκασμό, το κανάλι που ενώνει τον ψηφοφόρο με τις Αρχές πρέπει να είναι:

- *Μυστικό*: ούτως ώστε ο Καταναγκαστής (ο οποίος μπορεί να είναι ωτακουστής) να μη μπορεί να έχει πρόσβαση στην τιμή της ψήφου.

- *Ελεύθερο από Απόδειξη*: ούτως ώστε να μην είναι δυνατόν για το ψηφοφόρο, τον Καταναγκαστή, τις Αρχές ή κάποια άλλη οντότητα, να αποκτήσουν και να χρησιμοποιήσουν αποδείξεις για υποβληθείσες ψήφους.

- *Αυθεντικοποιημένο*: ούτως ώστε ο Καταναγκαστής να μη μπορεί να υποβάλλει ψήφους εξ' ονόματος των ψηφοφόρων.

Μυστικά Κανάλια με Στοχαστική Κρυπτογράφηση. Όλες οι ψήφοι πρέπει να κρυπτογραφηθούν για μυστικότητα. Δεν ενδείκνυται *συμμετρική κρυπτογράφηση*[12] [Sch96], επειδή ο Καταναγκαστής μπορεί να αποσπάσει από τον ψηφοφόρο το μυστικό κλειδί και έτσι να αποκτήσει πρόσβαση στην ψήφο. Επομένως, πρέπει να χρησιμοποιηθεί *κρυπτογράφηση δημοσίου κλειδιού* [Sch96], με τους ψήφους να κρυπτογραφούνται με το δημόσιο κλειδί των Αρχών. Η κρυπτογράφηση αυτή πρέπει να είναι επίσης *στοχαστική* (probabilistic) [Gol94], δηλαδή πρέπει κατά την κρυπτογράφηση να γίνει χρήση κάποιου τυχαίου αριθμού - *τυχαιότητα*[13] (randomness), αλλιώς το

[12] Σε έναν αλγόριθμο συμμετρικής κρυπτογράφησης (π.χ. DES, IDEA, AES) [Men97], το ίδιο κλειδί που χρησιμοποιείται για την κρυπτογράφηση ενός μηνύματος απαιτείται και για την αποκρυπτογράφηση του μηνύματος.

[13] Η Κατασκευή ενός γεννήτορα αληθινά τυχαίων αριθμών (random-number generator), δηλαδή μη προβλέψιμων, απασχόλησε και απασχολεί την ακαδημαϊκή κοινότητα. Η λειτουργία ενός τέτοιου γεννήτορα θα μπορούσε να βασίζεται σε ένα μη προβλέψιμο φυσικό φαινόμενο, όπως για παράδειγμα η *ραδιενεργή αποσύνθεση* (radioactive decay) στοιχείων [And01]. Σε συστήματα μεγάλης κλίμακας που χρησιμοποιούν προσωπικούς υπολογιστές, μια τέτοια πηγή τυχαιότητας θα μπορούσαν να αποτελέσουν οι μικρές μεταβολές στη ταχύτητα περιστροφής ενός σκληρού δίσκου, που οφείλονται στην επίδραση του αέρα (air turbulence) [Dav94].

κρυπτογραφημένο μήνυμα αποτελεί από μόνο του απόδειξη της ψήφου (εφόσον το σύνολο των πιθανών ψήφων είναι περιορισμένο) [Gol94].

- *Κρυπτογραφία τύπου Threshold*. Οι Αρχές μοιράζονται ένα ιδιωτικό κλειδί αποκρυπτογράφησης [Sha79], και αποκρυπτογραφούν από κοινού τις κρυπτογραφημένες ψήφους, με τη χρήση ενός threshold κρυπτογραφικού συστήματος [Desm94] (Ενότητα 2.3.5). Κατ' αυτόν τον τρόπο, η Προστασία από Καταναγκασμό δεν απειλείται στην περίπτωση όπου ο Καταναγκαστής επιτύχει να διαφθείρει ορισμένες από τις Αρχές του συστήματος (όχι όμως περισσότερες του αριθμού $t-1$, όπου t είναι η τιμή threshold του κρυπτογραφικού συστήματος).

Κανάλια Ελεύθερα Αποδείξεων με Κατανεμημένη Τυχαιότητα. Εάν ο ψηφοφόρος επιλέξει την τυχαιότητα της κρυπτογραφημένης ψήφου [Oka97], τότε η τυχαιότητα αυτή αποτελεί απόδειξη για τη ψήφο του. Επιπρόσθετα, και εφόσον στο μοντέλο μας επιτρέπουμε την *εκ των προτέρων* συνεργασία του ψηφοφόρου με τον Καταναγκαστή, ο Καταναγκαστής μπορεί να επιλέξει ο ίδιος την τυχαιότητα για λογαριασμό του ψηφοφόρου, και να απαιτήσει από αυτόν να τη χρησιμοποιήσει (ζητώντας αργότερα απόδειξη για το γεγονός αυτό).

Εάν η τυχαιότητα επιλέγεται μόνον από μια Κάρτα Ανθεκτική σε Παραβιάσεις, και όχι από τον ψηφοφόρο [Rie98_1], τότε προσδίνεται μεγάλη εμπιστοσύνη στην Κάρτα: από λάθη λογισμικού της κάρτας ή ακόμα και εσκεμμένα, η ψήφος μπορεί να αλλοιωθεί ή και να αποσταλεί, μέσω απομακρυσμένης σύνδεσης, σε κάποιον τρίτο. Επίσης η μυστικότητα της ψήφου μπορεί να αρθεί εάν ο Καταναγκαστής αποκτήσει έλεγχο στο εσωτερικό της κάρτας [And96,Bon97,Cry00].

Η *κατανομή* (distribution) της διαδικασίας κατασκευής της κρυπτογραφημένης ψήφου μεταξύ του ψηφοφόρου και της Κάρτας, φαίνεται πως είναι η μοναδική ασφαλής λύση. Εντούτοις, κι εφόσον ένα κομμάτι της τυχαιότητας στην τελική κρυπτογραφημένη ψήφο θα είναι άγνωστο στον

ψηφοφόρο, ο ψηφοφόρος πρέπει να πειστεί ότι η Κάρτα δεν έχει αλλοιώσει την ψήφο του (από σφάλμα του προγράμματος ή εσκεμμένα). Συνεπώς, η Κάρτα πρέπει να αποδείξει στον ψηφοφόρο ότι η κρυπτογράφηση ήταν σωστή, χωρίς όμως να εμφανίσει την τυχαιότητα που χρησιμοποίησε. Για αυτόν το λόγο θα χρησιμοποιήσουμε *Αλληλεπιδραστικές Αποδείξεις με Μηδενική Γνώση* (Interactive Zero-Knowledge Proofs) [Gol85]. Αυτές οι αποδείξεις είναι *μη μεταφέρσιμες* και επομένως δε μπορούν να χρησιμοποιηθούν ως απόδειξη σε έναν τρίτο.

- *Φυσική Προστασία του Καναλιού Ψηφοφόρος-Κάρτα*. Το κανάλι επικοινωνίας πρέπει να προστατεύεται με φυσικό τρόπο. Εάν ο Καταναγκαστής είναι ωτακουστής στο κανάλι, τότε μπορεί να λάβει γνώση της μερικώς κρυπτογραφημένης ψήφου που αποστέλλεται μέσω του καναλιού από τον ψηφοφόρο στην Κάρτα, πριν εκείνη συνεισφέρει τη δική της τυχαιότητα. Αν συμβεί κάτι τέτοιο, τότε ο Καταναγκαστής θα αρκείται στον εκβιασμό του ψηφοφόρου προκειμένου να μάθει το περιεχόμενο της ψήφου. Για να απαλλαχθούμε από την (μη πρακτική) υπόθεση ύπαρξης ενός φυσικά προστατευμένου καναλιού, υποθέτουμε ότι η επικοινωνία του ψηφοφόρου με την Κάρτα λαμβάνει χώρα μέσα στο «εικονικό» παραβάν (Ενότητα 2.4.2).

Σημείωση: Σε μια εργασία που δημοσιεύθηκε παράλληλα με τη [Mag01], οι Baudron et al [Bau01] πρότειναν την κατανομή της διαδικασίας κατασκευής της κρυπτογραφημένης ψήφου μεταξύ του ψηφοφόρου και της Αρχής του συστήματος, με τη χρήση τεχνικών ασφαλούς πολυμερούς υπολογισμού[33] *(secure multiparty computation) [Cha87]. Το μειονέκτημα αυτής της προσέγγισης είναι ότι απαιτεί την ύπαρξη ενός φυσικά προστατευμένου καναλιού μεταξύ της Αρχής και του ψηφοφόρου.*

Αυθεντικοποιημένα Κανάλια με Ψηφιακές Υπογραφές. Οι κρυπτογραφημένες ψήφοι πρέπει να υπογράφονται ψηφιακά από τους ψηφοφόρους, ώστε να είναι δύσκολη η υποβολή ψήφων εξ' ονόματος των. Για να ισχύσει κάτι

τέτοιο θα πρέπει να υπάρχει μια Υποδομή Δημοσίου Κλειδιού (PKI) με καλά σχεδιασμένες ιεραρχίες πιστοποίησης (π.χ. κατά τα πρότυπα X.509 [Iet99] ή DNSSEC [Gud01]).

2.4.4 Ένα Βασικό Σχήμα με Προστασία από Καταναγκασμό

Στη συνέχεια περιγράφουμε ένα *βασικό* σχήμα (χωρίς λεπτομέρειες υλοποίησης) που ικανοποιεί τις ελάχιστες απαιτήσεις που περιγράψαμε στην Ενότητα 2.4.3, για Προστασία από Καταναγκασμό. Τα στάδια της ψηφοφορίας, είναι τα εξής:

- **Κρυπτογράφηση**: Ο ψηφοφόρος εισέρχεται μέσα σε ένα «εικονικό» παραβάν και αλληλεπιδρά με την Κάρτα. Αρχικά αποδεικνύει την ταυτότητα του στην Κάρτα και στη συνέχεια δίνει στην είσοδο της Κάρτας την ψήφο του, κρυπτογραφημένη με το δημόσιο κλειδί των Αρχών, χρησιμοποιώντας ορισμένη τυχαιότητα στα πλαίσια ενός στοχαστικού αλγορίθμου κρυπτογράφησης. Η Κάρτα προσθέτει τυχαιότητα στην κρυπτογραφημένη ψήφο, επιστρέφει στην έξοδο της το τελικό κρυπτογράφημα και αποδεικνύει στον ψηφοφόρο, χρησιμοποιώντας ένα πρωτόκολλο *απόδειξης με μηδενική γνώση*, την ορθότητα της κρυπτογράφησης, δηλαδή ότι προσέθεσε τυχαιότητα χωρίς να αλλοιώσει την ψήφο. Στο βασικό αυτό σχήμα, μπορούμε να επικαλεστούμε ένα πρωτόκολλο απόδειξης με μηδενική γνώση για NP γλώσσες [Gol91]. Αργότερα, στην υλοποίηση που θα περιγράψουμε (Ενότητα 2.4.5), το πρωτόκολλο της απόδειξης θα εξαρτηθεί από το σύστημα κρυπτογράφησης που θα χρησιμοποιηθεί.

- **Δημοσίευση**: Εφόσον ο ψηφοφόρος δεχθεί την απόδειξη ορθότητας ως αληθή, υπογράφει ψηφιακά την κρυπτογραφημένη ψήφο του και τη δημοσιεύει στον Πίνακα Ανακοινώσεων, μαζί με το ψηφιακό

πιστοποιητικό (digital certificate) του δημοσίου κλειδιού του, υπογεγραμμένο από μια Αρχή Πιστοποίησης (Certification Authority).

- **Καταμέτρηση**: Κατά την καταμέτρηση οι Αρχές χρησιμοποιούν ένα πρωτόκολλο τύπου threshold [Desm94] και αποκρυπτογραφούν τις ψήφους, δημοσιεύοντας στη συνέχεια το τελικό αποτέλεσμα στον Πίνακα Ανακοινώσεων.

Προστασία από Καταναγκασμό. Αυτή επιτυγχάνεται εφόσον υποθέσουμε ότι ο Καταναγκαστής δεν μπορεί να ελέγξει από κοινού τον ψηφοφόρο και την Κάρτα. Όντως, για να αποκαλυφθεί η ψήφος είναι απαραίτητες τόσο η τυχαιότητα του ψηφοφόρου, όσο και η τυχαιότητα της Κάρτας. Επίσης, χάρη στην ιδιότητα των σχημάτων τύπου threshold, ο Καταναγκαστής θα πρέπει να διαφθείρει τουλάχιστον t από n Αρχές για να καταφέρει να λάβει γνώση της αποκρυπτογραφημένης ψήφου. Στο βασικό αυτό σχήμα δεν γίνεται καμία υπόθεση φυσικής προστασίας του καναλιού επικοινωνίας μεταξύ του ψηφοφόρου και των Αρχών του συστήματος. Στην επόμενη Ενότητα θα παρουσιάσουμε μια υλοποίηση του βασικού αυτού σχήματος.

2.4.5 Μία Υλοποίηση με Κρυπτογράφηση ElGamal

Βασιζόμαστε στο ομομορφικό μοντέλο ηλεκτρονικής ψηφοφορίας [Cra97]. Το κρυπτοσύστημα που χρησιμοποιούμε είναι μια παραλλαγή του κρυπτογραφικού συστήματος ElGamal [ElG85], ώστε να υποστηρίζεται ο ομομορφισμός στην πράξη της πρόσθεσης. Έστω p,q μεγάλοι πρώτοι αριθμοί, τέτοιοι ώστε $q/p-1$, έστω G_q η υποομάδα του Z_p^* τάξης q, και g,G, γεννήτορες του G_q. Δεδομένου ενός μηνύματος $m \in Z_q$, η κρυπτογράφηση του m ισούται με την κρυπτογράφηση του G^m με βάση g: δηλαδή, $(x,y) = (g^a, h^a G^m)$, όπου $h = g^s$ είναι το δημόσιο κλειδί, s το

ιδιωτικό κλειδί, και a ένα τυχαίο στοιχείο του συνόλου Z_q. Όλες οι πράξεις γίνονται modulo p. Χάριν απλότητας στη συνέχεια παραλείπουμε το $\bmod p$.

α) Υλοποίηση χωρίς Προστασία από Καταναγκασμό [Cra97]. Κατά τη διάρκεια της κρυπτογράφησης ο ψηφοφόρος κρυπτογραφεί τη ψήφο του $v \in \{-1,1\}$ ως το ζεύγος $(x,y)=(g^a, h^a G^v)$ Ο ψηφοφόρος κατασκευάζει επίσης μια απόδειξη εγκυρότητας με Μηδενική Γνώση, ότι η ψήφος που περιέχεται στο κρυπτογράφημα (x,y) ανήκει στο αποδεκτό σύνολο $\{-1,1\}$ και στη συνέχεια δημοσιεύει την κρυπτογραφημένη ψήφο του και την απόδειξη εγκυρότητας σε έναν Πίνακα Ανακοινώσεων. Μετά το τέλος της περιόδου υποβολής ψήφων, οι Αρχές αξιοποιούν την ομομορφική ιδιότητα της κρυπτογραφικής συνάρτησης και «πολλαπλασιάζουν» όλες τις κρυπτογραφημένες ψήφους, προκειμένου να αποκτήσουν την κρυπτογράφηση του «αθροίσματος» των ψήφων:

$$(X,Y)=(\prod_{i=1}^{\ell} g^{a_i}, \prod_{i=1}^{\ell} h^{a_i} G^{v_i}) = (g^{\sum a_i}, h^{\sum a_i} G^{T}), \quad T=\sum_{i=1}^{\ell} v_i,$$

όπου T είναι η διαφορά μεταξύ του αριθμού των «ναι» (1) και των «όχι» (-1) ψήφων και ℓ ο αριθμός των ψηφοφόρων του συστήματος. Οι Αρχές στη συνέχεια αποκρυπτογραφούν από κοινού την κάλπη των ψήφων χρησιμοποιώντας το (t,n) threshold πρωτόκολλο αποκρυπτογράφησης του Pedersen [Ped91] (χωρίς να είναι απαραίτητο να κατασκευαστεί ξανά το ιδιωτικό κλειδί κατά την κρυπτογράφηση – δηλαδή το ίδιο δημόσιο κλειδί μπορεί να χρησιμοποιηθεί και σε μελλοντική ψηφοφορία) και υπολογίζουν το $G^T = Y / X^s$. Τελικά το αποτέλεσμα T καθορίζεται με $O(\ell)$ modular πολλαπλασιασμούς.

Στο ανωτέρω σχήμα η μυστικότητα της ψήφου βασίζεται στο *πρόβλημα* εύρεσης *Διακριτού Λογαρίθμου*[14] [Dif76]. Επιπλέον η κρυπτογράφηση των ψήφων είναι ορθή και επιτυχής ακόμα και στην περίπτωση όπου (έως και) $t-1$ Αρχές συνωμοτούν ή απλά αποτυγχάνουν στην εκτέλεση των καθηκόντων τους.

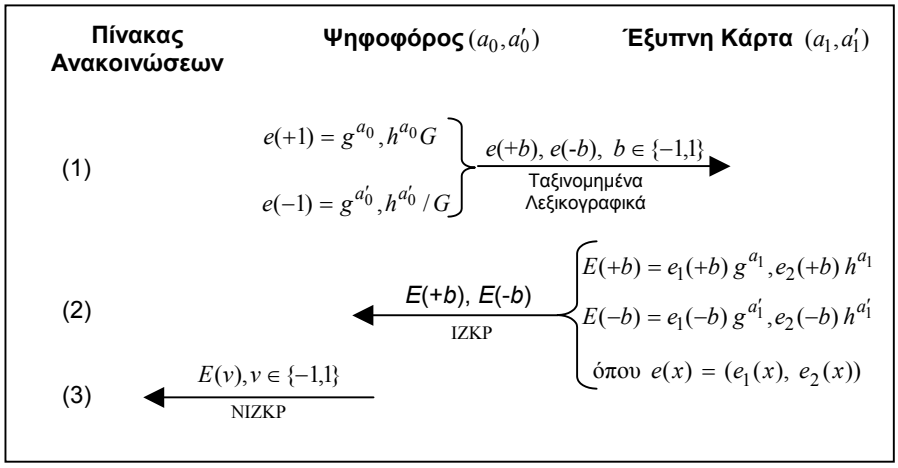
Σημείωση: Πρέπει να τονίσουμε ότι για μεγάλο αριθμό υποψηφίων, ο μόνος τρόπος να υπολογιστεί η αποκρυπτογραφημένη κάλπη είναι με εντατικούς υπολογισμούς : εάν ℓ είναι ο αριθμός των ψηφοφόρων και r είναι ο αριθμός των υποψηφίων, η πολυπλοκότητα των υπολογισμών είναι εκθετική ως προς τον αριθμό r: $(\Omega(\ell^{(r-1)/2}))$ [Bur_Mag02b].

Επιτυγχάνοντας Προστασία Από Καταναγκασμό. Τροποποιούμε [Mag01] την παραπάνω διαδικασία υποβολής ψήφου προκειμένου να εδραιώσουμε Προστασία από Καταναγκασμό, επιτυγχάνοντας παράλληλα ασφάλεια και αποδοτικότητα. Η τροποποίηση συνίσταται στο ότι η διαδικασία της κρυπτογράφησης της ψήφου κατανέμεται μεταξύ του ψηφοφόρου και μιας Έξυπνης Κάρτας. Η Κάρτα, η οποία μπορεί να χρησιμοποιηθεί σε περισσότερες από μια ψηφοφορίες, έχει τη δυνατότητα να προσθέτει τυχαιότητα σε κρυπτογραφημένα δεδομένα (ElGamal) που λαμβάνει στην είσοδο της, καθώς και να υπογράφει, χρησιμοποιώντας κάποιο σύστημα ψηφιακής υπογραφής (π.χ. RSA [Rsa78]), δεδομένα εκ μέρους του ψηφοφόρου. Για να αποκλειστεί η περίπτωση ο Καταναγκαστής να χρησιμοποιεί την Κάρτα για να υποβάλλει ψήφο εξ' ονόματος του ψηφοφόρου, η Κάρτα μπορεί να είναι εφοδιασμένη με τεχνολογίες

[14] Έστω ένας πρώτος αριθμός p, ο γεννήτορας g του Z_p^* και ένα στοιχείο $y \in Z_p^*$. Η εύρεση ενός ακεραίου x, $0 \le x \le p-2$, τέτοιου ώστε $g^x = y \pmod p$, αποτελεί το πρόβλημα του Διακριτού Λογαρίθμου.

αναγνώρισης βιολογικών χαρακτηριστικών[15] (biometrics) του εξουσιοδοτημένου χρήστη [Hac00]. Τα βήματα του πρωτοκόλλου παρουσιάζονται στο Σχήμα 5.

Βήμα (1): Ο χρήστης χρησιμοποιεί τυχαιότητες $a_0, a_0' \in Z_q$ για να κρυπτογραφήσει με το σύστημα ElGamal τις δύο πιθανές ψήφους {ναι,όχι} = {+1,-1}, ως $e(+1)$ και $e(-1)$ αντίστοιχα. Ο ψηφοφόρος αναδιατάσσει τυχαία τα κρυπτογραφήματα $e(+1)$, $e(-1)$ (π.χ. ταξινομώντας τα λεξικογραφικά) και στη συνέχεια τα υποβάλλει στην είσοδο της Κάρτας. Αυτό σημαίνει ότι η Κάρτα δε μπορεί να εξάγει κάποια πληροφορία για το ποιο κρυπτογράφημα αντιστοιχεί σε ποια ψήφο.



Σχήμα 5. Ψηφοφορία με τη βοήθεια της Έξυπνης Κάρτας

Βήμα (2): Η Κάρτα επιλέγει τυχαιότητες $a_1, a_1' \in Z_q$ και μετασχηματίζει την είσοδο του χρήστη, δημιουργώντας έτσι τα τελικά κρυπτογραφήματα για τις δύο πιθανές ψήφους, $E(+b)$ και $E(-b)$, όπου $b \in \{-1,1\}$. Οι κρυπτογραφημένες ψήφοι υπογράφονται ψηφιακά από την Κάρτα, για προστασία της

[15] Τα βιομετρικά συστήματα αξιολογούν την πιστότητα ενός φυσιολογικού (π.χ. δακτυλικό αποτύπωμα, γεωμετρία χεριού, ίριδα, ρετίνα, αναγνώριση προσώπου, φλεβική δομή χεριού, DNA, σχήμα χεριού, οσμή σώματος) ή συμπεριφορολογικού (π.χ. υπογραφή, αναγνώριση ομιλούντος, μοτίβο πληκτρολόγησης) χαρακτηριστικού που διαθέτει ο χρήστης.

ακεραιότητας της ψήφου. Η Κάρτα επιστρέφει στην έξοδο της τα υπογεγραμμένα κρυπτογραφήματα.

Για λόγους ορθότητας ο χρήστης πρέπει να πειστεί, χωρίς να λάβει γνώση της τυχαιότητας της Κάρτας, ότι η Κάρτα έχει πράξει ορθά και δεν αλλοίωσε την τιμή των ψήφων. Η *απόδειξη ορθότητας* πρέπει να είναι μη μεταφέρσιμη, για προστασία από καταναγκασμό: ο χρήστης χρησιμοποιεί τα κρυπτογραφήματα $E(+b), E(-b)$ καθώς και τα (γνωστά σε αυτόν) κρυπτογραφήματα $e(+1), e(-1)$, και υπολογίζει τα (g^{a_1}, h^{a_1}) και $(g^{a'_1}, h^{a'_1})$ Εάν η Κάρτα αποδείξει[16] στο χρήστη ότι $\log_g(g^{a_1}) = \log_h(h^{a_1})$ και $\log_g(g^{a'_1}) = \log_h(h^{a'_1})$ τότε ο χρήστης μπορεί να πειστεί ότι το $E(+b)$ είναι όντως κρυπτογράφημα του $v = b$ και ότι το $E(-b)$ είναι κρυπτογράφημα του $v = -b$. Η Κάρτα μπορεί να το αποδείξει αυτό με τη χρήση του Αλληλεπιδραστικού πρωτοκόλλου Απόδειξης με Μηδενική Γνώση (Interactive Zero Knowledge Proof – IZKP) της ισότητας δύο διακριτών λογαρίθμων, που έχει προταθεί από τους Chaum-Petersen [Cha92]. Από τη φύση τους, όπως έχουμε ήδη αναφέρει, οι αλληλεπιδραστικές αποδείξεις με μηδενική γνώση είναι μη μεταφέρσιμες: αυτό σημαίνει ότι ακόμα και αν ο χρήστης καταγράφει τα μηνύματα που ανταλλάσσονται μεταξύ αυτού και της Κάρτας κατά τη διάρκεια της απόδειξης, τα μηνύματα αυτά δεν έχουν καμία *offline* αξία στον Καταναγκαστή. Επομένως, ακόμα και σε ένα σενάριο αυτοκαταναγκασμού, όπου ο ψηφοφόρος επιθυμεί να πουλήσει τη ψήφο του, επιτυγχάνεται Προστασία από Καταναγκασμό.

Βήμα (3): Ο χρήστης αποφασίζει ποια ψήφο $v \in \{-1,1\}$ επιθυμεί να υποβάλλει. Για να θεωρηθεί έγκυρο[17] το κρυπτογράφημα $E(v)$ πρέπει να κατασκευαστεί μια *απόδειξη εγκυρότητας* της ψήφου, δηλαδή ότι το $E(v)$ περιέχει μια ψήφο

[16] Ο διάκριτος λογάριθμος (discrete logarithm) x ενός αριθμού g^x συμβολίζεται με $\log(g^x)$.

[17] Όπως είδαμε και στην αρχή της Ενότητας, το κρυπτογράφημα δεν θα αποκρυπτογραφηθεί απευθείας, αλλά θα συνδυαστεί, μέσω της ομομορφικής ιδιότητας της κρυπτογραφικής συνάρτησης, με τις άλλες κρυπτογραφημένες ψήφους, για να προκύψει το κρυπτογραφημένο «άθροισμα» των ψήφων. Επομένως, οι ψήφοι πρέπει να είναι έγκυρες (να ανήκουν δηλαδή στο σύνολο {-1,1}), ειδάλλως δεν θα είναι δυνατή η αποκρυπτογράφηση της τελικής κάλπης.

$v \in \{-1,1\}$. Η απόδειξη αυτή, που πρέπει να είναι με Μηδενική Γνώση, δηλαδή να μη φανερώνει τη ψήφο v, είναι απαραίτητη για την οικουμενική επαληθευσιμότητα της ψηφοφορίας. Ένα *αλληλεπιδραστικό* πρωτόκολλο για μια τέτοια απόδειξη κατασκευάζεται με συνεργασία του χρήστη και της Κάρτας, και θα παρουσιαστεί ξεχωριστά στο Παράρτημα Α, στο τέλος του Κεφαλαίου. Για να είναι οικουμενικά επαληθεύσιμη, η απόδειξη αυτή θα πρέπει να μετατραπεί αργότερα σε μια *Απόδειξη με Μηδενική Γνώση Χωρίς Αλληλεπίδραση* (Non Interactive Zero Knowledge Proof - NIZKP). Αυτό επιτυγχάνεται με την *ευριστική* προσέγγιση των Fiat-Shamir [Fia86].

Ο χρήστης δημοσιεύει την κρυπτογραφημένη ψήφο του $E(v)$ καθώς και την απόδειξη εγκυρότητας, στον Πίνακα Ανακοινώσεων – Σχήμα 5. Μετά το τέλος της περιόδου υποβολής ψήφων, όλες οι κρυπτογραφημένες ψήφοι αποκρυπτογραφούνται από τις Αρχές και τα αποτελέσματα ανακοινώνονται στον Πίνακα Ανακοινώσεων.

ΘΕΩΡΗΜΑ. Εάν το Πρόβλημα Απόφασης Diffie-Hellman[18] είναι δύσκολο, τότε το προτεινόμενο πρωτόκολλο (Σχήμα 5) παρέχει Προστασία από Καταναγκασμό.

Απόδειξη. Ας υποθέσουμε ότι ο Καταναγκαστής και ο Ψηφοφόρος μπορούν να αποδείξουν ότι το $E(v)$ είναι το κρυπτογράφημα της ψήφου v. Για παράδειγμα, ότι $E(v)=E(+1)=(g^{a_0+a_1}, h^{a_0+a_1}G)$ Δεδομένου ότι ο ψηφοφόρος γνωρίζει το a_0, τότε αρκεί να αποδείξουν ότι το ζεύγος (g^{a_1}, h^{a_1}) είναι της σωστής μορφής, όπου a_1 είναι η τυχαιότητα της Κάρτας. Εφόσον $h^{a_1} = DH_g(g^{a_1}, h)$ αυτό σημαίνει ότι ο ψηφοφόρος και ο Καταναγκαστής μπορούν από κοινού να λύσουν το Πρόβλημα Απόφασης Diffie-Hellman. Η απόδειξη για $v=-1$ είναι παρόμοια και παραλείπεται.

---

[18] Ο Diffie-Hellman τελεστής DH_g ορίζεται ως $DH_g(g^a, g^b) = g^{ab}$. Το πρόβλημα της αναγνώρισης εάν $z = DH_g(x,y)$ όπου $x,y,z \in G_q$, αποκαλείται ως Πρόβλημα Απόφασης Diffie-Hellman [Dif76].

Γενικεύσεις. Το σχήμα ηλεκτρονικής ψηφοφορίας που παρουσιάσαμε, μπορεί να επεκταθεί ώστε να υποστηρίζει συστήματα ψηφοφορίας με περισσότερους από δύο υποψηφίους [Mag01]. Ωστόσο, η αύξηση του αριθμού των υποψηφίων συνεπάγεται και αύξηση του μεγέθους της απόδειξης εγκυρότητας της ψήφου, όπως επίσης και σημαντική αύξηση της πολυπλοκότητας υπολογισμού της τελικής αποκρυπτογραφημένης κάλπης από τις Αρχές. Ο υπολογισμός αυτός είναι πρακτικά εφικτός μόνον για «λογικές» τιμές των ℓ, K, όπου ℓ είναι ο αριθμός των ψηφοφόρων και K ο αριθμός των πιθανών ψήφων.

2.5 Απόσυρση Ψήφου στο Μοντέλο των «Τυφλών» Υπογραφών

Στην Ενότητα 2.3.2 αναφερθήκαμε στο μοντέλο ηλεκτρονικής ψηφοφορίας με κεντρική διαχείριση, δηλαδή με τη χρήση μόνο μιας Αρχής για την λειτουργία (εγγραφή, ψηφοφορία, καταμέτρηση) του συστήματος [Cha81]. 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. Αυτό επιτυγχάνεται με τη χρήση του μηχανισμού των «τυφλών» υπογραφών [Cha82]. Η μυστικότητα της ψήφου έγκειται στον ψηφοφόρο, ο οποίος, μετά τη δημοσίευση των κρυπτογραφημένων αποτελεσμάτων χρησιμοποιεί ένα ανώνυμο κανάλι επικοινωνίας για να υποβάλλει το κλειδί αποκρυπτογράφησης της ψήφου του στην Αρχή του συστήματος.

2.5.1 Το Πρόβλημα των Απεχόντων Ψηφοφόρων

Ένα μειονέκτημα των συστημάτων ψηφοφορίας που βασίζονται στο μοντέλο των «τυφλών» υπογραφών [Cran97,Dav96, Hers97,Oka97,Pet95,Rie98,He98,

Jua97,Jua96], 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[19] του εκλογικού συστήματος. Στη συνέχεια θα δείξουμε [Mag02] ότι το πρόβλημα των απεχόντων ψηφοφόρων μπορεί να οδηγήσει και σε παραβίαση της Ακρίβειας (τρίτη ιδιότητα[20]) του συστήματος.

Εφεξής, ως *δέσμευση ψήφου* (vote-tag) θα αποκαλούμε την κρυπτογραφημένη ψήφο σε συστήματα που βασίζονται στο μοντέλο των «τυφλών» υπογραφών [Cha82]. 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 [Rie98] πρότεινε όλοι οι ψηφοφόροι να υποβάλλουν, μετά την εγγραφή τους και πριν υποβάλλουν την έγκυρη δέσμευση ψήφου τους, ένα ψηφιακά υπογεγραμμένο *μήνυμα αναγνώρισης M* 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 [Cha81], ώστε να μην υπάρχει συνδεσιμότητα των αποτελεσμάτων. Η λύση αυτή έχει το παρακάτω μειονέκτημα [Mag02]: μετά τη δημοσίευση των αποτελεσμάτων, και εάν υπάρχουν *περισσότερες ψήφοι από υπογραφές*, αυτό μπορεί να σημαίνει:

- Είτε ότι η Αρχή υπέβαλε πλαστές ψήφους,

[19] α) Μόνο εξουσιοδοτημένοι ψηφοφόροι μπορούν να υποβάλλουν ψήφους, και β) Κανένας ψηφοφόρος δε μπορεί να υποβάλει περισσότερες από μια ψήφους (Ενότητα 2.2.1).
[20] Καμιά ψήφος δε μπορεί να διαγραφεί, χωρίς κάτι τέτοιο να γίνει αντιληπτό (Ενότητα 2.2.1).

- Είτε ότι κάποιοι ψηφοφόροι υπέβαλαν (ανώνυμα) την έγκυρη δέσμευση ψήφου χωρίς να έχουν υποβάλλει νωρίτερα (επώνυμα) το μήνυμα αναγνώρισης M .

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 M 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.

Η Πρόταση μας

Στην Ενότητα αυτή προτείνουμε μια ασφαλή ηλεκτρονική ψηφοφορία με κεντρική διαχείριση [Mag02]. Επιλύσαμε το πρόβλημα των απεχόντων ψηφοφόρων, προστατεύοντας παράλληλα το δικαίωμα της μυστικής ψήφου, αλλά και εγκαθιδρύοντας ατομική επαληθευσιμότητα για την τελική κάλπη. Στο σύστημα μας, ενώ ένας εγγεγραμμένος ψηφοφόρος δικαιούται να απέχει από την ψηφοφορία, όλοι οι εγγεγραμμένοι ψηφοφόροι που αποφασίζουν να υποβάλλουν μια (έγκυρη) δέσμευση ψήφου, υποχρεούνται κάποια στιγμή αργότερα να υποβάλλουν μια *δήλωση αναγνώρισης* (acknowledgment) ότι

συμμετείχαν στις εκλογές[21]. Στο τέλος της περιόδου υποβολής ψήφων θα πρέπει να υπάρχουν *τόσες* κρυπτογραφημένες ψήφοι *όσες* και οι δηλώσεις αναγνώρισης, ούτως ώστε όλοι οι (εσωτερικοί και εξωτερικοί) παρατηρητές να είναι σίγουροι ότι η Αρχή δεν έχει υποβάλλει παράνομα ψήφους εκ μέρους των απεχόντων ψηφοφόρων. Εάν υπάρχουν ψηφοφόροι που ενώ υπέβαλλαν *ανώνυμα* τη δέσμευση ψήφου τους αποφεύγουν να υποβάλλουν *επώνυμα* τη δήλωση αναγνώρισης, τότε η ταυτότητα τους είναι δυνατόν να αποκαλυφθεί.

«Δίκαιες» Ψηφοφορίες. Ενώ θεωρείται ως δικαίωμα για κάποιον που υποβάλλει μια κρυπτογραφημένη ψήφο να απέχει μετέπειτα από την ψηφοφορία, κάτι τέτοιο δεν είναι *εξ' ίσου* δίκαιο (equitably fair) για την «κοινωνία»: ο όρος «κοινωνία» περιλαμβάνει τους ψηφοφόρους, τις Αρχές, καθώς και τους εσωτερικούς/εξωτερικούς παρατηρητές που επιθυμούν να επαληθεύσουν την ορθότητα των αποτελεσμάτων. Στο σχήμα μας [Mag02] επιτρέπεται στους ψηφοφόρους να απέχουν μετά την εγγραφή τους, αρκεί να μην έχουν ήδη υποβάλλει την κρυπτογραφημένη ψήφο τους (*νομότυπη αποχή*). Εάν ένας ψηφοφόρος υποβάλλει ανώνυμα τη ψήφο του, η ανωνυμία του προστατεύεται *υπό συνθήκη*: κάποια στιγμή αργότερα πρέπει να υποβάλλει τη δήλωση αναγνώρισης, αλλιώς (*παράτυπη αποχή*) η ταυτότητα του θα αποκαλυφθεί. Επιτρέποντας σε έναν ψηφοφόρο να απέχει από τις εκλογές, σε αυτό το χρονικό σημείο (δηλαδή μετά την υποβολή ψήφου), θα ήταν τόσο δίκαιο όσο και το να επιτρέπονταν σε ένα ψηφοφόρο στις παραδοσιακές εκλογές να ψηφίζει χωρίς να υπογράφει στην εκλογική λίστα.

2.5.2 Κρυπτογραφικές Κάψουλες

Για την επίλυση του προβλήματος των απεχόντων ψηφοφόρων χρησιμοποιούμε ειδικούς υποδοχείς μηνυμάτων, γνωστούς και ως

[21] Αυτό δεν πρέπει να συμβεί αμέσως μετά την ανώνυμη υποβολή ψήφου, διότι τότε μπορεί εύκολα να γίνει από την Αρχή ο συσχετισμός ψήφου-ψηφοφόρου, και να παραβιαστεί η μυστικότητα της ψήφου.

κρυπτογραφικές κάψουλες (cryptographic capsules) [Bon00]. Πρόκειται για υποδοχείς μηνυμάτων που προστατεύουν το μήνυμα τους κατά τέτοιον τρόπο ώστε η πρόσβαση κάποιου τρίτου στο μήνυμα (π.χ. η εύρεση της πραγματικής ταυτότητας των ψηφοφόρων που απέχουν παράτυπα) να απαιτεί ορισμένο υπολογιστικό κόστος, το οποίο αντανακλά την ισορροπία μεταξύ της ανάγκης για προστασία της *ιδιωτικότητας* (privacy) των ψηφοφόρων και της ανάγκης για *καταλογισμό ευθύνης* (non-repudiation) στους ψηφοφόρους που υπέβαλλαν την κρυπτογραφημένη ψήφο τους αλλά στη συνέχεια επέλεξαν να απέχουν από την ψηφοφορία. Ο χρόνος λοιπόν ανάκτησης των περιεχομένων της κάψουλας πρέπει να είναι [Mag02]:

- *Τόσο μεγάλος* ώστε να μην καθίσταται δυνατή η μαζική εκμετάλλευση προσωπικών δεδομένων των πολιτών, όπως οι εκλογικές προτιμήσεις τους.

- *Τόσο μικρός* ώστε να είναι (υπολογιστικώς) εφικτή η έγκαιρη ανάκτηση δεδομένων απαραίτητων για την ομαλή λειτουργία του συστήματος ή για την επιβολή κυρώσεων, όπου και όταν αυτό προκύπτει υπό προϋποθέσεις και μέσα σε νόμιμα πλαίσια.

Τα συστήματα αυτού του τύπου μπορούν να διακριθούν, ανάλογα με την υπολογιστική προσπάθεια που απαιτείται για την αποκάλυψη του μηνύματος, σε δυο κατηγορίες:

Κεντρικής Διαχείρισης. Η κάψουλα είναι ένας υποδοχέας στον οποίο μπορεί κάποιος, έστω η Alice, να τοποθετήσει ένα μήνυμα και να καθορίσει τον ακριβή υπολογιστικό χρόνο T που θα χρειαστεί ένας τρίτος, έστω ο Bob, για την αποκάλυψη του μηνύματος. Ενώ για την Alice είναι εύκολο να κατασκευάσει την κάψουλα, επειδή γνωρίζει μια επιπλέον *μυστική πληροφορία* (trapdoor), ο υπολογιστής του Bob πρέπει να δουλεύει συνεχώς για χρόνο T προκειμένου να ανακτήσει το μήνυμα. Ο χρόνος αυτός δε, δεν μπορεί να

συντομευτεί με κατανεμημένες διαδικασίες, δηλαδή η χρήση δυο ή περισσότερων υπολογιστών δεν προσφέρει ταχύτερα αποτελέσματα από τη χρήση ενός υπολογιστή.

Τα συστήματα Κεντρικής Διαχείρισης ενδείκνυνται για εφαρμογές όπου ο αριθμός των χρηστών του συστήματος, των οποίων τα προσωπικά δεδομένα πρέπει να προστατευτούν, είναι σχετικά μικρός (π.χ. σε μια ηλεκτρονική δημοπρασία [Mag00]).

Στο Κεφάλαιο 3, και στο πλαίσιο των ασφαλών δημοπρασιών (Ενότητα 3.5.1) επεξηγούμε το μαθηματικό αλγόριθμο των *Γρίφων Συγκεκριμένου Χρόνου Επίλυσης* (Time-lock puzzles), όπως αυτός προτάθηκε από τους Rivest, Shamir και Wagner [Riv96], όπου το «σπάσιμο» της κάψουλας από τον Bob απαιτεί τον υπολογισμό ενός αριθμού της μορφής $X = a^{2^t} (\mathrm{mod} n)$ όπου n είναι ένας μεγάλος σύνθετος αριθμός, a είναι ένας τυχαίος αριθμός και t είναι ο αριθμός των τετραγωνισμών (squarings) που πρέπει να πραγματοποιηθούν από τον Bob για το σπάσιμο της κάψουλας. Επειδή κάθε τετραγωνισμός γίνεται επί του αποτελέσματος του προηγούμενου τετραγωνισμού, δεν έχει βρεθεί τρόπος επιτάχυνσης της διαδικασίας με τη χρήση περισσότερων του ενός επεξεργαστών.

Στις [Mao01,Bon00] περιγράφονται μέθοδοι για τη σχεδίαση κάψουλας με βάση τον κρυπτογραφικό αλγόριθμο δημοσίου κλειδιού *RSA* [Rsa78]. Συγκεκριμένα στη [Mao01], περιγράφεται ένα πολύ αποδοτικό πρωτόκολλο απόδειξης με μηδενική γνώση, με το πέρας του οποίου ο Bob πείθεται ότι η κάψουλα περιέχει ένα μήνυμα κρυπτογραφημένο με τον αλγόριθμο RSA, και το οποίο μπορεί όντως να ανακτηθεί με το πέρας συγκεκριμένου χρόνου T.

Σημείωση: Στην [Mag01_2] προτείναμε ένα σχήμα που χρησιμοποιεί κάψουλες Κεντρικής Διαχείρισης για προστασία από καταναγκασμό, χωρίς τη χρήση ασφαλούς υλικού (π.χ. Έξυπνες Κάρτες) ή την υπόθεση φυσικά προστατευμένων καναλιών. Στο σχήμα αυτό η Alice κατασκευάζει την κρυπτογραφική κάψουλα της ψήφου της, χωρίς γνώση της μυστικής πληροφορίας (trapdoor). Σε αντίθετη περίπτωση, η πληροφορία αυτή θα αποτελούσε απόδειξη της ψήφου της. Σημαντικό μειονέκτημα αυτής της

προσέγγισης αποτελεί το γεγονός ότι η κατασκευή της ψήφου από την Alice απαιτεί υψηλό υπολογιστικό κόστος, κάτι που καθιστά το σχήμα μη πρακτικό.

Κατανεμημένα. Το μήνυμα κρυπτογραφείται με ένα κλειδί περιορισμένου μήκους (π.χ. ένα DES 40 bit) και η κρυπτογράφηση αποστέλλεται στον Bob μέσω ενός ανοικτού καναλιού επικοινωνίας (π.χ. μέσω Διαδικτύου). Στο συγκεκριμένο παράδειγμα, ο Bob θα χρειαστεί να εκτελέσει κατά μέσο όρο 2^{39} βήματα (στην χειρότερη περίπτωση 2^{40}) για την ανάκτηση του μηνύματος. Η διαδικασία ανάκτησης του κλειδιού κρυπτογράφησης μπορεί να συντομευτεί με κατανεμημένες διαδικασίες, π.χ. δύο υπολογιστές μπορούν να την επιταχύνουν κατά το ήμισυ. Για μεγαλύτερη ασφάλεια από ωτακουστές, όπως έχει προταθεί σχετικά από τον Shamir [Sha95], το μήνυμα M μπορεί να κρυπτογραφηθεί με ένα «ισχυρό» κλειδί, π.χ. *DES* 128 bit, του οποίου τα, έστω, 88 bit *υποθηκεύονται* (escrow) σε μια έμπιστη Αρχή Υποθήκευσης[22]. Η Αρχή θα φανερώσει το υποθηκευμένο τμήμα του κλειδιού, μόνον εάν λάβει τα απαραίτητα εχέγγυα. Στη συνέχεια, και αφού ο Bob λάβει το υποθηκευμένο τμήμα του κλειδιού, θα χρειαστεί πάλι κατά μέσο όρο 2^{39} βήματα για την ανάκτηση και του υπολοίπου τμήματος του κλειδιού.

Σε συστήματα όπου τα κλειδιά της κάψουλας είναι διαχρονικά, ή παραμένουν λειτουργικά για μεγάλο χρονικά διάστημα, υφίσταται το πρόβλημα της *πρόωρης ανάκτησης* (early recovery) του κλειδιού, όπου ο Bob πραγματοποιεί πρόωρα τα 2^{39} βήματα και στη συνέχεια συμμαχεί με την Αρχή Υποθήκευσης, ή υποκλέπτει τα υποθηκευμένα κλειδιά από την Αρχή Υποθήκευσης [Sha95]. Οι Bellare και Goldwasser [Bel96] πρότειναν επίσης κρυπτογραφικά συστήματα για την αντιμετώπιση παρόμοιων επιθέσεων.

[22] Τα συστήματα υποθήκευσης (ανάκτησης) κλειδιού καλύπτονται στο Κεφάλαιο 5.

2.5.3 Ένα Πρωτόκολλο για «Δίκαιες» Ψηφοφορίες

Οι συμμετέχοντες στο πρωτόκολλο είναι οι χρήστες (ψηφοφόροι) και το Εκλογικό Κέντρο (Voting Center-VC). Υποθέτουμε ότι υπάρχει μια Υποδομή Δημοσίου Κλειδιού για ψηφιακές υπογραφές και κρυπτογράφηση δημοσίου κλειδιού. Το Κέντρο χρησιμοποιεί έναν Πίνακα Ανακοινώσεων για την επικοινωνία του με τους χρήστες και τους εξωτερικούς παρατηρητές. Οι εκλογές ολοκληρώνονται σε τέσσερις διακριτές φάσεις (Σχήμα 6): Εγγραφή, Ψηφοφορία, Επαλήθευση και Καταμέτρηση.

Οι συμβολισμοί που θα χρησιμοποιηθούν στο πρωτόκολλο είναι:

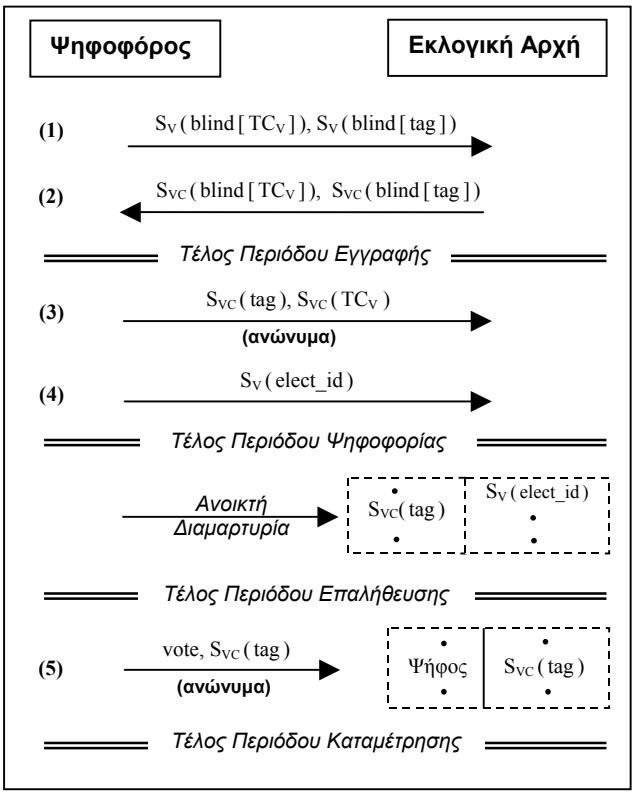
- V : ο Ψηφοφόρος.
- VC : το Εκλογικό Κέντρο.
- $S_x(m)$: η υπογραφή στο μήνυμα m με το ιδιωτικό κλειδί του x.
- *Blind(m)*: προετοιμασία ενός μηνύματος m ώστε να υπογραφεί «τυφλά».
- TC_m : κρυπτογραφική κάψουλα που περιέχει το μήνυμα m.
- *Tag* : η δέσμευση ψήφου (π.χ. κρυπτογράφηση με ένα DES κλειδί).
- $Elect_{id}$: ένας αριθμός που προσδιορίζει μοναδικά τη τρέχουσα ψηφοφορία.

Εγγραφή

Κατά τη διάρκεια της εγγραφής, και μέσω ενός αυθεντικοποιημένου καναλιού επικοινωνίας, ο ψηφοφόρος, ας πούμε ο Victor, εκτελεί σε συνεργασία με το Κέντρο ένα πρωτόκολλο «τυφλής» υπογραφής, στο τέλος του οποίου αποκτά υπογεγραμμένες τη δέσμευση ψήφου[23] *tag* και μία κάψουλα TC_V που περιέχει την αληθινή του ταυτότητα V (Βήματα 1,2, Σχήμα 6). Για την απόδειξη της ορθότητας των μηνυμάτων που πρόκειται να υπογραφούν «τυφλά» από το

[23] Θεωρούμε, για λόγους απλότητας, ότι η δέσμευση ψήφου *tag* προκύπτει ως η έξοδος μιας συνάρτησης κατακερματισμού (hash function) [Sch96] στην οποία δίδεται ως είσοδος η τιμή της ψήφου.

Κέντρο, ενδείκνυται η χρησιμοποίηση τεχνικών *Διαίρει και Επίλεξε*[24] (cut-and-choose) [Sch96]). Αυτές συγκαταλέγονται στα πρωτόκολλα απόδειξης με μηδενική γνώση (Ενότητα 2.3.5) και αποδεικνύουν στο Κέντρο ότι η κάψουλα μπορεί αργότερα να οδηγήσει στην ταυτότητα του Victor, ώστε να του καταλογιστεί ευθύνη σε περίπτωση παράτυπης αποχής.



Σχήμα 6. Μια ηλεκτρονική ψηφοφορία με κεντρική διαχείριση

Ψηφοφορία

Σε αυτό το σημείο ο Victor μπορεί να αποφασίσει εάν επιθυμεί να απέχει από τις εκλογές. Εάν επιθυμεί να συμμετάσχει, τότε αποστέλλει μέσω ενός ανώνυμου καναλιού επικοινωνίας (Βήμα 3) τη δέσμευση ψήφου *tag* καθώς και την κάψουλα TC_V, στο Εκλογικό Κέντρο. Αυτό είναι το *σημείο μη επιστροφής* για τον Victor. Κάποια στιγμή αργότερα, ο Victor πρέπει να αναγνωρίσει τη

[24] Περισσότερα για τις τεχνικές αυτές στο Κεφάλαιο 3, Ενότητα 3.5.1.2.

συμμετοχή του στη ψηφοφορία, αποστέλλοντας επώνυμα μια *δήλωση αναγνώρισης* (Βήμα 4). Η δήλωση αυτή αποτελείται από έναν αριθμό *elect_id*, υπογεγραμμένο ψηφιακά με το ιδιωτικό κλειδί υπογραφής του Victor.

Καταλογισμός ευθύνης στους παράνομα απέχοντες. Στο τέλος αυτής της φάσης, ο αριθμός των δηλώσεων αναγνώρισης $S_V(elect\_id)$ πρέπει να ισούται με τον αριθμό των έγκυρων δεσμεύσεων $S_{VC}(tag)$ Αλλιώς, υπάρχει η περίπτωση κάποιοι ψηφοφόροι να έχουν απόσχει παράτυπα. Η διαδικασία που ακολουθείται είναι η εξής: το Κέντρο ζητάει από όλους τους χρήστες που υπέβαλαν δήλωση αναγνώρισης στο Βήμα 4, να υποβάλλουν την μυστική πληροφορία (trapdoor) για την άμεση επίλυση της κάψουλας που υπέβαλαν στο βήμα 3. Τα ονόματα όσων χρηστών περάσουν επιτυχώς αυτό το στάδιο, τοποθετούνται σε μια λίστα *L*. Εάν ο χρήστης δε μπορεί να προσδιορίσει την κάψουλά του, στον κατάλογο που του παρουσιάζει το Κέντρο, τότε αυτό σημαίνει ότι εκτέλεσε το βήμα 4 αλλά απείχε παράτυπα από το βήμα 3. Όσες κάψουλες απομείνουν χωρίς να συνδεθούν με κάποιο χρήστη, ανήκουν προφανώς σε χρήστες που εκτέλεσαν το βήμα 3, αλλά απείχαν παράτυπα από το βήμα 4. Αυτές οι κάψουλες μπορούν να επιλυθούν ώστε να καταλογιστεί ευθύνη στους απέχοντες χρήστες.

Κόστος. Το κόστος που συνεπάγεται από την υιοθέτηση του μηχανισμού αυτού είναι ότι η ψηφοφορία πρέπει να επαναληφθεί *από την αρχή*, αυτή τη φορά όμως με συμμετέχοντες μόνον τους εξουσιοδοτημένους ψηφοφόρους της λίστας *L*. Οι απέχοντες της ψηφοφορίας, είτε νομότυποι είτε παράτυποι, δε δικαιούνται συμμετοχή στις εκλογές σε αυτό το χρονικό σημείο.

Επαλήθευση

Το Κέντρο δημοσιεύει όλες τις έγκυρες δεσμεύσεις ψήφου $S_{VC}(tag)$ καθώς και τις δηλώσεις αναγνώρισης $S_V(elect\_id)$ στον Πίνακα Ανακοινώσεων. Οι

ψηφοφόροι μπορούν να επαληθεύσουν ότι η κρυπτογραφημένη ψήφος τους έχει ληφθεί υπ' όψιν από το Κέντρο. Επίσης, οι εσωτερικοί/εξωτερικοί παρατηρητές μπορούν να επαληθεύσουν ότι το Κέντρο δεν έχει υποβάλει πλαστές ψήφους εκ μέρους κάποιου ψηφοφόρου.

Εάν η έγκυρη δέσμευση του Victor δεν είναι δημοσιευμένη στον Πίνακα Ανακοινώσεων, τότε ο Victor μπορεί να προβεί σε μια *ανοικτή διαμαρτυρία* (open objection) [Sak93], δηλαδή χωρίς να αποκαλύψει το περιεχόμενο της ψήφου του. Αυτό μπορεί να γίνει αναμεταδίδοντας ανώνυμα, σε ένα δημόσιο κανάλι επικοινωνίας, την υπογεγραμμένη (από το Κέντρο) δέσμευση ψήφου του.

Σημείωση: Η δυνατότητα των ψηφοφόρων για ανοικτή διαμαρτυρία αποτελεί τον κύριο λόγο για τον οποίο η περίοδος της Επαλήθευσης διαχωρίζεται από την περίοδο της Καταμέτρησης: εάν τα αποτελέσματα της ψηφοφορίας δημοσιεύονταν και στη συνέχεια επιτρέπονταν οι όποιες διαμαρτυρίες από τους ψηφοφόρους, τότε η πράξη καθ' αυτή της διαμαρτυρίας θα φανέρωνε εμμέσως το περιεχόμενο της ψήφου [Sak93]. Επίσης, ο διαχωρισμός των δύο περιόδων αποτρέπει το Κέντρο από την επιλεκτική απόρριψη ψήφων με βάση το περιεχόμενο τους, αφού οι δημοσιευμένες δεσμεύσεις κατά την περίοδο της Επαλήθευσης περιβάλλονται από μυστικότητα. Όταν κατά την περίοδο της Καταμέτρησης οι ψηφοφόροι αποκαλύψουν ανώνυμα τις ψήφους τους, τότε το Κέντρο δε μπορεί να προβεί σε επιλεκτική απόρριψη ψήφων, αφού έχει ήδη δημοσιεύσει τα κρυπτογραφημένα αποτελέσματα της ψηφοφορίας.

Καταμέτρηση

Στο Βήμα 5, ο Victor χρησιμοποιεί ένα ανώνυμο κανάλι επικοινωνίας και αποστέλλει την ψήφο του, καθώς και την αντίστοιχη έγκυρη δέσμευση ψήφου στο Εκλογικό Κέντρο. Στο τέλος αυτής της φάσης, το Κέντρο δημοσιεύσει τα τελικά αποτελέσματα της ψηφοφορίας.

Σημείωση: Σε ορισμένες υλοποιήσεις θα μπορούσε να επιτραπεί στους ψηφοφόρους να απέχουν από το Βήμα 5, δηλαδή από την ανώνυμη άρση της μυστικότητας της ψήφου τους. Αυτό δε θα επηρέαζε την ασφάλεια του συστήματος, αφού το Εκλογικό Κέντρο δε θα μπορεί πλέον να υποβάλει πλαστές ψήφους για τους ψηφοφόρους που απείχαν του Βήματος 5. Για να το κάνει αυτό, το Κέντρο θα πρέπει να «σπάσει» τη δέσμευση ψήφου, δηλαδή τον αλγόριθμο κατακερματισμού (hash algorithm) π.χ. MD5 [Riv91], ή τον αλγόριθμο κρυπτογράφησης (π.χ. ElGamal [ElG85]) που χρησιμοποιήθηκε. Η ασφάλεια των σύγχρονων αλγορίθμων κατακερματισμού/κρυπτογράφησης θεωρείται ισχυρή [And01].

Επιβεβαίωση παράδοσης ψήφου. Έως τώρα υποθέσαμε ότι το Εκλογικό Κέντρο δεν αρνείται ευθύνη για την παραλαβή των μηνυμάτων που του αποστέλλονται από τους ψηφοφόρους στα Βήματα 3,4,5 (Σχήμα 6). Ωστόσο, για να αποτραπεί ο κίνδυνος κάποιοι να εμφανιστούν παράτυπα απέχοντες χωρίς να είναι, μπορεί να γίνει χρήση υπηρεσιών Επιβεβαιωμένης Παράδοσης (Certified Delivery) [Tyg96,Aso98]. Οι υπηρεσίες αυτές είναι υπηρεσίες έμπιστης οντότητας οι οποίες θα επιστρέφουν στον ψηφοφόρο μια απόδειξη παραλαβής (receipt of delivery) του μηνύματος από το Κέντρο, και μπορούν να χρησιμοποιηθούν τόσο για την υποβολή των δεσμεύσεων ψήφου και κάψουλων (Βήμα 3), όσο και για την υποβολή της δήλωσης αναγνώρισης και την άρση της μυστικότητας της ψήφου (Βήματα 4,5). Έτσι το κακόβουλο Κέντρο δε μπορεί να αρνηθεί τη λήψη των μηνυμάτων που αποστέλλονται από τον Victor.

2.6 Συζήτηση

Η αυξημένη διείσδυση του Διαδικτύου στις δημοκρατικές χώρες καθιστά μονόδρομο την υιοθέτηση συστημάτων με τα οποία οι ψηφοφόροι θα χρησιμοποιούν τις τεχνολογίες του Διαδικτύου για να συμμετέχουν στις εκλογικές διαδικασίες. Για να γίνει ευρέως αποδεκτό, ένα σύστημα

ηλεκτρονικής ψηφοφορίας μέσω Διαδικτύου θα πρέπει να εκπληρώνει κάποιες βασικές απαιτήσεις ασφάλειας και πρακτικότητας.

Η κρυπτογραφία αποτελεί ένα σημαντικό εργαλείο στην προσπάθεια σχεδίασης ασφαλών συστημάτων ηλεκτρονικής ψηφοφορίας. Ωστόσο, από μόνη της η κρυπτογραφία δε μπορεί να αντιμετωπίσει προβλήματα που σχετίζονται με την εξασφάλιση ενός ασφαλούς περιβάλλοντος αλληλεπίδρασης των ψηφοφόρων (πελάτες) με τις Εκλογικές Αρχές (εξυπηρετητές). Η ασφάλεια ενός τέτοιου περιβάλλοντος, εξαρτάται επίσης από:

- Την ασφάλεια του συστήματος-πελάτη (π.χ. ασφάλεια λειτουργικού συστήματος, εργαλείων πλοήγησης στο Web, ψηφιακή ταυτοποίηση, αντιμετώπιση κακόβουλων προγραμμάτων, επιθέσεις άρνησης εξυπηρέτησης).

- Την ασφάλεια του καναλιού επικοινωνίας (ωτακουστές, επιθέσεις πλαστοπροσωπίας, επιθέσεις ενδιάμεσης οντότητας, περιορισμένο εύρος δικτύου, επιθέσεις άρνησης εξυπηρέτησης).

- Την ασφάλεια του συστήματος-εξυπηρετητή (επιθέσεις εισβολής, επιθέσεις από εσωτερικούς εχθρούς, επιθέσεις άρνησης εξυπηρέτησης, πλαστοπροσωπία, προστασία από κακόβουλα προγράμματα, προστασία από καταστροφή ή δυσλειτουργία των αποθηκευτικών μέσων).

Η κρυπτογραφία αντιμετωπίζει, σε χαμηλό επίπεδο, τα προβλήματα ασφάλειας που σχετίζονται με την προστασία της ιδιωτικότητας του χρήστη, της ορθότητας της εκλογικής διαδικασίας και της επαληθευσιμότητας των αποτελεσμάτων της ψηφοφορίας. Ωστόσο, λίγα είναι έως σήμερα τα πρωτόκολλα στη διεθνή βιβλιογραφία που προσφέρουν αποδεδειγμένη ασφάλεια και πρακτικότητα, ιδιαίτερα σε περιβάλλοντα μεγάλης κλίμακας.

Το πρόβλημα καταναγκασμού των ψηφοφόρων αποτελεί μια επιπλέον τροχοπέδη για την υλοποίηση συστημάτων ηλεκτρονικής ψηφοφορίας μέσω Διαδικτύου. Στο Κεφάλαιο αυτό προτείναμε ένα κρυπτογραφικό σχήμα για την επίτευξη Προστασίας από Καταναγκασμό, όπου οι χρήστες αλληλεπιδρούν κατά τρόπο επαληθεύσιμο με μία Έξυπνη Κάρτα ώστε να μην είναι δυνατή η κατασκευή ηλεκτρονικής απόδειξης για την τελική κρυπτογραφημένη ψήφο.

Μία ευρέως χρησιμοποιούμενη, σε πιλοτικό στάδιο, κατηγορία συστημάτων ηλεκτρονικής ψηφοφορίας βασίζεται στο μοντέλο των «τυφλών» υπογραφών για την προστασία της ιδιωτικότητας των ψηφοφόρων. Τα συστήματα αυτά πάσχουν από το πρόβλημα της υποβολής πλαστών ψήφων από την Εκλογική Αρχή εκ μέρους των ψηφοφόρων που απέχουν. Στο Κεφάλαιο αυτό επίσης μελετήσαμε κρυπτογραφικές τεχνικές για την αντιμετώπιση του προβλήματος, κατά τρόπο ώστε να επιτυγχάνεται η ορθότητα των εκλογικών αποτελεσμάτων, διατηρώντας παράλληλα την μυστικότητα της ψήφου και το δικαίωμα της ανωνυμίας για τους συμμετέχοντες ψηφοφόρους.

Είναι αδήριτη η ανάγκη περαιτέρω έρευνας και μελέτης ασφαλών και αποδοτικών κρυπτογραφικών τεχνικών για την υλοποίηση συστημάτων ηλεκτρονικής ψηφοφορίας. Στο μέλλον, αναμένεται να δοθεί έμφαση σε θέματα όπως:

- Κατασκευή αλγορίθμων κρυπτογράφησης δημοσίου κλειδιού, με εγγενή προστασία από καταναγκασμό.

- Ενσωμάτωση πολλών από τις λειτουργίες που καλείται να επιτελέσει ο χρήστης σε «έξυπνες» φορητές συσκευές (π.χ. έξυπνες κάρτες).

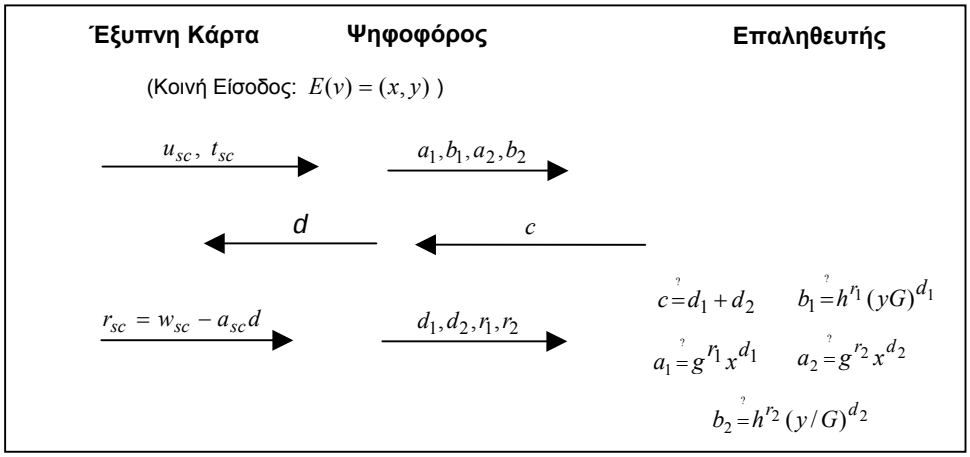
- Έμφαση στο σχεδιασμό «τεχνολογικά ουδέτερων» συστημάτων (πλατφόρμες, αρχιτεκτονικές, εργαλεία πλοήγησης).

- Ενσωμάτωση βιομετρικών τεχνολογιών αναγνώρισης (π.χ. φωνή, ίριδα ματιού, δακτυλικά αποτυπώματα) στα υποσυστήματα ταυτοποίησης των ψηφοφόρων.

- Εναλλακτικά συστήματα-πελάτες (π.χ. μηχανήματα ATM, κινητά τηλέφωνα, προσωπικούς ψηφιακούς βοηθούς, τηλεόραση, κονσόλες παιχνιδιών).

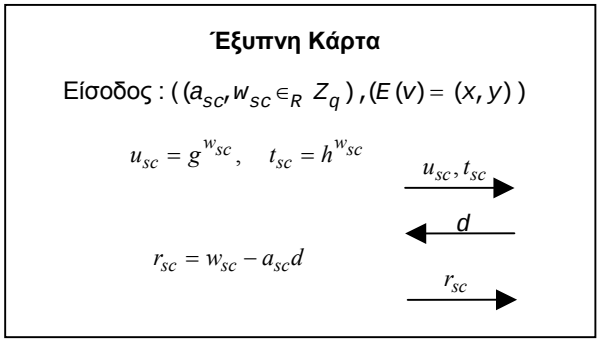
Παράρτημα Α - Απόδειξη Εγκυρότητας Ψήφου σε Εκλογές Προστατευμένες από Καταναγκασμό

Το πρωτόκολλο, με αλληλεπίδραση, της απόδειξης εγκυρότητας της ψήφου $E(v)$ με μηδενική γνώση (IZKP) [Mag01] (Σχήμα 7), αποτελεί μια τροποποίηση για *δύο-αποδεικνύοντες* (two-prover), του πρωτοκόλλου των Cramer, Gennaro και Schoenmakers [Cra97].

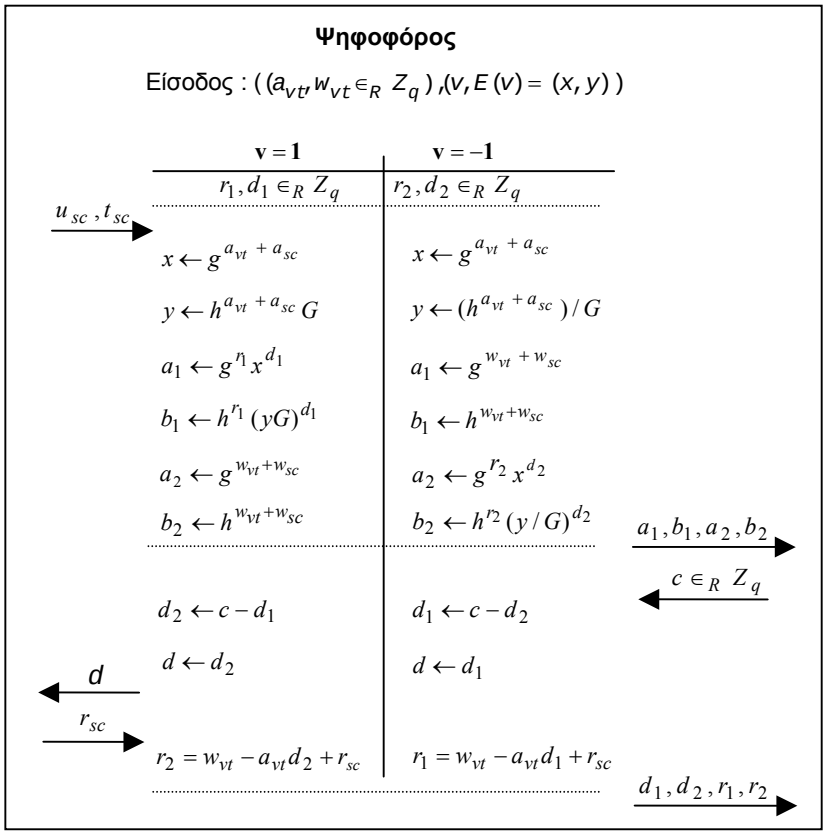


Σχήμα 7. Πρωτόκολλο για την απόδειξη εγκυρότητας της κρυπτογραφημένης ψήφου

Η κοινή είσοδος του ψηφοφόρου και της Κάρτας είναι το $E(v) = (x, y) = (g^{a_{sc}+a_{vt}}, h^{a_{sc}+a_{vt}} G^{v})$ όπου $v \in \{-1, +1\}$. Η συμμετοχή της Κάρτας στην απόδειξη εγκυρότητας περιγράφεται από την υπορουτίνα του Σχήματος 8. Η συμμετοχή του ψηφοφόρου στην απόδειξη εγκυρότητας περιγράφεται από την υπορουτίνα του Σχήματος 9.



Σχήμα 8. Συμμετοχή της Έξυπνης Κάρτας στην απόδειξη εγκυρότητας



Σχήμα 9. Συμμετοχή του Ψηφοφόρου στην απόδειξη εγκυρότητας

Θεώρημα. Το πρωτόκολλο απόδειξης με μηδενική γνώση, που περιγράφεται στο Σχήμα 6, αποδεικνύει ότι το $E(v) = (x, y)$ *είναι κρυπτογράφηση μιας έγκυρης ψήφου (δηλαδή, μιας ψήφου που ανήκει στο σύνολο {-1,1}) [Mag01].*

Μηδενική Γνώση. Η απόδειξη ότι το ζεύγος *(x,y)* είναι της σωστής μορφής, χωρίς να αποκαλυφθεί η τιμή της ψήφου v, ανάγεται στην απόδειξη γνώσης της σχέσης:

$$\log_g x = \log_g (y/G) \;\Rightarrow\; \log_g x = \log_g (y/G^{-1}) \quad (1)$$

Οι αποδεικνύοντες, δηλαδή ο Ψηφοφόρος και η Κάρτα, είτε έχουν τη γνώση να αποδείξουν την ισότητα στο αριστερό τμήμα της σχέσης (1), είτε την ισότητα στο δεξί τμήμα της (1), αλλά όχι και τις δύο ισότητες ταυτόχρονα,

ανάλογα με την τιμή της ψήφου που έχει προεπιλεγεί. Για να αποδείξουν οποιαδήποτε από τις δυο ισότητες της (1), οι αποδεικνύοντες πρέπει να χρησιμοποιήσουν την απόδειξη με μηδενική γνώση για την ισότητα των διακριτών λογαρίθμων που προτάθηκε από τους Chaum και Pedersen [Cha92]. Στην απόδειξη του Σχήματος 7, οι τυχαιότητες των μηνυμάτων που αποστέλλονται στον Επαληθευτή είναι συνδυασμός των τυχαιοτήτων του Ψηφοφόρου και της Κάρτας, κατά τρόπο ώστε κανείς από τους δυο δε μπορεί να μάθει την τυχαιότητα του άλλου, αφού κάτι τέτοιο θα παραβίαζε την Προστασία από Καταναγκασμό.

Στην εργασία [Cra97, Λήμμα 1] αποδεικνύεται η ιδιότητα της μηδενικής γνώσης για την απόδειξη των Chaum και Pedersen στην περίπτωση ενός *τίμιου επαληθευτή* (honest-verifier). Αυτό εξυπηρετεί το σκοπό μας, αφού το πρωτόκολλο απόδειξης που περιγράψαμε θα μετατραπεί σε απόδειξη *χωρίς αλληλεπίδραση*, προκειμένου να υπάρχει οικουμενική επαληθευσιμότητα. Για τη μετατροπή αυτή, ο Επαληθευτής μπορεί να υλοποιηθεί είτε ως μια έμπιστη πηγή τυχαίων συμβολοσειρών (π.χ. beacons [Rab83]) είτε με την *ευριστική* προσέγγιση των Fiat και Shamir [Fia86], όπου και γίνεται χρήση *συναρτήσεων κατακερματισμού*. Στην τελευταία περίπτωση η ασφάλεια βασίζεται στο μοντέλο *random oracle*[11] [Bel93].