ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΑΣΦΑΛΗ ΗΛΕΚΤΡΟΝΙΚΑ ΣΥΣΤΗΜΑΤΑ ΣΥΝΑΛΛΑΓΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Διδακτορική Διατριβή

Μάγκου Εμμανουήλ

Πειραιάς, 2003

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΙΑΤΡΙΒΗ

για την απόκτηση Διδακτορικού
Διπλώματος του Τμήματος Πληροφορικής

Εμμανουήλ Β. Μάγκου

ΑΣΦΑΛΗ ΗΛΕΚΤΡΟΝΙΚΑ ΣΥΣΤΗΜΑΤΑ ΣΥΝΑΛΛΑΓΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Τριμελής Συμβουλευτική Επιτροπή:
Επιβλέπων:

Αλεξανδρής Νικόλαος
Καθηγητής Πανεπιστημίου Πειραιώς

Μέλη:

Χρυσικόπουλος Βασίλειος
Καθηγητής Πανεπιστημίου Ιονίου

Τσιχριτζής Γεώργιος
Επίκουρος Καθηγητής
Πανεπιστημίου Πειραιώς

Επταμελής Εξεταστική Επιτροπή:

Αλεξανδρής Νικόλαος
Καθηγητής Πανεπιστημίου Πειραιώς

Χρυσικόπουλος Βασίλειος
Καθηγητής Πανεπιστημίου Ιονίου

Τσιχριτζής Γεώργιος
Επίκουρος Καθηγητής
Πανεπιστημίου Πειραιώς

Δουληγέρης Χρήστος
Αναπληρωτής Καθηγητής
Πανεπιστημίου Πειραιώς

Κάτσικας Σωκράτης
Καθηγητής Πανεπιστημίου Αιγαίου

Λυκοθανάσης Σπύρος
Αναπληρωτής Καθηγητής
Πανεπιστημίου Πατρών

Γκρίτζαλης Δημήτρης
Επίκουρος Καθηγητής
Οικονομικού Πανεπιστημίου Αθηνών

Πίνακας Περιεχομένων

1 Εισαγωγή 1

1.1 Ένα Μοντέλο Ηλεκτρονικών Συστημάτων Συναλλαγών και Εφαρμογές 1
1.2 Απαιτήσεις Ασφάλειας στα Ηλεκτρονικά Συστήματα Συναλλαγών 4
1.3 Μοντέλο Απειλής 6
1.3.1 Καταλογισμός Ευθύνης 7
1.3.2 Προστασία από Καταναγκασμό 10
1.4 Αντικείμενο και Στόχοι της Διατριβής 14
1.5 Δομή της Διατριβής 15
1.6 Συνεισφορά στην Ερευνητική Περιοχή - Δημοσιεύσεις 16
1.7 Ευχαριστίες 21

2 Ασφάλεια σε Συστήματα Ηλεκτρονικής Ψηφοφορίας 22

2.1 Εισαγωγή 22
2.2 Θεώρηση Συστημάτων Ηλεκτρονικής Ψηφοφορίας 27
2.2.1 Απαιτήσεις Ασφάλειας και Πρακτικότητας 27
2.2.2 Πλεονεκτήματα Συστημάτων Ηλεκτρονικής Ψηφοφορίας 29
2.2.3 Μειονεκτήματα Συστημάτων Ηλεκτρονικής Ψηφοφορίας 30
2.2.4 Συνιστώμενα Μέτρα Ασφάλειας 33
2.3 Κρυπτογραφικά Μοντέλα Ασφάλειας 35
2.3.1 Το Μοντέλο MIX-net 35
2.3.2 Το Μοντέλο των «Τυφλών» Υπογραφών 38
2.3.3 Το Μοντέλο του Benaloh 40
2.3.4 Το Ομομορφικό Μοντέλο Κρυπτογράφησης 41
2.3.5 Βασικά Κρυπτογραφικά Εργαλεία 42
2.4 Προστασία από Καταναγκασμό 45
2.4.1 Ελευθερία από Απόδειξη και Προστασία από Καταναγκασμό 45
2.4.2 Υποθέσεις για Επίτευξη Προστασίας από Καταναγκασμό 46
2.4.3 Ελάχιστες Απαιτήσεις Ασφάλειας 49
2.4.4 Ένα Βασικό Σχήμα με Προστασία από Καταναγκασμό 54
2.4.5 Μία Υλοποίηση με Κρυπτογράφηση ElGamal 55
2.5 Απόσυρση Ψήφου στο Μοντέλο των «Τυφλών» Υπογραφών 61
2.5.1 Το Πρόβλημα των Απεχόντων Ψηφοφόρων 61
2.5.2 Κρυπτογραφικές Κάψουλες 64
2.5.3 Ένα Πρωτόκολλο για «Δίκαιες» Ψηφοφορίες 68
2.6 Συζήτηση 72
Παράρτημα Α - Απόδειξη Εγκυρότητας Ψήφου σε Εκλογές Προστατευμένες από Καταναγκασμό 76

3 Ασφάλεια στις Ηλεκτρονικές Δημοπρασίες 79

3.1 Εισαγωγή 79
3.1.1 Τύποι Δημοπρασιών 80
3.2 Ζητήματα Ασφάλειας στις Ηλεκτρονικές Δημοπρασίες 85

3.2.1 Δακτύλιοι 85
3.2.2 Καταναγκασμός στις Ηλεκτρονικές Δημοπρασίες 88
3.2.3 Άλλες Επιθέσεις 89
3.3 Απαιτήσεις Ασφάλειας 93
3.4 Κρυπτογραφικά Μοντέλα Ασφάλειας 95
3.5 «Δίκαιες» Κλειστές Ηλεκτρονικές Δημοπρασίες 101
3.5.1 Κρυπτογραφικοί Μηχανισμοί 103
3.5.1.1 Γρίφοι Συγκεκριμένου Χρόνου Επίλυσης 103
3.5.1.2 «Τυφλές» Υπογραφές 105
3.5.2 Βασικές Υποθέσεις Ασφάλειας 106
3.5.3 Ένα Πρωτόκολλο «Δίκαιων» Δημοπρασιών 108
3.5.3.1 Ανάλυση της Ασφάλειας του Πρωτοκόλλου 112
3.6 Μια Ηλεκτρονική Δημοπρασία με Προστασία από Καταναγκασμό 120
3.6.1 Το Πρωτόκολλο 122
3.7 Συζήτηση 126

4 Ανίχνευση «Προδοτών» σε Συστήματα Αναμετάδοσης Κρυπτογραφημένου Υλικού 130

4.1 Εισαγωγή 130
4.1.1 Συστήματα Αναμετάδοσης 134
4.2 Θεώρηση Σχημάτων Ανίχνευσης «Προδοτών» σε Συστήματα Αναμετάδοσης 137
4.3 Βασικά Κρυπτογραφικά Εργαλεία 142
4.3.1 Το Συμμετρικό Σχήμα των Kurosawa-Desmedt 142
4.3.2 Επιλήσμονα Μεταφορά 144
4.4 Ένα Ασύμμετρο Πρωτόκολλο Ανίχνευσης «Προδοτών» 146
4.4.1 Έλεγχος της Ορθότητας των K-D κλειδιών 150
4.5 Συζήτηση 155

5 Ασφάλεια σε Συστήματα Ανάκτησης Κλειδιού 159

5.1 Εισαγωγή 159
5.2 Συστήματα Ανάκτησης Κλειδιού 161
5.3 Επιθέσεις στα Συστήματα Ανάκτησης Κλειδιού 163
5.3.1 Η Επίθεση των Pfitzmann-Waidner 165
5.4 Ανάκτηση Κλειδιού με Ισχυρή Χρονική Ασφάλεια 166
5.4.1 Ισχυρή Χρονική Ασφάλεια 167
5.4.2 Ένα «Δίκαιο» Κρυπτογραφικό Σχήμα Ανάκτησης Κλειδιού με Ισχυρή Χρονική Ασφάλεια 168
5.5 Ένα Υβριδικό Μοντέλο Ανάκτησης Κλειδιού 174
5.6 Συζήτηση 179
Παράρτημα Β – Ορθότητα Ανανέωσης Δημόσιου Κλειδιού (περίοδος t) στην Ανάκτηση Κλειδιού με Ισχυρή Χρονική Ασφάλεια 182

6 Συμπεράσματα της Διατριβής 184

Βιβλιογραφικές Αναφορές 192

Κεφάλαιο 1

Εισαγωγή

Στο κεφάλαιο αυτό περιγράφουμε ένα μοντέλο ηλεκτρονικών συναλλαγών μέσω Διαδικτύου, και αναφέρουμε τα προβλήματα ασφάλειας που εντοπίζονται σε συστήματα που βασίζονται σε αυτό το μοντέλο. Επίσης, περιγράφουμε τις απαιτήσεις ασφάλειας ενός ηλεκτρονικού συστήματος συναλλαγών, δίνοντας έμφαση στο σχεδιασμό «*Δίκαιων*» συστημάτων, δηλαδή συστημάτων στα οποία κανένα συμβαλλόμενο μέρος δεν αποκτά πλεονέκτημα έναντι του άλλου, καθώς και στον *καταλογισμό ευθύνης* και την προστασία της *ιδιωτικότητας* των χρηστών. Στη συνέχεια, αναφέρουμε το αντικείμενο και τους στόχους που πραγματεύεται η παρούσα Διατριβή. Τέλος, παρουσιάζεται η δομή της Διατριβής και περιγράφεται συνοπτικά η συνεισφορά της στο ερευνητικό πεδίο της ασφάλειας στα ηλεκτρονικά συστήματα συναλλαγών.

1.1 Ένα Μοντέλο Ηλεκτρονικών Συστημάτων Συναλλαγών και Εφαρμογές

Θεωρούμε ένα ηλεκτρονικό σύστημα συναλλαγών [Bur_Mag02a] στο οποίο:

- Κάθε χρήστης επιλέγει μια προσφορά από ένα σύνολο προσφορών *L*.
- Ο χρήστης χρησιμοποιεί τις υπηρεσίες του Διαδικτύου για να υποβάλλει την προσφορά του στην Αρχή του συστήματος (system Authority).

- Η Αρχή αξιολογεί την προσφορά ως επιτυχή ή ανεπιτυχή, βάση ενός συνόλου κανόνων *R*.

- Τα αποτελέσματα ανακοινώνονται στους χρήστες μέσω του Διαδικτύου.

Το παραπάνω μοντέλο συστημάτων ηλεκτρονικών συναλλαγών περιλαμβάνει μια ποικιλία εφαρμογών σε διαφορετικά περιβάλλοντα. Έτσι, για παράδειγμα, ένα ηλεκτρονικό σύστημα συναλλαγών που βασίζεται στο μοντέλο μας μπορεί να είναι:

- **Μία Ηλεκτρονική Ψηφοφορία** (e-voting) [Mag01], όπου οι προσφορές είναι ψήφοι, επιλέγονται από ένα πεπερασμένο σύνολο προσφορών, π.χ. το σύνολο {Ναι, Όχι}, κρυπτογραφούνται και αποστέλλονται μέσω του Διαδικτύου στις Εκλογικές Αρχές (ή την Εκλογική Αρχή) για καταμέτρηση. Μετά από το τέλος της περιόδου υποβολής ψήφων οι Αρχές αποκρυπτογραφούν και καταμετρούν τις ψήφους. Κατά την καταμέτρηση λαμβάνεται υπ' όψιν ένα σύνολο κανόνων *R* που καθορίζει ότι η προσφορά που συγκέντρωσε τις περισσότερες προτιμήσεις κερδίζει τη ψηφοφορία, είναι δηλαδή μια επιτυχής προσφορά. Τα αποτελέσματα ανακοινώνονται σε όλους τους χρήστες του συστήματος, καθώς και (προαιρετικά) σε εξωτερικούς παρατηρητές.

- **Μία Ηλεκτρονική Δημοπρασία** (e-auction) [Mag00], όπου επιλέγονται χρηματικές προσφορές από ένα πεπερασμένο σύνολο προσφορών, π.χ. {10,20,30,50,100,1000}, κρυπτογραφούνται και αποστέλλονται μέσω του Διαδικτύου στις Αρχές Δημοπρασίας (ή την Αρχή Δημοπρασίας) για καταμέτρηση. Μετά το τέλος της περιόδου υποβολής προσφορών οι προσφορές ανοίγονται και αξιολογούνται. Κατά την αξιολόγηση λαμβάνεται υπ' όψιν ένα σύνολο κανόνων *R* που καθορίζει ότι η

υψηλότερη προσφορά κερδίζει τη δημοπρασία, είναι δηλαδή επιτυχής. Τα αποτελέσματα ανακοινώνονται σε όλους τους χρήστες του συστήματος καθώς και (προαιρετικά) σε εξωτερικούς παρατηρητές.

- **Ένα Σύστημα Αναμετάδοσης Κρυπτογραφημένου Υλικού** (broadcast encryption) [Mag01_1], όπως για παράδειγμα σε κρυπτογραφικές εφαρμογές *συνδρομητικής τηλεόρασης* (pay-per-view TV). Σε αυτήν την περίπτωση οι ρόλοι του χρήστη και της Αρχής αντιστρέφονται: η Αρχή (Παροχέας) υποβάλλει μέσω Διαδικτύου κρυπτογραφημένες προσφορές στους χρήστες (πελάτες). Οι προσφορές είναι κρυπτογραφικά κλειδιά για την αποκρυπτογράφηση του υλικού που πρόκειται να αναμεταδοθεί, και επιλέγονται από ένα σύνολο πιθανών κλειδιών (π.χ. το σύνολο των ακεραίων Z_n). Οι προσφορές αποκρυπτογραφούνται από τους πελάτες και αξιολογούνται ως επιτυχείς εφόσον είναι ικανές να αποκρυπτογραφήσουν το αναμεταδιδόμενο υλικό.

- **Ένα Σύστημα Ανάκτησης Κλειδιού** (key recovery) [Bur_Mag01, Mag03]. Σε ένα τέτοιο σύστημα οι προσφορές είναι ιδιωτικά κλειδιά αποκρυπτογράφησης, επιλεγμένα από ένα σύνολο κλειδιών (π.χ. το σύνολο ακεραίων Z_n), τα οποία υποθηκεύονται στις Αρχές Ανάκτησης Κλειδιού (Key Recovery Agencies). Οι προσφορές χαρακτηρίζονται ως επιτυχείς όταν και μόνο όταν το ιδιωτικό κλειδί μπορεί να ανασκευαστεί και να αποκρυπτογραφήσει κατά τρόπο ορθό τα μηνύματα που είναι κρυπτογραφημένα με το αντίστοιχο δημόσιο κλειδί.

1.2 Απαιτήσεις Ασφάλειας στα Ηλεκτρονικά Συστήματα Συναλλαγών

Ένα ηλεκτρονικό σύστημα συναλλαγών πρέπει να πληροί τις παρακάτω βασικές ιδιότητες ασφάλειας (Σχήμα 1).

- **Αυθεντικότητα** (Authenticity). Μόνο *εξουσιοδοτημένοι* χρήστες μπορούν να υποβάλλουν έγκυρες προσφορές. Κανείς (χρήστης ή Αρχή) δεν μπορεί να *αρνηθεί την ευθύνη* για πράξεις που τελεί κατά τη διάρκεια της εφαρμογής. Το τελευταίο σημαίνει πως σε περίπτωση αντιδικίας, ένα τρίτο μέρος μπορεί να επιλύσει τις όποιες διαφωνίες, κατά τρόπο αδιαμφισβήτητο.

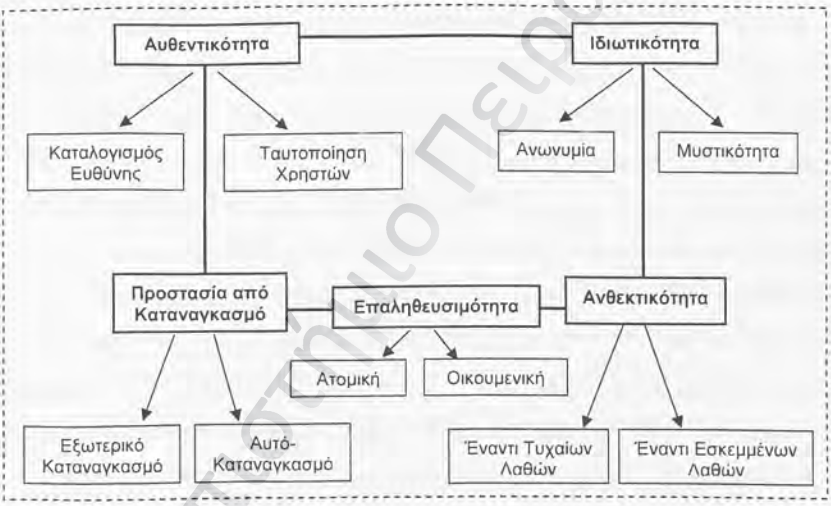
- **Ιδιωτικότητα** (Privacy). Τα ευαίσθητα προσωπικά δεδομένα (π.χ. κλειδιά, προσφορές) των χρηστών, πρέπει να περιβάλλονται από *μυστικότητα* (secrecy) ή/και από *ανωνυμία* (anonymity). Στα ανώνυμα συστήματα, η ταυτότητα του χρήστη που υπέβαλε μια προσφορά δεν πρέπει να αποκαλύπτεται σε μη εξουσιοδοτημένα άτομα.

- **Προστασία από Καταναγκασμό** (Uncoercibility), δηλαδή από επιθέσεις όπου ο χρήστης ή οι Αρχές εκβιάζονται από μια τρίτη οντότητα ώστε να άρουν την μυστικότητα μιας προσφοράς. Σε ένα παραπλήσιο σενάριο επίθεσης, ο χρήστης ή οι Αρχές παραβιάζουν εκουσίως την μυστικότητα της προσφοράς, για ίδιον όφελος. Η επίθεση αυτή έχει χαρακτηριστεί ως *αυτό-καταναγκασμός* (self-coercion) [Bur_Mag02a].

- **Επαληθευσιμότητα** (Verifiability). Η ορθότητα της διαδικασίας και η ακρίβεια των αποτελεσμάτων πρέπει να είναι πιστοποιήσιμη ανά πάσα στιγμή από τους συμμετέχοντες ή/και από εξωτερικούς παρατηρητές. Η επαληθευσιμότητα μπορεί να είναι είτε *ατομική* (atomic verifiability),

όπου η πιστοποίηση της ορθότητας της διαδικασίας και των αποτελεσμάτων έγκειται στους χρήστες, είτε *οικουμενική* (universal verifiability), όπου κάθε εξωτερικός παρατηρητής μπορεί να πιστοποιήσει την ορθότητα της διαδικασίας και των αποτελεσμάτων.

- **Ανθεκτικότητα** (Robustness). Οι παραπάνω απαιτήσεις ασφάλειας πρέπει να πληρούνται παρά την δυσλειτουργία, τυχαία ή σκόπιμη, κάποιας ή κάποιων οντοτήτων που λαμβάνουν μέρος στο σύστημα (χρήστες ή Αρχές).



Σχήμα 1. Απαιτήσεις ασφάλειας σε ηλεκτρονικά συστήματα συναλλαγών

Ορισμένες από τις παραπάνω απαιτήσεις ασφάλειας μπορούν να εκπληρωθούν με κρυπτογραφικές τεχνικές που χρησιμοποιούνται ευρέως σε εφαρμογές ηλεκτρονικού εμπορίου. Για παράδειγμα, οι απαιτήσεις της *μυστικότητας* και της *αυθεντικότητας* των δεδομένων μπορούν να εξασφαλιστούν με συστήματα κρυπτογράφησης *μυστικού* ή *δημόσιου κλειδιού* καθώς και με συστήματα *ψηφιακής υπογραφής* [Sch96,Men97]. Η δυσκολία παρουσιάζεται σε *ηλεκτρονικά συστήματα συναλλαγών* όπου η κρυπτογραφία

καλείται επιπλέον να εκπληρώσει απαιτήσεις όπως η *ανωνυμία*, η *επαληθευσιμότητα*[1], η *προστασία από καταναγκασμό* και η *ανθεκτικότητα*.

1.3 Μοντέλο Απειλής

Στα συστήματα ηλεκτρονικών συναλλαγών ελλοχεύουν σημαντικές παραβιάσεις ασφάλειας [Mag02_1]. Οι χρήστες που συμμετέχουν σε ένα τέτοιο σύστημα επιθυμούν κατά κύριο λόγο την εξασφάλιση της ιδιωτικότητας των επιλογών τους. Επιπλέον, οι χρήστες, οι Αρχές καθώς και οι εξωτερικοί παρατηρητές του συστήματος επιθυμούν την ακρίβεια και την ορθότητα της διαδικασίας. Πολλές φορές οι στόχοι αυτοί αντιτίθενται: οι χρήστες μπορεί να καταχραστούν την ιδιωτικότητα που τους παρέχεται και να δημιουργήσουν καταστάσεις οι οποίες θα οδηγήσουν στην δυσλειτουργία του συστήματος. Από την άλλη μεριά, οι Αρχές μπορεί να καταχραστούν την εξουσία που τους δόθηκε για την εξασφάλιση της ομαλής λειτουργίας του συστήματος, και να παραβιάσουν την ιδιωτικότητα των χρηστών. Στην παρούσα Διατριβή θεωρούμε ότι τόσο οι Αρχές όσο και οι χρήστες μπορούν να συμπεριφερθούν κακόβουλα.

Επιπλέον στη Διατριβή αυτή δίνεται έμφαση σε επιθέσεις όπου οι συμμετέχοντες στο σύστημα (χρήστες ή Αρχές):

- **Αρνούνται την ευθύνη** (repudiation) για την προσφορά που υπέβαλαν / έλαβαν ή για άλλες έγκυρες πράξεις που διετέλεσαν κατά τη λειτουργία του συστήματος [Mag02,Mag00]. Στην Ενότητα 1.3.1 θα παρουσιάσουμε τις πτυχές του προβλήματος, προσδιορίζοντας το στα πλαίσια συγκεκριμένων εφαρμογών.

[1] Η επαληθευσιμότητα περιλαμβάνει την ακεραιότητα των δεδομένων αλλά επίσης την επεκτείνει σε ολόκληρη τη διαδικασία: κάθε βήμα ενός πρωτοκόλλου συναλλαγών πρέπει να εκτελείται κατά τρόπο ορθό (ακέραιο), και αυτό πρέπει να είναι πιστοποιήσιμο από τους συμμετέχοντες ή/και εξωτερικούς παρατηρητές.

- **Καταναγκάζονται** (coercion), είτε *εξωτερικά* από μια τρίτη οντότητα (*εξωτερικός καταναγκασμός*) είτε *εκουσίως*, από ίδιον συμφέρον (*αυτο-καταναγκασμός*), ώστε να άρουν τη μυστικότητα των προσφορών τους [Mag01,Bur_Mag02a]. Στην Ενότητα 1.3.2 θα παρουσιάσουμε τις πτυχές του προβλήματος, προσδιορίζοντας το στα πλαίσια συγκεκριμένων εφαρμογών.

1.3.1 Καταλογισμός Ευθύνης

Στην Ενότητα αυτή συζητούμε και καταδεικνύουμε τις συνέπειες που μπορεί να έχει η άρνηση ευθύνης σε εφαρμογές ηλεκτρονικών συναλλαγών.

Συστήματα Ηλεκτρονικής Ψηφοφορίας

Στα συστήματα ηλεκτρονικής ψηφοφορίας το πρόβλημα εντοπίζεται στα κρυπτογραφικά πρωτόκολλα ηλεκτρονικής ψηφοφορίας με κεντρική διαχείριση (π.χ. [Fuj93,Rie98]), δηλαδή με τη χρήση μόνο μιας Αρχής για τη λειτουργία (εγγραφή, ψηφοφορία, καταμέτρηση) του συστήματος. Στα συστήματα αυτά, εάν ένας εξουσιοδοτημένος ψηφοφόρος α) εγγράφεται στο σύστημα και β) υποβάλλει την κρυπτογραφημένη ψήφο του, αλλά στη συνέχεια αποφασίζει να απόσχει από τις εκλογές, δηλαδή να μην αποκαλύψει το κλειδί για την αποκρυπτογράφηση της ψήφου, τότε η Αρχή μπορεί να υποβάλλει μια (παράνομη) ψήφο για λογαριασμό του ψηφοφόρου, χωρίς μάλιστα αυτό να γίνει αντιληπτό από τον ψηφοφόρο ή τους εξωτερικούς παρατηρητές [Mag02].

Ηλεκτρονικές Δημοπρασίες

Οι επιθέσεις άρνησης ευθύνης εντοπίζονται κυρίως σε Κλειστές ηλεκτρονικές δημοπρασίες κεντρικής διαχείρισης στις οποίες η μυστικότητα των προσφορών και η ανωνυμία των χρηστών προστατεύονται κρυπτογραφικά (π.χ. [Sta99,Stu99]). Σε αυτές τις δημοπρασίες, ένας χρήστης μπορεί να αρνηθεί την ευθύνη που συνεπάγεται η υποβολή της προσφοράς. Το γεγονός αυτό σημαίνει οικονομική ζημία για τον Πωλητή (και κατ' επέκταση για τον Δημοπράτη), δεδομένου ότι μια προσφορά σε μια δημοπρασία θεωρείται ένα *συμβόλαιο* μεταξύ του πωλητή και του υποψήφιου αγοραστή [Mag00].

Συστήματα Αναμετάδοσης Κρυπτογραφημένου Υλικού

Στα συστήματα αυτά ο Παροχέας αναμεταδίδει κρυπτογραφημένο υλικό και μόνον όσοι έχουν τα σωστά κλειδιά αποκρυπτογράφησης, τα οποία έχουν λάβει κάποια στιγμή στο παρελθόν από τον Παροχέα, μπορούν να το αποκρυπτογραφήσουν. Εάν ένας μη εξουσιοδοτημένος χρήστης («*πειρατής*») λάβει παράνομα ένα ακριβές αντίγραφο του κλειδιού αποκρυπτογράφησης από έναν εξουσιοδοτημένο χρήστη («*προδότης*» [Cho94]), τότε ο πειρατικός αποκωδικοποιητής θα περιέχει το κλειδί ή αλλιώς το *αποτύπωμα* (fingerprint) του «προδότη», ως ενδεικτικό της ταυτότητας του.

Το πρόβλημα εμφανίζεται σε κρυπτογραφικά συστήματα *ανίχνευσης «προδοτών»* (tracing traitors) τα οποία είναι *συμμετρικά* (π.χ. [Chor94,Kur98]), δηλαδή ο Παροχέας γνωρίζει *εκ των προτέρων* το αποτύπωμα του αγοραστή. Στα συστήματα αυτά, εάν ο Παροχέας εντοπίσει το αποτύπωμα σε έναν «πειρατικό» αποκωδικοποιητή, δεν μπορεί να καταλογίσει ευθύνη στον «προδότη» (ο «προδότης» μπορεί να ισχυριστεί ότι ο Παροχέας τοποθέτησε το αποτύπωμα του στον πειρατικό αποκωδικοποιητή ώστε να τον ενοχοποιήσει).

Συστήματα Ανάκτησης Κλειδιού

Τα συστήματα *ανάκτησης κλειδιού* (key recovery) ή αλλιώς *υποθήκευσης κλειδιού* (key escrow) [Den96] βρίσκουν εφαρμογή στους ακόλουθους τομείς:

- Στις Διαδικτυακές επικοινωνίες, με σκοπό την πρόσβαση των *υπηρεσιών επιβολής του νόμου* (law enforcement agencies) στις ηλεκτρονικές συνομιλίες πολιτών που ενέχονται σε αξιόποινες πράξεις.

- Στο περιβάλλον των επιχειρήσεων, στα πλαίσια μιας πολιτικής ασφάλειας για τη *διαχείριση των κλειδιών* (key management) των εργαζομένων, ώστε να είναι εφικτή η πρόσβαση σε αρχειοθετημένα δεδομένα, ή άλλα εταιρικά δεδομένα που ανταλλάσσονται μέσω του ενδοδικτύου (intranet) της επιχείρησης.

Οι μηχανισμοί ανάκτησης κλειδιού εφαρμόζονται σε περίπτωση *απώλειας κλειδιών* ή *άρνησης ευθύνης* από τον χρήστη που διαχειρίζεται το κρυπτογραφημένο υλικό. Ωστόσο, στη διεθνή βιβλιογραφία έχουν περιγραφεί τεχνικές με τις οποίες οι χρήστες μπορούν να παρακάμψουν τον μηχανισμό ανάκτησης, αποτρέποντας έτσι την πρόσβαση στα κρυπτογραφημένα δεδομένα που φυλάσσουν ή ανταλλάσσουν.

1.3.2 Προστασία από Καταναγκασμό

Η Προστασία από Καταναγκασμό αποτελεί σημαντική προϋπόθεση ασφάλειας σε ηλεκτρονικές συναλλαγές στις οποίες υπάρχει η ανάγκη προστασίας της ιδιωτικότητας των χρηστών από «ισχυρούς» εξωτερικούς εχθρούς (π.χ. «Μαφία», πολιτικά πρόσωπα, μυστικές υπηρεσίες, κυβερνήσεις, οικονομικά ιδρύματα, Τράπεζες κ.λ.π.) [Bur_Mag02a].

Σε όλα τα συστήματα ηλεκτρονικών συναλλαγών είναι υπαρκτός ο κίνδυνος καταναγκασμού των χρηστών/Αρχών του συστήματος που κατέχουν μυστικά, η εκχώρηση των οποίων συνιστά παραβίαση της ιδιωτικότητας των ιδίων (π.χ. όταν καταναγκάζεται ο ψηφοφόρος για να φανερώσει τη ψήφο του) ή κάποιας άλλης οντότητας του συστήματος (π.χ. όταν καταναγκάζεται η Αρχή Υποθήκευσης για να φανερώσει το κλειδί αποκρυπτογράφησης του χρήστη).

Συστήματα Ηλεκτρονικής Ψηφοφορίας

Στις παραδοσιακές εκλογές, ο ρόλος του *παραβάν* (voting booth) δεν περιορίζεται απλώς στο να επιτρέπει στους ψηφοφόρους να ρίξουν με απόλυτη μυστικότητα τη ψήφο τους στην κάλπη: η ύπαρξη του ουσιαστικά αποτρέπει επιθέσεις όπως ο καταναγκασμός και η πώληση της ψήφου. Η αποτροπή τέτοιων επιθέσεων στα συστήματα ηλεκτρονικής ψηφοφορίας αποτελεί σημαντικό κομμάτι της έρευνας για ασφαλή συστήματα [Mag01].

Πρόσφατα έχουν προταθεί αρκετά κρυπτογραφικά πρωτόκολλα τα οποία επιτυγχάνουν προστασία από καταναγκασμό καθώς και οικουμενική επαληθευσιμότητα (π.χ. [Hirt00,Oka97]). Ωστόσο, τα πρωτόκολλα αυτά επικαλούνται την ύπαρξη «φυσικά» προστατευμένων καναλιών (physically untappable channels) από την Αρχή προς τον ψηφοφόρο ή/και αντίστροφα. Τα κανάλια αυτά είναι φυσικά κανάλια μονής/διπλής κατεύθυνσης, τα οποία χρησιμοποιούν η Αρχή και ο ψηφοφόρος για να ανταλλάξουν μηνύματα με

απόλυτη μυστικότητα. Ωστόσο οι φυσικές αυτές υποθέσεις είναι μη πρακτικές, ειδικά για εκλογές μεγάλης κλίμακας που διενεργούνται μέσω Διαδικτύου [Mag01,Bur_Mag02a].

Ηλεκτρονικές Δημοπρασίες

Οι ηλεκτρονικές δημοπρασίες είναι ιδιαίτερα ευάλωτες σε «συμπαιγνίες» (collusions) μεταξύ των χρηστών, μια επίθεση γνωστή επίσης και ως Δακτύλιος (Ring): ένα σύνολο από χρήστες συμφωνούν η προσφορά τους να μην ξεπεράσει ένα ορισμένο ποσό ενώ ένας «προκαθορισμένος νικητής» θα υποβάλλει μια συγκεκριμένη προσφορά ώστε να κερδίσει τη δημοπρασία. Αυτό θα έχει ως αποτέλεσμα το αγαθό να πωλείται σε τιμή πολύ χαμηλότερη από την αναμενόμενη.

Ενώ στις παραδοσιακές δημοπρασίες η καταπολέμηση των Δακτυλίων συνήθως βασίζεται στην ανωνυμία των χρηστών [Saku00] (ώστε το μέλος του δακτυλίου που διαφοροποιείται και παρεκκλίνει από τις επιταγές του Δακτυλίου να παραμένει ατιμώρητο), στις ηλεκτρονικές δημοπρασίες, όπως εξηγούμε στο Κεφάλαιο 3, αυτό δεν είναι αρκετό [Bur_Mag02a]: κάθε χρήστης μπορεί, κατόπιν καταναγκασμού, να αποδείξει το περιεχόμενο της κρυπτογραφημένης προσφοράς του. Κάτι τέτοιο είναι δυνατό, αφού αρκεί η γνώση του κλειδιού κρυπτογράφησης και της όποιας τυχαιότητας έχει χρησιμοποιηθεί κατά την κρυπτογράφηση της προσφοράς.

Συστήματα Αναμετάδοσης Κρυπτογραφημένου Υλικού

Στα περισσότερα συστήματα ανίχνευσης «προδοτών» που έχουν προταθεί στη διεθνή βιβλιογραφία, ο Παροχέας ενδέχεται να καταναγκαστεί από τρίτες οντότητες ώστε να φανερώσει το αποτύπωμα ενός εξουσιοδοτημένου χρήστη ή

να τον ενοχοποιήσει τοποθετώντας το αποτύπωμα του σε έναν «πειρατικό» αποκωδικοποιητή.

Σε ένα άλλο παρόμοιο σενάριο ο Παροχέας αυτοβούλως εκχωρεί το ίδιο ακριβώς αποτύπωμα σε δύο ή περισσότερους χρήστες ώστε κάποιος από αυτούς να κατηγορηθεί αργότερα ως «προδότης» [Mag01_1].

Συστήματα Ανάκτησης Κλειδιού

Οι περισσότερες ενστάσεις κατά της εφαρμογής των συστημάτων ανάκτησης κλειδιού, αφορούν το ενδεχόμενο μετάβασης σε ολοκληρωτικά καθεστώτα [Abel98]. Σε αυτήν την περίπτωση, και εάν δεν υπάρχει καθορισμός της χρονικής διάρκειας ισχύος ενός κρυπτογραφικού κλειδιού που υποθηκεύεται, είναι δυνατή η μαζική παρακολούθηση, χωρίς χρονικό περιορισμό, των κρυπτογραφημένων συνομιλιών των πολιτών. Μια προϋπόθεση αυτής της επίθεσης θα μπορούσε να είναι ο καταναγκασμός των Αρχών Ανάκτησης Κλειδιού, ή ακόμα και η αυτόβουλη συνεργασία των Αρχών με το καθεστώς [Bur_Mag02a].

Άλλες Εφαρμογές

Η έννοια της Προστασίας από Καταναγκασμό μπορεί να βρει πολλές εφαρμογές στον ευρύτερο τομέα των ηλεκτρονικών συναλλαγών μέσω του Διαδικτύου. Για παράδειγμα, σε εφαρμογές όπως [Bur_Mag02a]:

Ανώνυμο Ηλεκτρονικό Χρήμα (Anonymous e-Cash). Το ανώνυμο ηλεκτρονικό χρήμα χρησιμοποιείται σε ηλεκτρονικές συναλλαγές οι οποίες πρέπει, όπως και τα μετρητά στην καθημερινή μας ζωή, να είναι *ανεξιχνίαστες* (untraceable) [Cha82,Cha85]. Δηλαδή ένας χρήστης θα λαμβάνει ηλεκτρονικό χρήμα από την τράπεζα χωρίς η τράπεζα να μπορεί να συσχετίσει το όνομα

του χρήστη με τα χρήματα που του διανέμονται, και που αργότερα θα περιέλθουν στην κατοχή π.χ. ενός εμπόρου. Αυτό επιτυγχάνεται με τη χρήση του μηχανισμού των *«τυφλών» υπογραφών* (Κεφάλαιο 3, Ενότητα 3.5.1). Κατά τη διάρκεια ενός τέτοιου μηχανισμού η Alice προσθέτει τυχαιότητα (randomness) σε ένα ηλεκτρονικό νόμισμα, και το υποβάλλει στην τράπεζα για έγκριση. Η τράπεζα υπογράφει ψηφιακά το νόμισμα και το επιστρέφει στην Alice, η οποία αφαιρεί την τυχαιότητα με τέτοιο τρόπο ώστε το νόμισμα να μην απολέσει την εγκυρότητα του [Cha85].

Σύμφωνα με ένα πιθανό σενάριο επίθεσης [Bur_Mag02a], η Alice μπορεί να *κατανα)γκαστεί* ώστε να φανερώσει την τυχαιότητα που χρησιμοποίησε στο πρωτόκολλο με την τράπεζα και έτσι να αποκαλυφθούν οι οικονομικές της δοσοληψίες. Εναλλακτικά, ένας αυτό-καταναγκαζόμενος χρήστης θα μπορούσε να επιλέξει την τυχαιότητα κατά τέτοιον τρόπο ώστε να αποδείξει αργότερα σε κάποιον τρίτο, ενδεχομένως έναντι αμοιβής, τις λεπτομέρειες των δοσοληψιών του. Σε ένα πρωτόκολλο ηλεκτρονικού χρήματος με Προστασία από Καταναγκασμό (uncoercible e-cash), κάτι τέτοιο δε θα ήταν δυνατό [Bur_Mag02a].

Ηλεκτρονική Χρηματοδότηση Πολιτικής Εκστρατείας (Campaign e-Finance). Ένα πιθανό σενάριο επίθεσης αφορά πολιτικές εκστρατείες υποψηφίων. Κατά τη διάρκεια μιας τέτοιας εκστρατείας ο υποψήφιος μπορεί να αποσπάσει χρήματα από δωρητές, χρησιμοποιώντας μη θεμιτά μέσα (π.χ. απειλώντας με δυσμένεια στην περίπτωση που εκλεγεί) [Fra00]. Αντίστοιχα, ένας δωρητής μπορεί να επιθυμεί να αποδείξει στον υποψήφιο ότι έκανε μια δωρεά προκειμένου να αποκτήσει επιρροή σε αυτόν (αυτό-καταναγκασμός). Ένα πρωτόκολλο ηλεκτρονικών δωρεών Προστατευμένο από Καταναγκασμό (uncoercible e-donation), θα επέτρεπε στους δωρητές να προβούν σε δωρεές προς έναν υποψήφιο, χωρίς να μπορούν αργότερα να αποδείξουν τη δωρεά τους [Bur_Mag02a].

1.4. Αντικείμενο και Στόχοι της Διατριβής

Το αντικείμενο της Διδακτορικής Διατριβής είναι η αναζήτηση κρυπτογραφικών μηχανισμών για την εκπλήρωση των απαιτήσεων ασφάλειας σε ηλεκτρονικά συστήματα συναλλαγών, στα οποία θεωρούμε ότι τόσο οι χρήστες όσο και οι Αρχές του συστήματος μπορούν να συμπεριφερθούν κακόβουλα. Στο πλαίσιο αυτό, οι βασικοί επιμέρους στόχοι ήταν:

α) Ο Σχεδιασμός *«Δίκαιων»* (Equitable) Συστημάτων. Ως «δίκαιο» ονομάζουμε ένα σύστημα στο οποίο διατηρείται μια ισορροπία μεταξύ της ανάγκης των χρηστών για ιδιωτικότητα και της ανάγκης της «κοινωνίας» για ακρίβεια και ορθότητα των αποτελεσμάτων [Mag02]. Με τον όρο «κοινωνία» εννοούμε τις Αρχές, τους χρήστες του συστήματος, τις οντότητες που έχουν έννομο ή άλλο άμεσο/έμμεσο συμφέρον από την ηλεκτρονική συναλλαγή, καθώς και τους εξωτερικούς παρατηρητές.

Στην κατηγορία των «Δίκαιων» συστημάτων ηλεκτρονικών συναλλαγών κατατάσσουμε επίσης τα συστήματα εκείνα τα οποία θα μπορούν να επιλύουν τα ζητήματα *άρνησης ευθύνης* (Ενότητα 1.3.1), προστατεύοντας παράλληλα την ιδιωτικότητα των χρηστών του συστήματος.

β) Ο Σχεδιασμός Συστημάτων με Προστασία από Καταναγκασμό. Σε ένα τέτοιο σύστημα, θα επιτυγχάνεται προστασία τόσο έναντι σεναρίων εξωτερικού καταναγκασμού, όσο και έναντι σεναρίων αυτό-καταναγκασμού, όπου ο χρήστης επιθυμεί την κατάργηση της ιδιωτικότητας της προσφοράς του για ίδιον όφελος.

1.5. Δομή της Διατριβής

Η παρούσα Διδακτορική Διατριβή περιλαμβάνει έξι (6) Κεφάλαια.

Στο Κεφάλαιο 1 «*Εισαγωγή*» περιγράφεται το γνωστικό αντικείμενο, οι γενικότεροι στόχοι, η δομή της Διατριβής και η συνεισφορά στην ερευνητική περιοχή.

Στο Κεφάλαιο 2 «*Ασφάλεια σε Συστήματα Ηλεκτρονικής Ψηφοφορίας*» εξετάζονται οι διάφοροι τύποι συστημάτων ηλεκτρονικής ψηφοφορίας από τη σκοπιά της ασφάλειας, αναφέρονται τα κρυπτογραφικά μοντέλα υλοποίησης ηλεκτρονικής ψηφοφορίας που έχουν προταθεί στη διεθνή βιβλιογραφία και συζητούνται τρόποι αντιμετώπισης των προβλημάτων ασφάλειας στα συστήματα ηλεκτρονικής ψηφοφορίας. Προτείνονται ένα κρυπτογραφικό πρωτόκολλο για την επίτευξη προστασίας από καταναγκασμό καθώς και ένα «δίκαιο» πρωτόκολλο για καταλογισμό ευθύνης σε ηλεκτρονικές εκλογές που διεξάγονται στο Διαδίκτυο.

Στο Κεφάλαιο 3 «*Ασφάλεια στις Ηλεκτρονικές Δημοπρασίες*» καταδεικνύονται τα ζητήματα ασφάλειας που τίθενται κατά τη σχεδίαση και υλοποίηση συστημάτων ηλεκτρονικών δημοπρασιών, αναφέρονται τα βασικά κρυπτογραφικά μοντέλα που απαντώνται στη διεθνή βιβλιογραφία και περιγράφεται ένα «δίκαιο» πρωτόκολλο ηλεκτρονικής δημοπρασίας για καταλογισμό ευθύνης στους χρήστες που υποβάλλουν προσφορά αλλά στη συνέχεια αποφασίζουν να την αποσύρουν. Επίσης περιγράφεται ένα πρωτόκολλο με προστασία από καταναγκασμό για τους υποψήφιους αγοραστές.

Στο Κεφάλαιο 4 «*Ανίχνευση 'Προδοτών' σε Συστήματα Αναμετάδοσης Κρυπτογραφημένου Υλικού*» αναλύονται, από άποψη ασφάλειας και πρακτικότητας, τα σχήματα ανίχνευσης «προδοτών» που έχουν προταθεί στη

διεθνή βιβλιογραφία για την προστασία των πνευματικών δικαιωμάτων σε εφαρμογές αναμετάδοσης κρυπτογραφημένου υλικού και προτείνεται ένα «δίκαιο» σχήμα ανίχνευσης «προδοτών» χωρίς τρίτη έμπιστη οντότητα, όπου ο παροχέας του υλικού δε γνωρίζει εκ των προτέρων το αποτύπωμα που περιέχει ο αποκωδικοποιητής ενός εξουσιοδοτημένου χρήστη.

Στο Κεφάλαιο 5 «*Ασφάλεια σε Συστήματα Ανάκτησης Κλειδιού*» αναλύονται οι μηχανισμοί ασφάλειας των συστημάτων ανάκτησης κλειδιού και προτείνεται ένα «δίκαιο» πρωτόκολλο ανάκτησης κλειδιού για την αποκρυπτογράφηση, σε περίπτωση απώλειας κλειδιών ή αξιόποινων πράξεων, των κρυπτογραφημένων συνομιλιών ενός χρήστη που αφορούν μία συγκεκριμένη χρονική περίοδο, ή των αρχειοθετημένων δεδομένων του. Επίσης προτείνεται ένα μοντέλο για την αντιμετώπιση επιθέσεων όπου οι χρήστες παρακάμπτουν το μηχανισμό ανάκτησης κλειδιού με σκοπό τη μη αποκρυπτογράφηση της πληροφορίας από τις Αρχές.

Στο Κεφάλαιο 6 «*Συμπεράσματα της Διατριβής*» συνοψίζονται τα γενικότερα συμπεράσματα από την εκπόνηση της Διατριβής.

1.6 Συνεισφορά στην Ερευνητική Περιοχή - Δημοσιεύσεις

Σε αυτήν τη Διατριβή μελετώνται και προτείνονται κρυπτογραφικά πρωτόκολλα [Bur_Mag01,Mag01,Bur_Mag02b,Mag02,Bur_Mag02a,Mag02_1, Mag01_1,Mag00,Mag01_2,Mag03], με σκοπό την εκπλήρωση των απαιτήσεων ασφάλειας και πρακτικότητας σε ένα ηλεκτρονικό σύστημα συναλλαγών.

Συστήματα Ηλεκτρονικής Ψηφοφορίας. Παρουσιάζουμε ένα «δίκαιο» κρυπτογραφικό πρωτόκολλο [Mag02] το οποίο προστατεύει τη μυστικότητα και την ανωνυμία των ψήφων, καταλογίζοντας παράλληλα ευθύνη στους ψηφοφόρους για κρυπτογραφημένες ψήφους που έχουν ήδη υποβληθεί: όλοι

θα πρέπει να ακολουθήσουν την προβλεπόμενη διαδικασία και να αποκαλύψουν κατά τη φάση της καταμέτρησης το κλειδί αποκρυπτογράφησης της ψήφου. Αν δεν το πράξουν (άρνηση ευθύνης), η ταυτότητα τους θα αποκαλυφθεί.

Επίσης αναλύουμε τις ιδιαίτερες παραμέτρους του προβλήματος του καταναγκασμού στα συστήματα ηλεκτρονικής ψηφοφορίας, καθορίζουμε τις ελάχιστες απαιτήσεις ασφάλειας που πρέπει να τηρούνται και παρουσιάζουμε ένα πρωτόκολλο [Mag01] το οποίο επιτυγχάνει Προστασία από Καταναγκασμό με τη χρήση Έξυπνων Καρτών που συνεισφέρουν κάποια τυχαιότητα στην κρυπτογράφηση της ψήφου, με τρόπο που δεν αφήνει περιθώρια κακόβουλων ενεργειών στον χρήστη ή στην κάρτα. Η προσέγγιση μας παρουσιάζει ιδιαίτερο ενδιαφέρον, επειδή είναι ιδανική για εφαρμογές όπου το κανάλι επικοινωνίας είναι ανοικτό, και επομένως ευάλωτο σε ωτακουστές.

Ηλεκτρονικές Δημοπρασίες. Προτείνουμε ένα σύστημα ηλεκτρονικών δημοπρασιών που είναι «δίκαιο» [Mag00] για τους χρήστες και τους δημοπράτες. Αυτό σημαίνει πως το σύστημα προστατεύει την ταυτότητα των χρηστών (ανωνυμία) και την μυστικότητα των προσφορών τους, καταλογίζοντας παράλληλα ευθύνη για υποβληθείσες προσφορές. Επιγραμματικά:

- Παρέχεται ανωνυμία στους χρήστες,
- Κανείς χρήστης δε μπορεί να αποσύρει την προσφορά του.

Επίσης παρουσιάζουμε ένα δεύτερο κρυπτογραφικό πρωτόκολλο [Bur_Mag02a] που εκπληρώνει όλες τις απαιτήσεις ασφάλειας για ηλεκτρονικές δημοπρασίες μέσω Διαδικτύου και επιπλέον παρέχει οικουμενική επαληθευσιμότητα για τα τελικά αποτελέσματα καθώς και προστασία από καταναγκασμό: κανένας χρήστης δε μπορεί να αποδείξει την τιμή της προσφοράς του, ακόμα και αν το επιθυμεί ο ίδιος.

Ανίχνευση «Προδοτών». Περιγράφουμε ένα «δίκαιο» πρωτόκολλο ασύμμετρης ανίχνευσης «προδοτών» [Mag01_1] χωρίς τη χρήση τρίτων έμπιστων οντοτήτων, όπου ο Παροχέας δε γνωρίζει το αποτύπωμα του αγοραστή, αλλά παράλληλα μπορεί να ανιχνεύσει έναν «προδότη» από το αποτύπωμα του. Ως αποτέλεσμα, οι «προδότες» δε μπορούν να αρνηθούν ευθύνη για τα αποτυπώματα τους, ενώ οι Παροχείς δε μπορούν να ενοχοποιήσουν άδικα έναν ανυποψίαστο χρήστη. Στο πρωτόκολλο αυτό ενσωματώνουμε επιπλέον ελέγχους ορθότητας ώστε ο παροχέας να μη μπορεί να συμπεριφερθεί κακόβουλα και να ενοχοποιήσει άδικα έναν χρήστη του συστήματος. Το πρωτόκολλο μπορεί να χρησιμοποιηθεί για την ανίχνευση «προδοτών» σε εφαρμογές αναμετάδοσης πληροφοριών όπως συνδρομητική τηλεόραση (pay-per-view), παροχή ηλεκτρονικών υπηρεσιών σε πραγματικό χρόνο μέσω Web, διανομή CD-ROM με εμπορικό software κ.λ.π.

Ανάκτηση Κλειδιού. Προτείνουμε ένα «δίκαιο» σύστημα ανάκτησης κλειδιού [Bur_Mag01] με το οποίο οι Αρχές Επιβολής Νόμου έχουν την δυνατότητα να αποκρυπτογραφούν τα κρυπτογραφημένα μηνύματα ενός χρήστη που αφορούν μια συγκεκριμένη χρονική περίοδο. Ο μηχανισμός μας προσφέρει *ισχυρή χρονική ασφάλεια* (strong forward security) [Bur_Mag01], δηλαδή η παρακολούθηση των κρυπτογραφημένων συνομιλιών του χρήστη είναι δυνατή κατά το χρονικό διάστημα που ορίζει το ένταλμα παρακολούθησης, και όχι για συνομιλίες που αφορούν περιόδους πριν ή μετά από αυτό το διάστημα, ακόμα και στην περίπτωση καταναγκασμού των χρηστών ή των Αρχών Ανάκτησης Κλειδιού [Bur_Mag01].

Στη συνέχεια προτείνουμε ένα *υβριδικό* μοντέλο ανάκτησης κλειδιού [Mag03], το οποίο απευθύνεται κυρίως στο περιβάλλον των επιχειρήσεων, για την αντιμετώπιση επιθέσεων κατά τις οποίες οι χρήστες μεταχειρίζονται τεχνικές *διπλής κρυπτογράφησης* για να αποτρέψουν την πρόσβαση στις αποκρυπτογραφημένες συνομιλίες τους ή τα αρχειοθετημένα δεδομένα τους. Η ιδιαιτερότητα της επίθεσης συνίσταται στο ότι οι χρήστες επιστρατεύουν το

κρυπτοσύστημα που προβλέπεται από το μηχανισμό ανάκτησης ως «δούρειο ίππο» για την παράκαμψη του συστήματος ανάκτησης κλειδιού. Στο μοντέλο που προτείνουμε επικαλούμαστε έναν συνδυασμό από παραδοσιακές τεχνικές *υποθήκευσης κλειδιού* μακράς διαρκείας καθώς και τεχνικές ανάκτησης *κλειδιών συνόδου* (περιορισμένης διαρκείας), ώστε η εφαρμογή του μοντέλου να μη συνιστά υψηλή πολυπλοκότητα για τους χρήστες και τις Αρχές.

Στα πλαίσια των παραπάνω συνεισφορών στον ευρύτερο χώρο της ασφάλειας σε συστήματα ηλεκτρονικών συναλλαγών, δημοσιεύτηκαν ερευνητικές εργασίες τόσο σε διεθνή επιστημονικά συνέδρια με έκδοση πρακτικών μετά από κρίση πλήρους κειμένου, όσο και σε διεθνή επιστημονικά περιοδικά:

- Magkos, E. Burmester, M., and Chrissikopoulos, V.: An Equitably Fair On-line Auction Scheme. In: Proceedings of the 1st International Conference on Electronic Commerce and Web technologies – ECWEB '2000, Lecture Notes in Computer Science, Vol. 1875, Springer-Verlag, pp. 72-84, 2000.

- Burmester, M., Chrissikopoulos, V., Kotzanikolaou, P., and Magkos, E.: Strong Forward Security. In: Proceedings of the International Information Security Conference IFIP-SEC '01, Kluwer Academic Publishers, pp. 109-119, 2001.

- Magkos, E., Burmester, M., and Chrissikopoulos V.: Receipt-Freeness in Large-scale Elections without Untappable Channels. In: Proceedings of the 1st IFIP Conference on E-Commerce/E-business/E-Government, Kluwer Academic Publishers, pp. 683-693, 2001.

- Magkos, E., Kotzanikolaou, P., and Chrissikopoulos, V.: An Asymmetric Traceability Scheme for Copyright Protection without Trust Assumptions. In: Proceedings of the 2nd International Conference on

Electronic Commerce and Web technologies - ECWEB '2001, Lecture Notes in Computer Science, Vol. 2115, Springer-Verlag, pp. 186-195, 2001.

- Magkos, E., Chrissikopoulos, V., and Alexandris, N.: Software-based Receipt-Freeness in On-line Elections. In: Proceedings of the IFIP TG11-WG11.4 1st Annual Working Conference on Network Security, Kluwer Academic Publishers, pp. 33-43, 2001.

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

- Magkos, E., Chrissikopoulos, V., and Alexandris, N.: A Common Security Model for Conducting e-Auctions and e-Elections. In: Proceedings of the 6th WSEAS International Conference on Communications, WSEAS Press, pp. 463-467, 2002.

- Burmester, M., Magkos, E., and Chrissikopoulos, V.: Uncoercible e-bidding Games. In: Electronic Commerce Research Journal, Special Issue on Security Aspects in E-Commerce, Kluwer Academic Publishers. To be published, 2003.

- Burmester, M., and Magkos, E.: Towards Secure and Practical e-Elections in the New Era. In: Advances in Information Security - Secure Electronic Voting, Kluwer Academic Publishers pp. 63-76, 2003.

- Magkos, E.: A Hybrid Key Recovery Scheme. Cyprus Computer Society Journal "Pliroforiki", Issue 3. To be published, 2003.

1.7 Ευχαριστίες

Αρχικά, θα ήθελα να ευχαριστήσω τον Καθηγητή κ. Βασίλειο Χρυσικόπουλο για τη συμπαράσταση, αρωγή και στήριξη που μου προσέφερε κατά τη διάρκεια εκπόνησης της Διδακτορικής μου Διατριβής. Επίσης, θα ήθελα να ευχαριστήσω τον Καθηγητή κ. Νίκο Αλεξανδρή για την επιλογή του προσώπου μου ως υποψήφιο Διδάκτορα, τις πολύτιμες συμβουλές του ως επιβλέπων Καθηγητής μου, και τη σχέση που αναπτύξαμε από την θητεία μου ως φοιτητής στο Πανεπιστήμιο Πειραιώς έως σήμερα.

Θα ήθελα να αναφερθώ ξεχωριστά στον άνθρωπο και επιστήμονα Καθηγητή κ. Mike Burmester, που στάθηκε δίπλα μου όποτε τον χρειάστηκα, προσφέροντας αμέριστα τις νουθεσίες του και τις γνώσεις του.

Επίσης οφείλω ευχαριστίες προς τα υπόλοιπα μέλη της Συμβουλευτικής και της επταμελούς Εξεταστικής Επιτροπής: κ. Γεώργιο Τσιχριτζή (Επίκουρος Καθηγητής Πανεπιστημίου Πειραιώς), κ. Σωκράτη Κάτσικα (Καθηγητής Πανεπιστημίου Αιγαίου), κ. Σπύρο Λυκοθανάση (Αναπληρωτής Καθηγητής Πανεπιστημίου Πατρών), κ. Δημήτρη Γκρίτζαλη (Επίκουρος Καθηγητής Οικονομικού Πανεπιστημίου Αθηνών), και κ. Χρήστο Δουληγέρη (Αναπληρωτής Καθηγητής Πανεπιστημίου Πειραιώς), για τα εποικοδομητικά τους σχόλια κατά την τελική φάση μελέτης και παρουσίασης της παρούσας Διατριβής.

Επιθυμώ ακόμα να ευχαριστήσω τους φίλους και συναδέλφους κκ. Σπύρο Βοσινάκη, Πάνο Κοτζανικολάου και Γιάννη Παπαδάκη γιατί στάθηκαν δίπλα μου όλα αυτά τα χρόνια. Επίσης, τους υποψήφιους διδάκτορες Βικτόρια Τσιρίγκα, Κατερίνα Καμπάση και Μαρία Μουντρίδου, με τις οποίες είχα την τύχη να βρίσκομαι στον ίδιο χώρο κατά τη διάρκεια της θητείας μου ως υποψήφιος Διδάκτωρ.

Τέλος, ευχαριστώ την οικογένεια μου για την αγάπη και την υπομονή τους.

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[2], 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

[2] 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[3] (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»[4] σύνδεσης Διαδικτύου ή μέσω του δικτύου ATM[5] [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

[3] 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).

[4] 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).

[5] 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[6], δηλαδή:

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

[6] 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[7] 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

[7] 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

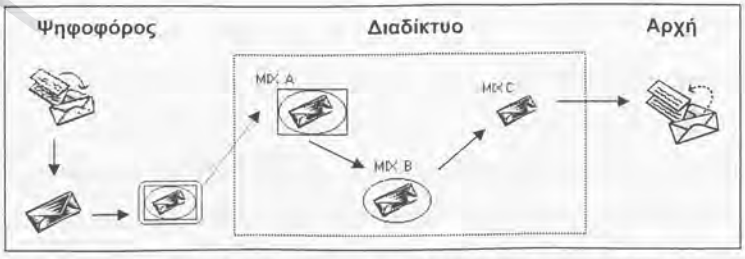
Τα βασικά κρυπτογραφικά μοντέλα ηλεκτρονικής ψηφοφορίας που έχουν προταθεί έως σήμερα είναι τέσσερα: το μοντέλο *MIX-net* [Cha81], το μοντέλο των *«τυφλών» υπογραφών* (blind signatures) [Fuj93], το *μοντέλο του Benaloh* [Ben87] και το *ομομορφικό μοντέλο* [Cra97].

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[8].

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

[8] 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*[9] (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

[9] 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 *ανθεκτικότητα* (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* [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*[10] (proactive security) [Herz97] καθώς και με τεχνικές *ισχυρής χρονικής ασφάλειας* (strong forward security - Ενότητα 5.4.1) [Bur_Mag01].

[10] 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*[11] [Bel93]

[11] 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*[12] (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.

[12] 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*[13] [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*[14] (randomness), αλλιώς το

[13] 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.

[14] 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 $q \mid p-1$, 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 mod 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 $G^T = Y / X^x$. Τελικά το αποτέλεσμα T καθορίζεται με $O(\ell)$ modular πολλαπλασιασμούς.

Στο ανωτέρω σχήμα η μυστικότητα της ψήφου βασίζεται στο *πρόβλημα εύρεσης Διακριτού Λογαρίθμου*[15] [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.

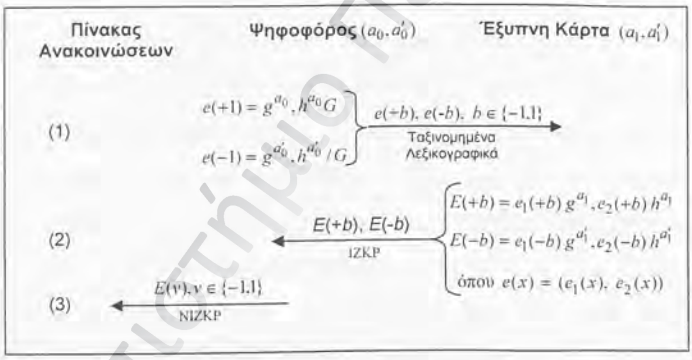
Σημείωση: Πρέπει να τονίσουμε ότι για μεγάλο αριθμό υποψηφίων, ο μόνος τρόπος να υπολογιστεί η αποκρυπτογραφημένη κάλπη είναι με εντατικούς υπολογισμούς : εάν ℓ είναι ο αριθμός των ψηφοφόρων και r είναι ο αριθμός των υποψηφίων, η πολυπλοκότητα των υπολογισμών είναι εκθετική ως προς τον αριθμό r : $((\Omega(\ell^{(r-1)/2}))$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

[15] 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[16] (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

[16] 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[17] στο χρήστη ότι $\log(g^{a_1}) = \log(h^{a_1})$ και $\log(g^{a'_1}) = \log(h^{a'_1})$, 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[18] το κρυπτογράφημα $E(v)$, πρέπει να κατασκευαστεί μια *απόδειξη εγκυρότητας* της ψήφου, δηλαδή ότι το $E(v)$ περιέχει μια ψήφο

---

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

[18] 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[19] *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.

---

[19] 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[20] του εκλογικού συστήματος. Στη συνέχεια θα δείξουμε [Mag02] ότι το πρόβλημα των απεχόντων ψηφοφόρων μπορεί να οδηγήσει και σε παραβίαση της Ακρίβειας (τρίτη ιδιότητα[21]) 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,

---

[20] α) Μόνο εξουσιοδοτημένοι ψηφοφόροι μπορούν να υποβάλλουν ψήφους, και β) Κανένας ψηφοφόρος δε μπορεί να υποβάλει περισσότερες από μια ψήφους (Ενότητα 2.2.1).

[21] 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[22]. 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

[22] 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 $X = a^{2^t} \pmod{n}$, 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[23]. 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.

[23] 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:

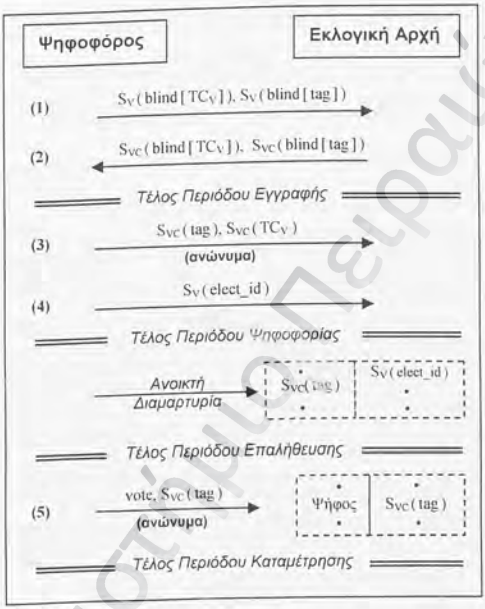
- V : ο Ψηφοφόρος.
- VC : το Εκλογικό Κέντρο.
- $S_x(m)$: η υπογραφή στο μήνυμα m με το ιδιωτικό κλειδί του x.
- $Blind(m)$: προετοιμασία ενός μηνύματος m ώστε να υπογραφεί «τυφλά».
- TC_m : κρυπτογραφική κάψουλα που περιέχει το μήνυμα m.
- Tag : η δέσμευση ψήφου (π.χ. κρυπτογράφηση με ένα DES κλειδί).
- $Elect_{id}$: 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[24] 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

[24] 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*[25] (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

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

συμμετοχή του στη ψηφοφορία, αποστέλλοντας επώνυμα μια *δήλωση ανα)γνώρισης* (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 δημοσιεύει 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).

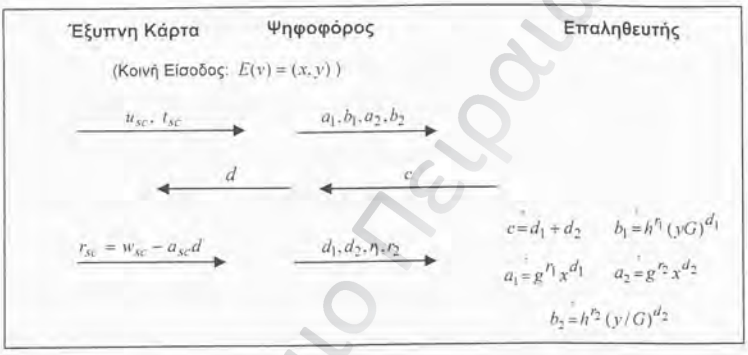
- Έμφαση στο σχεδιασμό «τεχνολογικά ουδέτερων» συστημάτων (πλατφόρμες, αρχιτεκτονικές, εργαλεία πλοήγησης).

- 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).

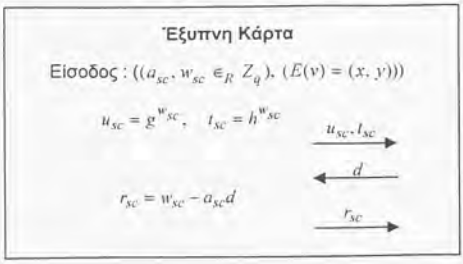
Παράρτημα Α - Απόδειξη Εγκυρότητας Ψήφου σε Εκλογές Προστατευμένες από Καταναγκασμό

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].

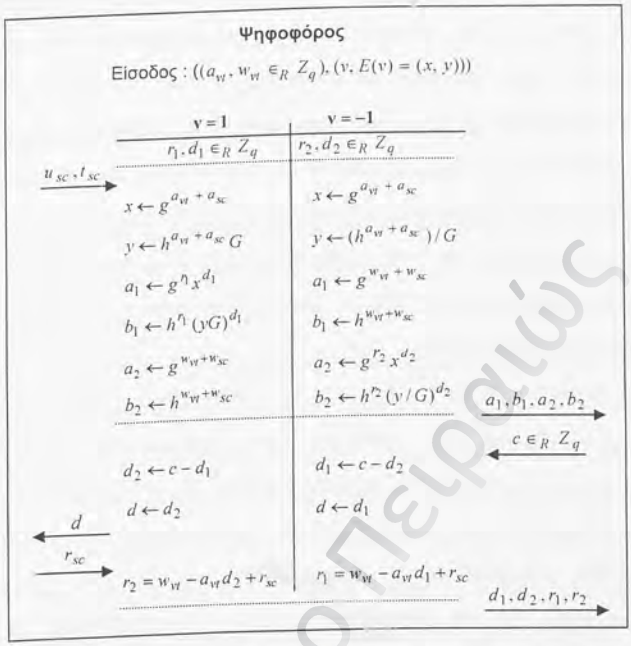


Σχήμα 7. Πρωτόκολλο για την απόδειξη εγκυρότητας της κρυπτογραφημένης ψήφου

Η κοινή είσοδος του ψηφοφόρου και της Κάρτας είναι το $E(v) = (x, y) = (g^{a_{sc}+a_{vi}}, h^{a_{sc}+a_{vi}} G^v)$, 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:

$$\log_g x = \log_h (y/G) \quad \acute{\eta} \quad \log_g x = \log_h (y/G^{-1}) \quad (1)$$

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].

Κεφάλαιο 3

Ασφάλεια στις Ηλεκτρονικές Δημοπρασίες

Στο Κεφάλαιο αυτό καταδεικνύουμε τα προβλήματα ασφάλειας και τις απαιτήσεις που πρέπει να πληροί ένα σύστημα ηλεκτρονικής δημοπρασίας στο Διαδίκτυο. Καταγράφουμε τα βασικά κρυπτογραφικά μοντέλα που απαντώνται στη διεθνή βιβλιογραφία και παρουσιάζουμε ένα πρωτόκολλο για Κλειστές ηλεκτρονικές Δημοπρασίες όπου η μυστικότητα των προσφορών δε βασίζεται σε τρίτη έμπιστη οντότητα ή σε κατανεμημένους εξυπηρετητές. Το πρωτόκολλο είναι «δίκαιο» υπό την έννοια ότι προστατεύει την ιδιωτικότητα των χρηστών χωρίς να τους επιτρέπει να αποσύρουν μια προσφορά που ήδη υπέβαλαν. Επίσης, παρουσιάζουμε ένα πρωτόκολλο Κλειστής ηλεκτρονικής Δημοπρασίας με κατανεμημένους δημοπράτες, στο οποίο παρέχεται προστασία από καταναγκασμό για όλους τους χρήστες, καθώς και οικουμενική επαληθευσιμότητα για τα τελικά αποτελέσματα.

3.1 Εισαγωγή

Οι δημοπρασίες (auctions), ως ένας διαπραγματευτικός μηχανισμός για την πώληση/αγορά αγαθών απροσδιόριστης αξίας [Vic61,Mil89], αποτελούν ένα ιδιαίτερο κομμάτι της οικονομικής ζωής στις σύγχρονες κοινωνίες. Σε αρκετές περιπτώσεις, η επιλογή μιας δημοπρασίας για την πώληση ενός αγαθού είναι προτιμότερη από την θέσπιση σταθερών και αδιαπραγμάτευτων τιμών για το αγαθό. Το ιδιαίτερο χαρακτηριστικό των δημοπρασιών είναι το γεγονός ότι η τιμή δεν αποφασίζεται από τον πωλητή, αλλά από τους αγοραστές. Ο πωλητής απλά θέτει τους κανόνες, αποφασίζοντας π.χ. τη μορφή που θα έχει η δημοπρασία, ενώ ο δημοπράτης λειτουργεί ως μεσολαβητής για λογαριασμό του πωλητή στη διαπραγμάτευση του με τους χρήστες (bidders).

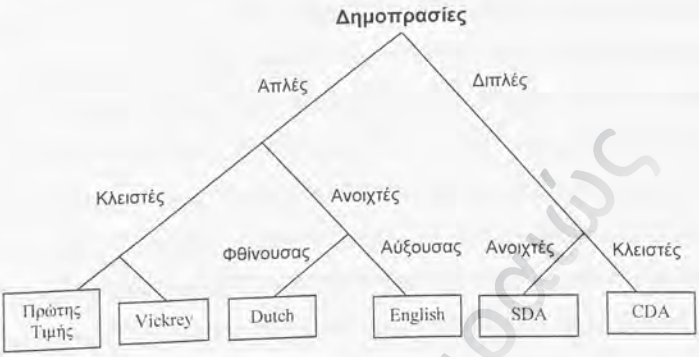
Οι *ηλεκτρονικές δημοπρασίες* (e-auctions), ως υπηρεσίες προστιθέμενης αξίας, παρέχουν σημαντικά επιχειρησιακά πλεονεκτήματα στον πωλητή αλλά και υπηρεσίες στον υποψήφιο αγοραστή [Chu00]. Μια τυπική εμπορική συναλλαγή ολοκληρώνεται σε τρία διακριτά στάδια: πρώτον, οι υποψήφιοι αγοραστές και οι πωλητές πρέπει να εντοπίσουν ο ένας τον άλλον, στη συνέχεια να διαπραγματευτούν τους όρους της συναλλαγής και τέλος να εκτελέσουν τη συναλλαγή καθ' αυτή. Τα συστήματα ηλεκτρονικών πληρωμών (electronic payments), που χρησιμοποιούνται ευρέως στο Διαδίκτυο [Sta02], έχουν αυτοματοποιήσει ως ένα βαθμό το τρίτο στάδιο μιας συναλλαγής. Εντούτοις οι αυτοματοποιημένες διαπραγματεύσεις μεταξύ αγοραστών και πωλητών δεν έχουν λάβει τη δέουσα προσοχή έως σήμερα. Η *θεωρία δημοπρασιών* (auction theory) καλείται λοιπόν να διαδραματίσει ένα σημαντικό ρόλο στα πρωτόκολλα διαπραγμάτευσης στο ηλεκτρονικό εμπόριο [Wur98].

Η στρατηγική που ένας υποψήφιος αγοραστής υιοθετεί κατά τη διάρκεια μιας δημοπρασίας αποτελεί ένα σημαντικό κομμάτι της θεωρίας των δημοπρασιών. Οι οικονομολόγοι αξιοποιούν κυρίως συμπεράσματα και γνώσεις που άπτονται της *θεωρίας παιγνίων* (game theory) [Mil89] ώστε να εξετάσουν ορθολογικά τη συμπεριφορά των συμμετεχόντων σε μια δημοπρασία, καθώς και τις αποφάσεις που λαμβάνονται κάτω από διαρκώς εναλλασσόμενες συνθήκες [Kle99,Mil89]. Στην παρούσα Διατριβή δε θα ασχοληθούμε με την πτυχή αυτή των δημοπρασιών, αλλά με τα προβλήματα ασφάλειας που αφορούν τις ηλεκτρονικές δημοπρασίες που διενεργούνται μέσω Διαδικτύου.

3.1.1 Τύποι Δημοπρασιών

Ο W. Vickrey [Vic61] κατηγοριοποίησε τις δημοπρασίες με βάση τον τρόπο με τον οποίο υποβάλλονται οι προσφορές, καθώς και τον τρόπο αξιολόγησης και καταμέτρησης των προσφορών (Σχήμα 10). Έτσι, μια ηλεκτρονική

δημοπρασία εμπίπτει σε μια από τις ακόλουθες κατηγορίες [Mil89,Cramp98, Mag00]:



Σχήμα 10. Μία κατηγοριοποίηση των δημοπρασιών

- **Ανοικτή Δημοπρασία Αύξουσας Τιμής** (Open Ascending). Στην αρχή της δημοπρασίας ο Δημοπράτης ανακοινώνει μια *ελάχιστη αποδεκτή τιμή* (reserve price) πώλησης του αγαθού. Στη συνέχεια δέχεται προσφορές από τους συμμετέχοντες. Κάθε προσφορά που υποβάλλεται γίνεται δεκτή εφόσον είναι μεγαλύτερη από την τελευταία υψηλότερη προσφορά. Η δημοπρασία ολοκληρώνεται όταν, και για συγκεκριμένο χρονικό διάστημα, δεν υπάρξει υψηλότερη προσφορά. Οι δημοπρασίες αυτού του τύπου αποκαλούνται συχνά και *Αγγλικές δημοπρασίες* (English auctions) [Cramp98].

  Σχεδόν όλες οι ηλεκτρονικές δημοπρασίες που διενεργούνται μέσω Διαδικτύου ανήκουν σε αυτήν την κατηγορία. Ένα πλεονέκτημα στην επιλογή μιας τέτοιας δημοπρασίας είναι ότι το αγαθό τελικά θα πωληθεί στον υποψήφιο αγοραστή με την υψηλότερη εκτίμηση για την αξία του αγαθού. Μειονέκτημα των Ανοικτών Δημοπρασιών Αύξουσας Τιμής είναι η συνήθως μεγάλη χρονική διάρκεια που απαιτείται για τη διεξαγωγή τους [Har98].

- **Ανοικτή Δημοπρασία Φθίνουσας Τιμής** (Open Descending). Ο Δημοπράτης θέτει μια υψηλή τιμή εκκίνησης, η οποία ελαττώνεται βαθμιαία με την πάροδο (συγκεκριμένου) χρόνου. Ο πρώτος που θα ανακοινώσει ότι δέχεται την τρέχουσα τιμή, είναι και ο νικητής της δημοπρασίας. Οι Ανοικτές Δημοπρασίες Φθίνουσας Τιμής αποκαλούνται συχνά και *Ολλανδικές δημοπρασίες* (Dutch auctions) [Kle99].

  Οι δημοπρασίες αυτού του τύπου έχουν επίσης το μειονέκτημα της χρονοβόρας διαδικασίας. Σε οικονομικούς όρους, τα οφέλη του πωλητή από μια Ανοικτή Δημοπρασία Φθίνουσας Τιμής είναι (κατά κανόνα) μικρότερα από τα οφέλη μιας δημοπρασίας Αύξουσας Τιμής [Vic61].

- **Κλειστή Δημοπρασία Πρώτης Τιμής** (Closed First-price). Οι συμμετέχοντες έχουν το δικαίωμα να υποβάλλουν μυστικές προσφορές, μέχρις ότου εκπνεύσει η προθεσμία υποβολής προσφορών (bidding period). Στο τέλος της προθεσμίας οι προσφορές ανοίγονται και καθορίζεται ο νικητής, ο οποίος θα πληρώσει ένα ποσό ίσο με την προσφορά που έκανε, αρκεί η προσφορά αυτή να είναι μεγαλύτερη από την ελάχιστη αποδεκτή τιμή πώλησης του αγαθού [Vic61].

  Το πλεονέκτημα των δημοπρασιών αυτής της κατηγορίας, πέρα από τη μυστικότητα από την οποία περιβάλλονται οι προσφορές, είναι ότι οι δημοπρασίες ολοκληρώνονται συνήθως με μία και μοναδική επικοινωνία μεταξύ υποψήφιων αγοραστών και Δημοπράτη. Ωστόσο, σε οικονομικούς όρους, οι Κλειστές Δημοπρασίες Πρώτης Τιμής είναι ισοδύναμες με τις Ανοικτές Δημοπρασίες Φθίνουσας Τιμής [Mil89].

- **Κλειστή Δημοπρασία Δεύτερης Τιμής** (Closed Second-price) [Ung98,Vic61]. Ακολουθείται η ίδια διαδικασία υποβολής προσφορών και ανάδειξης του τελικού νικητή όπως στις δημοπρασίες Πρώτης Τιμής. Το ποσό όμως που θα πληρώσει ο νικητής είναι ίσο με τη *δεύτερη*

υψηλότερη προσφορά, ή με την ελάχιστη αποδεκτή τιμή πώλησης του αγαθού, εάν αυτή είναι υψηλότερη από τη δεύτερη προσφορά.

Οι δημοπρασίες αυτού του τύπου, οι οποίες αποκαλούνται και *Vickrey* δημοπρασίες (Vickrey auctions), θεωρούνται ως ιδιαίτερα επωφελείς για τον Πωλητή[26], παρουσιάζουν χαμηλό φόρτο επικοινωνίας και είναι ιδιαίτερα ελκυστικές για τους χρήστες που συμμετέχουν σε αυτές, αφού συνήθως ολοκληρώνονται σε σύντομο χρονικό διάστημα [Har98].

Υπάρχουν αρκετές παραλλαγές και υποκατηγορίες των τεσσάρων βασικών τύπων δημοπρασιών που αναφέραμε. Για παράδειγμα, οι διαδικασίες διαφοροποιούνται στις περιπτώσεις όπου δημοπρατούνται περισσότερα του ενός αγαθά (multiple-item auctions) [Cramp98_1,Cramp97].

Οι δημοπρασίες που περιγράψαμε είναι τύπου *ένα-προς-πολλά* (δηλαδή υπάρχει ένας πωλητής και πολλοί αγοραστές) ή αλλιώς *Απλές Δημοπρασίες* (simple auctions). Εκτός από τις δημοπρασίες αυτού του τύπου, υπάρχουν και οι δημοπρασίες τύπου *πολλά-προς-πολλά* (δηλαδή με πολλούς πωλητές και πολλούς αγοραστές), οι οποίες αποκαλούνται και *Διπλές Δημοπρασίες* (double auctions) [Fri93]. Αυτές διακρίνονται στις *Συνεχείς Διπλές Δημοπρασίες* (Continuous Double Auctions – CDA) και στις *Κλειστές Διπλές Δημοπρασίες* (Sealed Double Auctions – SDA) [McC90]. Στις *CDA* δημοπρασίες, οι πωλητές και οι αγοραστές διασταυρώνονται απευθείας με την ανίχνευση συμβατών προσφορών αγοράς/ζήτησης. Οι *SDA* δημοπρασίες αντίθετα, συγκεντρώνουν όλες τις προσφορές (αγοράς και ζήτησης) μέχρι τη λήξη μιας συγκεκριμένης προθεσμίας, και στη συνέχεια καθορίζουν τις αγοροπωλησίες που θα πραγματοποιηθούν, ώστε να υπάρχουν βέλτιστες αντιστοιχίες των προσφορών αγοράς-ζήτησης.

[26] Μια χρήσιμη ιδιότητα των δημοπρασιών Δεύτερης Τιμής είναι ότι η *βέλτιστη στρατηγική* των υποψήφιων αγοραστών είναι να υποβάλλουν προσφορά ίση με την αληθινή εκτίμηση που έχουν για την αξία του αγαθού που δημοπρατείται [Mil89]. Το ίδιο ισχύει και για τις Ανοικτές Δημοπρασίες Αύξουσας Τιμής.

Μια εις βάθος ανάλυση όλων των διαφοροποιήσεων των βασικών τύπων που περιγράψαμε θα παρέκκλινε από το σκοπό της παρούσας Διατριβής. Παραπέμπουμε τον αναγνώστη στις εργασίες των Klemperer και Ungar et al [Kle99,Ung98] για περισσότερες πληροφορίες.

Συνεισφορά / Δομή του Κεφαλαίου.

Στην Ενότητα 3.2 παρουσιάζουμε τα προβλήματα ασφάλειας που παρουσιάζονται σε ηλεκτρονικά συστήματα δημοπρασιών. Ιδιαίτερη έμφαση δίνεται στη δημιουργία *Δακτυλίων* [Bur_Mag02a], δηλαδή συμπαιγνιών που σκοπό έχουν να αλλοιώσουν το τελικό αποτέλεσμα μιας δημοπρασίας, καθώς και στο πρόβλημα της *απόσυρσης προσφορών* (bid withdrawal) στις ανώνυμες δημοπρασίες [Mag00]. Επίσης εισαγάγουμε την ανάγκη για Προστασία από Καταναγκασμό (uncoercibility) στις ηλεκτρονικές δημοπρασίες, ως μέσο καταπολέμησης των Δακτυλίων [Bur_Mag02a]. Στην Ενότητα 3.3 περιγράφουμε τις απαιτήσεις ασφάλειας που πρέπει να πληροί ένα ηλεκτρονικό σύστημα δημοπρασίας. Στην Ενότητα 3.4. αναφέρουμε υλοποιήσεις κρυπτογραφικών συστημάτων για ασφαλείς δημοπρασίες που έχουν προταθεί έως σήμερα στη σχετική διεθνή βιβλιογραφία, ενώ στις Ενότητες 3.5 και 3.6 περιγράφουμε δύο πρωτόκολλα για ασφαλείς δημοπρασίες. Στο πρώτο πρωτόκολλο (Ενότητα 3.5) επιτυγχάνουμε ανωνυμία και μυστικότητα για τους χρήστες ενός συστήματος ηλεκτρονικών δημοπρασιών πρώτης ή δεύτερης τιμής, χωρίς την ύπαρξη τρίτης έμπιστης οντότητας, αποτρέποντας παράλληλα τους χρήστες από το να αποσύρουν μια ήδη υποβληθείσα προσφορά [Mag00]. Στο δεύτερο πρωτόκολλο (Ενότητα 3.6) παρέχουμε Προστασία από Καταναγκασμό για όλους τους χρήστες που συμμετέχουν σε μια ηλεκτρονική δημοπρασία Πρώτης ή Δεύτερης Τιμής [Bur_Mag02a]. Το Κεφάλαιο ολοκληρώνεται με τη συζήτηση στην Ενότητα 3.7.

3.2 Ζητήματα Ασφάλειας στις Ηλεκτρονικές Δημοπρασίες

Η εξάπλωση των δημοπρασιών στο ηλεκτρονικό εμπόριο, τόσο σε εφαρμογές τύπου «Επιχείρηση προς Πελάτη» (Business-to-Customer, B2C) καθώς και σε εφαρμογές τύπου «Επιχείρηση προς Επιχείρηση» (Business-to-Business, B2B) και «Κυβέρνηση προς Επιχείρηση» (Government-to-Business, G2B) για την ανάθεση προμηθειών, καθιστά σημαντική την εύρεση μηχανισμών για τη διασφάλιση των συναλλαγών που πραγματοποιούνται.

Η ασφάλεια συνιστά έναν σημαντικό παράγοντα που πρέπει να λαμβάνεται υπ' όψιν στο σχεδιασμό συστημάτων δημοπρασιών. Συμπαιγνίες (collusions) μεταξύ των χρηστών, πλαστογράφηση προσφορών, κακόβουλοι δημοπράτες, κακώς σχεδιασμένα πρωτόκολλα, είναι μερικές από τις απειλές που αφορούν μια δημοπρασία, είτε αυτή λαμβάνει χώρα σε φυσικό περιβάλλον, είτε μέσω Διαδικτύου [Mag00,Fra96].

3.2.1 Δακτύλιοι

Όλες οι δημοπρασίες, ανεξαρτήτως του τύπου τους, είναι ευάλωτες σε μικρό ή μεγάλο βαθμό στις *συμπαιγνίες* (collusions) μεταξύ των υποψήφιων αγοραστών, μια επίθεση γνωστή επίσης και ως *Δακτύλιος* (Ring) [Bur_Mag02a,Rob85].

Πώς Λειτουργεί ένας Δακτύλιος. Ένα σύνολο από υποψήφιους αγοραστές, συνήθως αυτοί που έχουν την υψηλότερη εκτίμηση για το αγαθό που δημοπρατείται, συμφωνούν σε μια *προκαθορισμένη προσφορά*, η οποία δε ξεπερνάει ένα ορισμένο ποσό. Το ποσό αυτό θα είναι:

- Χαμηλό σε σχέση με την υψηλότερη (μέση) εκτίμηση που έχουν τα μέλη του Δακτυλίου για την αξία του αγαθού που δημοπρατείται,

- Υψηλό σε σχέση με την εκτίμηση που αναμένεται να έχουν άλλοι υποψήφιοι αγοραστές[27] που δεν ανήκουν στο Δακτύλιο [Rob85].

Ένας *προκαθορισμένος νικητής* θα υποβάλλει την προκαθορισμένη προσφορά ώστε να κερδίσει (με μεγάλη πιθανότητα) την επίσημη δημοπρασία. Αυτό έχει ως αποτέλεσμα το αγαθό να πωλείται σε τιμή πολύ χαμηλότερη από την αναμενόμενη. Αργότερα, τα μέλη του Δακτυλίου εκτελούν εκ νέου μεταξύ τους μια *«ιδιωτική» δημοπρασία* για την εκχώρηση του αγαθού, και στο τέλος μοιράζονται μεταξύ τους το επιπλέον ποσό που θα καρπώνονταν ο αρχικός πωλητής του αγαθού, στην επίσημη δημοπρασία, εάν δεν υπήρχε ο Δακτύλιος[28].

Στη συνέχεια θα δούμε πώς ο βαθμός επικινδυνότητας των δακτυλίων ποικίλλει ανάλογα με τον τύπο της δημοπρασίας [Bur_Mag02a].

Δακτύλιοι στις Ανοικτές Δημοπρασίες Αύξουσας Τιμής. Κατά τη διάρκεια μιας Ανοικτής δημοπρασίας *Αύξουσας Τιμής* ένα μέλος ενός δακτυλίου, ας πούμε η Alice, δεν μπορεί να διαφοροποιηθεί από τις επιταγές του δακτυλίου, διότι, λόγω της φύσης της δημοπρασίας (επαναλαμβανόμενες προσφορές ανά τακτά χρονικά διαστήματα) αυτό θα ανακαλυφθεί εγκαίρως από τα άλλα μέλη του δακτυλίου [Ung98]. Οι δημοπρασίες Αύξουσας Τιμής είναι ευάλωτες στους δακτυλίους περισσότερο από κάθε άλλο τύπο δημοπρασίας.

---

[27] Σε ένα παραπλήσιο σενάριο Δακτυλίου, οι «ασήμαντοι» υποψήφιοι αγοραστές δωροδοκούνται ώστε να μη δημιουργήσουν προβλήματα στα μέλη του Δακτυλίου με την υψηλότερη εκτίμηση (π.χ. υποβάλλοντας μια προσφορά μεγαλύτερη από την προκαθορισμένη προσφορά) [Wra66].

[28] Εναλλακτικά, η «ιδιωτική» δημοπρασία μεταξύ των μελών του Δακτυλίου μπορεί να πραγματοποιηθεί νωρίτερα από την επίσημη δημοπρασία. Ο νικητής της «ιδιωτικής» δημοπρασίας θα είναι και ο *προκαθορισμένος νικητής* στην επίσημη δημοπρασία, ενώ το ποσό που θα μοιραστούν τα μέλη του Δακτυλίου θα αντανακλά τη διαφορά μεταξύ της προκαθορισμένης προσφοράς και της νικητήριας προσφοράς που έκρινε την «ιδιωτική» δημοπρασία. Ο Wraight [Wra66] μάλιστα περιέγραψε σενάρια *εσωτερικών δακτυλίων* (inner rings) μέσα στον ίδιο τον Δακτύλιο, όπου κάποια μέλη του Δακτυλίου μπορούν να συνωμοτήσουν μεταξύ τους προκειμένου να εξαπατήσουν άλλα μέλη του Δακτυλίου.

Δακτύλιοι στις Ανοικτές Δημοπρασίες Φθίνουσας Τιμής. Οι Ανοικτές δημοπρασίες *Φθίνουσας Τιμής* είναι λιγότερο ευάλωτες στους δακτυλίους [Mea87] σε σχέση με τις δημοπρασίες Αύξουσας Τιμής, αφού το μέλος του δακτυλίου που διαφοροποιείται, δηλαδή υποβάλλει προσφορά πιο γρήγορα από τα προσυμφωνηθέντα, δεν μπορεί να «τιμωρηθεί» (να χάσει το αγαθό) κατά τη διάρκεια της δημοπρασίας.

Δακτύλιοι στις Κλειστές Δημοπρασίες Πρώτης Τιμής. Οι δακτύλιοι δεν είναι ιδιαίτερα απειλητικοί στις Κλειστές δημοπρασίες *Πρώτης Τιμής* αφού τα μέλη που θέλουν να εξαπατήσουν τον δακτύλιο μπορούν να το κάνουν εύκολα. Σε μια δημοπρασία Πρώτης Τιμής, όλα τα μέλη του δακτυλίου θα πρέπει να κάνουν σχετικά μικρές προσφορές, ενώ ο προκαθορισμένος νικητής θα αρκεστεί στο να κάνει μια ελάχιστα υψηλότερη προσφορά [Rob85]. Είναι εξαιρετικά εύκολο για ένα μέλος που διαφοροποιείται να υποβάλλει μια προσφορά ελαφρώς μεγαλύτερη από την προκαθορισμένη προσφορά και τελικά να κερδίσει τη δημοπρασία σε ιδιαίτερα χαμηλή τιμή.

Δακτύλιοι στις Κλειστές Δημοπρασίες Δεύτερης Τιμής. Κατά τη διάρκεια μιας Κλειστής δημοπρασίας *Δεύτερης Τιμής* οι δακτύλιοι είναι περισσότερο εύκολο να σχηματιστούν από ότι στις Κλειστές δημοπρασίες Πρώτης Τιμής [Mea87]. Οι χρήστες συμφωνούν πως ο προκαθορισμένος νικητής θα προσφέρει ένα εξαιρετικά υψηλό ποσό, ενώ τα υπόλοιπα μέλη του δακτυλίου θα υποβάλλουν σχεδόν μηδενικές προσφορές. Κανείς δεν έχει υψηλό κίνητρο να διαφοροποιηθεί από το δακτύλιο, αφού αν πράξει κάτι τέτοιο θα αναγκαστεί κατά πάσα πιθανότητα να πληρώσει ένα ποσό κατά πολύ μεγαλύτερο από την υψηλότερη εκτίμηση που έχει για την αξία του αγαθού.

3.2.2 Καταναγκασμός στις Ηλεκτρονικές Δημοπρασίες

Ανωνυμία στις Φυσικές Δημοπρασίες. Ένα μέσο προστασίας απέναντι στους δακτυλίους, θα μπορούσε να είναι η ανωνυμία των υποψήφιων αγοραστών [Saku00]. Εάν η υποβολή των προσφορών γίνεται ανώνυμα (δηλαδή καμία προσφορά δε μπορεί να συνδεθεί με την ταυτότητα ενός χρήστη), τότε είναι πιθανόν τα μέλη του δακτυλίου να διαφοροποιηθούν από το δακτύλιο και να υποβάλλουν μεγαλύτερες προσφορές από τις συμφωνηθείσες. Χωρίς ανωνυμία, ένα μέλος του δακτυλίου θα μπορούσε να υποστεί *καταναγκασμό*, π.χ. εκβιασμό, χρηματισμό, απειλή τιμωρίας, ώστε να υποκύψει στις επιταγές του δακτυλίου. Στην επίθεση του Καταναγκασμού υπάγουμε και αυτή του Αυτο-Καταναγκασμού [Bur_Mag02a], όπου ένας χρήστης μπορεί να επιθυμεί ο ίδιος να αποκαλύψει προσωπικά του δεδομένα (π.χ. την προσφορά του), για ίδιον όφελος (χρήματα, εύνοια, κ.λ.π). Ακόμα και αν ο τύπος της δημοπρασίας δεν ευνοεί τους δακτυλίους, π.χ. σε μια Κλειστή Δημοπρασία Πρώτης Τιμής, ο συνδυασμός της μη ανωνυμίας με συνθήκες καταναγκασμού θα έχει ως αποτέλεσμα ο δακτύλιος να είναι επιτυχής.

Ανωνυμία στις Ηλεκτρονικές Δημοπρασίες. Η ανωνυμία των χρηστών, ενώ είναι αρκετά αποτελεσματική στις παραδοσιακές δημοπρασίες, δεν λύνει το πρόβλημα του καταναγκασμού στις ηλεκτρονικές δημοπρασίες [Bur_Mag02a]. Αυτό συμβαίνει διότι οι προσφορές, για λόγους *μυστικότητας*, πρέπει να κρυπτογραφούνται, π.χ. με το δημόσιο κλειδί του Δημοπράτη. Επίσης, για λόγους *επαληθευσιμότητας* οι κρυπτογραφημένες προσφορές ενδεχομένως να δημοσιεύονται σε έναν *πίνακα ανακοινώσεων*, ή ανάλογα με το πρωτόκολλο που εκτελείται, να στέλνεται από το Δημοπράτη μια απόδειξη παραλαβής της κρυπτογραφημένης προσφοράς. Σε όλες τις περιπτώσεις, τα μέλη του Δακτυλίου μπορούν εκ των υστέρων να αποδείξουν σε έναν Καταναγκαστή το περιεχόμενο των κρυπτογραφημένων προσφορών τους. Αυτό γίνεται διότι με την *κρυπτογράφηση δημόσιου κλειδιού*, και έχοντας ως

δεδομένα ένα μήνυμα M (π.χ. την προσφορά) και την υποτιθέμενη κρυπτογράφηση του, C, η ορθότητα της κρυπτογράφησης μπορεί να ελεγχθεί κρυπτογραφώντας ξανά το M με το δημόσιο κλειδί του παραλήπτη, χρησιμοποιώντας παράλληλα την όποια τυχαιότητα έχει χρησιμοποιηθεί – σε περίπτωση που ο αλγόριθμος κρυπτογράφησης E είναι *στοχαστικός* [Gol94], π.χ. ο αλγόριθμος δημοσίου κλειδιού ElGamal [ElG85]. Στη συνέχεια το αποτέλεσμα της κρυπτογράφησης συγκρίνεται με το (ήδη γνωστό) κρυπτογράφημα C: θα πρέπει να ισχύει $C = E(M)$. Ακόμα και αν η ταυτότητα του χρήστη προστατεύεται [Saku00], όλα τα μέλη του Δακτυλίου μπορούν να αποδείξουν στο Δακτύλιο ότι οι προσφορές τους ήταν διαφορετικές από τη υψηλότερη προσφορά. Όποιο μέλος του Δακτυλίου δεν είναι ικανό να αποδείξει του λόγου του το αληθές, θα εκτεθεί στο Δακτύλιο.

Προστασία από Καταναγκασμό στις Ηλεκτρονικές Δημοπρασίες. Από τα παραπάνω προκύπτει πως το πρόβλημα των δακτυλίων είναι περισσότερο έντονο στις ηλεκτρονικές, από ότι στις παραδοσιακές δημοπρασίες. Είναι προφανής λοιπόν η ανάγκη κατασκευής πρωτοκόλλων ηλεκτρονικών δημοπρασιών που προσφέρουν *Προστασία από Καταναγκασμό*. Εάν οι χρήστες δε μπορούν να αποδείξουν το περιεχόμενο της προσφοράς τους σε έναν Καταναγκαστή, τότε παύει να υπάρχει το κίνητρο δημιουργίας δακτυλίων, ακόμα και αν δεν παρέχεται ανωνυμία για τους συμμετέχοντες. Στην Ενότητα 3.6 περιγράφουμε ένα πρωτόκολλο για ηλεκτρονικές δημοπρασίες Προστατευμένες από Καταναγκασμό [Bur_Mag02a].

3.2.3 Άλλες Επιθέσεις

Οι επιθέσεις στην ασφάλεια του συστήματος που μπορούν να λάβουν χώρα κατά τη διάρκεια μιας ηλεκτρονικής δημοπρασίας ποικίλλουν ανάλογα με το τύπο της δημοπρασίας και τις συνθήκες κάτω από τις οποίες εκτελείται.

Επιγραμματικά μπορούμε να αναφέρουμε ορισμένες από αυτές [Fra96, Kum98,Nao00,Bur_Mag02a]:

- **Απόσυρση Προσφοράς** (αφορά τις δημοπρασίες όλων των τύπων). Ο χρήστης υποβάλλει μια προσφορά και στη συνέχεια αρνείται την ευθύνη που συνεπάγεται η υποβολή της προσφοράς. Το γεγονός αυτό συνεπάγεται οικονομική ζημία για τον Πωλητή (και κατ' επέκταση τον Δημοπράτη), δεδομένου ότι κάθε προσφορά θεωρείται ένα εν δυνάμει *συμβόλαιο* μεταξύ του πωλητή και του υποψήφιου αγοραστή.

- **Μη Ανωνυμία των Χρηστών** (αφορά τις δημοπρασίες όλων των τύπων). Η ανωνυμία των χρηστών μπορεί να έχει δύο σκέλη: Πρώτον, σημαίνει *απόκρυψη της ταυτότητας* όσων συμμετέχουν στη δημοπρασία. Δεύτερον, σημαίνει *απόκρυψη της σχέσης μεταξύ προσφοράς και χρήστη* που την υπέβαλε.

  Ως προς το *πρώτο σκέλος*, η μη ανωνυμία μπορεί να επηρεάσει σημαντικά το αποτέλεσμα μιας δημοπρασίας: σε συστήματα που δεν προσφέρουν ανωνυμία στους υποψήφιους αγοραστές, η στρατηγική των χρηστών βασίζεται στην εκτίμηση που προβλέπεται να έχουν οι υπόλοιποι χρήστες [Cramp98]. Ιδίως σε συστήματα Ανοικτών Δημοπρασιών Αύξουσας Τιμής, τα οποία είναι και τα περισσότερο δημοφιλή, η μη ανωνυμία των χρηστών μπορεί να μειώσει δραστικά τον ανταγωνισμό με αποτέλεσμα την πώληση του αγαθού σε τιμή χαμηλότερη από την αναμενόμενη.

  Στις Κλειστές Δημοπρασίες, η προστασία του *δεύτερου σκέλους* της ανωνυμίας (δηλαδή η μη σύνδεση μιας δεδομένης προσφοράς με την ταυτότητα του χρήστη που την υποβάλλει) μπορεί να είναι περισσότερο σημαντική από ότι στις Ανοικτές Δημοπρασίες Αύξουσας Τιμής [Nao00]. Αυτό συμβαίνει διότι οι Κλειστές Δημοπρασίες, και ιδίως οι Δημοπρασίες Δεύτερης Τιμής, ευνοούν την υποβολή προσφορών ίσων με την υψηλότερη εκτίμηση που έχουν οι χρήστες για την αξία του αγαθού.

Η εκτίμηση αυτή είναι σημαντικής σημασίας και πρέπει να περιβάλλεται από ανωνυμία, ειδάλλως ένας δημοπράτης μπορεί να εκμεταλλευτεί την πληροφορία αυτή με κακόβουλο τρόπο.

Για παράδειγμα, έστω ότι η Alice συμμετέχει σε μια Κλειστή Δημοπρασία Δεύτερης Τιμής και πλειοδοτεί στη δημοπρασία με μία προσφορά 800 €, πληρώνοντας ένα ποσό ίσο με τη δεύτερη προσφορά, έστω 400 €. Την επόμενη φορά που θα συμμετάσχει σε μια δημοπρασία για το ίδιο αγαθό, η Alice παρατηρεί ότι η ελάχιστη τιμή εκκίνησης ανήλθε στα 799 €. Ή, εάν αργότερα συμμετάσχει σε μια Ανοικτή Δημοπρασία Αύξουσας Τιμής για το ίδιο αγαθό, ο Δημοπράτης μπορεί (εκ του ασφαλούς) να υποβάλλει «κάλπικες» προσφορές (γνωστές και ως shills [Har98]) ώστε να εξωθήσει την Alice σε υψηλότερες προσφορές, τουλάχιστον μέχρι του ποσού των 800 €.

- **Υποβολή Μη Έγκυρων Προσφορών** (αφορά τις δημοπρασίες όλων των τύπων). Οι επιθέσεις αυτού του τύπου συνήθως αφορούν το Δημοπράτη του συστήματος, ή κάποιον άλλον εσωτερικό εχθρό [Fra96]. Σε μια Ανοικτή Δημοπρασία Αύξουσας Τιμής για παράδειγμα, ο Δημοπράτης[29] μπορεί να εκμεταλλευθεί την ανωνυμία του συστήματος υποβολής προσφορών και να υποβάλλει ή να δεχθεί μια υψηλή «κάλπικη» προσφορά ώστε να ενθαρρύνει τον ανταγωνισμό και να δώσει νέο ενδιαφέρον στη δημοπρασία [Wan02].

  Σε μια Κλειστή Δημοπρασία ο Δημοπράτης μπορεί να αλλάξει το χρόνο λήξης της προθεσμίας υποβολής προσφορών ώστε να συμπεριληφθεί η προσφορά κάποιου «γνωστού» του, ή για να αποκλειστούν καινούριες προσφορές. Τέλος, σε μια Κλειστή Δημοπρασία Δεύτερης Τιμής ο Δημοπράτης μπορεί να προσθέσει μια κάλπικη

[29] Σε πολλές δημοπρασίες ο Δημοπράτης και ο Πωλητής μπορεί είναι το ίδιο πρόσωπο, ή απλά μπορεί να συνεργάζονται. Ένα άλλο κίνητρο υποβολής «κάλπικων» προσφορών από τον Δημοπράτη για το ανέβασμα του ανταγωνισμού είναι το γεγονός ότι μια υψηλότερη τιμή πώλησης συνεπάγεται περισσότερα έσοδα (ποσοστό επί της τιμής πώλησης) για τον Δημοπράτη.

προσφορά με ποσό ελαφρώς χαμηλότερο από την υψηλότερη προσφορά, ώστε η τελική τιμή πώλησης του αγαθού να είναι υψηλή [Kum98].

- **Πρόωρη Αποκάλυψη των Προσφορών** (αφορά τις Κλειστές Δημοπρασίες). Ο Δημοπράτης «ανοίγει» τις υποβληθείσες προσφορές και πληροφορεί σχετικά έναν «γνωστό» του, ο οποίος υποβάλλει εγκαίρως μια προσφορά με το ελάχιστο επιπλέον ποσό που απαιτείται. Αυτή η επίθεση μπορεί να θεωρηθεί και ως ένα είδος Δακτυλίου, όπου ο Δημοπράτης είναι ο ίδιος μέλος του Δακτυλίου [Mea87]. Σε ένα άλλο παρόμοιο σενάριο επίθεσης, ο Δημοπράτης μεταφέρει μια ή περισσότερες έγκυρες προσφορές μιας Κλειστής Δημοπρασίας σε μια άλλη Κλειστή Δημοπρασία της οποίας η προθεσμία υποβολής προσφορών έχει νωρίτερο χρόνο λήξης, ώστε να ανοιχτούν οι προσφορές νωρίτερα από το κανονικό. Στη συνέχεια πληροφορεί τον «γνωστό» του, ο οποίος υποβάλλει εγκαίρως μια προσφορά με το ελάχιστο επιπλέον ποσό που απαιτείται [Fra96]. Εναλλακτικά στο ίδιο σενάριο, και σε μια Δημοπρασία Δεύτερης Τιμής, ο Δημοπράτης μπορεί πάλι να προσθέσει μια ελαφρώς χαμηλότερη «κάλπικη» προσφορά (σε σχέση με την υψηλότερη προσφορά) ώστε να αυξήσει την τελική τιμή πώλησης.

- **Αλλοίωση των Αποτελεσμάτων** (αφορά τις δημοπρασίες όλων των τύπων). Ο Δημοπράτης μπορεί να αλλάζει τις προσφορές που έχουν υποβληθεί ώστε να εξυπηρετήσει συμφέροντα τρίτων, ή να αγνοήσει έγκυρες προσφορές από εξουσιοδοτημένους χρήστες του συστήματος με σκοπό να ευνοήσει τρίτους. Σε μια παρεμφερή επίθεση, που εμπίπτει στις επιθέσεις *Άρνησης Εξυπηρέτησης* και αφορά κυρίως τις Ανοικτές Δημοπρασίες, ο Δημοπράτης ισχυρίζεται ότι μια προσφορά υποβλήθηκε *εκπρόθεσμα* ή αρνείται την παραλαβή μιας συγκεκριμένης προσφοράς, ή εμποδίζει την ηλεκτρονική πρόσβαση στη δημοπρασία, επιλεκτικά για συγκεκριμένους χρήστες (π.χ. με βάση την ταυτότητα ή την διεύθυνση IP ή το όνομα DNS ενός χρήστη) [Wel98].

3.3 Απαιτήσεις Ασφάλειας

Ανεξάρτητα από τον τύπο της δημοπρασίας που πρόκειται να διεξαχθεί, οι ακόλουθες απαιτήσεις ασφάλειας πρέπει να λαμβάνονται υπ' όψιν στο σχεδιασμό και την υλοποίηση ηλεκτρονικών δημοπρασιών [Fra96,Kum98,Bur_Mag02a]:

- **Ανωνυμία** (Anonymity).

    - Η ταυτότητα των χρηστών πρέπει να είναι μυστική και να μην αποκαλύπτεται σε κανέναν (π.χ. σε άλλους χρήστες, ή στον Δημοπράτη).

    - Καμία προσφορά δεν πρέπει να είναι δυνατόν να συνδεθεί με την ταυτότητα ενός συγκεκριμένου χρήστη. Με την ολοκλήρωση της δημοπρασίας, όλες οι προσφορές (εκτός, ενδεχομένως, από τη νικητήρια) πρέπει επίσης να περιβάλλονται από ανωνυμία.

- **Μυστικότητα** (Secrecy). Οι προσφορές δεν πρέπει να αποκαλύπτονται σε κανέναν, ούτε και στον ίδιο τον Δημοπράτη, παρά μόνον υπό προϋποθέσεις. Σε μια Κλειστή Δημοπρασία για παράδειγμα, η προϋπόθεση είναι η λήξη της προθεσμίας υποβολής προσφορών. Οι Stubblebine και Syverson [Stu99] επίσης εισήγαγαν την έννοια της *προσωρινής μυστικότητας* των προσφορών για την αντιμετώπιση των επιθέσεων Άρνησης Εξυπηρέτησης στις Ανοικτές Δημοπρασίες Αύξουσας Τιμής, απαιτώντας από το Δημοπράτη να δεσμεύεται σε μια ληφθείσα κρυπτογραφημένη προσφορά, προτού αυτή αποκαλυφθεί [Stu99].

- **Ορθότητα** (Correctness). Για να εδραιωθεί η ορθότητα σε μια δημοπρασία, πρέπει να εξασφαλίζονται οι ακόλουθες συνθήκες:

    - Μόνο εξουσιοδοτημένοι χρήστες μπορούν να υποβάλλουν έγκυρες προσφορές.

    - Κανείς δεν είναι ικανός να πλαστοπροσωπήσει έναν χρήστη.

    - Οι έγκυρες προσφορές δεν είναι δυνατόν να αλλοιωθούν / διαγραφούν από το Δημοπράτη.

    - Οι προσφορές είναι έγκυρες μόνο για τη δημοπρασία στην οποία έχουν υποβληθεί.

    - Ο νικητής της δημοπρασίας είναι αυτός που έχει κάνει την υψηλότερη προσφορά και μόνον αυτός.

- **Καταλογισμός Ευθύνης** (Non-Repudiation). Οι χρήστες δεν μπορούν να αποσύρουν μια ήδη υποβληθείσα προσφορά ή να αρνηθούν την υποβολή της.

- **Επαληθευσιμότητα** (Verifiability). Όλοι οι συμμετέχοντες πρέπει να μπορούν να επαληθεύσουν την ορθότητα της διαδικασίας και την πιστότητα των αποτελεσμάτων. Η επαληθευσιμότητα είναι *ατομική* όταν η πιστοποίηση της ορθότητας της διαδικασίας και των αποτελεσμάτων επαφίεται στους χρήστες, ή *οικουμενική* όταν κάθε εξωτερικός παρατηρητής μπορεί να πιστοποιήσει την ορθότητα της διαδικασίας και την αυθεντικότητα των αποτελεσμάτων.

- **Προστασία από Καταναγκασμό** (Uncoercibility). Κανείς χρήστης δεν πρέπει να μπορεί να αποδείξει σε κάποιον τρίτο την τιμή της προσφοράς που υπέβαλε.

3.4 Κρυπτογραφικά Μοντέλα Ασφάλειας

Οι περισσότερες δημοπρασίες που διενεργούνται σήμερα μέσω Διαδικτύου είναι Ανοικτές Δημοπρασίες Αύξουσας Τιμής (π.χ. eBay.com, Yahoo!Auction, Amazon.com) [Auc02]. Οι υπηρεσίες ασφάλειας που παρέχονται στις δημοπρασίες αυτές είναι χαμηλού επιπέδου[30]. Οι Ανοιχτές Δημοπρασίες θέτουν προβλήματα όπως η *ανωνυμία* των χρηστών, η ευκολία δημιουργίας *Δακτυλίων* [Mea87], η *χρονική* εγκυρότητα των προσφορών [Har98,Wel98] αλλά και οι επιθέσεις *Άρνησης Εξυπηρέτησης* από την πλευρά του Δημοπράτη.

Πρόσφατα προτάθηκαν κρυπτογραφικά συστήματα υλοποίησης Ανοικτών Δημοπρασιών Αύξουσας Τιμής [Sta99,Stu99], χωρίς την ύπαρξη τρίτης έμπιστης οντότητας. Οι Stajano και Anderson [Sta99] αντιμετωπίζουν το πρόβλημα της ανωνυμίας[31] των χρηστών, ενώ οι Stubblebine και Syverson [Stu99] προτείνουν μηχανισμούς για την αντιμετώπιση επιθέσεων Άρνησης Εξυπηρέτησης[32] από το Δημοπράτη, όπως η άρνηση παραλαβής μιας έγκυρης προσφοράς ή ο παράτυπος χαρακτηρισμός της ως εκπρόθεσμη.

---

[30] Κάθε χρήστης μπορεί να εγγραφεί στο σύστημα, και να υποβάλει μια προσφορά. Εάν η προσφορά είναι η νικητήρια αλλά ο χρήστης αρνείται να πληρώσει, τότε η δημοπρασία επαναλαμβάνεται. Στις υπηρεσίες αυτές δεν παρέχεται ανωνυμία στους χρήστες, προσωρινή μυστικότητα της προσφοράς, ή έλεγχος της ορθότητας των αποτελεσμάτων. Επίσης δεν προσφέρεται προστασία από καταναγκασμό.

[31] Για εδραίωση της ανωνυμίας ο πωλητής και οι υποψήφιοι αγοραστές εκτελούν το κρυπτογραφικό πρωτόκολλο των *δειπνούντων κρυπτογράφων* (dining cryptographers) όπως αυτό περιγράφτηκε από τον Chaum [Cha88_1]. Η υποβολή προσφοράς καθώς και η δέσμευση του δημοπράτη στην προσφορά γίνονται με χρήση του μηχανισμού *ανταλλαγής κλειδιών* των Diffie-Hellman [Dif76].

[32] Για το λόγο αυτό χρησιμοποιούν τεχνικές *Επιβεβαιωμένης Παράδοσης* (certified delivery) [Cer02] και *Υπηρεσίες Χρονολόγησης* (timestamping) [Sur02]. Οι υπηρεσίες αυτές προσφέρουν επίσημη χρονολόγηση σε μηνύματα, με σκοπό τη διευθέτηση διενέξεων που αφορούν το *πότε* έχει δημιουργηθεί ή υποβληθεί ένα δεδομένο μήνυμα. Συνήθως η υπηρεσία αυτή προσφέρεται από τρίτες οντότητες, οι οποίες επισυνάπτουν τη χρονική πληροφορία σε ένα μήνυμα και κατόπιν το υπογράφουν ψηφιακά.

Κλειστές Δημοπρασίες

Ως βασικό αντικείμενο μελέτης για την εύρεση κρυπτογραφικών μηχανισμών και τεχνικών που διασφαλίζουν την ομαλή λειτουργία συστημάτων δημοπρασιών μεγάλης κλίμακας (large-scale), επιλέξαμε τις Κλειστές Δημοπρασίες. Οι Κλειστές Δημοπρασίες δίνουν έμφαση σε ζητήματα ασφάλειας που είναι εγγενή σε κάθε δραστηριότητα ηλεκτρονικού εμπορίου. Από τη σκοπιά της ασφάλειας, τα συστήματα Κλειστών Δημοπρασιών προσιδιάζουν κυρίως στα συστήματα *ηλεκτρονικής ψηφοφορίας* [Mag02_1].

Όπως είδαμε στην Ενότητα 3.1 οι Κλειστές Δημοπρασίες Δεύτερης Τιμής είναι ιδιαίτερα ελκυστικές για πωλητές και υποψήφιους αγοραστές, σε σχέση με τις Ανοικτές Δημοπρασίες. Ωστόσο έως σήμερα δεν έχουν επιλυθεί με αποτελεσματικό τρόπο τα ζητήματα ασφάλειας (Ενότητα 3.2) στη σχεδίαση Κλειστών ηλεκτρονικών Δημοπρασιών (Πρώτης/Δεύτερης Τιμής). Η έρευνα μας αποσκοπεί ακριβώς στην επίλυση αυτών των προβλημάτων [Bur_Mag02a,Mag00].

Μυστικότητα της Προσφοράς. Σε αντίθεση με τις Ανοικτές Δημοπρασίες, όπου η μυστικότητα των προσφορών δεν είναι σημαντική, στις Κλειστές Δημοπρασίες η μυστικότητα αποτελεί την πιο σημαντική από τις απαιτήσεις ασφάλειας. Τρεις είναι οι βασικές προσεγγίσεις που προτείνονται στη διεθνή βιβλιογραφία για την προστασία της μυστικότητας μιας προσφοράς κατά τη διάρκεια της περιόδου υποβολής προσφορών σε μια Κλειστή ηλεκτρονική Δημοπρασία Πρώτης ή Δεύτερης Τιμής:

- **Μυστικότητα με χρήση Έμπιστης Οντότητας.** Η οντότητα αυτή συνήθως είναι *ο* Δημοπράτης ή κάποια άλλη Τρίτη Έμπιστη Οντότητα (Trusted Third Party – TTP). Στα συστήματα αυτά (π.χ. [Nao00,Sak99]) η μυστικότητα των προσφορών καταργείται εάν η τρίτη οντότητα

παραβιάσει την εμπιστοσύνη που τρέφουν για αυτήν οι χρήστες του συστήματος.

- **Μυστικότητα με Κατανεμημένα Συστήματα.** Στα συστήματα αυτά, όπως π.χ. στις δημοπρασίες των Franklin-Reiter [Fra96], Harkavy et al [Har98,Har99] και Kudo [Kud98], ο Δημοπράτης περιγράφεται ως ένα κατανεμημένο σύστημα εξυπηρετητών, ανεξάρτητων μεταξύ τους. Η προστασία της μυστικότητας των προσφορών από ένα υποσύνολο *πλημμελών* (δηλαδή κακόβουλων ή απλά δυσλειτουργικών) εξυπηρετητών επιτυγχάνεται με κρυπτογραφικά εργαλεία όπως ο *διαμοιρασμός μυστικού*[9] με τεχνικές threshold [Sha79]. Οι Harkavy et al [Har98,Har99] επίσης χρησιμοποιούν τεχνικές *ασφαλούς πολυμερούς υπολογισμού*[33], που εκτελούνται μεταξύ των εξυπηρετητών, για την προστασία της μυστικότητας των προσφορών ακόμα και μετά το τέλος της περιόδου υποβολής προσφορών.

Σημείωση: Τα συστήματα εκείνα τα οποία, για προστασία της μυστικότητας των προσφορών της δημοπρασίας, περιγράφουν το Δημοπράτη ως ένα κατανεμημένο σύστημα με τρίτες ανεξάρτητες οντότητες (π.χ.[Fra96,Har98]) παρουσιάζουν μια σημαντική αδυναμία: τα συστήματα αυτά συνιστούν υψηλό επικοινωνιακό και υπολογιστικό φόρτο για τους εξυπηρετητές, αφού αφενός οι χρήστες επικοινωνούν απευθείας με τους εξυπηρετητές, αφετέρου οι εξυπηρετητές πρέπει να συνεργαστούν μεταξύ τους για την εξαγωγή των τελικών αποτελεσμάτων. Η υψηλή πολυπλοκότητα αποτελεί ένα αντι-κίνητρο για μια επιχείρηση που σκέφτεται να συμμετάσχει ως εξυπηρετητής σε πολλές δημοπρασίες. Μια ρεαλιστικότερη υλοποίηση τέτοιων συστημάτων θα περιελάμβανε ένα σύνολο από εξυπηρετητές που θα ελέγχονταν από

---

[33] Για κάθε συνάρτηση $f(x_1, x_2, \ldots, x_n)$ είναι δυνατή η κατασκευή ενός πρωτοκόλλου που επιτρέπει σε μια ομάδα από n χρήστες, όπου ο χρήστης i έχει μια μυστική είσοδο a_i, να εκτιμήσουν από κοινού την $f(a_1, a_2, \ldots, a_n)$. Ακολουθώντας το πρωτόκολλο, όλοι οι χρήστες μαθαίνουν την $f(a_1, a_2, \ldots, a_n)$ αλλά κανένας χρήστης i δε μπορεί να εξάγει περισσότερες πληροφορίες για τις άλλες εισόδους $\{a_j\}_{j \neq i}$, από αυτές που μπορεί να εξάγει από τα a_i και $f(a_1, a_2, \ldots, a_n)$ [Ben88].

την ίδια επιχείρηση. Ωστόσο, στην αρχιτεκτονική αυτή είναι δύσκολο να εξασφαλιστεί η τιμιότητα (δηλαδή η μη συνεργία ενός αριθμού threshold) των εξυπηρετητών στην προστασία της μυστικότητας των προσφορών [Mag00,Kum98].

- **Μυστικότητα Ελεγχόμενη από τον Χρήστη.** Τα συστήματα στα οποία η μυστικότητα της προσφοράς έγκειται στον χρήστη που την υποβάλλει, δεν απαιτούν τρίτη έμπιστη οντότητα ή κατανεμημένους εξυπηρετητές. Οι Stubblebine-Syverson [Stu99] πρότειναν ένα σύστημα για Ανοικτές Δημοπρασίες όπου η προσωρινή μυστικότητα της προσφοράς ελέγχεται από τον χρήστη. Στην Κλειστή Δημοπρασία που προτείνουμε στην Ενότητα 3.5, και που ακολουθεί την ίδια προσέγγιση, ο χρήστης αποκαλύπτει το κλειδί αποκρυπτογράφησης της προσφοράς του στον Δημοπράτη, μετά το τέλος της περιόδου υποβολής προσφορών [Mag00].

  Ένα μειονέκτημα των συστημάτων αυτών είναι ότι ο χρήστης πρέπει να είναι ενεργός (online) κατά τη διάρκεια της καταμέτρησης των προσφορών.

Σημείωση: Στα συστήματα όπου η μυστικότητα είναι ελεγχόμενη από τον χρήστη, εάν το κανάλι επικοινωνίας μεταξύ του χρήστη και του Δημοπράτη είναι ανώνυμο, όπως π.χ. στο πρωτόκολλο των Stubblebine-Syverson [Stu99], τότε το σύστημα παρουσιάζει αδυναμίες στον καταλογισμό ευθύνης, αφού είναι δύσκολο να αποτρέψει την απόσυρση προσφορών. Αυτό συμβαίνει διότι η άνευ όρων ανωνυμία των χρηστών του συστήματος μπορεί να χρησιμοποιηθεί ως μέσο για να εξαπατηθεί το σύστημα [Mag00]. Στην Ενότητα 3.5 περιγράφουμε ένα «δίκαιο» πρωτόκολλο κλειστών ηλεκτρονικών δημοπρασιών όπου η μυστικότητα ελέγχεται από τον χρήστη, χωρίς όμως να είναι δυνατή η απόσυρση μιας προσφοράς.

- **Συστήματα Διάσκεψης.** Στα συστήματα *διάσκεψης* (boardroom), όπως η Κλειστή Δημοπρασία του Cachin[34] [Cac99] ή η Ανοικτή Δημοπρασία των Stajano-Anderson [Sta99], οι δημοπρασίες εκτελούνται μεταξύ των

[34] Στο σύστημα αυτό εκτελείται ένα πρωτόκολλο *ασφαλούς πολυμερούς υπολογισμού* [Ben88] μεταξύ των χρηστών, για την ανάδειξη του τελικού νικητή.

υποψήφιων αγοραστών, χωρίς την ανάγκη ύπαρξης Δημοπράτη ή άλλης έμπιστης οντότητας για την προστασία της μυστικότητας των προσφορών.

Τα συστήματα διάσκεψης συνεπάγονται υψηλή υπολογιστική πολυπλοκότητα για μεγάλο αριθμό χρηστών. Ένα επίσης σημαντικό μειονέκτημα των συστημάτων αυτών, από τη σκοπιά της ασφάλειας, είναι ότι κάποιος ή κάποιοι χρήστες μπορούν να παρεμποδίσουν την ομαλή διεξαγωγή της δημοπρασίας. Ως εκ τούτου ενδείκνυνται για ηλεκτρονικές δημοπρασίες μικρής κλίμακας (small scale) και δεν είναι κατάλληλα για εφαρμογές μεγάλης κλίμακας (large scale) που διεξάγονται μέσω Διαδικτύου [Mag00].

Ανωνυμία. Κανένα σύστημα για Κλειστές Δημοπρασίες δεν προσφέρει πλήρη (ως και προς τα δυο σκέλη) προστασία της ανωνυμίας των χρηστών έναντι του Δημοπράτη. Ορισμένα από τα συστήματα που έχουν προταθεί, για να αντισταθμίσουν το γεγονός αυτό διατηρούν την μυστικότητα των προσφορών, εκτός της νικητήριας προσφοράς, ακόμα και *μετά το τέλος* της περιόδου υποβολής προσφορών [Har98,Har99,Nao00,Cac99]. Για να το πετύχουν αυτό χρησιμοποιούν τεχνικές *ασφαλούς πολυμερούς υπολογισμού* [Ben88], οι οποίες δεν είναι αποδοτικές: η υπολογιστική πολυπλοκότητα τέτοιων τεχνικών είναι υψηλή, ιδίως για μεγάλο αριθμό χρηστών, κάτι που καθιστά τα συστήματα αυτά μη πρακτικά για εφαρμογές μεγάλης κλίμακας. Στο πρωτόκολλο Κλειστών ηλεκτρονικών Δημοπρασιών που προτείνουμε στην Ενότητα 3.5, επιτυγχάνουμε απόκρυψη της σχέσης μεταξύ προσφοράς και χρήστη που την υπέβαλε, χωρίς την ανάγκη ύπαρξης τρίτων έμπιστων οντοτήτων.

Καταλογισμός Ευθύνης. Για την επίτευξη καταλογισμού ευθύνης, στα συστήματα των Franklin-Reiter [Fra96] και Harkavy et al [Har98,Har99], οι προσφορές προτείνεται να περιέχουν ένα ποσό *ηλεκτρονικού χρήματος* (digital cash) [Cha88] ίσο με την αξία της προσφοράς. Ωστόσο σε τέτοια συστήματα

κάθε προσφορά αποτελεί πιθανό στόχο για τους εσωτερικούς/εξωτερικούς εχθρούς του συστήματος. Επίσης, η χρήση ψηφιακού χρήματος σε ηλεκτρονικές δημοπρασίες που πιθανόν να διαρκέσουν μεγάλο χρονικό διάστημα, συνεπάγεται για όλους τους χρήστες το επιπλέον κόστος του μη τοκισμού των χρημάτων τους [Har98].

Στις εργασίες [Har98,Sta99] συζητείται η χρήση τεχνικών *υποθήκευσης ταυτότητας* (identity escrow) [Kil98], όπου μια ή περισσότερες έμπιστες οντότητες αναλαμβάνουν να προστατεύσουν την ανωνυμία του χρήστη, εφόσον αυτός δεν αρνείται την ευθύνη για μια προσφορά που υπέβαλε κατά τη διάρκεια της δημοπρασίας. Μια παραπλήσια, ως προς το αποτέλεσμα που επιφέρει, τεχνική προτείνουμε στην Ενότητα 3.5 χωρίς όμως να κάνουμε χρήση έμπιστης οντότητας για τον καταλογισμό ευθύνης.

Επαληθευσιμότητα. Η επαληθευσιμότητα που παρέχεται από τα περισσότερα συστήματα ηλεκτρονικών δημοπρασιών που έχουν προταθεί είναι *ατομική*. Στην Ενότητα 3.6 το πρωτόκολλο Κλειστών Δημοπρασιών που προτείνουμε, εξασφαλίζει οικουμενική επαληθευσιμότητα για τα αποτελέσματα της δημοπρασίας.

Προστασία από Καταναγκασμό. Στην εργασία των Sakurai-Miyiazaki [Saku00] προτάθηκε η ανωνυμία των χρηστών ως μέσο καταπολέμησης του καταναγκασμού στις Κλειστές Δημοπρασίες. Όπως δείξαμε στην Ενότητα 3.2 η προστασία αυτή δεν είναι αρκετή. Στην Ενότητα 3.6 περιγράφουμε ένα πρωτόκολλο για Κλειστές Δημοπρασίες όπου κανένας χρήστης, ακόμα και αν το επιθυμεί, δε μπορεί να αποδείξει σε κάποιον τρίτο την τιμή της κρυπτογραφημένης προσφοράς που υπέβαλε στη δημοπρασία [Bur_Mag02a].

3.5 «Δίκαιες» Κλειστές Ηλεκτρονικές Δημοπρασίες

Στην Ενότητα αυτή παρουσιάζουμε ένα ασφαλές κρυπτογραφικό σχήμα για Κλειστές Δημοπρασίες Πρώτης ή Δεύτερης Τιμής, χωρίς να απαιτούμε την ύπαρξη τρίτης έμπιστης οντότητας για την προστασία της μυστικότητας των προσφορών [Mag00]. Η μέθοδος που προτείνουμε είναι «δίκαιη» (equitably fair) για τους χρήστες και τους δημοπράτες. Αυτό σημαίνει πως το σύστημα προστατεύει την *ανωνυμία* των χρηστών και την *μυστικότητα* των προσφορών τους, εδραιώνοντας παράλληλα *καταλογισμό ευθύνης* για κάθε έγκυρη προσφορά που υποβάλλεται. Επιγραμματικά:

- Παρέχεται ανωνυμία και μυστικότητα στους χρήστες,
- Κανείς χρήστης δε μπορεί να αποσύρει την προσφορά του.

Το πρωτόκολλο που προτείνουμε επεκτείνει συστήματα όπως αυτό των Stubblebine και Syverson [Stu99], καθώς όχι μόνο προστατεύει την ιδιωτικότητα των χρηστών (μυστικότητα και ανωνυμία) αλλά επίσης αποτρέπει τους χρήστες από το να αποσύρουν την προσφορά τους, ακόμα και αν δεν έχει ξεκινήσει το στάδιο της αποκρυπτογράφησης των προσφορών. Πιστεύουμε ότι η απόσυρση μιας προσφοράς, έστω και αν καμία προσφορά δεν έχει «ανοιχτεί» ακόμα, ενδεχομένως να θεωρείται «δίκαιη» για τον χρήστη, αλλά δεν είναι *εξ' ίσου* «δίκαιη» [Bur98] και για τον δημοπράτη: εάν ορισμένες συγκυρίες καθιστούν μια προσφορά μη επωφελή, και ο χρήστης επιτρέπεται να αποσύρει την προσφορά του, τότε αυτό θα ήταν τόσο δίκαιο όσο το να επιτραπεί στον δημοπράτη (ή τον πωλητή) να αποσύρει το αγαθό που δημοπρατείται, επειδή ορισμένες επίσης συγκυρίες καθιστούν την πώληση μη επωφελή [Mag00].

Η προσέγγιση μας επιτρέπει, μετά την ολοκλήρωση της δημοπρασίας, την ανίχνευση των χρηστών που απέσυραν την προσφορά τους. Για αυτόν το

σκοπό χρησιμοποιούμε *Γρίφους Συγκεκριμένου Χρόνου Επίλυσης*[35] ώστε να εκπληρωθεί η απαίτηση του καταλογισμού ευθύνης.

Επίσης κάνουμε χρήση κρυπτογραφικών μηχανισμών όπως «*Τυφλές*» *Υπογραφές*[36] [Cha85], και τεχνικές *Διαίρει και Επίλεξε*[37] [Sch96] για την ορθότητα της υποβληθείσας προσφοράς, καθώς και μηχανισμών *Επιβεβαιωμένης Παράδοσης* [Cam96] προκειμένου να αποτρέψουμε επιθέσεις Άρνησης Εξυπηρέτησης κατά τη διάρκεια της δημοπρασίας.

Παράλληλα διενεργούνται έλεγχοι, ώστε να εξασφαλιστεί ότι οι προσφορές υποβάλλονται από εξουσιοδοτημένους χρήστες και μόνον.

Ένα Σενάριο Εφαρμογής του Προτεινόμενου Πρωτοκόλλου. Θεωρούμε μια Κλειστή Δημοπρασία Πρώτης ή Δεύτερης τιμής στην οποία οι μη πλειοδότες διατηρούν την ανωνυμία τους, ενώ κανείς χρήστης δεν είναι ικανός να αποσύρει την προσφορά του. Μια εφαρμογή ηλεκτρονικής δημοπρασίας που θα σχεδιαστεί ενσωματώνοντας τα ανωτέρω χαρακτηριστικά, απευθύνεται κυρίως σε περιβάλλοντα B2C ή G2B που απαιτούν δημοπρασίες υψηλής ασφάλειας, όπου η ορθότητα της διαδικασίας υποβολής προσφορών, η ανωνυμία των χρηστών και ο καταλογισμός ευθύνης για όλους τους συμμετέχοντες (χρήστες και δημοπράτες) αποτελούν υπηρεσίες προστιθέμενης αξίας [Mag00].

---

[35] Με τους Γρίφους Συγκεκριμένου Χρόνου Επίλυσης, ένα μήνυμα κρυπτογραφείται ούτως ώστε να μην μπορεί να αποκρυπτογραφηθεί παρά μόνον από έναν υπολογιστή που εκτελεί συνεχείς υπολογισμούς για συγκεκριμένο χρόνο (Ενότητα 3.5.1.1).

[36] Οι «τυφλές» υπογραφές [Cha85] στην κρυπτογραφία, μπορούν, χρησιμοποιώντας ένα παράδειγμα της καθημερινής ζωής, να αντιστοιχιστούν με την υπογραφή (εξωτερικά) ενός σφραγισμένου φακέλου που περιέχει ένα χαρτί τοποθετημένο κάτω από καρμπόν. Όταν ο φάκελος αργότερα ανοιχτεί από τον νόμιμο παραλήπτη, το χαρτί θα έχει αποτυπωμένη την υπογραφή (Ενότητα 3.5.1.2).

[37] Οι μηχανισμοί «διαίρει και επίλεξε» (cut and choose) χρησιμοποιούνται για να επιτευχθεί ορθότητα (correctness) σε πρωτόκολλα «τυφλών» υπογραφών: Στο ανωτέρω παράδειγμα, ο υπογράφων θα ανοίξει όλους τους φακέλους που θα του υποβληθούν, εκτός από έναν. Στη συνέχεια θα υπογράψει εξωτερικά τον εναπομείναντα σφραγισμένο φάκελο (Ενότητα 3.5.1.2).

3.5.1 Κρυπτογραφικοί Μηχανισμοί

Στη συνέχεια παρουσιάζουμε και επεξηγούμε τους κρυπτογραφικούς μηχανισμούς, στους οποίους βασιστήκαμε κατά τη σχεδίαση του συστήματος των «Δίκαιων» δημοπρασιών.

3.5.1.1 Γρίφοι Συγκεκριμένου Χρόνου Επίλυσης

Η ιδέα των Γρίφων Συγκεκριμένου Χρόνου Επίλυσης (Time-Lock Puzzles) προτάθηκε από τους Rivest, Shamir και Wagner [Riv96]. Με έναν Γρίφο Συγκεκριμένου Χρόνου Επίλυσης η Alice μπορεί να κρυπτογραφήσει ένα μήνυμα M ούτως ώστε ο Bob να μπορέσει να το αποκρυπτογραφήσει μετά από την πάροδο συγκεκριμένου χρόνου T. Το πρωτόκολλο θεωρεί ότι η Alice γνωρίζει, ή μπορεί να υποθέσει την δυνατότητα της Κεντρικής Μονάδας Επεξεργασίας (CPU) του Bob.

Η Alice κατασκευάζει ένα modulus $n = pq$ ως το γινόμενο δύο μεγάλων πρώτων αριθμών p και q. Υπολογίζει επίσης το $\Phi(n) = (p-1)(q-1)$ και $t = TS$ όπου S είναι ο αριθμός των τετραγωνισμών (squarings) modulo n που μπορεί να εκτελέσει ο υπολογιστής του Bob. Η Alice επιλέγει ένα κλειδί K στα πλαίσια ενός συμμετρικού αλγορίθμου κρυπτογράφησης (π.χ. AES 128-bit) και κρυπτογραφεί το μήνυμα M με το κλειδί K, λαμβάνοντας έτσι το κρυπτογράφημα $C_M = Enc(K, M)$. Για να «κρύψει» το κλειδί K, η Alice επιλέγει έναν τυχαίο αριθμό $a \in Z_n$ και κρυπτογραφεί το K ως εξής:

$$C_K = (K + a^{2^t}) \bmod n.$$

Για να το κάνει αυτό κατά τρόπο αποδοτικό, χρησιμοποιεί την μυστική πληροφορία (trapdoor) $\Phi(n)$ και υπολογίζει:

$$e = 2^t \bmod \Phi(n),$$

και στη συνέχεια:

$$b = a^e \bmod n.$$

Το «δημόσιο» κομμάτι του Γρίφου είναι το σύνολο (n, a, t, C_M, C_K), ενώ η Alice διαγράφει κάθε άλλη πληροφορία (όπως το p και το q).

Επίλυση του Γρίφου. Ο πιο γρήγορος τρόπος για τον Bob να επιλύσει τον γρίφο είναι να υπολογίσει:

$$b = a^{2^t} \bmod n$$

Ο Bob θα μπορούσε να εκτελέσει εύκολα τον υπολογισμό, μόνον εάν γνώριζε την μυστική πληροφορία $\Phi(n)$. Δεδομένου ότι η Alice έχει διαγράψει τους πρώτους παράγοντες p και q, ο υπολογισμός του $\Phi(n)$ από το modulus n έχει αποδειχθεί ότι είναι τόσο δύσκολος όσο και η παραγοντοποίηση του n [Riv96]. Ως αποτέλεσμα, για τον Bob δεν υπάρχει άλλος τρόπος υπολογισμού του b από το να χρησιμοποιήσει ως είσοδο το a και να επιτελέσει t τετραγωνισμούς (υψώνοντας κάθε φορά το αποτέλεσμα της προηγούμενης πράξης στη δύναμη του 2).

Τονίζουμε ότι το υπολογιστικό πρόβλημα της επίλυσης του Γρίφου δεν μπορεί να αντιμετωπιστεί με κατανεμημένες διαδικασίες [Riv96]: η χρήση δύο υπολογιστών δεν θα έχει καλύτερο αποτέλεσμα από τη χρήση ενός υπολογιστή (βεβαίως, η χρήση ενός γρήγορου υπολογιστή θα έχει καλύτερα αποτελέσματα από ότι η χρήση ενός αργού υπολογιστή).

3.5.1.2 «Τυφλές» Υπογραφές

Ο κρυπτογραφικός μηχανισμός των «τυφλών» υπογραφών (blind signatures) χρησιμοποιήθηκε αρχικά σε εφαρμογές ηλεκτρονικού χρήματος [Cha85,Cha82], επιτρέποντας στον αγοραστή να λάβει ηλεκτρονικό χρήμα από μια τράπεζα χωρίς η τράπεζα να μπορεί να συσχετίσει το όνομα του αγοραστή με τα χρήματα που του αποδίδονται, όταν αυτά χρησιμοποιηθούν αργότερα σε μια ηλεκτρονική συναλλαγή. Γενικότερα ο εν λόγω μηχανισμός μπορεί να χρησιμοποιηθεί σε οποιαδήποτε κρυπτογραφική εφαρμογή επιθυμούμε ο υπογράφων να μην γνωρίζει το μήνυμα που υπογράφει.

Υλοποίηση στο RSA [Sch96]. Στη συνέχεια περιγράφουμε μια υλοποίηση του πρωτοκόλλου των «τυφλών» υπογραφών για τον αλγόριθμο RSA [Rsa78]. Η Alice επιθυμεί ο Bob να υπογράψει «τυφλά» ένα μήνυμα m. Ο Bob έχει ένα δημόσιο κλειδί e, ένα ιδιωτικό κλειδί d, και ένα δημόσιο modulus n.

α) Η Alice επιλέγει έναν τυχαίο αριθμό $1 < k < n$ και υπολογίζει, χρησιμοποιώντας το δημόσιο κλειδί e του Bob, το $t = m \times k^e \bmod n$. Στέλνει το t στον Bob.

β) Ο Bob υπογράφει το t με το ιδιωτικό του κλειδί d, υπολογίζοντας $t^d = (m \times k^e)^d \bmod n$, και στέλνει το υπογεγραμμένο t στην Alice.

γ) Η Alice εκτελεί την πράξη $(t^d / k) \bmod n$ και λαμβάνει ως αποτέλεσμα το $m^d \bmod n$, το οποίο είναι το μήνυμα m, υπογεγραμμένο από τον Bob.

Διαίρει και Επίλεξε. Επειδή οι «τυφλές» υπογραφές εγκυμονούν προφανείς κινδύνους για τον υπογράφοντα, έχουν προταθεί τεχνικές «Διαίρει και Επίλεξε» για την απόδειξη της ορθότητας του μηνύματος που πρόκειται να υπογραφεί «τυφλά», χωρίς όμως να αίρεται η μυστικότητα του μηνύματος

[Sch96]. Τα πρωτόκολλα αυτά είναι δηλαδή πρωτόκολλα *απόδειξης με μηδενική γνώση* [Gol91]. Έτσι, στο ανωτέρω παράδειγμα η Alice θα μπορούσε να ετοιμάσει x διαφορετικά μηνύματα προς υπογραφή t_i, $i = 1..x$, και θα απεκάλυπτε, καθ' υπόδειξη του Bob, τους τυχαίους αριθμούς k_i για $x-1$ μηνύματα. Ο Bob, αφού ελέγξει τα μηνύματα m_i και επαληθεύσει ότι είναι της σωστής μορφής, θα υπογράψει το εναπομείναν μήνυμα m. Η πιθανότητα της Alice να κλέψει επιτυχώς είναι $1/x$.

3.5.2 Βασικές Υποθέσεις Ασφάλειας

Στην Ενότητα αυτή αναφέρουμε ορισμένες βασικές υποθέσεις που κάναμε κατά το σχεδιασμό του πρωτοκόλλου των «Δίκαιων» δημοπρασιών [Mag00].

Υποδομή Δημοσίου Κλειδιού. Θεωρούμε ότι υπάρχει εγκατεστημένη μια *Υποδομή Δημοσίου Κλειδιού*. Οι χρήστες, προτού συμμετάσχουν στη δημοπρασία, έχουν ήδη αποκτήσει ένα ζεύγος ιδιωτικού / δημοσίου κλειδιού και το αντίστοιχο ψηφιακό πιστοποιητικό του δημοσίου κλειδιού τους, από μια Αρχή Πιστοποίησης. Το πιστοποιητικό αυτό χρησιμοποιείται για την επαλήθευση των ψηφιακών υπογραφών καθώς και για την ασφαλή ανταλλαγή κρυπτογραφικών κλειδιών. Όλοι οι χρήστες δεσμεύονται από την υπογραφή τους: έχουν ήδη προταθεί αρκετοί μηχανισμοί για τον καταλογισμό ευθύνης στις ψηφιακές υπογραφές (π.χ. [You97]).

Ανώνυμο Κανάλι Επικοινωνίας. Υπάρχει ένα κανάλι στο οποίο οι χρήστες αποστέλλουν μηνύματα των οποίων η προέλευση δεν είναι δυνατόν να καθοριστεί (π.χ. με τεχνικές ανάλυσης κίνησης – traffic analysis). Για παράδειγμα, η ανωνυμία στα μηνύματα ηλεκτρονικού ταχυδρομείου (e-mail) μπορεί να επιτευχθεί με τεχνικές δικτύων MIX-net [Cha81,Cot02]. Σε επίπεδο HTTP, η ανωνυμία επιτυγχάνεται με υπηρεσίες όπως το Anonymizer [Com02], το σύστημα CROWDS [Rei97], το LUCENT (Lucent Personalized

Web Assistant) [Luc02], καθώς και την τεχνική Onion Routing [Gol99]. Οι τεχνικές LPWA και Onion Routing, εκτός από δεδομένα HTTP, μπορούν επίσης να χειριστούν μηνύματα ηλεκτρονικού ταχυδρομείου. Η τεχνική Onion Routing επίσης επιτρέπει τη δρομολόγηση απαντήσεων σε ανώνυμα μηνύματα.

Επιβεβαιωμένη Παράδοση (Certified Delivery). Θεωρούμε την ύπαρξη μιας υπηρεσίας *Επιβεβαιωμένης Παράδοσης*. Η υπηρεσία αυτή μπορεί να υλοποιηθεί κρυπτογραφικά με τις τεχνικές που περιγράφονται στις εργασίες [Aso98,Cam96,Tyg96] και ικανοποιεί τις απαιτήσεις της *ατομικότητας* και της *ανωνυμίας* των χρηστών. Η ατομικότητα εξασφαλίζει ότι ο χρήστης υποβάλλει μια *κρυπτογραφημένη προσφορά* και λαμβάνει πίσω μια *απόδειξη παραλαβής* (receipt of delivery) της προσφοράς του από το Δημοπράτη, χωρίς να είναι δυνατή κάποια ενδιάμεση κατάσταση π.χ.:

- Ο Δημοπράτης να λαμβάνει την προσφορά αλλά ο χρήστης να μην έχει λάβει την απόδειξη, ή

- Ο χρήστης να λαμβάνει την απόδειξη αλλά ο Δημοπράτης να μην έχει λάβει την προσφορά.

Στην εργασία [Cam96] οι απαιτήσεις της ανωνυμίας και της ατομικότητας εκπληρώνονται χωρίς την ανάγκη ύπαρξης μιας τρίτης οντότητας, ενώ στην [Aso98] μια τρίτη έμπιστη οντότητα συμμετέχει κατά *βέλτιστο* τρόπο, καθώς αναμειγνύεται στο πρωτόκολλο μόνον εφόσον κάποιο από τα δυο συμβαλλόμενα μέρη συμπεριφέρεται κακόβουλα (ή απλά δυσλειτουργεί).

Σήμερα υπάρχουν μη κρυπτογραφικές ηλεκτρονικές υπηρεσίες έμπιστης οντότητας που παρέχουν Επιβεβαιωμένη Παράδοση (π.χ. [Cer02]). Αρκετά κρυπτογραφικά πρωτόκολλα επικαλούνται τη λειτουργία τέτοιων υπηρεσιών (π.χ. [Stu99]).

Αντιμετώπιση Ισόποσων Προσφορών (Tie Breaking). Υποθέτουμε ότι δεν μπορεί να υπάρξει ισοπαλία μεταξύ δύο νικητήριων προσφορών[38]. Εναλλακτικά, το πρόβλημα των ισόποσων προσφορών θα μπορούσε να αντιμετωπιστεί με κρυπτογραφικές τεχνικές *Ρίψης Κερμάτων* (Coin Flipping) [Rab83] για τον καθορισμό του νικητή, η επίσης με τεχνικές παρόμοιες με αυτές που περιγράφονται στην εργασία [Har99], όπου το πρόβλημα αντιμετωπίζεται προσθέτοντας επιπλέον γύρους, κάθε φορά που προκύπτει ισοπαλία μεταξύ των υψηλότερων προσφορών.

3.5.3 Ένα Πρωτόκολλο «Δίκαιων» Δημοπρασιών

Το σύστημά μας χρησιμοποιεί δύο ανεξάρτητες οντότητες, τον Ληξίαρχο (Registrar) και τον Δημοπράτη (Auctioneer). Ο Ληξίαρχος αυθεντικοποιεί τους εξουσιοδοτημένους χρήστες ενώ ο Δημοπράτης επεξεργάζεται τις υποβληθείσες προσφορές [Mag00].

Ο λόγος που χρησιμοποιούμε δύο οντότητες, αντί για μία, είναι για επιπλέον προστασία της ανωνυμίας των χρηστών, ώστε ο δημοπράτης να μη γνωρίζει την ταυτότητα όσων συμμετέχουν στη δημοπρασία. Ο Ληξίαρχος είναι έμπιστη οντότητα, μόνο ως προς το πρώτο σκέλος της απαίτησης για ανωνυμία (Ενότητα 3.3): οι χρήστες εμπιστεύονται το Ληξίαρχο να μην αποκαλύψει τα ονόματα τους στον Δημοπράτη ή σε άλλο χρήστη.

Οι Ληξίαρχος και Δημοπράτης δεν χρειάζεται να επικοινωνήσουν κατά τη διάρκεια του πρωτοκόλλου, δηλαδή δεν υφίστανται υψηλό επικοινωνιακό φόρτο, επομένως μπορούν στην πράξη να υλοποιηθούν ως δυο ανεξάρτητοι εξυπηρετητές.

Για την εγγραφή των χρηστών στο σύστημα χρησιμοποιούμε μια τεχνική παρόμοια με την τεχνική των *Ανώνυμων Πιστοποιητικών Δημοσίου Κλειδιού* (Anonymous Public Key Certificates) [Ois98], *ΑΠΔΚ* στη συνέχεια, τα οποία

[38] Για παράδειγμα, το σύστημα μπορεί να απαιτεί οι προσφορές που υποβάλλονται κατά τη διάρκεια της δημοπρασίας να είναι της μορφής ευρώ / λεπτά (π.χ 154.56 ευρώ) ώστε να περιοριστεί η πιθανότητα ισοπαλίας μεταξύ δυο προσφορών.

πιστοποιούν την εγκυρότητα ενός δημοσίου κλειδιού αλλά δεν επιτρέπουν σε κάποιον τρίτο τη σύνδεση του κλειδιού με την πραγματική ταυτότητα του χρήστη. Τα ανώνυμα αυτά δημόσια κλειδιά μπορούν να χρησιμοποιηθούν είτε ως *ψευδώνυμα* για την επικοινωνία του χρήστη με τον Δημοπράτη, είτε για την επαλήθευση ψηφιακών υπογραφών.

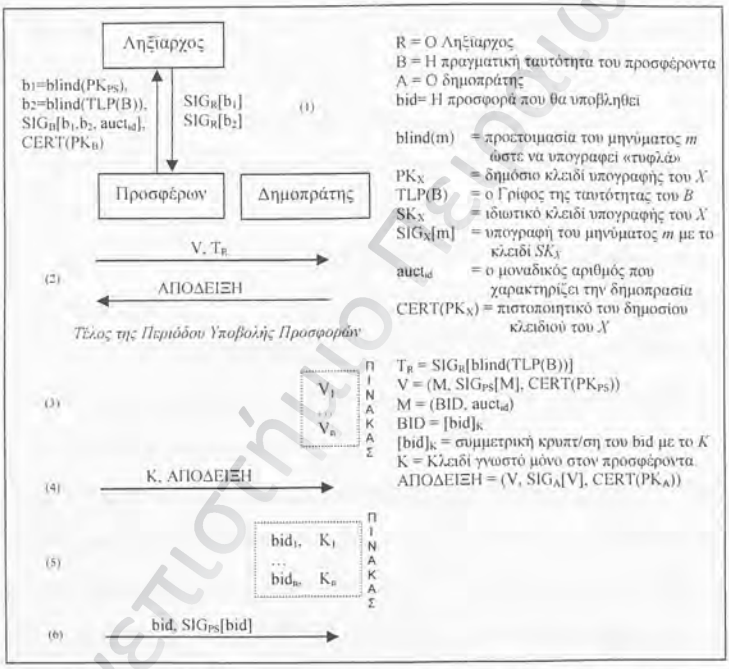
Για *καταλογισμό ευθύνης* σε περίπτωση απόσυρσης μιας προσφοράς, η ανωνυμία των δημοσίων κλειδιών (ή αλλιώς ψευδωνύμων) είναι ανακλήσιμη. Η πραγματική ταυτότητα του χρήστη «κρύβεται» κρυπτογραφικά σε έναν Γρίφο Συγκεκριμένου Χρόνου Επίλυσης ο οποίος περιέχεται στο *ΑΠΔΚ* και μπορεί να ανακληθεί σε περίπτωση απόσυρσης της προσφοράς από τον χρήστη.

Η Δημοπρασία ολοκληρώνεται σε έξι διακριτά βήματα (Σχήμα 11):

Βήμα 1, Εγγραφή. Ένας χρήστης, ας πούμε ο Bob, κατασκευάζει ένα ψευδώνυμο με το οποίο αργότερα θα συσταθεί στον Δημοπράτη. Αυτό γίνεται δημιουργώντας ένα ζεύγος ιδιωτικού / δημοσίου κλειδιού $\{SK_{PS}, PK_{PS}\}$ και έναν Γρίφο Συγκεκριμένου Χρόνου Επίλυσης που περιέχει την ταυτότητα του, $TLP(B)$. Ο Bob μετασχηματίζει τα $TLP(B)$ και PK_{PS} προκειμένου να τα υποβάλλει στον Ληξίαρχο για «τυφλή» υπογραφή. Ας ονομάσουμε τους δύο μετασχηματισμούς b_1, b_2 αντίστοιχα. Στη συνέχεια, ο Bob υπογράφει ένα μήνυμα το οποίο απαρτίζεται από τα b_1, b_2 και έναν μοναδικό αριθμό που καθορίζει τη δημοπρασία στην οποία θα υποβληθεί η προσφορά, $auct_{id}$. Ο Bob στέλνει το υπογεγραμμένο μήνυμα στον Ληξίαρχο ο οποίος το υπογράφει «τυφλά». Για την ορθότητα των μετασχηματισμών μπορεί να χρησιμοποιηθεί ένα πρωτόκολλο «Διαίρει και Επίλεξε», το οποίο εξασφαλίζει ότι σε περίπτωση απόσυρσης της προσφοράς, ο Γρίφος μπορεί να επιλυθεί και να αποκαλύψει την ταυτότητα του Bob.

Μετά το Βήμα 1, ο Bob ανακτά τα $TLP(B)$ και PK_{PS}, υπογεγραμμένα από τον Ληξίαρχο. Η υπογραφή του Ληξίαρχου στο δημόσιο κλειδί PK_{PS} και τον Γρίφο $TLP(B)$ μπορεί να θεωρηθεί ως ένα Ανώνυμο Πιστοποιητικό

Δημοσίου Κλειδιού $CERT(PK_{PS})$ το οποίο θα χρησιμοποιηθεί από το Δημοπράτη, στο Βήμα 2, για να επαληθεύσει οποιοδήποτε υπογεγραμμένο μήνυμα υποβληθεί από την οντότητα με ψευδώνυμο PK_{PS} (δηλαδή τον Bob). Στη συνέχεια του πρωτοκόλλου, θα χρησιμοποιήσουμε το συμβολισμό T_R για να συμβολίσουμε τον Γρίφο $TLP(B)$ του Bob, όταν αυτός υπογραφεί από τον Ληξίαρχο.



Σχήμα 11. Μία Κλειστή Δημοπρασία Πρώτης/Δεύτερης Τιμής

Βήμα 2, Υποβολή της Προσφοράς. Ο Bob κρυπτογραφεί την προσφορά του με ένα μυστικό συμμετρικό κλειδί K, έπειτα ετοιμάζει ένα μήνυμα M το οποίο αποτελείται από την προσφορά $[bid]_K$ και το μοναδικό αριθμό $auct_{id}$. Ο Bob υπογράφει το M με το ιδιωτικό κλειδί υπογραφής SK_{PS} που αντιστοιχεί στο ψευδώνυμό του PK_{PS} δημιουργώντας έτσι μία έγκυρη

προσφορά V. Ο Bob στέλνει ανώνυμα[39] τα V και T_R στον Δημοπράτη, χρησιμοποιώντας επίσης την υπηρεσία Επιβεβαιωμένης Παράδοσης, και λαμβάνει μια απόδειξη λήψης της προσφοράς από το Δημοπράτη. Ο Δημοπράτης χρησιμοποιεί το πιστοποιητικό $CERT(PK_{PS})$ για να επαληθεύσει την υπογραφή, ελέγχει το $auct_{id}$ και επαληθεύει την υπογραφή του Ληξίαρχου στο T_R. Εάν όλοι οι έλεγχοι είναι επιτυχείς, ο Δημοπράτης αποθηκεύει τα V και T_R στη βάση δεδομένων που διατηρεί.

Βήμα 3, Δημοσίευση των Κρυπτογραφημένων Προσφορών. Μόλις εκπνεύσει η προθεσμία υποβολής προσφορών, ο Δημοπράτης δημοσιεύει σε ένα Πίνακα Ανακοινώσεων όλα τα V_i, συμπεριλαμβανομένων και των κρυπτογραφημένων προσφορών. Κατ' αυτόν τον τρόπο, ο Δημοπράτης δεσμεύεται ότι τα κρυπτογραφημένα αποτελέσματα είναι έγκυρα. Προαιρετικά ο Δημοπράτης μπορεί επίσης να δημοσιεύσει και τους χρόνους παραλαβής των προσφορών V_i, τους οποίους θα έχει προμηθευτεί από την υπηρεσία Επιβεβαιωμένης Παράδοσης, ώστε να είναι σαφές πως δεν έχουν γίνει δεκτές προσφορές πέρα από τη λήξη της προθεσμίας υποβολής προσφορών.

Βήμα 4, Αποκάλυψη των Προσφορών. Ο Bob στέλνει στο Δημοπράτη, μέσω ενός ανώνυμου καναλιού επικοινωνίας, το κλειδί για την αποκρυπτογράφηση της προσφοράς, K, καθώς και την απόδειξη λήψης που κατέχει από το Βήμα 2. Ο Δημοπράτης χρησιμοποιεί την απόδειξη για να ανακτήσει από τη βάση δεδομένων την αντίστοιχη κρυπτογραφημένη προσφορά, και στη συνέχεια με τη βοήθεια του κλειδιού K αποκρυπτογραφεί την προσφορά. Στην περίπτωση που ο Bob δεν υποβάλλει το κλειδί, μέσα σε προκαθορισμένα χρονικά πλαίσια, τότε ο Δημοπράτης μπορεί να επιλύσει τον Γρίφο T_R και να αποκαλύψει την ταυτότητα του Bob.

[39] Χρησιμοποιώντας ένα ανώνυμο κανάλι επικοινωνίας, όπως αυτό που περιγράφεται στην Ενότητα 3.5.2.

Βήμα 5, Τελικά Αποτελέσματα. Ο Δημοπράτης δημοσιοποιεί όλες τις αποκρυπτογραφημένες προσφορές, καθώς και τα κλειδιά με τα οποία αυτές αποκρυπτογραφήθηκαν. Ο νικητής της δημοπρασίας καθορίζεται και όλοι οι συμμετέχοντες μπορούν να επαληθεύσουν τα αποτελέσματα της δημοπρασίας. Το ποσό που θα πληρώσει ο νικητής εξαρτάται από το εάν η δημοπρασία είναι Πρώτης Τιμής ή Δεύτερης Τιμής.

Βήμα 6, Η αξίωση του Νικητή. Εάν ο Bob είναι ο πλειοδότης, υπογράφει με το ιδιωτικό ψευδώνυμο κλειδί υπογραφής του, SK_{PS}, ένα μήνυμα, το οποίο θα αναφέρει π.χ. τη νικητήρια προσφορά της δημοπρασίας, και στέλνει το υπογεγραμμένο μήνυμα στον Δημοπράτη.

Ο Bob ανακηρύσσεται νικητής και καλείται να συναλλαγεί με τον πωλητή του αγαθού, για την πληρωμή και την παραλαβή του αγαθού. Τονίζουμε πως ο Bob, προκειμένου αργότερα να ολοκληρώσει τη συναλλαγή με τον πωλητή, δε χρειάζεται να αποκαλύψει την αληθινή του ταυτότητα [Cha85].

3.5.3.1 Ανάλυση της Ασφάλειας του Πρωτοκόλλου

Το πρωτόκολλο για Κλειστές Δημοπρασίες που παρουσιάσαμε στην προηγούμενη Ενότητα παρέχει προστασία για τους χρήστες, τον Δημοπράτη και τον Ληξίαρχο ενάντια σε κακόβουλη συμπεριφορά οποιουδήποτε συμμετέχοντα [Mag00]. Θεωρούμε ότι οι Ληξίαρχος και Δημοπράτης δεν είναι έμπιστες οντότητες, καθώς υπάρχει περίπτωση να συμπεριφερθούν κακόβουλα. Στη συνέχεια αναλύουμε την ασφάλεια του πρωτοκόλλου εξετάζοντάς το βαθμό στον οποίο ικανοποιεί τις απαιτήσεις ασφάλειας που περιγράψαμε στην Ενότητα 3.3.

Ανωνυμία. Εξετάζουμε την ανωνυμία που παρέχει το πρωτόκολλο στους χρήστες, ως προς κάθε ένα από τα δύο σκέλη της απαίτησης για ανωνυμία:

- **Η ταυτότητα των χρηστών είναι μυστική.** Ο δημοπράτης δε γνωρίζει την ταυτότητα των χρηστών που συμμετέχουν στη δημοπρασία. Αυτές τις γνωρίζει ο Ληξίαρχος, τον οποίο οι χρήστες εμπιστεύονται πως δεν θα τις αποκαλύψει στον Δημοπράτη ή κάποιον άλλο χρήστη. Εάν ωστόσο ο Ληξίαρχος παραβιάσει την εμπιστοσύνη αυτή και συνεργαστεί με τον Δημοπράτη, τότε ο Δημοπράτης θα μάθει τις ταυτότητες όλων των συμμετεχόντων στη Δημοπρασία. Οι συνέπειες στην ασφάλεια του συστήματος από μια τέτοια κατάσταση μπορούν να χαρακτηριστούν ως αποδεκτές (όπως συζητήσαμε στην Ενότητα 3.2, το πρώτο αυτό σκέλος της ανωνυμίας είναι περισσότερο σημαντικό στις Ανοικτές Δημοπρασίες).

Σημείωση: Εφόσον θεωρήσαμε υπαρκτή την πιθανότητα συνεργίας μεταξύ Ληξίαρχου και Δημοπράτη, το σύστημα μας τελικά θα ήταν το ίδιο ασφαλές, ως προς το πρώτο σκέλος της ανωνυμίας, αν χρησιμοποιούσαμε μόνο μια αντί για δύο οντότητες. Εντούτοις η σκοπιμότητα χρησιμοποίησης των δυο οντοτήτων εξακολουθεί να υφίσταται, για λόγους καθαρά σχεδιαστικούς και για την σωστή διαχείριση της πρόσβασης στους υπολογιστικούς πόρους του συστήματος. Έτσι, σε ένα σύστημα δημοπρασιών μεγάλης κλίμακας ο Ληξίαρχος θα αυθεντικοποιούσε τους συμμετέχοντες σε όλες τις δημοπρασίες για τις οποίες θα ήταν υπεύθυνος, απαλλάσσοντας τους εξυπηρετητές των δημοπρασιών από το επιπρόσθετο επικοινωνιακό φόρτο [Mag00,Mil87].

- **Καμία προσφορά δεν είναι δυνατόν να συνδεθεί με την ταυτότητα ενός συγκεκριμένου χρήστη.** Ο Bob χρησιμοποιεί την αληθινή του ταυτότητα για να αυθεντικοποιήσει το ψευδώνυμο που υποβάλλει στον Ληξίαρχο. Ωστόσο το ψευδώνυμο έχει ήδη μετασχηματιστεί κατάλληλα ώστε ο Ληξίαρχος να το υπογράψει «τυφλά». Ως αποτέλεσμα, ο

Ληξίαρχος δεν μπορεί να συνδέσει το ψευδώνυμο PK_{PS}, με το οποίο αργότερα ο Bob συστήνεται στον Δημοπράτη, με την αληθινή ταυτότητα του Bob.

Ο Δημοπράτης επίσης λαμβάνει προσφορές οι οποίες δεν μπορούν να συνδεθούν με την ταυτότητα του αποστολέα τους (το κανάλι επικοινωνίας είναι ανώνυμο) και οι οποίες είναι υπογεγραμμένες με ένα πιστοποιημένο ψευδώνυμο. Ο Δημοπράτης δε μπορεί να συνδέσει το ψευδώνυμο με την αληθινή ταυτότητα του Bob, επομένως ο μοναδικός τρόπος να ανακαλύψει την προέλευση της προσφοράς είναι να επιλύσει τον Γρίφο $TLP(B)$ ο οποίος του υποβλήθηκε στο Βήμα 2.

Εάν ο Δημοπράτης συμμαχήσει με τον Ληξίαρχο, τότε και πάλι δε θα μπορούν να συνδέσουν μια δεδομένη προσφορά με τον Bob, αφού η *μη συνδεσιμότητα* μεταξύ των προσφορών και των ταυτοτήτων των χρηστών που τις υπέβαλαν εξακολουθεί να υφίσταται, χάρη στο πρωτόκολλο της «τυφλής» υπογραφής που εκτελείται μεταξύ των χρηστών και του Ληξίαρχου κατά τη διάρκεια της Εγγραφής. Εντούτοις εάν ο Bob υποβάλλει την προσφορά του στον Δημοπράτη αμέσως μετά την εκτέλεση του Βήματος 1, τότε οι Δημοπράτης και Ληξίαρχος μπορούν μαζί να μαντέψουν σωστά την προέλευση της προσφοράς. Αυτό το πρόβλημα μπορεί να λυθεί εν μέρει χρησιμοποιώντας έναν *remailer* τύπου *MIX* (Ενότητα 2.3.1) που θα ενσωματώνει υπηρεσίες *καθυστέρησης* (latency) και *αναδιάταξης* (reordering) [Cot02] των μηνυμάτων που διαχειρίζεται. Εναλλακτικά, συνίσταται στους χρήστες να μην υποβάλλουν προσφορές αμέσως μετά την Εγγραφή τους. Το είδος της Δημοπρασίας που επιλέχθηκε για υλοποίηση (Κλειστή), ευνοεί αυτήν την προσέγγιση.

Επισημαίνουμε επίσης πως στο Βήμα 6 ο νικητής αξιώνει το αγαθό χωρίς να αποκαλύψει την αληθινή του ταυτότητα στον Δημοπράτη. Για να μάθει την αληθινή ταυτότητα του νικητή, ο Δημοπράτης πρέπει να επιλύσει τον αντίστοιχο Γρίφο.

Μυστικότητα. Μετά από το Βήμα 2 και μέχρι το τέλος της περιόδου υποβολής των προσφορών, οι προσφορές προστατεύονται από τη συμμετρική κρυπτογράφηση (π.χ. AES με κλειδί 128-bit). Κάποιος θα πρέπει να «σπάσει» το συμμετρικό αλγόριθμο προκειμένου να άρει τη μυστικότητα της προσφοράς. Μετά από το Βήμα 4, και όταν όλοι οι χρήστες υποβάλλουν τα κρυπτογραφικά κλειδιά, δεν υπάρχει μυστικότητα για τις προσφορές, ωστόσο η ανωνυμία των χρηστών (ως και προς τα δύο σκέλη) εξακολουθεί να υφίσταται.

Ορθότητα. Ελέγχουμε τις επιμέρους ιδιότητες της απαίτησης της ορθότητας, όπως αυτές ορίστηκαν στην Ενότητα 3.3.

- **Μόνο εξουσιοδοτημένοι χρήστες υποβάλλουν έγκυρες προσφορές.** Υπάρχουν δυο παράγοντες που στοιχειοθετούν το δικαίωμα του Bob να συμμετάσχει στη δημοπρασία: Το πιστοποιητικό $CERT(PK_{PS})$ και ο Γρίφος T_R.

  Ο Δημοπράτης χρησιμοποιεί το πιστοποιητικό $CERT(PK_{PS})$ για να επαληθεύσει ότι ο Bob είναι νόμιμος χρήστης του συστήματος, ενώ απορρίπτει όλες τις προσφορές που δε συνοδεύονται από αντίστοιχο πιστοποιητικό. Κάποιος εξωτερικός παρατηρητής μπορεί επίσης να επαληθεύσει, με τη χρήση του πιστοποιητικού $CERT(PK_{PS})$ ότι οι προσφορές που έχουν δημοσιευτεί στο Βήμα 3 έχουν υποβληθεί από εξουσιοδοτημένους χρήστες και όχι από το Δημοπράτη.

  Ο Γρίφος T_R χρησιμοποιείται από τον Δημοπράτη στον καταλογισμό ευθύνης για τις υποβληθείσες προσφορές. Ο Bob λαμβάνει τον T_R υπογεγραμμένο από τον Ληξίαρχο κατά το Βήμα 1, έχοντας ήδη αποδείξει, με τη βοήθεια ενός «Διαίρει και Επίλεξε» πρωτοκόλλου, ότι ο T_R συνδέεται με την ταυτότητα του. Ο Δημοπράτης γνωρίζει επομένως ότι ο ιδιοκτήτης του T_R είναι ένας εξουσιοδοτημένος χρήστης του οποίου

η ταυτότητα μπορεί να ανακαλυφθεί σε περίπτωση απόσυρσης της προσφοράς.

- **Κανείς δε μπορεί να πλαστοπροσωπήσει έναν χρήστη.** Υπάρχουν αρκετοί λόγοι για τους οποίους κάποιος θα ήθελε να συνδέσει μια προσφορά με την ταυτότητα ενός άλλου εξουσιοδοτημένου χρήστη, ας πούμε του Bob. Για παράδειγμα, ώστε να ενοχοποιήσει τον Bob κάνοντας μια πολύ υψηλή προσφορά και στη συνέχεια αποσύροντας την προσφορά. Εναλλακτικά, ο Δημοπράτης θα μπορούσε να υποβάλλει μια υψηλή προσφορά ώστε να είναι σίγουρος ότι το αγαθό υπό δημοπρασία δεν πρόκειται να αγοραστεί κάτω από αυτήν τιμή.

  Ο Ληξίαρχος γνωρίζει την ταυτότητα του Bob, επομένως μπορεί να κατασκευάσει έναν «πλαστό» T_R^* και να πλαστοπροσωπήσει τον Bob στο Δημοπράτη (ή να δώσει τον T_R^* σε έναν γνωστό του). Εντούτοις, ο T_R^* δε στοιχειοθετεί καταλογισμό ευθύνης για τον Bob, στην περίπτωση που η «πλαστή» προσφορά αποδειχθεί η υψηλότερη (ή στην περίπτωση που η προσφορά αποσυρθεί): ο Bob μπορεί να αποδείξει αργότερα την αθωότητα του εμφανίζοντας το δικό του έγκυρο Γρίφο T_R. Εάν ο T_R είναι διαφορετικός από το πλαστό T_R^* (και θα είναι, με μεγάλη πιθανότητα, αφού ο Bob έλαβε το T_R κατά το Βήμα 1 με τη βοήθεια ενός Διαίρει και Επίλεξε πρωτοκόλλου) τότε όλοι θα γνωρίζουν ότι ο Ληξίαρχος έχει φερθεί κακόβουλα.

  Ο Δημοπράτης γνωρίζει τον Γρίφο T_R του Bob έπειτα από το Βήμα 2, επομένως μπορεί να τον χρησιμοποιήσει για να κατασκευάσει μία πλαστή προσφορά (ή να τον δώσει σε έναν γνωστό του για τον ίδιο σκοπό) προκειμένου να παγιδεύσει τον Bob. Όμως, και σε αυτήν την περίπτωση ο Bob μπορεί να αποδείξει ότι ο Δημοπράτης έκλεψε: όταν ο Bob υποβάλλει την προσφορά του μαζί με τον αυθεντικό T_R, λαμβάνει μια απόδειξη παραλαβής, υπογεγραμμένη σε συγκεκριμένο χρόνο από την υπηρεσία Επιβεβαιωμένης Παράδοσης. Η απόδειξη παραλαβής

μπορεί λοιπόν να χρησιμοποιηθεί από τον Bob για να αποδείξει ότι η προσφορά του έχει υποβληθεί νωρίτερα.

- **Οι προσφορές δεν αλλοιώνονται / διαγράφονται από το Δημοπράτη.** Η χρήση της υπηρεσίας Επιβεβαιωμένης Παράδοσης, κατά το Βήμα 2, αποτρέπει το Δημοπράτη από το να αλλοιώσει έγκυρες προσφορές. Η ίδια υπηρεσία επίσης επιτρέπει στους χρήστες να αποδείξουν, σε έναν διαιτητή (arbitrator) ότι, για παράδειγμα, ο Δημοπράτης έλαβε ένα μήνυμα M σε χρόνο t. Συνεπώς, ο Δημοπράτης δε μπορεί να διαγράψει μία προσφορά με το πρόσχημα ότι αυτή υποβλήθηκε καθυστερημένα. Μετά τη δημοσίευση των προσφορών, στο Βήμα 3, ο Δημοπράτης δεσμεύεται έναντι των κρυπτογραφημένων αποτελεσμάτων και δε μπορεί να τα αλλοιώσει, χωρίς αυτό να γίνει αντιληπτό.

- **Οι προσφορές είναι έγκυρες μόνον για αυτήν τη δημοπρασία.** Κατά τη διάρκεια του πρωτοκόλλου, ένας μοναδικός αριθμός $auct_{id}$ χρησιμοποιείται ως ενδεικτικό του *επίκαιρου* (freshness) της προσφοράς. Ο Δημοπράτης απορρίπτει όλα τα μηνύματα που δεν είναι υπογεγραμμένα και που δεν περιέχουν τον αριθμό $auct_{id}$. Στο Βήμα 3, το $auct_{id}$ δημοσιεύεται μαζί με την κρυπτογραφημένη προσφορά, ως τμήμα του μηνύματος V.

- **Ο νικητής είναι αυτός που κάνει την υψηλότερη προσφορά.** Αυτή η απαίτηση εκπληρώνεται σε κάθε περίπτωση. Ουσιαστικά εμπίπτει στην απαίτηση της επαληθευσιμότητας, η οποία αναλύεται στη συνέχεια.

Επαληθευσιμότητα. Όλοι οι συμμετέχοντες μπορούν να επαληθεύσουν τα αποτελέσματα της δημοπρασίας. Τα κρυπτογραφημένα αποτελέσματα δημοσιεύονται στο Βήμα 3. Στο Βήμα 5, όλες οι αποκρυπτογραφημένες προσφορές δημοσιεύονται μαζί με τα κλειδιά που χρησιμοποιήθηκαν. Τα αποτελέσματα αυτά, έναντι των οποίων ο Δημοπράτης έχει ήδη δεσμευτεί,

πρέπει να αντιστοιχίζονται μοναδικά με τα αποτελέσματα του Βήματος 3. Ο Δημοπράτης θα είναι υπεύθυνος για οποιαδήποτε αναντιστοιχία. Ένας παρατηρητής μπορεί να επαληθεύσει τα αποτελέσματα π.χ. κρυπτογραφώντας τις τελικές προσφορές με τα συμμετρικά κλειδιά που δημοσιεύονται και επαληθεύοντας τις υπογραφές στις υποβληθείσες προσφορές (χρησιμοποιώντας τα δημοσιευμένα πιστοποιητικά).

Καταλογισμός Ευθύνης. Το «σημείο μη επιστροφής» για τον Bob μπορεί να είναι είτε η ανώνυμη αποστολή προσφοράς στο Βήμα 2, πριν τη λήξη της περιόδου υποβολής προσφορών (*Ισχυρός Καταλογισμός Ευθύνης*), είτε η ανώνυμη αποστολή του συμμετρικού κλειδιού αποκρυπτογράφησης K στο Βήμα 4, μετά το πέρας της περιόδου υποβολής προσφορών (*Ασθενής Καταλογισμός Ευθύνης*).

Σε κάθε περίπτωση ο πλειοδότης δε μπορεί να αποποιηθεί την ευθύνη για την προσφορά του. Εάν το κάνει αυτό, δηλαδή εάν δεν ολοκληρώσει το Βήμα 6 μέσα σε προκαθορισμένο χρονικό διάστημα, τότε ο Δημοπράτης μπορεί να ανακαλύψει την ταυτότητα του πλειοδότη επιλύνοντας τον Γρίφο Συγκεκριμένου Χρόνου Επίλυσης. Ο πλειοδότης τότε, θα υπόκειται σε μια χρηματική ποινή, εκ των προτέρων γνωστή και συμφωνηθείσα μεταξύ των χρηστών και των Αρχών του συστήματος [Stu99]. Για παράδειγμα η ποινή θα μπορούσε να είναι ίση με το κόστος της επίλυσης του Γρίφου, συν τη διαφορά της αποσυρθείσας προσφοράς από τη δεύτερη καλύτερη προσφορά (που τελικά θα είναι και η νικητήρια).

Σημείωση: Τονίζουμε ξανά πως η επίλυση του Γρίφου δεν διευκολύνεται με την εκ παραλλήλου λειτουργία δύο ή περισσότερων υπολογιστικών συστημάτων. Εάν συνέβαινε αυτό, π.χ. στην περίπτωση κρυπτογράφησης της αληθινής ταυτότητας του Bob με ένα ασθενές κλειδί – π.χ. 40 bit, τότε η ιδιωτικότητα των χρηστών των δημοπρασιών θα τίθονταν υπό αμφισβήτηση, αν αναλογιστούμε τους τεράστιους υπολογιστικούς πόρους που διαθέτουν σήμερα τα διαφημιστικά δίκτυα πώλησης και αγοράς προσωπικών δεδομένων. Αυτός είναι και ο λόγος για τον οποίον επιλέξαμε το

μηχανισμό των Γρίφων Συγκεκριμένου Χρόνου Επίλυσης, ως βασικό μηχανισμό καταλογισμού ευθύνης.

- **Ισχυρός Καταλογισμός Ευθύνης – (Strong Non Repudiation)**. Όλοι οι χρήστες δεσμεύονται από τις προσφορές που δημοσιεύονται στο Βήμα 3, και πρέπει να διαθέσουν στο Δημοπράτη τα απαραίτητα κλειδιά για την αποκρυπτογράφηση τους. Για κάθε χρήστη που δεν διαθέτει το κλειδί K, ο Δημοπράτης εξουσιοδοτείται να επιλύσει το Γρίφο T_R προκειμένου να αποκαλυφθεί η αληθινή ταυτότητα του χρήστη που απέσυρε την προσφορά του (και να του επιβληθεί η προκαθορισμένη ποινή). Η προστασία της δημοπρασίας από χρήστες που αποσύρουν τις προσφορές τους, σε συνδυασμό με την προστασία της ανωνυμίας των υπόλοιπων χρηστών, καθιστά το πρωτόκολλο «Δίκαιο» για τους χρήστες και τον Δημοπράτη / Πωλητή.

- **Ασθενής Καταλογισμός Ευθύνης – (Weak Non Repudiation)**. Κατά την υλοποίηση αυτή είναι επιτρεπτό για ένα χρήστη να μην φανερώσει το κλειδί K για την αποκρυπτογράφηση της προσφοράς του που έχει δημοσιευτεί στο Βήμα 3 (δηλαδή να αποσύρει την προσφορά του). Σε αυτήν την περίπτωση, και για να υπάρξει νικητής, πρέπει τουλάχιστον ένας χρήστης να εκτελέσει το Βήμα 4. Όλες οι προσφορές, για τις οποίες υποβλήθηκαν τα κλειδιά αποκρυπτογράφησης μέσα στο προκαθορισμένο χρονικό πλαίσιο, δημοσιεύονται στο Βήμα 5. Οι χρήστες δεσμεύονται (υπάρχει δηλαδή καταλογισμός ευθύνης) μόνον για αυτές τις προσφορές.

Προστασία από Καταναγκασμό. Το πρωτόκολλο μας δεν παρέχει προστασία από καταναγκασμό. Στην Ενότητα 3.6 θα συζητήσουμε μηχανισμούς για την επίτευξη προστασίας από καταναγκασμό στις Κλειστές Δημοπρασίες και θα προτείνουμε ένα πρωτόκολλο Κλειστών Ηλεκτρονικών Δημοπρασιών με προστασία από καταναγκασμό και οικουμενική επαληθευσιμότητα.

3.6 Μια Ηλεκτρονική Δημοπρασία με Προστασία από Καταναγκασμό

Στην Ενότητα 3.2 καταδείξαμε την αναγκαιότητα για *προστασία από καταναγκασμό* στις ηλεκτρονικές δημοπρασίες. Στη συνέχεια περιγράφουμε ένα πρωτόκολλο για Κλειστές Δημοπρασίες Πρώτης/Δεύτερης Τιμής, στο οποίο επιτυγχάνεται Προστασία από Καταναγκασμό [Bur_Mag02a].

Το πρωτόκολλο που προτείνουμε εκπληρώνει όλες τις απαιτήσεις ασφάλειας για τις ηλεκτρονικές δημοπρασίες, όπως αυτές διατυπώθηκαν στην Ενότητα 3.3, και επιπλέον παρέχει *οικουμενική επαληθευσιμότητα*: ένας εξωτερικός παρατηρητής μπορεί να βεβαιωθεί ότι τα αποτελέσματα της δημοπρασίας είναι έγκυρα. Αυτό επεκτείνει την ασφάλεια σε πρωτόκολλα δημοπρασιών που έχουν προταθεί έως σήμερα, συμπεριλαμβανομένου και του «Δικαίου» πρωτοκόλλου (Ενότητα 3.5), τα οποία παρέχουν μόνο *ατομική επαληθευσιμότητα*, π.χ. αν διαγραφεί η προσφορά του Bob από το Δημοπράτη τότε μόνον ο Bob μπορεί να αποδείξει την κακόβουλη πράξη του Δημοπράτη.

Οι συμμετέχοντες στο πρωτόκολλο είναι οι χρήστες και οι Δημοπράτες. Η επιλογή περισσότερων του ενός δημοπρατών στα πλαίσια μιας κατανεμημένης Αρχής δημοπρασίας, έγινε για την προστασία της μυστικότητας των προσφορών όσο διαρκεί η περίοδος υποβολής προσφορών. Έτσι η υποβολή των προσφορών δεν χρειάζεται να γίνει σε δύο βήματα, αλλά μόνο σε ένα: οι χρήστες απλά δημοσιεύουν τις προσφορές τους σε έναν Πίνακα Ανακοινώσεων. Το μειονέκτημα αυτής της προσέγγισης είναι η πολυπλοκότητα που εισαγάγουν τα κατανεμημένα πρωτόκολλα, κατά τη *διανομή των κλειδιών* (key distribution) και την αποκρυπτογράφηση των μηνυμάτων.

Κάθε χρήστης διαθέτει μια *Κάρτα Ανθεκτική σε Παραβιάσεις* (Tamper-Resistant Card), για παράδειγμα μια Έξυπνη Κάρτα (Smart Card). Η Προστασία από Καταναγκασμό βασίζεται στο ότι ο Χρήστης και η Κάρτα

συνεισφέρουν από κοινού κάποια τυχαιότητα στην κρυπτογράφηση της προσφοράς, κατά τρόπο ώστε κανένας από τους δύο δε γνωρίζει την τυχαιότητα που επέλεξε ο άλλος. Ωστόσο, κατά την κρυπτογράφηση της προσφοράς δεν επιτρέπουμε στην Κάρτα να συμπεριφερθεί κακόβουλα και να αλλοιώσει την προσφορά που έχει επιλέξει αρχικά ο χρήστης: η Κάρτα θα πρέπει να αποδείξει στο χρήστη, με ένα πρωτόκολλο Απόδειξης με Μηδενική Γνώση, την ορθότητα των μετασχηματισμών που πραγματοποίησε.

Για κρυπτογράφηση χρησιμοποιούμε τον αλγόριθμου Δημοσίου Κλειδιού ElGamal [ElG85]. Πρόκειται για ένα *ομομορφικό* σχήμα στην πράξη του πολλαπλασιασμού, που περιγράφουμε στη συνέχεια:

Έστω $p.q$ μεγάλοι πρώτοι ώστε q διαιρέτης του $p-1$. Z_p^* η ομάδα των ακεραίων $\{x : 1 \le x \le p-1\}$ στην πράξη του πολλαπλασιασμού modulo p, G_q η υποομάδα τάξης q του Z_p^*, και g γεννήτορας του G_q. Το ιδιωτικό κλειδί επιλέγεται ως ένας τυχαίος $s : 1 \le s \le q-1$, ενώ το αντίστοιχο δημόσιο κλειδί είναι το σύνολο (p, g, h) όπου $h = g^s \bmod p$. Όλες οι πράξεις είναι modulo p, ενώ στη συνέχεια για απλότητα παραλείπουμε το $\bmod p$. Η κρυπτογράφηση ενός μηνύματος $m \in Z_p^*$ είναι $(x, y) = (g^r, h^r m)$, όπου $r : 1 \le r \le q-1$ τυχαίος. Η αποκρυπτογράφηση του (x, y) προκύπτει υπολογίζοντας $m = y / x^s$, όπου s είναι το ιδιωτικό κλειδί. Έχουμε λοιπόν:

$$\begin{aligned} e_{r_1}(m_1) \times e_{r_2}(m_2) &= (g^{r_1}, h^{r_1} m_1) \times (g^{r_2}, h^{r_2} m_2) \\ &= (g^{r_1 + r_2}, h^{r_1 + r_2} m_1 \times m_2) \\ &= (g^r, h^r m) \\ &= e_r(m) \end{aligned}$$

όπου $r = r_1 + r_2$ και $m = m_1 \times m_2$. Επομένως η κρυπτογράφηση είναι *ομομορφική* στην πράξη του πολλαπλασιασμού. Η ασφάλεια του σχήματος

ανάγεται στη δυσκολία της επίλυσης του Προβλήματος[40] Diffie-Hellman [Dif76].

Σημείωση: Στο Κεφάλαιο 2, κατά την κατασκευή ενός πρωτοκόλλου ηλεκτρονικής ψηφοφορίας με προστασία από καταναγκασμό (Ενότητα 2.4.5), χρησιμοποιήσαμε μια παραλλαγή του αλγόριθμου κρυπτογράφησης ElGamal, με ομομορφισμό στην πράξη της πρόσθεσης. Ωστόσο, στο πρωτόκολλο των Κλειστών Ηλεκτρονικών Δημοπρασιών που θα παρουσιάσουμε στη συνέχεια, ο ομομορφισμός στην πράξη του πολλαπλασιασμού, που υποστηρίζει εγγενώς ο αλγόριθμος ElGamal, είναι επαρκής ώστε η Κάρτα να συνεισφέρει τη δική της τυχαιότητα στην κρυπτογραφημένη προσφορά. Εξάλλου, σε αντίθεση με τα συστήματα ηλεκτρονικής ψηφοφορίας, σε μια κλειστή ηλεκτρονική δημοπρασία όλες οι αποκρυπτογραφημένες προσφορές πρέπει να δημοσιευτούν για εδραίωση της επαληθευσιμότητας του συστήματος.

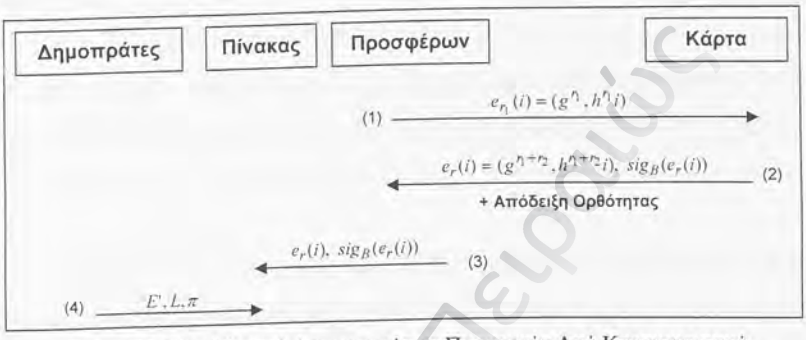
3.6.1 Το Πρωτόκολλο

1. Κρυπτογράφηση. Ένας εξουσιοδοτημένος χρήστης, έστω B επιλέγει μια προσφορά i από μια λίστα προσφορών $I \subset \{1,2,\ldots,p-1\}$, και έναν τυχαίο αριθμό $r_1 : 1 \le r_1 \le q-1$, και κρυπτογραφεί το i με το δημόσιο κλειδί h των Δημοπρατών: Υπάρχει μόνον ένα δημόσιο κλειδί, ενώ οι δημοπράτες μοιράζονται το ιδιωτικό κλειδί αποκρυπτογράφησης σύμφωνα με τις threshold τεχνικές Διαμοιρασμού Μυστικών[9] του Pedersen [Ped91]. Έστω $e_{r_1}(i) = (g^{r_1}, h^{r_1} i)$ η κρυπτογράφηση. Ο χρήστης στέλνει το $e_{r_1}(i)$ ως είσοδο στην Κάρτα (Σχήμα 12, Βήμα 1).

2. Τυχαιότητα Έξυπνης Κάρτας. Η Κάρτα συνεισφέρει τη δική της τυχαιότητα, επιλέγοντας έναν τυχαίο αριθμό $r_2 : 1 \le r_2 \le q-1$, και

[40] Σε αυτό το πρόβλημα κάποιος πρέπει να υπολογίσει το $z = g^{ab}$, δεδομένων των $x = g^a$ και $y = g^b$ στο G_q, αλλά όχι και των εκθετών a, b. Θεωρείται ένα πολύ δύσκολο πρόβλημα [Dif76].

υπολογίζοντας $e_{r_2}(1) = (g^{r_2}, h^{r_2})$. Στη συνέχεια υπολογίζει το γινόμενο $e_{r_1}(i) \times e_{r_2}(1) = e_r(i)$, όπου $r = r_1 + r_2$. Η Κάρτα επιστρέφει στην έξοδο το $e_r(i)$, μαζί με μια ψηφιακή υπογραφή $sig_B(e_r(i))$ της κρυπτογραφημένης προσφοράς (Σχήμα 12, Βήμα 2).



Σχήμα 12. Μία Κλειστή Δημοπρασία με Προστασία Από Καταναγκασμό

Για προστασία της ορθότητας, η κάρτα πρέπει να αποδείξει στον χρήστη ότι η συνεισφορά της στην τυχαιότητα, έστω $e_{r_2}(1) = (x, y)$, είναι κρυπτογράφηση του «1». Για αυτόν το λόγο η Κάρτα χρησιμοποιεί ένα πρωτόκολλο Απόδειξης με Μηδενική Γνώση για την *ισότητα δύο διακριτών λογαρίθμων* [Cha92]. Αυτή η απόδειξη ορθότητας χρησιμοποιείται για την επιβεβαίωση του ότι οι αριθμοί $x, y, g, h \in G_q$ σχετίζονται με την εξίσωση $\log_g x = \log_h y$, το οποίο είναι ισοδύναμο με την: $(x.y) = (g^{r_2}, h^{r_2})$, που αποτελεί μια κρυπτογράφηση του «1». Σε αυτό το σημείο πρέπει να αναφέρουμε ότι ο χρήστης μπορεί να υπολογίσει το $e_{r_2}(1)$ εκτελώντας $e_r(i) / e_{r_1}(i)$.

3. Δημοσίευση. Εάν η απόδειξη ορθότητας είναι έγκυρη, ο χρήστης B δημοσιεύει την κρυπτογραφημένη προσφορά $e_r(i)$ μαζί με την υπογραφή $sig_B(e_r(i))$ στον Πίνακα Ανακοινώσεων (Σχήμα 12, Βήμα 3).

4. Αποτελέσματα Δημοπρασίας. Οι δημοπράτες από κοινού αποκρυπτογραφούν τις κρυπτογραφημένες προσφορές και δημοσιεύουν στον Πίνακα Ανακοινώσεων τη λίστα L με τις αποκρυπτογραφημένες προσφορές i, η οποία συνυπάρχει με τη λίστα E' των κρυπτογραφημένων προσφορών $e_r(i)$ κατά τέτοιον τρόπο ώστε οι προσφορές i και οι κρυπτογραφήσεις τους να μην μπορούν να συνδεθούν μεταξύ τους. Για αυτόν το σκοπό επικαλούμαστε το μηχανισμό δικτύων MIX-net, που περιγράφει ο Abe [Abe98], για μηνύματα κρυπτογραφημένα με τον αλγόριθμο ElGamal. Βάσει του μηχανισμού οι δημοπράτες συμμετέχουν ως ανεξάρτητοι εξυπηρετητές σε ένα δίκτυο MIX-net και υλοποιούν τα ακόλουθα βήματα:

α) **Τυχαιότητα και Αναδιάταξη.** Οι δημοπράτες εργάζονται σειριακά και προσθέτουν τυχαιότητα σε κάθε κρυπτογραφημένη προσφορά, αναδιατάσσοντας (π.χ. επιλέγοντας μια εκ των πιθανών μεταθέσεων των στοιχείων της λίστας) κάθε φορά την προκύπτουσα λίστα των προσφορών. Κάθε δημοπράτης κρατάει μυστικούς τους τυχαίους παράγοντες και τη μετάθεση στοιχείων που χρησιμοποίησε.

β) **Απόδειξη Ορθότητας Μετασχηματισμών.** Οι δημοπράτες συνεργάζονται και εκτελούν ένα πρωτόκολλο για την έκδοση μιας απόδειξης π_1, με μηδενική γνώση, του ότι γνωρίζουν τυχαίους παράγοντες και μεταθέσεις τέτοιες ώστε η λίστα E των προσφορών που δημοσιεύτηκε αρχικά στον Πίνακα Ανακοινώσεων να σχετίζεται μοναδικά με τη λίστα E' που προέκυψε κατόπιν των μετασχηματισμών. Κάθε δημοπράτης επαληθεύει την απόδειξη ατομικά. Εάν η απόδειξη αποτύχει, οι δυσλειτουργικοί (ή κακόβουλοι) δημοπράτες εντοπίζονται και καταργούνται, ενώ οι υπόλοιποι δημοπράτες ξαναρχίζουν τη διαδικασία από τη φάση (α).

γ) **Threshold Αποκρυπτογράφηση.** Ένας αριθμός από δημοπράτες συνεργάζονται για την αποκρυπτογράφηση της λίστας E' των

κρυπτογραφημένων προσφορών, δίνοντας ως αποτέλεσμα τη λίστα L, η οποία και δημοσιεύεται στον Πίνακα Ανακοινώσεων.

δ) **Απόδειξη Ορθότητας Αποκρυπτογράφησης.** Οι δημοπράτες συνεργάζονται και εκτελούν ένα πρωτόκολλο για την έκδοση μιας απόδειξης π_2, με μηδενική γνώση, του ότι η αποκρυπτογράφηση είναι ορθή. Εάν η απόδειξη αποτύχει, τότε οι δυσλειτουργικοί δημοπράτες εντοπίζονται και καταργούνται, ενώ στη συνέχεια η διαδικασία αρχίζει από τη φάση (γ), αυτή τη φορά με ένα διαφορετικό υποσύνολο από δημοπράτες.

Οι αποδείξεις π_1 και π_2, οι οποίες για οικουμενική επαληθευσιμότητα μετατρέπονται σε αποδείξεις χωρίς αλληλεπίδραση, με την *ευριστική* προσέγγιση των Fiat-Shamir [Fia86], συνθέτουν την τελική απόδειξη π, η οποία δημοσιεύεται στον Πίνακα Ανακοινώσεων μαζί με τις λίστες E' και L. Η ασφάλεια των αποδείξεων π_1 και π_2 συζητείται στην εργασία [Abe98]. Τονίζεται επίσης πως η αποκρυπτογράφηση της λίστας E' των μετασχηματισμένων κρυπτογραφημάτων ElGamal βασίζεται στον αλγόριθμο του Pedersen [Ped91].

ΘΕΩΡΗΜΑ. Εάν το Πρόβλημα Απόφασης Diffie-Hellman[41] *είναι δύσκολο και εάν ο Καταναγκαστής δεν ελέγχει και τον χρήστη και την Κάρτα, τότε το προτεινόμενο πρωτόκολλο παρέχει Προστασία από Καταναγκασμό.*

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι ο Καταναγκαστής και ο Χρήστης μπορούν από κοινού να αποδείξουν ότι το $e_r(i)$ αποτελεί την κρυπτογράφηση της προσφοράς i. Αυτό σημαίνει ότι μπορούν να αποδείξουν ότι $e_{r_2}(1) = e_r(i) / e_{r_1}(i) = (x, z)$, έστω, είναι η κρυπτογράφηση του «1». Αυτό ισχύει

[41] Ο 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 το Πρόβλημα Απόφασης Diffie-Hellman [Dif76].

όταν και μόνο όταν $\log_g x = \log_h z = r'$, έστω. Εάν είναι ικανοί να αποδείξουν αυτήν τη σχέση, τότε θα μπορούν επίσης να αποφασίσουν εάν $z = h^{r'} = (g^s)^{r'} = g^{sr'} = DH_g(x, y)$, αφού $h = g^s$ και $x = g^{r'}$.

Στη συνέχεια θα χρησιμοποιήσουμε τον Καταναγκαστή και τον χρήστη ως μια υπορουτίνα για να σχεδιάσουμε έναν αλγόριθμο που θα επιλύνει το Πρόβλημα Απόφασης Diffie-Hellman. Έστω (x, y, z) μία υλοποίηση (instance) του προβλήματος, με $y = h$ να είναι το δημόσιο κλειδί των Δημοπρατών. Δίνουμε το (x, z) στην είσοδο (input) του Καταναγκαστή και του χρήστη, ως την κρυπτογράφηση του «1». Εάν ο Καταναγκαστής και ο χρήστης πετύχουν να αποδείξουν ότι το (x, z) είναι πράγματι μια κρυπτογράφηση του «1», τότε θα ισχύει $z = DH_g(x, y)$. Επομένως έχουμε έναν αλγόριθμο ο οποίος λύνει το Πρόβλημα Απόφασης Diffie-Hellman. Η περίπτωση όπου ο Καταναγκαστής και η Κάρτα μπορούν να αποδείξουν από κοινού ότι το $e_r(i)$ είναι η κρυπτογράφηση του i, είναι παρόμοια και παραλείπεται.

3.7 Συζήτηση

Σήμερα οι οίκοι ηλεκτρονικών δημοπρασιών σε B2C εφαρμογές υλοποιούν υποτυπώδεις μηχανισμούς ασφάλειας με αποτέλεσμα τη μη ανωνυμία των υποψήφιων αγοραστών και τη μη μυστικότητα των προσφορών τους, κάτι που καθιστά δυνατή την καταγραφή όλων των δοσοληψιών που λαμβάνουν χώρα κατά τη διάρκεια μιας δημοπρασίας. Αυτό έχει ως αποτέλεσμα να καταγράφονται οι αγοραστικές συνήθειες και οι προτιμήσεις των χρηστών, με απώτερο σκοπό, μέσω διαφημιστικών πρακτικών marketing, την προσέλκυση νέων πελατών και την αύξηση των πωλήσεων.

Η κρυπτογραφία καλείται να λύσει ένα μεγάλο μέρος των προβλημάτων ασφάλειας που παρουσιάζονται κατά το σχεδιασμό και την υλοποίηση συστημάτων ηλεκτρονικών δημοπρασιών μέσω Διαδικτύου. Στο παρών Κεφάλαιο καταδείξαμε τα προβλήματα αυτά ασφάλειας και παρουσιάσαμε

ένα ασφαλές κρυπτογραφικό πρωτόκολλο για ηλεκτρονικές Δημοπρασίες στο Διαδίκτυο, χωρίς τη χρήση τρίτης έμπιστης οντότητας. Το σύστημα μας ικανοποιεί τις περισσότερες απαιτήσεις ασφάλειας των ηλεκτρονικών δημοπρασιών και επιπλέον είναι «Δίκαιο»: προσφέρει ανωνυμία και μυστικότητα για όλους τους χρήστες, χωρίς όμως να επιτρέπει την απόσυρση μιας προσφοράς. Οι χρήστες χρησιμοποιούν ψευδώνυμα μιας χρήσης και οι προσφορές τους συνδέονται μοναδικά με την αληθινή ταυτότητα τους μέσω ενός Γρίφου Συγκεκριμένου Χρόνου Επίλυσης που υποβάλλουν στο Δημοπράτη. Ο Γρίφος αυτός απαιτεί συγκεκριμένο χρόνο επίλυσης, για λόγους προστασίας της ιδιωτικότητας των χρηστών. Ο χρόνος αυτός δε, δεν μπορεί να συντομευτεί με κατανεμημένες διαδικασίες.

Το πρωτόκολλο που προτείναμε, χρησιμοποιεί επίσης ένα μηχανισμό «Διαίρει και Επίλεξε» για τον έλεγχο της ορθότητας του Γρίφου που κατασκευάζει και υποβάλλει ο χρήστης κατά τη διάρκεια της εγγραφής του στο σύστημα. Οι μηχανισμοί αυτοί, που εμπίπτουν στους μηχανισμούς απόδειξης με Μηδενική Γνώση, απαιτούν έναν ορισμένο αριθμό αλληλεπιδράσεων, οι οποίες επιβαρύνουν το σύστημα. Προφανώς υπάρχει ένας συμβιβασμός (tradeoff) μεταξύ ασφάλειας και αποτελεσματικότητας. Το πρωτόκολλο που προτείναμε λοιπόν είναι κατά βάση σχεδιασμένο για δημοπρασίες (B2C, B2B, ή G2B) που απαιτούν υψηλό επίπεδο προστασίας.

Θέτουμε, ως μελλοντικό στόχο, την επέκταση του πρωτοκόλλου των «Δίκαιων» δημοπρασιών ώστε να υποστηρίζει και δημοπρασίες άλλων τύπων, όπως Ανοικτές Δημοπρασίες και Διπλές Δημοπρασίες, όπου συμμετέχουν περισσότεροι του ενός πωλητές και αγοραστές.

Στο Κεφάλαιο αυτό επίσης εισαγάγαμε την ιδέα της προστασίας από καταναγκασμό, ως μέσο για την καταπολέμηση των δακτυλίων, δηλαδή εκείνων των συμπαιγνιών μεταξύ υποψήφιων αγοραστών που επιθυμούν να επιτύχουν χαμηλότερη τιμή πώλησης για το αγαθό που δημοπρατείται. Επίσης προτείναμε ένα ασφαλές κρυπτογραφικό πρωτόκολλο ηλεκτρονικών δημοπρασιών στο οποίο επιτυγχάνεται προστασία από καταναγκασμό για

τους χρήστες καθώς και οικουμενική επαληθευσιμότητα για τα τελικά αποτελέσματα της δημοπρασίας.

Θεωρούμε πως είναι απαραίτητη η θεώρηση των ηλεκτρονικών δημοπρασιών από τη σκοπιά της ασφάλειας του περιβάλλοντος στο οποίο αυτές εκτελούνται. Οι παρατηρήσεις που έγιναν στο Κεφάλαιο 2 (Ενότητα 2.2.4) και στο πλαίσιο των συστημάτων ηλεκτρονικής ψηφοφορίας, μπορούν να βοηθήσουν προς αυτήν την κατεύθυνση. Παράλληλα, απαιτείται περαιτέρω έρευνα και μελέτη ασφαλών και αποδοτικών κρυπτογραφικών μηχανισμών για την υλοποίηση συστημάτων ηλεκτρονικών δημοπρασιών, και πιο συγκεκριμένα, μεταξύ άλλων:

- Αποδοτικές τεχνικές αντιμετώπισης του προβλήματος των ισόποσων προσφορών στις Κλειστές Δημοπρασίες, με παράλληλη διατήρηση της ιδιωτικότητας των χρηστών που τις υποβάλλουν.

- Κατασκευή ασφαλών συστημάτων με χαμηλό επικοινωνιακό κόστος, για περιβάλλοντα μικρο-συναλλαγών (micropayments). Οι δημοπρασίες προϊόντων χαμηλής αξίας αναμένεται να διαδραματίσουν σημαντικό ρόλο στην εξάπλωση του ηλεκτρονικού εμπορίου τα επόμενα χρόνια.

- Μηχανισμοί ασφαλούς υλοποίησης ιεραρχικών μοντέλων δημοπρασιών, όπου οι νικητές των επιμέρους δημοπρασιών (π.χ. ένας από κάθε δημοπρασία) θα συμμετέχουν στην τελική δημοπρασία. Σε ένα τέτοιο μοντέλο, τα ονόματα των νικητών των επιμέρους δημοπρασιών καθώς και οι τιμές των προσφορών τους, πρέπει να περιβάλλονται από ανωνυμία και μυστικότητα αντίστοιχα.

- Κατασκευή μοντέλων ασφάλειας, που θα είναι προσαρμόσιμα και υλοποιήσιμα για κάθε τύπο δημοπρασίας (Ανοικτές ή Κλειστές δημοπρασίες, Απλές ή Διπλές δημοπρασίες).

- Παράλληλη έρευνα σε μηχανισμούς και υπηρεσίες που συνεισφέρουν άμεσα ή έμμεσα στην ασφάλεια και λειτουργικότητα ενός συστήματος ηλεκτρονικών δημοπρασιών μέσω Διαδικτύου, όπως υπηρεσίες ανωνυμίας, επιβεβαιωμένης παράδοσης, καθώς και υπηρεσίες χρονολόγησης για την επίλυση διενέξεων περί της χρονικής εγκυρότητας των προσφορών.

Κεφάλαιο 4

Ανίχνευση «Προδοτών» σε Συστήματα Αναμετάδοσης Κρυπτογραφημένου Υλικού

Στο Κεφάλαιο αυτό περιγράφουμε και προτείνουμε τρόπους αντιμετώπισης της παράνομης αντιγραφής και αναδιανομής ηλεκτρονικής πληροφορίας. Θεωρούμε, με κριτήρια ασφάλειας και πρακτικότητας, τα σχήματα ανίχνευσης «προδοτών» που έχουν προταθεί στη διεθνή βιβλιογραφία για την προστασία των πνευματικών δικαιωμάτων σε εφαρμογές αναμετάδοσης κρυπτογραφημένου υλικού. Επίσης προτείνουμε ένα ασύμμετρο σχήμα ανίχνευσης «προδοτών» χωρίς τρίτη έμπιστη οντότητα, όπου ο παροχέας του υλικού δε γνωρίζει εκ των προτέρων το αποτύπωμα που περιέχει ο αποκωδικοποιητής ενός εξουσιοδοτημένου χρήστη, αλλά μπορεί να ανιχνεύσει την ταυτότητα ενός «προδότη» που διαθέτει το αποτύπωμα του στην κατασκευή ενός πειρατικού αποκωδικοποιητή. Στο σχήμα ενσωματώνουμε επιπλέον ελέγχους ορθότητας ώστε ο παροχέας να μη μπορεί να συμπεριφερθεί κακόβουλα και να ενοχοποιήσει άδικα έναν χρήστη.

4.1 Εισαγωγή

Με την ταχεία εξάπλωση των εφαρμογών ηλεκτρονικού εμπορίου εγείρονται ζητήματα προστασίας της *πνευματικής ιδιοκτησίας* επί των ψηφιακών αγαθών που αντιγράφονται και αναδιανέμονται παράνομα μέσω του Διαδικτύου ή άλλων ηλεκτρονικών δικτύων. Οι βασικοί άξονες προστασίας που μπορούν να υιοθετηθούν για την αντιμετώπιση του προβλήματος, είναι δύο: η *αποτροπή της αναδιανομής*, και η *ανίχνευση «προδοτών»*.

Αποτροπή Αναδιανομής

Για την αποτροπή ή/και την αποθάρρυνση της παράνομης αναδιανομής ψηφιακών αγαθών απαιτείται ένας συνδυασμός από τεχνικά (π.χ. υδατογραφήματα, χρήση ειδικού hardware) και μη τεχνικά (π.χ. λήψη νομικών μέτρων) μέσα προστασίας.

Υδατογραφήματα. Οι τεχνικές υδατογράφησης χρησιμοποιούνται για την εισαγωγή ειδικών αναγνωριστικών (watermarks), κρυφών ή φανερών, σε ψηφιακό ή αναλογικό υλικό (κείμενο, εικόνα, ήχος, video), με στόχο την εξασφάλιση της αυθεντικότητας και την αποτροπή της παράνομης χρήσης του υλικού από μη εξουσιοδοτημένες οντότητες [Pet99]. Η διαγραφή των υδατογραφημάτων, εφόσον πρόκειται για φανερά υδατογραφήματα, θα πρέπει να καθιστά το αγαθό δύσχρηστο ή μη λειτουργικό. Αντίθετα, οι τεχνικές εισαγωγής κρυφών υδατογραφημάτων συνήθως αξιοποιούν και εφαρμόζουν μεθόδους που άπτονται της επιστήμης της *στεγανογραφίας*[42] [And98]. Πρέπει να τονιστεί ότι τα υδατογραφήματα καταδεικνύουν, κατά τρόπο αδιαμφισβήτητο, τον δημιουργό του υλικού.

Ανίχνευση «Προδοτών»

Οι τεχνικές ανίχνευσης «προδοτών» αποσκοπούν, όχι τόσο στην παρεμπόδιση της αναδιανομής αλλά στον εντοπισμό των «προδοτών» που εκχώρησαν παράνομα σε τρίτους («πειρατές») τα δικαιώματα χρήσης του αγαθού που οι ίδιοι νόμιμα απέκτησαν. Τα ψηφιακά αποτυπώματα αποτελούν το χαρακτηριστικότερο παράδειγμα αυτής της κατηγορίας.

[42] Σε αντίθεση με την κρυπτογραφία, η οποία έχει ως κύριο στόχο την απόκρυψη του περιεχομένου ενός μηνύματος, η επιστήμη της στεγανογραφίας αποσκοπεί στην απόκρυψη της ύπαρξης του μηνύματος καθ' αυτού.

Ψηφιακά Αποτυπώματα. Σε αντίθεση με τα υδατογραφήματα, τα αποτυπώματα καταδεικνύουν τον παραλήπτη του ψηφιακού ή αναλογικού υλικού. Με τα ψηφιακά αποτυπώματα (digital fingerprints) ο δημιουργός του ψηφιακού αγαθού εξατομικεύει κάθε αντίγραφο του αγαθού ώστε να μπορεί να ανακαλύψει την ταυτότητα ενός «προδότη» [Cho94] που αναδιανέμει το αντίγραφο που κατέχει σε τρίτους, οι οποίοι αποκαλούνται και «πειρατές».

Κάθε αποτύπωμα μπορεί να είναι ένα σύνολο από ειδικά *σημάδια* (marks), δηλαδή μια μοναδική σειρά δυαδικών ψηφίων (bits) που ενσωματώνονται στην ηλεκτρονική πληροφορία κατά τρόπο ώστε ο εντοπισμός τους να είναι δύσκολος ακόμα και στην περίπτωση όπου συνεργάζονται δύο ή και περισσότεροι αγοραστές[43], π.χ. συγκρίνοντας τα αντίγραφα μεταξύ τους [Wag83, Bon95]. Επίσης η διαγραφή των αποτυπωμάτων θα πρέπει να καθιστά το αγαθό δύσχρηστο ή μη λειτουργικό.

Στο χώρο των ψηφιακών αποτυπωμάτων, η κρυπτογραφική προστασία από την παράνομη αντιγραφή ψηφιακών αγαθών μπορεί γενικά να επιτευχθεί με τρεις τρόπους:

- **Με συμμετρικές τεχνικές** [Cho94,Bon95,Sti98,Bon99], όπου ο παροχέας και ο αγοραστής γνωρίζουν το εξατομικευμένο αντίγραφο του αγαθού που πωλείται. Το σημαντικότερο μειονέκτημα των συμμετρικών τεχνικών είναι ότι εάν ο παροχέας εντοπίσει ένα παράνομα αναδιανεμημένο αντίγραφο του ψηφιακού αγαθού, η πρότερη γνώση του αποτυπώματος καθιστά δύσκολη, αν όχι αδύνατη, την απόδειξη ενοχής του «προδότη» ενώπιον μιας Αρχής: ο αγοραστής μπορεί να ισχυριστεί ότι ο παροχέας (ή κάποιος υπάλληλος του) επιχείρησε να τον ενοχοποιήσει, αφού γνώριζε το αποτύπωμα του.

[43] Τα συστήματα εισαγωγής ψηφιακών αποτυπωμάτων βασίζονται στην υπόθεση ότι η συνεργασία δυο χρηστών με διαφορετικά αντίγραφα, στα οποία το bit που αντιστοιχεί σε ένα σημάδι έχει την ίδια τιμή, δεν μπορεί να έχει ως αποτέλεσμα τη δημιουργία ενός τρίτου αντίγραφου με διαφορετική τιμή για αυτό το bit [Bon95].

- **Με ασύμμετρες τεχνικές** [Pfi96,Pfi96_1,Bie97,Pfi97_2], όπου ο παροχέας και ο αγοραστής συνεργάζονται για την κατασκευή ή/και την εισαγωγή του αποτυπώματος στο αντίγραφο του αγαθού που πρόκειται να πουληθεί. Στο τέλος του πρωτοκόλλου, ο αγοραστής κατέχει ένα εξατομικευμένο αντίγραφο του αγαθού, ενώ ο παροχέας γνωρίζει την ταυτότητα του αγοραστή καθώς επίσης και μια «ειδική» πληροφορία. Η πληροφορία αυτή, εάν εντοπιστεί κάποιο παράνομα αναδιανεμημένο αντίγραφο, επιτρέπει στον παροχέα να ανακαλύψει (με μεγάλη πιθανότητα) την ταυτότητα του αγοραστή και να αποδείξει σε μια Αρχή ότι είναι «προδότης». Παράλληλα, η «ειδική» αυτή πληροφορία είναι τέτοιας μορφής ώστε η πιθανότητα ο παροχέας να δημιουργήσει ένα αντίγραφο του αγαθού που θα ενοχοποιήσει τον χρήστη, να είναι πολύ μικρή.

Εάν μια συμπαιγνία από k αγοραστές συνδυάσουν τα αντίγραφα τους για να δημιουργήσουν και στη συνέχεια να αναδιανείμουν ένα καινούριο αντίγραφο, τότε υπάρχει ένας αλγόριθμος ο οποίος, εάν δεχθεί ως είσοδο την «ειδική» πληροφορία που κατέχει ο παροχέας, επιτρέπει την ανίχνευση *τουλάχιστον ενός* «προδότη». Εάν ο αλγόριθμος ανακαλύπτει όλους τους «προδότες» που συμμετέχουν στη συμπαιγνία (π.χ. [Bon99]) τότε λέμε ότι προσφέρει *ολική ανιχνευσιμότητα*.

Τα ασύμμετρα συστήματα ανίχνευσης «προδοτών», εμπίπτουν στην κατηγορία των «δίκαιων» (equitable) συστημάτων ηλεκτρονικών συναλλαγών, όπως αυτά ορίστηκαν στο Κεφάλαιο 1.

- **Με ανώνυμες ασύμμετρες τεχνικές** [Pfi97, Dom98,Dom99], όπου επιτυγχάνεται για τον αγοραστή η επιπλέον προστασία της ανωνυμίας: ο αγοραστής μπορεί να αγοράσει ανώνυμα το ψηφιακό αγαθό, αλλά η ανωνυμία του θα καταργηθεί εάν ο παροχέας ανακαλύψει μια παράνομα αναδιανεμημένη έκδοση του αγαθού.

Η ανωνυμία των συστημάτων αυτής της κατηγορίας βασίζεται είτε στην ύπαρξη μιας τρίτης έμπιστης οντότητας η οποία βοηθάει τον

παροχέα στην ανακάλυψη της ταυτότητας του «προδότη» [Pfi97], είτε στη εκτέλεση πρωτοκόλλων *ασφαλούς πολυμερούς υπολογισμού*[33] μεταξύ του παροχέα και του αγοραστή [Dom98,Dom99].

4.1.1 Συστήματα Αναμετάδοσης

Γενικά στα συστήματα ανίχνευσης «προδοτών», δυο είναι οι βασικές προσεγγίσεις που ακολουθούνται:

- **Εξατομίκευση του αγαθού** (π.χ. αποτύπωμα σε ένα αρχείο ήχου).

- **Εξατομίκευση του τρόπου πρόσβασης στο αγαθό** (π.χ. διαφορετικός κωδικός ή κλειδί αποκρυπτογράφησης για πρόσβαση σε ηλεκτρονικά βιβλία, software, CD-ROM, τα οποία και παράγονται μαζικά).

Η δεύτερη προσέγγιση χρησιμοποιείται όταν η αξία της πληροφορίας που διανέμεται δεν είναι πολύ μεγάλη, σε σχέση με το κόστος διανομής της. Κατά την έρευνα αυτή επικεντρώσαμε το ενδιαφέρον μας στα συστήματα αναμετάδοσης κρυπτογραφημένου υλικού (broadcast encryption), όπως συνδρομητική τηλεόραση (pay-per-view TV), παροχή ηλεκτρονικών υπηρεσιών σε πραγματικό χρόνο μέσω Διαδικτύου (π.χ. online ενημέρωση για τιμές μετοχών), διανομή οπτικών δίσκων (CD-ROM) με εμπορικό software, κ.λ.π.

Το «Παλαιό» Μοντέλο (παράδειγμα: Συνδρομητική Ψηφιακή Τηλεόραση). Ο παροχέας διανέμει ψηφιακό υλικό στους συνδρομητές μέσω ενός καναλιού αναμετάδοσης. Τυπικά, ο παροχέας δίνει σε κάθε συνδρομητή έναν αποκωδικοποιητή (software ή hardware) που περιέχει ένα μυστικό κλειδί αποκρυπτογράφησης. Στη συνέχεια ο παροχέας αναμεταδίδει το κρυπτογραφημένο ψηφιακό υλικό. Οι συνδρομητές μπορούν να

αποκρυπτογραφήσουν και να αποκτήσουν πρόσβαση στο υλικό. Εντούτοις, τίποτε δεν αποτρέπει έναν εξουσιοδοτημένο συνδρομητή («προδότη») από το να δώσει ένα αντίγραφο του software αποκρυπτογράφησης σε κάποιον άλλο. Ή, ένας «προδότης» μπορεί να αποπειραθεί να εξάγει το μυστικό κλειδί που περιέχεται στον hardware αποκωδικοποιητή [Cry99], να κάνει αντίγραφα του και να τα καταστήσει γνωστά στο ευρύ κοινό.

Το Μοντέλο «Ανίχνευσης Προδοτών». Οι Chor, Fiat και Naor [Cho94] εισήγαγαν την έννοια της ανίχνευσης «προδοτών» (traitor tracing) με σκοπό την αποθάρρυνση των συνδρομητών που θέλουν να αναδιανείμουν αντίγραφα του κλειδιού τους. Στο μοντέλο αυτό κάθε κλειδί είναι προσωπικό, υπό την έννοια ότι αντιστοιχίζεται μοναδικά με την ταυτότητα ενός συνδρομητή. Ο παροχέας του υλικού εκχωρεί τα προσωπικά κλειδιά και στη συνέχεια αναμεταδίδει κρυπτογραφημένη πληροφορία την οποία μπορούν να αποκρυπτογραφήσουν μόνον οι εξουσιοδοτημένοι χρήστες, με τη χρήση των μοναδικών κλειδιών τους αποκρυπτογράφησης. Εάν κατασκευαστεί ένας πειρατικός αποκωδικοποιητής με ένα ή περισσότερα κλειδιά από έναν ή περισσότερους εξουσιοδοτημένους χρήστες («προδότες») αντίστοιχα, τότε ο αποκωδικοποιητής θα περιέχει ορισμένη μυστική πληροφορία, ικανή ώστε ο παροχέας να μπορεί να ταυτοποιήσει τουλάχιστον ένα «προδότη».

Στο πλαίσιο αυτό έχουν κατά καιρούς προταθεί τεχνικές ανίχνευσης «προδοτών» [Sti98,Bon99,Pfi96,Pfi96_1,Pfi97_2,Pfi97,Kur98] οι οποίες υπάγονται στην κατηγορία των τεχνικών εισαγωγής ψηφιακών αποτυπωμάτων: στα συστήματα αναμετάδοσης κρυπτογραφημένου υλικού,

το ψηφιακό αποτύπωμα ισούται με το προσωπικό
κρυπτογραφικό κλειδί κάθε χρήστη

που είναι απαραίτητο για την αποκρυπτογράφηση του αναμεταδιδόμενου υλικού.

Σημείωση: Στη συνέχεια του Κεφαλαίου χρησιμοποιούμε τον όρο «πειρατικός αποκωδικοποιητής» για να αναφερθούμε στη διαδικασία αποκρυπτογράφησης που εκτελεί ο «πειρατής» προκειμένου να αποκτήσει πρόσβαση στο αποκρυπτογραφημένο υλικό. Η διαδικασία αυτή μπορεί να εκτελείται σε μια φυσική συσκευή ή απλά να είναι κώδικας software που μεταγλωττίζεται και εκτελείται σε έναν υπολογιστή.

Ένα Δυσεπίλυτο Σενάριο Επίθεσης. Στο σενάριο αυτό, ο «προδότης» ενδέχεται να αναδιανείμει το αντίγραφο του αγαθού αφότου αυτό έχει αποκρυπτογραφηθεί. Η επίθεση αυτή είναι δύσκολο να αντιμετωπιστεί, ωστόσο μπορεί να χαρακτηριστεί ως μη πρακτική για τον επιτιθέμενο, ιδιαίτερα σε εφαρμογές όπως:

- Αναμετάδοση εικόνας συνδρομητικής τηλεόρασης: θεωρείται ριψοκίνδυνο καθώς και οικονομικά/υπολογιστικά επαχθές για κάποιον να στήσει έναν «πειρατικό» σταθμό αναμετάδοσης. Μια παρόμοια εφαρμογή είναι και η διανομή περιεχομένου μέσω Διαδικτύου με τεχνολογίες «push» [Fia99].

- Online υπηρεσίες ή βάσεις δεδομένων μέσω Διαδικτύου, όπου η πρόσβαση σε κάποια ή όλες τις εγγραφές (records) επιτρέπεται κατόπιν οικονομικού αντιτίμου. Ο «προδότης» θα πρέπει να αντιγράψει ολόκληρη την πληροφορία που προσφέρεται από την online υπηρεσία, καθώς επίσης και να ανανεώνει τακτικά, ανάλογα με την υπηρεσία, τα αντίγραφα που διατηρεί.

Η αναλογία «ρίσκο/προσδοκώμενο όφελος» σε αυτές τις περιπτώσεις ενδεχομένως να καθίσταται μη ιδιαίτερα ελκυστική για τον «προδότη» [Fia99]. Εναλλακτικά, ο «προδότης» μπορεί να προμηθεύσει τους πειρατές με πληροφορίες μικρότερου μεγέθους – τα κλειδιά αποκρυπτογράφησης. Κατά την έρευνα μας επικεντρώσαμε το ενδιαφέρον μας στην αποτροπή τέτοιων επιθέσεων.

Συνεισφορά / Δομή του Κεφαλαίου

Στα πλαίσια της έρευνας μας, θεωρήσαμε τα σχήματα ανίχνευσης «προδοτών» σε συστήματα αναμετάδοσης, από τη σκοπιά της ασφάλειας και της πρακτικότητας (Ενότητα 4.2). Επίσης μετατρέψαμε το ιδιαίτερα πρακτικό και ασφαλές συμμετρικό σχήμα ανίχνευσης «προδοτών» των Kurosawa-Desmedt [Kur98] (Ενότητα 4.3.1) σε ασύμμετρο (Ενότητα 4.4), χωρίς να υποθέτουμε την ανάμειξη τρίτης έμπιστης οντότητας [Mag01_1]. Για αυτό το σκοπό κάναμε χρήση ενός κρυπτογραφικού μηχανισμού που αποκαλείται *Επιλήσμονα Μεταφορά* [Eve85] – Ενότητα 4.3.2. Η λύση που προτείναμε μπορεί να εφαρμοστεί απευθείας στη διαδικασία *δημιουργίας κλειδιών* του σχήματος των Kurosawa-Desmedt [Kur98]. Επιπλέον, προτείναμε έναν μηχανισμό «*Διαίρει και Επίλεξε*» (Ενότητα 4.4.1) με τον οποίο εξασφαλίζεται, με μεγάλη πιθανότητα, η ορθότητα των αποτυπωμάτων που αποδίδονται στους χρήστες του συστήματος. Ο μηχανισμός αυτός μπορεί να γενικευθεί ώστε να επιτυγχάνεται ορθότητα σε κάθε πρωτόκολλο που χρησιμοποιεί επιλήσμονα μεταφορά για την ανταλλαγή μηνυμάτων μεταξύ δύο οντοτήτων.

4.2 Θεώρηση Σχημάτων Ανίχνευσης «Προδοτών» σε Συστήματα Αναμετάδοσης

Το Μοντέλο. Υπάρχουν $n+2$ συμμετέχοντες, ένας παροχέας υλικού T, ένα σύνολο n εξουσιοδοτημένων χρηστών και ένας «πειρατικός» αποκωδικοποιητής. Ο T κατασκευάζει ένα κλειδί κρυπτογράφησης e_T, και ένα προσωπικό κλειδί αποκρυπτογράφησης e_i για κάθε εξουσιοδοτημένο χρήστη i (συμμετρικά σχήματα) ή συμμετέχει με το χρήστη i σε ένα πρωτόκολλο για την κατασκευή και απόδοση στον i του προσωπικού του κλειδιού e_i (ασύμμετρα σχήματα). Για να σταλούν τα δεδομένα m στους εξουσιοδοτημένους χρήστες και μόνον, ο T επιλέγει ένα κλειδί συνόδου s.

Στη συνέχεια ο T αναμεταδίδει $(e_T(s), ENC_s(m))$, όπου το $h = e_T(s)$ αποκαλείται *επικεφαλίδα* του κρυπτογραφήματος, ενώ ENC είναι μια συνάρτηση κρυπτογράφησης συμμετρικού κλειδιού [Fia93].

Ασφάλεια. Θεωρούμε (k,n) σχήματα ανίχνευσης «προδοτών» σε ένα σύστημα n εξουσιοδοτημένων χρηστών, το οποίο μπορεί να αντιμετωπίσει έως k συμμετέχοντες «προδότες». Η ασφάλεια ενός σχήματος ανίχνευσης «προδοτών» για συστήματα αναμετάδοσης ανάγεται:

- Στην ασφάλεια του υποσυστήματος αναμετάδοσης, δηλαδή στην αποτροπή της πρόσβασης στο αποκρυπτογραφημένο υλικό από μη εξουσιοδοτημένους χρήστες.

- Στην ασφάλεια του υποσυστήματος ανίχνευσης, δηλαδή στον εντοπισμό του «προδότη» ή ενός εκ των (έως k) «προδοτών» ή όλων των (έως k) «προδοτών» (*ολική ανιχνευσιμότητα*) που συνεργάζονται για την κατασκευή του πειρατικού αποκωδικοποιητή. Πρέπει επίσης να τονιστεί πως ο μέγιστος αριθμός k των συνεργούντων «προδοτών» που μπορεί να αντιμετωπίσει το υποσύστημα ανίχνευσης αποτελεί καθοριστικό παράγοντα για την αναλογία πρακτικότητα/ασφάλεια ολόκληρου του συστήματος.

  Ορισμένοι αλγόριθμοι ανίχνευσης επιτρέπουν τον εντοπισμό της ταυτότητας ενός «προδότη» μεταχειριζόντας τον πειρατικό αποκωδικοποιητή σαν ένα «μαύρο κουτί» (black box): αυτό σημαίνει πως εξετάζεται και αναλύεται η συμπεριφορά του αποκωδικοποιητή, χωρίς να είναι απαραίτητο το «άνοιγμα» του και η ανάγνωση των πληροφοριών που αυτός περιέχει. Η ιδιότητα αυτή αποκαλείται και *ανιχνευσιμότητα black-box* [Bon99,Kur00].

Σημείωση: Σε αρκετά σχήματα ανίχνευσης «προδοτών» [Cho94,Bon95], ο αριθμός k έχει διττή σημασία ως προς την ασφάλεια του συστήματος. Εάν συμμαχήσουν

περισσότεροι από k «προδότες», τότε μπορούν να κατασκευάσουν έναν «πειρατικό» αποκωδικοποιητή που όχι απλά θα εμποδίζει την ανίχνευση κάποιου (-ων) από αυτούς, αλλά θα ενοχοποιεί έναν «αθώο» εξουσιοδοτημένο χρήστη.

Πρακτικότητα. Εκτός από την ασφάλεια, πρωτεύοντα ρόλο στην αξιολόγηση ενός σχήματος ανίχνευσης «προδοτών» έχει η πρακτικότητα του. Αυτή συνήθως μετριέται συναρτήσει της παραμέτρου ασφάλειας k, όπου k είναι ο αριθμός των συνεργούντων «προδοτών» που μπορεί να ανεχθεί το σύστημα. Σημαντικοί παράγοντες στην αξιολόγηση της πρακτικότητας των σχημάτων αυτών είναι:

- Οι απαιτήσεις σε μνήμη και υπολογισμούς για τους εξουσιοδοτημένους χρήστες. Η παράμετρος αυτή αποκτά ιδιαίτερη σημασία όταν ο χρήστης έχει περιορισμένες υπολογιστικές ικανότητες, π.χ. στην περίπτωση των έξυπνων καρτών (smartcards).

- Οι απαιτήσεις σε μνήμη και υπολογισμούς για τον παροχέα του υλικού. Αυτή η παράμετρος είναι δευτερεύουσας σημασίας, αφού ο παροχέας αφενός μπορεί να εκτελεί τους υπολογισμούς του off-line, αφετέρου αναμένεται (ή υποτίθεται) ότι έχει υψηλές αποθηκευτικές δυνατότητες.

- Οι απαιτήσεις σε πλεονάζοντα δεδομένα, δηλαδή το επιπλέον μέγεθος των δεδομένων που αποστέλλονται προκειμένου να είναι εφικτή η ανίχνευση. Στα συστήματα αναμετάδοσης τα επιπλέον δεδομένα μεταφράζονται σε κόστος σε επικοινωνία, ενώ σε εφαρμογές τύπου CD-ROM στον επιπλέον αποθηκευτικό χώρο του μέσου που ενδεχομένως σπαταλείται.

Συμμετρικά Σχήματα

Τα πρώτα σχήματα ανίχνευσης «προδοτών» ήταν αυτά των Chor, Fiat και Naor [Cho94] και βασίζονται στο υποσύστημα αναμετάδοσης των Fiat και Naor [Fia93]. Στο αποδοτικότερο των σχημάτων αυτών, και σε σύνολο n εξουσιοδοτημένων χρηστών, το προσωπικό κλειδί του κάθε χρήστη αποτελείται από $O(k^2 \log n)$ κλειδιά αποκρυπτογράφησης και ο παροχέας του αναμεταδιδόμενου υλικού πρέπει να μεταδώσει $O(k^4 \log n)$ κρυπτογραφήματα. Αργότερα, οι Stinson και Wei [Sti98], καθώς και οι Gafni et al [Gaf99] πρότειναν εναλλακτικούς μηχανισμούς ανίχνευσης, ανεξάρτητους με το υποσύστημα αναμετάδοσης που χρησιμοποιείται, οι οποίοι προσφέρουν καλύτερες αποδόσεις για μικρές τιμές των k και n.

Πρόσφατα, οι Boneh και Franklin πρότειναν ένα σχήμα ανίχνευσης «προδοτών» [Bon99] για εφαρμογές αναμετάδοσης, όπου η ασφάλεια του υποσυστήματος ανίχνευσης ανάγεται στο πρόβλημα εύρεσης διακριτών λογαρίθμων[15] [Dif76] ενώ η ασφάλεια του υποσυστήματος αναμετάδοσης στο πρόβλημα Diffie-Hellman[44] [Dif76]. Το σχήμα τους απαιτεί ένα κλειδί κρυπτογράφησης, ένα προσωπικό κλειδί αποκρυπτογράφησης και την αναμετάδοση $O(2k+1)$ κρυπτογραφημάτων από τον παροχέα. Επίσης παρέχει ολική επαληθευσιμότητα και επαληθευσιμότητα blackbox.

Το Βέλτιστο (Optimum) Σύστημα των Kurosawa-Desmedt [Kur98]. Πρόσφατα οι Kurosawa και Desmedt όρισαν κατώτατες τιμές (lower bounds) απόδοσης για σχήματα ανίχνευσης «προδοτών» σε εφαρμογές αναμετάδοσης κρυπτογραφημένου υλικού και πρότειναν δυο *συμμετρικά* σχήματα. Το πρώτο σχήμα είναι μιας χρήσης (one-time) και επιτυγχάνει τις κατώτατες τιμές, καθώς απαιτούνται ένα κλειδί κρυπτογράφησης, ένα προσωπικό κλειδί αποκρυπτογράφησης και η αναμετάδοση $O(k)$ κρυπτογραφημάτων από τον παροχέα. Το σχήμα αυτό περιγράφεται ξεχωριστά στην Ενότητα 4.3.1, καθώς

αποτελεί τη βάση για το ασύμμετρο σχήμα ανίχνευσης που περιγράφουμε στην Ενότητα 4.4.

Το δεύτερο σχήμα που περιγράφεται στην εργασία [Kur98] είναι ένα σχήμα πολλαπλών χρήσεων (multiple use). Η ασφάλεια του υποσυστήματος αναμετάδοσης ανάγεται στην ασφάλεια του κρυπτογραφικού αλγορίθμου ElGamal [ElG85], ενώ η ανίχνευση «προδοτών» στο πρόβλημα εύρεσης διακριτών λογαρίθμων [Dif76]. Επίσης, απαιτούνται $O(k)$ κλειδιά κρυπτογράφησης, ένα προσωπικό κλειδί αποκρυπτογράφησης, και $O(k)$ κρυπτογραφήματα. Τέλος, η πολυπλοκότητα της αποκρυπτογράφησης για τους εξουσιοδοτημένους χρήστες είναι ανεξάρτητη του μεγέθους k της συμπαιγνίας.

Αργότερα, οι Kurosawa-Desmedt πρότειναν έναν βελτιωμένο αλγόριθμο ανίχνευσης για τα ίδια σχήματα. Μάλιστα προσέδωσαν στα σχήματα τους την ιδιότητα της *ολικής ανιχνευσιμότητας* και της *black-box ανιχνευσιμότητας* [Kur00].

Σύμφωνα με τις έως τώρα γνώσεις μας, τα βέλτιστα σχήματα ανίχνευσης «προδοτών» των Kurosawa-Desmedt [Kur98] είναι τα πλέον πρακτικά μεταξύ των σχημάτων ανίχνευσης «προδοτών» που έχουν παρουσιαστεί στη διεθνή βιβλιογραφία [Mag01_1].

Ασύμμετρα Σχήματα

Η Pfitzmann [Pfi96,Pfi96_1] εφάρμοσε τεχνικές *ασφαλούς διμερούς υπολογισμού*[33] [Cha87] ώστε να μετατρέψει το σχήμα των Fiat και Naor [Cho94] σε ασύμμετρο σχήμα. Αργότερα, οι Pfitzmann-Waidner [Pfi97_2] και Biehl-Meyer [Bie97] πέτυχαν το ίδιο αποτέλεσμα, αυτή τη φορά όμως χρησιμοποιώντας άλλες τεχνικές ασφαλούς διμερούς υπολογισμού ([Gol87] και [Bra87] αντίστοιχα) καθώς και κρυπτογραφικές *συναρτήσεις κατακερματισμού* [Cha81]. Εντούτοις, τα παραπάνω ασύμμετρα σχήματα

βασίζονται στο μη ιδιαίτερα αποδοτικό σχήμα, όπως αναφέρθηκε, των Chor, Fiat και Naor [Cho94].

Ασυμμετρία στα Σχήματα των Kurosawa-Desmedt – «Δίκαια» Συστήματα. Οι Kurosawa και Desmedt επίσης περιέγραψαν μια *ασύμμετρη* εκδοχή για κάθε ένα από τα δύο βασικά συμμετρικά τους σχήματα [Kur98]. Ωστόσο, η ασυμμετρία των σχημάτων οφείλεται στην ύπαρξη έμπιστων οντοτήτων (π.χ. έμπιστοι κατανεμημένοι πράκτορες). Οι οντότητες αυτές κατέχουν τα κλειδιά αποκρυπτογράφησης όλων των χρηστών (αγοραστών) του συστήματος, και οι χρήστες τις εμπιστεύονται ότι δεν θα επιχειρήσουν να τους ενοχοποιήσουν. Στην Ενότητα 4.4 θα περιγράψουμε ένα «δίκαιο» σχήμα για ασύμμετρη ανίχνευση «προδοτών», βασισμένο στο βέλτιστο συμμετρικό σχήμα μιας χρήσης των Kurosawa-Desmedt, χωρίς την ανάγκη ύπαρξης τρίτης έμπιστης οντότητας.

4.3 Βασικά Κρυπτογραφικά Εργαλεία

Στην Ενότητα αυτή περιγράφουμε εν συντομία το συμμετρικό σχήμα ανίχνευσης «προδοτών» των Kurosawa-Desmedt [Kur98]. Επίσης περιγράφουμε τον τρόπο λειτουργίας των μηχανισμών *επιλήσμονος μεταφοράς* και συγκεκριμένα ενός μηχανισμού που *δεν απαιτεί αλληλεπίδραση* (non-interactive) μεταξύ του αποστολέα και του παραλήπτη [Bel89].

4.3.1 Το συμμετρικό σχήμα των Kurosawa-Desmedt

Στην εργασία [Kur98] περιγράφονται δύο σχήματα ανίχνευσης «προδοτών». Όπως αναφέρθηκε το πρώτο είναι ένα βέλτιστο (k, n) σχήμα μιας χρήσης, όπου k είναι ο μέγιστος αριθμός συνεργούντων «προδοτών», σε σύνολο n χρηστών, που μπορεί να αντέξει το σύστημα. Το δεύτερο σχήμα είναι μια

τροποποίηση του πρώτου, για πολλαπλές χρήσεις, το οποίο είναι επίσης βέλτιστο και ασφαλές. Η τροποποίηση που προτείνουμε στην Ενότητα 4.4 μπορεί να εφαρμοστεί και στα δυο σχήματα, ωστόσο σε αυτήν την Ενότητα, χάριν απλότητας, περιγράφουμε το σχήμα μιας χρήσης.

Ο παροχέας υλικού επιλέγει ένα τυχαίο πολυώνυμο $f(x) = a_0 + a_1 x + ... + a_k x^k$ στο σύνολο Z_q ως το κλειδί κρυπτογράφησης e_T, όπου q είναι ένας πρώτος αριθμός, με $q > n$ για ένα σύνολο n εξουσιοδοτημένων χρηστών.

Δημιουργία Κλειδιού (Key Generation). Ο παροχέας δίνει σε κάθε εξουσιοδοτημένο χρήστη i το προσωπικό του κλειδί αποκρυπτογράφησης, $e_i =< f(i) >$, $i \leq 0 \leq n-1$.

Κρυπτογράφηση (Encryption). Ο παροχέας υλικού κρυπτογραφεί ένα *κλειδί συνόδου* s ως $e_T(s) = h = (h_0, h_1, ..., h_k) = (s + a_0, a_1, ..., a_k)$. Στη συνέχεια ο παροχέας αναμεταδίδει τα κρυπτογραφήματα h σε όλους τους χρήστες του συστήματος. Αργότερα, ο παροχέας κρυπτογραφεί συμμετρικά το υλικό (π.χ. εικόνα συνδρομητικής τηλεόρασης) με το κλειδί συνόδου s και αναμεταδίδει το κρυπτογράφημα σε όλους τους χρήστες τους συστήματος.

Σημείωση: Στην εκδοχή του σχήματος για πολλαπλές χρήσεις που περιγράφεται στην εργασία [Kur98], το κλειδί συνόδου ανανεώνεται ανά τακτά χρονικά διαστήματα.

Αποκρυπτογράφηση (Decryption). Από την επικεφαλίδα h και το κλειδί αποκρυπτογράφησης e_i, κάθε χρήστης i υπολογίζει το κλειδί συνόδου

$$s = (h_0 + h_1 i + ... + h_k i^k) - f(i).$$

Ανίχνευση (Tracing). Όταν ανακαλυφθεί ένας «πειρατικός» αποκωδικοποιητής, τότε εκτίθεται το πειρατικό κλειδί e_p [Kur98]. Εάν το e_p περιέχει το

ζεύγος $< j, f(j) >$ για κάποιον εξουσιοδοτημένο χρήστη j. τότε ο παροχέας αποφασίζει ότι ο χρήστης j είναι «προδότης».

Θεώρημα: Το σχήμα των Kurosawa Desmedt [Kur98] ανιχνεύει τουλάχιστον ένα «προδότη» στην περίπτωση μιας συμπαιγνίας μεγέθους k.

Απόδειξη. Έστω μια συμπαιγνία C «προδοτών» $\{i_1,....i_k\}$ δημιουργεί έναν «πειρατικό» αποκωδικοποιητή e_p, τέτοιον ώστε η πιθανότητα ο e_p να μην περιέχει το ζεύγος $(i_1, f(i_1))$ ή το ζεύγος $(i_1, f(i_1))$ ή..., ή το ζεύγος $(i_k, f(i_k))$ να είναι μεγαλύτερη από $1/q$. Αφού ο e_p μπορεί να αποκρυπτογραφήσει το κλειδί συνόδου s, τότε ο e_p θα πρέπει να περιέχει τουλάχιστον ένα $(x_0, f(x_0))$ για κάποιο $x_0 \notin \{i_1,....i_k\}$. Εντούτοις αυτό είναι αδύνατο, αφού ο βαθμός της συνάρτησης $\deg f(x) = k$ και η συμπαιγνία C γνωρίζει μόνον τα k σημεία της $f(x)$.

4.3.2 Επιλήσμονα Μεταφορά

Η έννοια της $\binom{1}{2}$ *επιλήσμονος μεταφοράς* (oblivious transfer) προτάθηκε από τους Even, Goldreich και Lempel [Eve85] ως μια γενίκευση του κρυπτογραφικού πρωτοκόλλου επιλήσμονος μεταφοράς που είχε προτείνει ο Rabin για εφαρμογές *υπογραφής συμβολαίων* (contract signing) [Rab81] μεταξύ δύο οντοτήτων που δεν εμπιστεύονται η μία την άλλη.

Έστω ότι ο Bob έχει στην κατοχή του δύο αλφαριθμητικά S_0 και S_1. Συναρτήσει των δυο αυτών αλφαριθμητικών και του δημοσίου κλειδιού της Alice, ο Bob κατασκευάζει ένα μήνυμα $OT(S_0, S_1)$ και το αποστέλλει στην Alice. Η Alice χρησιμοποιώντας το ιδιωτικό της κλειδί μπορεί να εξάγει από

το $OT(S_0, S_1)$ ακριβώς ένα εκ των δύο αλφαριθμητικών S_0 ή S_1, και ο Bob δε μπορεί να γνωρίζει ποιο από τα δύο εξήγαγε η Alice.

Στην αρχική υλοποίηση των Even, Goldreich και Lempel, η Alice και ο Bob πρέπει να ανταλλάξουν μια σειρά από μηνύματα, πρόκειται δηλαδή για ένα *αλληλεπιδραστικό* (interactive) πρωτόκολλο [Eve85]. Το γεγονός αυτό καθιστά το πρωτόκολλο μη πρακτικό για εφαρμογές όπως αναμετάδοση κρυπτογραφημένου υλικού. Στη συνέχεια περιγράφουμε ένα αντίστοιχο *μη αλληλεπιδραστικό* (non-interactive) πρωτόκολλο.

Επιλήσμονα Μεταφορά Χωρίς Αλληλεπίδραση. Οι Bellare και Micali [Bel89] πρότειναν μια αποδοτικότερη εκδοχή του πρωτοκόλλου των Even, Goldreich και Lempel, όπου δεν υπάρχει αλληλεπίδραση μεταξύ της Alice και του Bob. Εν συντομία:

- **Αρχικοποίηση (Setup).** Έστω p πρώτος αριθμός και g γεννήτορας του Z_p^*. Έστω ο αριθμός $C \in Z_p^*$ είναι μια σταθερά, γνωστή σε όλους, η οποία δεν έχει διάκριτο λογάριθμο modulo p. Στην [Bel89] συζητούνται τρόποι εύρεσης τέτοιων αριθμών.

- **Δημιουργία Κλειδιού (Key Generation).** Η Alice επιλέγει ένα $x \in \{0,\ldots, p-2\}$ τυχαία και θέτει $a_0 = g^x \bmod p$ και $a_1 = C(g^x)^{-1} \bmod p$. Στη συνέχεια παραλείπουμε τον τελεστή $\bmod p$, χάριν απλότητας. Το δημόσιο κλειδί της είναι το ζεύγος (a_0, a_1) και το ιδιωτικό της κλειδί είναι το x. Η ορθότητα του δημόσιου κλειδιού της Alice επαληθεύεται ελέγχοντας ότι $a_0 a_1 = C$.

- **Επιλήσμονα Μεταφορά.** Ο Bob διαλέγει τυχαίους αριθμούς $\psi_0, \psi_1 \in \{0,\ldots, p-2\}$ και υπολογίζει τα $\beta_0 = g^{\psi_0}$ και $\beta_1 = g^{\psi_1}$. Επίσης χρησιμοποιεί το δημόσιο κλειδί της Alice ώστε να υπολογίσει τα

$\gamma_0 = a_0^{\psi_0}$ και $\gamma_1 = a_1^{\psi_1}$. Τέλος ο Bob υπολογίζει τα $r_0 = S_0 \oplus \gamma_0$ και $r_1 = S_1 \oplus \gamma_1$, και στέλνει στην Alice το:

$$OT(S_0, S_1) = (\beta_0, \beta_1, r_0, r_1).$$

Με τη λήψη των β_0, β_1, η Alice χρησιμοποιηθεί το ιδιωτικό της κλειδί και υπολογίζει τα $\gamma_i = \beta_i^x$, όπου $i = 0$ ή $i = 1$. Στο τέλος υπολογίζει το ζητούμενο μυστικό $r_i \oplus \gamma_i = S_i$. Σύμφωνα με την *υπόθεση των Diffie-Hellman*[44] [Dif76], η Alice μπορεί να κατασκευάσει το γ_0 ή το γ_1, αλλά σε καμία περίπτωση και τα δύο. Ως αποτέλεσμα, η Alice καταλήγει να έχει στην κατοχή της ακριβώς ένα εκ των δύο μυστικών, και ο Bob δε γνωρίζει ποιο από τα δύο μυστικά κατέχει η Alice.

4.4 Ένα Ασύμμετρο Πρωτόκολλο Ανίχνευσης «Προδοτών»

Στην Ενότητα αυτή παρουσιάζουμε μια ασύμμετρη εκδοχή του σχήματος των Kurosawa και Desmedt (στο εξής K-D) [Kur98] χωρίς να κάνουμε καμία υπόθεση για ύπαρξη έμπιστων οντοτήτων [Mag01_1]. Το βασικά εργαλεία που χρησιμοποιούμε είναι η τεχνική της *επιλήσμονος μεταφοράς* (oblivious transfer -*OT*) – Ενότητα 4.3.2, καθώς και τεχνικές «*διαίρει και επίλεξε*» (Ενότητα 4.4.1) για τον έλεγχο της ορθότητας των ιδιωτικών κλειδιών που αποδίδει ο παροχέας στους χρήστες. Ο έλεγχος της ορθότητας είναι απαραίτητος, ώστε να αποτραπούν επιθέσεις όπως οι ακόλουθες:

- Ο παροχέας χρησιμοποιεί δύο πανομοιότυπα κλειδιά ως τιμές εισόδου (input) στον *OT* αλγόριθμο μεταφοράς κλειδιού στον χρήστη Α.

---

[44] Ο τελεστής *DH* (Diffie-Hellman [Dif76]) ορίζεται ως $DH(g^a, g^b) = g^{ab}$. Δεδομένων των αριθμών g^a, g^b, το πρόβλημα του υπολογισμού του $DH(g^a, g^b)$ αποκαλείται και ως *πρόβλημα Diffie-Hellman*.

- Ο παροχέας χρησιμοποιεί δύο πανομοιότυπα κλειδιά ως τιμές εισόδου στους *OT* αλγόριθμους μεταφοράς κλειδιού σε δύο χρήστες A, B.

Υποθέτουμε ότι υπάρχει μια *Υποδομή Δημοσίου Κλειδιού* για κρυπτογράφηση δημοσίου κλειδιού, και ότι ο παροχέας έχει στη διάθεση του τα πιστοποιητικά με τα δημόσια κλειδιά των χρηστών του συστήματος. Ο παροχέας επίσης χρησιμοποιεί έναν *πίνακα ανακοινώσεων* [Rei95] για την επικοινωνία του με τους χρήστες και τους εξωτερικούς παρατηρητές.

Το πρωτόκολλο

Ο παροχέας υλικού επιλέγει ένα πολυώνυμο $f(x) = w_0 + w_1 x + ... + w_k x^k$ στο σύνολο Z_q ως το κλειδί κρυπτογράφησης e_T για το αναμεταδιδόμενο κρυπτογραφημένο υλικό (ή αλλιώς *δημόσιο κλειδί αναμετάδοσης*) για ένα σύνολο n εξουσιοδοτημένων χρηστών.

Μεταφορά Κλειδιού. Ο παροχέας επιλέγει για κάθε έναν εξουσιοδοτημένο χρήστη u_{ij} δύο K-D κλειδιά $S_i =< i, f(i) >$ και $S_j =< j, f(j) >$. Στη συνέχεια χρησιμοποιεί το δημόσιο κλειδί του χρήστη και εκτελεί τον αλγόριθμο επιλήσμονος μεταφοράς χωρίς αλληλεπίδραση, όπως φαίνεται στο Σχήμα 13. Στην έξοδο του *OT* αλγορίθμου, ο χρήστης λαμβάνει *ακριβώς ένα* ιδιωτικό κλειδί αποκρυπτογράφησης (ή αλλιώς αποτύπωμα), $e_{ij} =< i, f(i) >$ ή $< j, f(j) >$, όπου $i, j = 1,2,...,n$, με $i \neq j$. Ο παροχέας δε γνωρίζει ποιο από τα δύο κλειδιά S_i, S_j, έλαβε ο χρήστης.

Κρυπτογράφηση. Ο παροχέας υλικού κρυπτογραφεί το κλειδί συνόδου s ως $h = (h_0, h_1, ..., h_k) = (s + w_0, w_1, ..., w_k)$ και αναμεταδίδει το h σε όλους τους χρήστες του συστήματος. Αργότερα, χρησιμοποιεί το κλειδί s για να

κρυπτογραφήσει συμμετρικά το υλικό (π.χ. εικόνα συνδρομητικής τηλεόρασης) και αναμεταδίδει το κρυπτογράφημα σε όλους τους χρήστες του συστήματος.

Αποκρυπτογράφηση. Με βάση την επικεφαλίδα h και το κλειδί αποκρυπτογράφησης S_i ή S_j, που έλαβε στην έξοδο του OT αλγορίθμου, κάθε χρήστης u_{ij} υπολογίζει το κλειδί συνόδου: $(h_0 + h_1 i + ... + h_k i^k) - f(i) = s$ ή $(h_0 + h_1 j + ... + h_k j^k) - f(j) = s$.

Σχήμα 13. Το στάδιο της μεταφοράς ενός K-D κλειδιού αποκρυπτογράφησης

Ανίχνευση. Όταν ανακαλυφθεί ένας «πειρατικός» αποκωδικοποιητής, τότε εκτίθεται το «πειρατικό» κλειδί e_{ij}. Εάν το e_{ij} περιέχει το ζεύγος $< i, f(i) >$ ή το ζεύγος $< j, f(j) >$ για κάποιον εξουσιοδοτημένο χρήστη u_{ij}, τότε ο παροχέας αποφασίζει ότι ο χρήστης u_{ij} είναι «προδότης».

Για την ανίχνευση μπορεί επίσης ο καινούριος αλγόριθμος των Kurosawa-Desmedt [Kur00] που, όπως αναφέρθηκε, υποστηρίζει *ολική ανίχνευση* και *ανίχνευση blackbox*.

Ασφάλεια του Πρωτοκόλλου

Είναι προφανές ότι ως προς τα υποσυστήματα αναμετάδοσης και ανίχνευσης, το πρωτόκολλο κληρονομεί την ασφάλεια του σχήματος των Kurosawa-Desmedt [Kur98]. Στη συνέχεια θα εξετάσουμε την ασυμμετρία του πρωτοκόλλου.

Εάν ο παροχέας επιθυμούσε να ενοχοποιήσει έναν εξουσιοδοτημένο χρήστη, π.χ. την Alice, τότε θα επιχειρούσε να κατασκευάσει έναν κάλπικο «πειρατικό» αποκωδικοποιητή στον οποίο θα εισήγαγε, με τυχαία επιλογή, ένα από τα δύο μυστικά κλειδιά τα οποία μετέφερε, με το πρωτόκολλο της επιλήσμονος μεταφοράς, στην Alice.

Η πιθανότητα επιτυχίας για έναν κακόβουλο παροχέα που επιθυμεί να ενοχοποιήσει την Alice είναι ½.

Θεωρούμε πως ο παροχέας δε θα διακινδυνεύσει τη ζημία που θα υποστεί από μια αποτυχημένη απόπειρα ενοχοποίησης της Alice, κατά την οποία η Alice φυσικά θα μπορεί να αποδείξει στο δικαστήριο, με πιθανότητα ½, πως ο αποκωδικοποιητής της περιέχει ένα αποτύπωμα διαφορετικό από αυτό που περιέχεται στον κάλπικο «πειρατικό» αποκωδικοποιητή. Είναι προφανές ότι το κόστος που θα υποστεί ο παροχέας από μια αποτυχημένη απόπειρα ενοχοποίησης της Alice είναι μεγαλύτερο από τα οφέλη που θα αποκομίσει από μια επιτυχημένη ενοχοποίηση.

Σημείωση: Αντί για τη χρήση του $\binom{1}{2}$ *πρωτοκόλλου επιλήσμονος μεταφοράς, όπου η Alice αποκτά τυχαία πρόσβαση μόνον σε ένα από τα δύο μηνύματα που της αποστέλλονται, θα μπορούσε να γίνει χρήση ενός* $\binom{1}{N}$ *πρωτοκόλλου [Nao99], όπου η Alice λαμβάνει, κατά τυχαίο τρόπο, ένα από N μηνύματα που της αποστέλλονται. Σε*

αυτήν την περίπτωση η πιθανότητα επιτυχίας μιας απόπειρας ενοχοποίησης της Alice, θα ήταν ίση με 1/N. Πρέπει να τονιστεί ωστόσο ότι το πρωτόκολλο που περιγράφεται στο [Nao99] απαιτεί αλληλεπίδραση μεταξύ αποστολέα και παραλήπτη, και θεωρείται μη πρακτικό για μεγάλες τιμές του N [Mag01_1].

4.4.1 Έλεγχος της Ορθότητας των K-D κλειδιών.

Στο πρωτόκολλο που παρουσιάσαμε στην προηγούμενη Ενότητα, υποθέσαμε ότι ο παροχέας επιλέγει κατά τρόπο ορθό τα K-D κλειδιά που θα χρησιμοποιήσει ως είσοδο στον αλγόριθμο της επιλήσμονος μεταφοράς. Στο τέλος του πρωτοκόλλου, ο παροχέας δε γνωρίζει ποιο κλειδί κατέχει η Alice, ενώ η Alice κατέχει ακριβώς ένα και μόνον ένα από τα δύο K-D κλειδιά. Όμως, τί γίνεται στην περίπτωση όπου ο παροχέας επιλέγει δύο πανομοιότυπα K-D κλειδιά ως είσοδο στον *OT* αλγόριθμο; Ή ακόμη χειρότερα, τι θα συμβεί εάν ο παροχέας μεταφέρει το ίδιο κλειδί σε παραπάνω από έναν εξουσιοδοτημένους χρήστες;

Επίθεση Α. Εάν ο παροχέας χρησιμοποιεί δύο ίδια κλειδιά ως είσοδο στον *OT* αλγόριθμο που εκτελεί με αποδέκτη την Alice, τότε ο παροχέας τελικά θα γνωρίζει το αποτύπωμα της Alice, αφού η Alice θα έχει να επιλέξει μεταξύ δύο πανομοιότυπων κλειδιών. Σε αυτήν την περίπτωση, η ασυμμετρία του πρωτοκόλλου καταλύεται και ένας κακόβουλος παροχέας έχει τη δυνατότητα να ενοχοποιήσει την Alice. Αντίστοιχα η Alice, εφόσον συμπεριφερθεί ως «προδότης», μπορεί αργότερα να *αρνηθεί ευθύνη* (repudiation) για τις πράξεις της, κάτι που επίσης παραβιάζει την ασφάλεια του συστήματος.

Επίθεση Β. Εάν πάλι το πρωτόκολλο δε μπορεί να εξασφαλίσει ότι κάθε υλοποίηση (instance) του *OT* αλγορίθμου αφορά δυο μοναδικά K-D κλειδιά τα οποία δε θα επαναχρησιμοποιηθούν σε μια άλλη υλοποίηση του αλγορίθμου με έναν άλλον εξουσιοδοτημένο χρήστη, τότε υπάρχει η (μη

αμελητέα) πιθανότητα δύο χρήστες να λάβουν το ίδιο K-D κλειδί ως έξοδο δυο διαφορετικών υλοποιήσεων του ίδιου αλγόριθμου. Κάτι τέτοιο θα έχει ως αποτέλεσμα να δημιουργούνται δυσεπίλυτες αντιδικίες σχετικά με το εάν ένας χρήστης κατηγορείται δίκαια ή άδικα ως «προδότης».

Στη συνέχεια της Ενότητας περιγράφουμε τεχνικές «διαίρει και επίλεξε» (cut-and-choose) βάσει των οποίων ο παροχέας υποχρεώνεται να επιλέξει ορθά K-D κλειδιά ως είσοδο για τον *OT* αλγόριθμο. Ο μηχανισμός που προτείνουμε θα πρέπει να ικανοποιεί τις ακόλουθες δύο συνθήκες:

- **Συνθήκη Α.** Για κάθε χρήστη i, $i=1,\ldots,n$, η υλοποίηση της επιλήσμονος μεταφοράς $OT_i(S_{i,0},S_{i,1})$ πρέπει να περιέχει δύο διαφορετικά K-D κλειδιά αποκρυπτογράφησης, δηλαδή $S_{i,0} \neq S_{i,1}$.

- **Συνθήκη Β.** Για δύο χρήστες i, j, $i, j=1,\ldots,n$, με $i \neq j$, οι υλοποιήσεις της επιλήσμονος μεταφοράς $OT_i(S_{i,0},S_{i,1})$ και $OT_j(S_{j,0},S_{j,1})$ πρέπει να περιέχουν διαφορετικά K-D κλειδιά αποκρυπτογράφησης, δηλαδή $S_{i,0} \neq S_{i,1} \neq S_{j,0} \neq S_{j,1}$.

Για την υπόλοιπη Ενότητα θα χρησιμοποιήσουμε το συμβολισμό $Enc_X(m)$ για να δηλώσουμε τη συμμετρική κρυπτογράφηση (π.χ. με τον αλγόριθμο DES [Sch96]) ενός μηνύματος m με ένα κλειδί X, καθώς και το συμβολισμό $hash(m)$ για να δηλώσουμε την κρυπτογραφική τιμή κατακερματισμού[45] (hash) ενός μηνύματος m π.χ. με τον αλγόριθμο MD5 [Riv91].

[45] Οι συναρτήσεις κατακερματισμού αντιστοιχίζουν δυαδικά αλφαριθμητικά οποιουδήποτε μεγέθους σε δυαδικά αλφαριθμητικά συγκεκριμένου μεγέθους (π.χ. 128 ή 160 bit) που αποκαλούνται τιμές hash. Προκειμένου να χρησιμοποιηθεί σε ένα κρυπτογραφικό πρωτόκολλο, μια συνάρτηση κατακερματισμού h επιλέγεται κατά τέτοιον τρόπο ώστε να είναι υπολογιστικά ανέφικτη η εύρεση δυο διαφορετικών τιμών εισόδου x και y που να δίνουν ως έξοδο την ίδια τιμή hash, $h(x)=h(y)$. Επίσης, δοθείσης μιας τιμής y, πρέπει να είναι υπολογιστικά ανέφικτη η εύρεση μιας τιμής εισόδου x ούτως ώστε $h(x)=y$.

Εξασφαλίζοντας τη Συνθήκη Α. Έστω $OT_i =< Enc_{K_i}(S_{i,0}), Enc_{K_i}(S_{i,1}) >$, $i \in \{0,1\}$, δύο υλοποιήσεις του αλγορίθμου επιλήσμονος μεταφοράς για τον ίδιο χρήστη, έστω την Alice, όπου $S_{i,0}, S_{i,1}$ είναι τέσσερα διαφορετικά K-D κλειδιά αποκρυπτογράφησης και K_i είναι δυο συμμετρικά κλειδιά κρυπτογράφησης. Ο παροχέας δεσμεύεται εκ των προτέρων στα κλειδιά K_i με τη χρήση συναρτήσεων κατακερματισμού, και στέλνει, αφού πρώτα τα υπογράψει ψηφιακά, τα ζεύγη $(OT_0.hash(K_0) \parallel OT_1.hash(K_1))$ στην Alice.

- **Φάση 1: έλεγχος της ορθότητας των κρυπτογραφήσεων.** Η Alice επιλέγει τυχαία μία από τις δύο υλοποιήσεις (έστω, χωρίς απώλεια γενικότητας, την OT_0) και ο παροχέας αποκαλύπτει όλες τις μυστικές πληροφορίες που αφορούν την υλοποίηση αυτή (δηλαδή τα $\psi_0, \psi_1, \gamma_0, \gamma_1$ - Σχήμα 13) προκειμένου να αποδείξει ότι η υλοποίηση είναι ορθή. Δεδομένων των πληροφοριών αυτών, η Alice λαμβάνει στην έξοδο του αλγορίθμου και τις δύο τιμές $Enc_{K_0}(S_{0,0})$ και $Enc_{K_0}(S_{0,1})$. Συγκρίνει τις τιμές αυτές, και εφόσον ισχύει $Enc_{K_0}(S_{0,0}) \neq Enc_{K_0}(S_{0,1})$ πείθεται ότι $S_{0,0} \neq S_{0,1}$, αφού το ίδιο κλειδί K_0 χρησιμοποιήθηκε για να κρυπτογραφηθούν και τα δύο K-D κλειδιά. Εάν δεν ισχύει η ανισότητα, τότε αυτό σημαίνει πως τα K-D κλειδιά είναι επίσης ίσα, επομένως ο παροχέας έχει «κλέψει» και μπορεί να καταγγελθεί.

- **Φάση 2: έλεγχος της ορθότητας του συμμετρικού κλειδιού.** Εάν οι έλεγχοι στη φάση 1 είναι επιτυχείς, η Alice εκτελεί την εναπομείνασα υλοποίηση OT_1. Η έξοδος του αλγορίθμου θα επιστρέψει στην Alice είτε το $Enc_{K_1}(S_{1,0})$ είτε το $Enc_{K_1}(S_{1,1})$. Σε αυτό το σημείο ζητείται από τον παροχέα να αποστείλει το αντίστοιχο συμμετρικό κλειδί K_1. Η Alice ελέγχει την ορθότητα του K_1 κατά δύο τρόπους: πρώτα

ανακατασκευάζει τη δέσμευση $hash(K_1)$ - αυτό είναι εύκολο, αφού η συνάρτηση hash είναι δημόσια - και ελέγχει εάν η δέσμευση είναι αυτή που είχε λάβει αρχικά. Δεύτερον, χρησιμοποιεί το κλειδί K_1 για να αποκρυπτογραφήσει την έξοδο του αλγορίθμου, δηλαδή το $Enc_{K_1}(S_{1,0})$ ή το $Enc_{K_1}(S_{0,1})$ και ελέγχει εάν προκύπτει ένα έγκυρο K-D κλειδί. Εάν κάποιος από τους δυο ελέγχους αποτύχει, τότε ο παροχέας καταγγέλλεται.

Ένας κακόβουλος παροχέας δε γνωρίζει *εκ των προτέρων* ποια υλοποίηση του αλγορίθμου θα επιλέξει η Alice στην Φάση 1, και ποια θα εκτελέσει εν τέλει στη Φάση 2. Επομένως, εάν μια από τις δύο υλοποιήσεις δεν είναι ορθώς κατασκευασμένη τότε η πιθανότητα να εκτεθεί ο παροχέας είναι ½ για κάθε εξουσιοδοτημένο χρήστη.

Πρέπει να τονιστεί επίσης ότι ο παροχέας θα μπορούσε να «κλέψει» κρυπτογραφώντας δυο πανομοιότυπα K-D κλειδιά $S = S^*$ με δυο διαφορετικά συμμετρικά κλειδιά $K \neq K^*$. Σε αυτήν την περίπτωση ισχύει $Enc_K(S) \neq Enc_{K^*}(S^*)$, και ο έλεγχος στην Φάση 1 θα είναι επιτυχής. Εντούτοις, ο παροχέας έχει ήδη δεσμευτεί στο K ή στο K^* και δε μπορεί εκ των προτέρων να γνωρίζει ποια από τις δυο κρυπτογραφήσεις θα λάβει η Alice στην έξοδο του αλγορίθμου. Επομένως, η πιθανότητα να εκτεθεί ο παροχέας είναι πάλι ½.

Σημείωση: Στο προηγούμενο παράδειγμα, τα κλειδιά που εμπεριέχονται στην υλοποίηση που επιλέγεται από την Alice στη Φάση 1, δηλαδή τα $S_{0,0}$ και $S_{0,1}$ δεν αχρηστεύονται μετά την ολοκλήρωση του ελέγχου ορθότητας: η Alice δε λαμβάνει ποτέ από τον παροχέα το κλειδί K_0, αφού σε αυτήν την περίπτωση θα κατέληγε να έχει (κατά τρόπο παράνομο) δύο έγκυρα K-D κλειδιά. Αντίθετα, τα κλειδιά αυτά μπορούν να χρησιμοποιηθούν σε συναλλαγές με άλλους χρήστες (αρκεί τα συμμετρικά κλειδιά που χρησιμοποιούνται να είναι διαφορετικά).

Εξασφαλίζοντας τη Συνθήκη Β. Προκειμένου να υποχρεώσουμε τον παροχέα να μεταφέρει διαφορετικά κλειδιά σε διαφορετικούς χρήστες, κάνουμε χρήση του Πίνακα Ανακοινώσεων. Η τεχνική μας μπορεί να θεωρηθεί ως μια επέκταση της τεχνικής που χρησιμοποιήσαμε για τη Συνθήκη Α. Απαιτούμε λοιπόν κάθε υλοποίηση της επιλήσμονος μεταφοράς να περιέχει επιπλέον τις hash τιμές των K_D κλειδιών:

$$OT_i' = < Enc_{K_i}(S_{i,0}), Enc_{K_i}(S_{i,1}), hash(S_{i,0}), hash(S_{i,1}), hash(K_i) > .$$

Αφού εκτελεστεί το πρωτόκολλο για την τήρηση της Συνθήκης Α (υπενθυμίζουμε ότι στο προηγούμενο παράδειγμα μας η Alice εκτέλεσε την υλοποίηση OT_1) ο παροχέας δημοσιεύει στον Πίνακα Ανακοινώσεων το ζεύγος των τιμών $< hash(S_{1,0}), hash(S_{1,1}) >$ καθώς και μια δήλωση (π.χ. υπογεγραμμένη ψηφιακά) ότι τα K-D κλειδιά που αντιστοιχούν σε αυτές τις τιμές hash έχουν ήδη κατοχυρωθεί σε κάποιον εξουσιοδοτημένο χρήστη. Μετά την εκτέλεση της OT_1', η Alice έχει ήδη λάβει ένα εκ των $S_{1,0}$, $S_{1,1}$. Τότε η Alice υπολογίζει τη τιμή hash του κλειδιού και ελέγχει εάν το αποτέλεσμα συμπίπτει με την αντίστοιχη τιμή hash που είναι δημοσιευμένη στον Πίνακα Ανακοινώσεων. Εάν όχι, ο παροχέας καταγγέλλεται. Το ίδιο θα συμβεί στην περίπτωση που η τιμή hash του κλειδιού της Alice εμφανίζεται να έχει κατοχυρωθεί περισσότερο από μία φορές.

Σημείωση: Ο μηχανισμός «Διαίρει και Επίλεξε» που παρουσιάσαμε σε αυτήν την Ενότητα μπορεί να γενικευθεί για κάθε πρωτόκολλο το οποίο χρησιμοποιεί τον αλγόριθμο της επιλήσμονος μεταφοράς για την ανταλλαγή μηνυμάτων μεταξύ δύο οντοτήτων. Ωστόσο ο παραπάνω μηχανισμός απαιτεί αλληλεπίδραση μεταξύ του αποστολέα και του παραλήπτη. Θεωρούμε πως μια επέκταση του μηχανισμού αυτού, χωρίς αλληλεπίδραση, θα παρουσίαζε εξαιρετικό ενδιαφέρον.

4.5 Συζήτηση

Το αντικείμενο του Κεφαλαίου ήταν η προστασία των πνευματικών δικαιωμάτων κατά τη διανομή ψηφιακών αγαθών μέσω ηλεκτρονικών καναλιών επικοινωνίας. Χαρακτηριστικότερο παράδειγμα αποτελούν τα συστήματα ακρόασης τηλεοπτικών εκπομπών επί πληρωμή (pay-per-view), όπου οι συνδρομητές αγοράζουν τα δικαιώματα ακρόασης συγκεκριμένων καναλιών ή προγραμμάτων. Στα συστήματα αυτά το ψηφιακό περιεχόμενο διανέμεται μέσω επίγειων, καλωδιακών ή δορυφορικών καναλιών εκπομπής, ενώ ένα σύστημα ελεγχόμενης πρόσβασης χρησιμοποιείται ώστε να εξασφαλίσει ότι μόνο οι εξουσιοδοτημένοι συνδρομητές έχουν πρόσβαση στο περιεχόμενο το οποίο πληρώνουν. Παρότι τα συστήματα συνδρομητικής τηλεόρασης αποτελούν τη χαρακτηριστικότερη εφαρμογή του μοντέλου μας, παρόμοια συστήματα ελεγχόμενης πρόσβασης χρησιμοποιούνται εκτενώς σήμερα για την προστασία ηλεκτρονικών υπηρεσιών επί πληρωμή, μέσω Web.

Χρήση Ασφαλούς Υλικού. Σήμερα, για την αποτροπή της πειρατείας θεωρείται επαρκής η υιοθέτηση λύσεων ασφαλούς υλικού (π.χ. έξυπνες κάρτες, αποκωδικοποιητές hardware). Οι συσκευές αυτές σχεδιάζονται ώστε να αποτρέπουν την επέμβαση και την πρόσβαση στα κρυπτογραφικά κλειδιά. Ωστόσο οι υποθέσεις που γίνονται σχετικά με την ασφάλεια των μηχανισμών αυτών δεν ευσταθούν πάντα. Στο παρελθόν έχουν περιγραφεί μέθοδοι που εκμεταλλεύονται «λάθη» του υλικού με αποτέλεσμα την πρόσβαση στα εσώκλειστα κρυπτογραφικά κλειδιά [And96,Bon97,Bih97,Cry00].

Τα σχήματα που συζητήθηκαν στο Κεφάλαιο αυτό αποδεικνύονται ασφαλή χωρίς να απαιτούν τη χρήση ασφαλούς υλικού. Βεβαίως, η χρήση ασφαλούς υλικού θα καθιστούσε μια επίθεση ακόμα περισσότερο δύσκολη.

Σημείωση: Κατ'ουσίαν, η χρήση αποκωδικοποιητών hardware, ανθεκτικών σε παραβιάσεις (tamper-resistant) σημαίνει πως ο αριθμός k των «προδοτών», έναντι των οποίων ένα σύστημα παρέχει προστασία, μπορεί να είναι ιδιαίτερα μικρός, σε σχέση με

το σύνολο των χρηστών του συστήματος. Κάτι τέτοιο προφανώς βελτιώνει την πρακτικότητα του συστήματος.

Στα πλαίσια της έρευνας μας παρουσιάσαμε ένα ασύμμετρο σχήμα ανίχνευσης «προδοτών» χωρίς έμπιστες οντότητες, για την προστασία από παράνομη αναδιανομή κλειδιών σε εφαρμογές αναμετάδοσης κρυπτογραφημένης πληροφορίας [Mag01_1]. Για αυτόν το λόγο, αξιοποιήσαμε το ιδιαίτερα αποδοτικό και ασφαλές (συμμετρικό) σχήμα των Kurosawa-Desmedt [Kur98,Kur00] και τροποποιήσαμε το στάδιο της εκχώρησης κλειδιών ώστε ο παροχέας του υλικού να μη γνωρίζει το αποτύπωμα που αποδίδεται σε έναν εξουσιοδοτημένο χρήστη του συστήματος. Εάν ένας ή περισσότεροι «προδότες» συνδυάσουν τα αποτυπώματα τους και κατασκευάσουν ένα «πειρατικό» αποκωδικοποιητή, τότε ο αποκωδικοποιητής θα περιέχει πληροφορίες που οδηγούν στην ταυτότητα τουλάχιστον ενός εκ των «προδοτών».

Περιγράψαμε επίσης τρόπους με τους οποίους οι χρήστες μπορούν να εξασφαλίσουν ότι τα κλειδιά που τοποθετούνται από τον παροχέα στην είσοδο του αλγορίθμου εκχώρησης είναι διαφορετικά μεταξύ τους, αλλά και ότι δεν πρόκειται να εκχωρηθούν σε κάποιον άλλον εξουσιοδοτημένο χρήστη. Η τεχνική μας βασίζεται στις αρχές των πρωτοκόλλων «διαίρει και επίλεξε» [Sch96] και μπορεί να επεκταθεί σε κάθε εφαρμογή που χρησιμοποιεί επιλήσμονα μεταφορά για την απόδοση-μεταφορά μυστικών μεταξύ δύο οντοτήτων.

Το σχήμα που προτείναμε είναι «δίκαιο» (equitable), υπό την έννοια ότι αφενός προστατεύει την ιδιωτικότητα των χρηστών του συστήματος, και αφετέρου εξασφαλίζει την ορθότητα της διαδικασίας ανίχνευσης ενός «προδότη» που αναδιανέμει το κρυπτογραφικό του κλειδί, χωρίς να γίνεται κάποια υπόθεση για την ύπαρξη τρίτης έμπιστης οντότητας. Ως στόχο θέτουμε την επέκταση του πρωτοκόλλου ανίχνευσης «προδοτών» ώστε να προσφέρει ανωνυμία στους εξουσιοδοτημένους χρήστες του συστήματος.

Μελλοντική Έρευνα. Πρέπει να τονιστεί ότι η προστασία των πνευματικών δικαιωμάτων για αναλογικά ή ηλεκτρονικά αγαθά μπορεί να επιτευχθεί μόνον μέσα από ένα συνονθύλευμα *τεχνικών* και *νομικών* μέτρων. Από τεχνικής άποψης, η μελλοντική έρευνα στο χώρο της προστασίας των πνευματικών δικαιωμάτων για ηλεκτρονικά αγαθά, αναμένεται να στραφεί:

- Στην χρήση έξυπνων καρτών για την ασφαλή εκτέλεση τμήματος ή όλων των λειτουργιών που καλείται να εκτελέσει ο αγοραστής του ψηφιακού αγαθού.

- Στη μελέτη για την εύρεση ασφαλών και πρακτικών μεθόδων εισαγωγής υδατογραφημάτων σε αρχεία πολυμέσων (κείμενο, εικόνα, ήχος, video).

- Στην εύρεση μηχανισμών και μεθόδων αποτροπής (όχι απλά αποθάρρυνσης) της αντιγραφής και της αναδιανομής του αγαθού. Οι μηχανισμοί αυτοί λογικά θα βασίζονται σε λύσεις ασφαλούς υλικού χαμηλού επιπέδου και θα υποστηρίζονται και σε επίπεδο λειτουργικού συστήματος, θα είναι δηλαδή ανεξάρτητοι της εφαρμογής ή του αγαθού που προφυλάσσεται.

Ειδικότερα για τα συστήματα αναμετάδοσης κρυπτογραφημένου υλικού, ιδιαίτερη έμφαση αναμένεται να δοθεί σε ζητήματα όπως:

- Εύρεση αποδοτικότερων αλγορίθμων ανίχνευσης «προδοτών», των οποίων η ασφάλεια έναντι μιας συμπαιγνίας «προδοτών» θα είναι ανεξάρτητη του μεγέθους της συμπαιγνίας.

- Αντιμετώπιση της παράνομης αναδιανομής του ψηφιακού υλικού, μετά την αποκρυπτογράφηση του (π.χ. παράνομοι πειρατικοί σταθμοί

εκπομπής, αναδιανομή ταινιών που έχουν ήδη εγγραφεί σε μονάδες αποθήκευσης κ.λ.π.).

Κεφάλαιο 5

Ασφάλεια σε Συστήματα Ανάκτησης Κλειδιού

Στο Κεφάλαιο αυτό αναλύουμε τους μηχανισμούς ασφάλειας των συστημάτων ανάκτησης κλειδιού και προτείνουμε έναν μηχανισμό ανάκτησης κλειδιού με ισχυρή χρονική ασφάλεια, σύμφωνα με τον οποίο οι κρυπτογραφημένες συνομιλίες ενός χρήστη που αφορούν μία περίοδο t μπορούν να αποκρυπτογραφηθούν από τις Αρχές Επιβολής του Νόμου, χωρίς να είναι δυνατή η πρόσβαση σε συνομιλίες που αφορούν προγενέστερες ή μεταγενέστερες περιόδους. Επίσης προτείνουμε ένα υβριδικό μοντέλο ανάκτησης κλειδιού για την αντιμετώπιση επιθέσεων όπου χρησιμοποιούνται τεχνικές διπλής κρυπτογράφησης για την παράκαμψη του συστήματος ανάκτησης κλειδιού.

5.1 Εισαγωγή

Στο κεφάλαιο αυτό προσεγγίζουμε τα θέματα ασφάλειας σε συστήματα *ανάκτησης κλειδιού*[46] (key recovery) [Bur98,Den96], τα οποία επιτρέπουν την πρόσβαση σε αποκρυπτογραφημένο υλικό, υπό ορισμένες προϋποθέσεις. Οι προϋποθέσεις αυτές, για παράδειγμα, μπορεί να είναι η *επιβολή του νόμου* (law enforcement) [Mic92], η απώλεια κλειδιών που αντιστοιχούν σε *αρχειοθετημένα δεδομένα* (archived data) προσωπικής χρήσης [Mah96], ή η απώλεια κλειδιών που αντιστοιχούν σε αρχειοθετημένο ή διακινούμενο υλικό στο ενδοδίκτυο (intranet) μιας επιχείρησης – *εμπορική ανάκτηση κλειδιού* (commercial key

[46] Η έννοια της ανάκτησης κλειδιού, παρότι αναφέρεται στην ανάκτηση ενός συγκεκριμένου κλειδιού, έχει κατά καιρούς χρησιμοποιηθεί για να συνοψίσει όλες εκείνες τις μεθόδους οι οποίες επιτρέπουν την ανάκτηση αποκρυπτογραφημένων μηνυμάτων. Άλλοι όροι που μπορεί να συναντήσει κανείς στη διεθνή βιβλιογραφία είναι: «υποθήκευση κλειδιού» (key escrow), «backup κλειδιού» (key backup), «κατάθεση κλειδιού» (key deposit), «ανάκτηση μηνύματος» (message recovery), «τοποθέτηση σε κάψουλα» (key encapsulation), «τρίτες έμπιστες οντότητες» (trusted third parties) κ.α.

recovery) [You98]. Στο περιβάλλον των επιχειρήσεων, τα συστήματα ανάκτησης κλειδιού εμπίπτουν στην ευρύτερη κατηγορία των συστημάτων *διαχείρισης κλειδιού* (key management) [Abel98].

Τα συστήματα ανάκτησης κλειδιού, ιδίως αυτά που προορίζονται για παρακολούθηση (κατόπιν εντάλματος) των κρυπτογραφημένων συνομιλιών των πολιτών, έχουν δεχθεί αρνητικές κριτικές, για δύο λόγους: πρώτον, πιστεύεται ότι παραβιάζουν βασικές αρχές της ιδιωτικότητας των πολιτών, και ότι εν δυνάμει μπορούν να επιτρέψουν τη μαζική παρακολούθηση των πολιτών για συνομιλίες που έχουν λάβει χώρα στο παρόν ή/και στο παρελθόν αλλά και για αυτές που θα λάβουν χώρα στο μέλλον [Abel98, Bur98,Bur_Mag01]. Δεύτερον, στα περισσότερα συστήματα που έχουν προταθεί έως σήμερα έχουν εντοπιστεί αδυναμίες και παραλείψεις που επιτρέπουν την παράκαμψη του μηχανισμού ανάκτησης κλειδιού [Fran95,Kim99,Pfi97_1].

Η έρευνα μας επικεντρώθηκε σε συστήματα ανάκτησης κλειδιού που επιτρέπουν την πρόσβαση σε κρυπτογραφημένες συνομιλίες (Ενότητα 5.4), στα πλαίσια των υπηρεσιών επιβολής του νόμου [Bur_Mag01]. Εντούτοις, το σύστημα ανάκτησης κλειδιού που προτείνουμε στην Ενότητα 5.5 απευθύνεται κυρίως σε εφαρμογές εμπορικής ανάκτησης κλειδιού στο εταιρικό περιβάλλον [Mag03].

Συνεισφορά / Δομή του Κεφαλαίου

Συνοψίζουμε τις διάφορες προσεγγίσεις για ανάκτηση κλειδιού που έχουν προταθεί και υλοποιηθεί έως σήμερα (Ενότητα 5.2) και περιγράφουμε τις πιθανές επιθέσεις ασφάλειας στα συστήματα ανάκτησης κλειδιού (Ενότητα 5.3). Εισάγουμε την έννοια της *ισχυρής χρονικής ασφάλειας* (Ενότητα 5.4), καταδεικνύουμε τη σημασία της και προτείνουμε ένα σύστημα ανάκτησης κλειδιού με ισχυρή χρονική ασφάλεια [Bur_Mag01] για μηνύματα που κρυπτογραφούνται με τον αλγόριθμο ElGamal [ElG85]. Τέλος, περιγράφουμε

ένα *υβριδικό* μοντέλο ανάκτησης κλειδιού για την αντιμετώπιση επιθέσεων *διπλής κρυπτογράφησης* στο περιβάλλον των επιχειρήσεων, όπου οι χρήστες χρησιμοποιούν το σύστημα ανάκτησης κλειδιού ως «δούρειο ίππο» για να το παρακάμψουν (Ενότητα 5.5). Η Ενότητα 5.6 ολοκληρώνει το παρών Κεφάλαιο.

5.2 Συστήματα Ανάκτησης Κλειδιού

Η Παραδοσιακή Προσέγγιση - π.χ. Clipper [Fip94]. Η προσέγγιση αυτή, που συχνά ονομάζεται και *υποθήκευση κλειδιού μακράς διαρκείας* (long-term key escrow) αναφέρεται στην υποθήκευση του ιδιωτικού κλειδιού αποκρυπτογράφησης π.χ. της Alice σε ένα σύνολο *πρακτόρων ανάκτησης κλειδιού* (key escrow agents) [Mic92,Mic95,You98]. Κάποια στιγμή η Αρχή Επιβολής Νόμου (Law Enforcement Agency - LEA), η οποία έχει υποκλέψει τις κρυπτογραφημένες συνομιλίες m της Alice κατά την περίοδο t και έχει λάβει ένα ένταλμα για την αποκρυπτογράφηση τους, αξιώνει από τους πράκτορες το κλειδί της Alice ή, σε ορισμένες υλοποιήσεις, απλά την αποκρυπτογράφηση του m [Des94]. Το κλειδί που υποθηκεύεται είναι μακράς διαρκείας. Ένα μειονέκτημα των περισσοτέρων συστημάτων αυτής της κατηγορίας είναι ότι, εφόσον ανακτηθεί το ιδιωτικό κλειδί, με νόμιμους ή παράνομους τρόπους (π.χ. hacking, κακόβουλη συμπεριφορά των πρακτόρων) δεν υπάρχει επαρκής έλεγχος στην χρονική περίοδο κατά την οποία είναι δυνατή η αποκρυπτογράφηση των συνομιλιών / δεδομένων του χρήστη. Δεν υπάρχει δηλαδή, *χρονική ασφάλεια* [Bur_Mag01].

Μερικώς Αδύνατα Κρυπτοσυστήματα (Partially Weak Crypto) – π.χ. κρυπτογραφικά συστήματα με κλειδιά περιορισμένου μήκους (40 bits) [Koo02]. Στα συστήματα αυτά είναι υπολογιστικά εφικτό για την Αρχή να ανακτήσει το κείμενο που αντιστοιχεί σε κρυπτογραφημένη συνομιλία. Εντούτοις, η μαζική υποκλοπή και παρακολούθηση συνομιλιών των πολιτών

συνεπάγεται υψηλό υπολογιστικό κόστος για την Αρχή. Στη διεθνή βιβλιογραφία, ο Shamir [Sha95] πρότεινε τη *μερική υποθήκευση κλειδιών* (partial key escrow) ως μια μέθοδο όπου υποθηκεύονται όλα εκτός από k bits του κλειδιού (π.χ. $k = 48$). Έκτοτε έχουν προταθεί παρόμοια σχήματα, είτε βασισμένα στο *διακριτό λογάριθμο* (π.χ. για ElGamal [Bel97]) είτε στην *παραγοντοποίηση* μεγάλων πρώτων αριθμών (π.χ. για RSA [Mao01_1]).

Εικονική Διευθυνσιοδότηση (Virtual Addressing) – π.χ. IBM SKR [Gen97]. Η μέθοδος αυτή αποκαλείται συχνά και ως *ανάκτηση κλειδιού συνόδου* (session key recovery), ή ως *τοποθέτηση σε κάψουλα* (key encapsulation). Αναφέρεται στην κρυπτογράφηση κλειδιών περιορισμένης εμβέλειας ή αλλιώς κλειδιών συνόδου, με το δημόσιο κλειδί του παραλήπτη καθώς και με το δημόσιο κλειδί μιας προκαθορισμένης Αρχής [Ver97,Wal96]. Τα συστήματα αυτά παρέχουν από τη φύση τους χρονική ασφάλεια.

Τρίτες Έμπιστες Οντότητες (Trusted Third Parties - TTP) – π.χ. Royal Holloway [Jef95]. Τα κλειδιά συνόδου διανέμονται online από τρίτες έμπιστες οντότητες, κατά τρόπο παρόμοιο με το συμμετρικό σύστημα διανομής κλειδιού Kerberos [Mil87]. Οι μηχανισμοί ανάκτησης κλειδιού που εμπίπτουν σε αυτήν την κατηγορία σχεδιάστηκαν ειδικά για επικοινωνίες μεταξύ περισσότερων του ενός τομέων (multiple domains), π.χ. μεταξύ των πολιτών δύο κρατών. Ως μειονεκτήματα μπορούν να αναφερθούν οι υψηλές απαιτήσεις σε χώρο αποθήκευσης και σε επικοινωνία [Knu98]. Στις [And97,Fou99] έχουν επίσης περιγραφεί συγκεκριμένες παραβιάσεις ασφάλειας σε συστήματα έμπιστων οντοτήτων.

Δήμευση Κλειδιού (Key Confiscation) – RIP Act 2000 [Reg00]. Σε αρκετές χώρες ψηφίζονται νόμοι [Koo02] που επιτρέπουν στις Αρχές, κατόπιν εντάλματος, να προβούν στη δήμευση κλειδιών για την αποκρυπτογράφηση συνομιλιών των πολιτών. Ο πολίτης είναι υποχρεωμένος να παραδώσει στις Αρχές το ιδιωτικό του κλειδί ή άλλη πληροφορία που θα επιτρέψει την

αποκρυπτογράφηση των δεδομένων. Η προσέγγιση αυτή έχει εγείρει πολλές κριτικές καθώς υπάρχουν εγγενείς αδυναμίες εφαρμογής ενός τέτοιου συστήματος. Για παράδειγμα, κατά την ερμηνεία του νόμου RIP-ACT 2000 [Reg00] που ψηφίστηκε στη Μ. Βρετανία, η απόδειξη κατοχής ή μη του κλειδιού αποκρυπτογράφησης έγκειται στην Alice, η οποία π.χ. πρέπει να αποδείξει ότι έχασε το κλειδί της, κάτι που θεωρείται ως μη αποδεκτό. Στην [Des01] συζητούνται κρυπτογραφικοί μηχανισμοί για την ενίσχυση της χρονικής ασφάλειας των συστημάτων δήμευσης κλειδιού.

5.3 Επιθέσεις στα Συστήματα Ανάκτησης Κλειδιού

Στη διεθνή βιβλιογραφία έχουν διατυπωθεί κατά καιρούς ενστάσεις για τη σκοπιμότητα της ανάκτησης κλειδιού στις ηλεκτρονικές επικοινωνίες. Ένα σημαντικό κομμάτι των ενστάσεων αυτών αφορά επιθέσεις στην ασφάλεια των συστημάτων [Bur98,Abel98,Fran95,Kim99,Pfi97_1]. Οι επιθέσεις αυτές μπορούν να κατηγοριοποιηθούν ως εξής:

- **Οι Αρχές καταχράζονται την εξουσία που διαθέτουν.** Οι επιθέσεις αυτές συνήθως αφορούν συστήματα της παραδοσιακής προσέγγισης, όπου, εφόσον ανακτηθούν τα κλειδιά μακράς διαρκείας ενός χρήστη, είναι δύσκολο να ελεγχθεί ο χρόνος κατά τον οποίο η Αρχή θα μπορεί να αποκρυπτογραφεί μηνύματα που προορίζονται για τον χρήστη [Abel98,Bur98].

- **Οι χρήστες παρακάμπτουν το σύστημα ανάκτησης κλειδιού.** Οι επιθέσεις αυτές διακρίνονται σε επιθέσεις όπου:

  α) Οι χρήστες εκ των προτέρων μοιράζονται μυστική πληροφορία ή

  β) Οι χρήστες δε μοιράζονται κάποια μυστική πληροφορία.

Οι επιθέσεις τύπου (α) είναι αδύνατο να αντιμετωπιστούν [Pfi97_1]. Πράγματι, εάν ο αποστολέας και ο παραλήπτης μοιράζονται εκ των προτέρων μια μυστική πληροφορία, τότε μπορούν να εγκαθιδρύσουν ένα απόλυτα μυστικό κανάλι επικοινωνίας (π.χ. χρησιμοποιώντας κρυπτογράφηση *one-time pad*[47] [Sti95]).

Οι επιθέσεις τύπου (β) διακρίνονται επιπλέον στις εξής επιθέσεις:

- *Η Γενικευμένη Επίθεση Διπλής Κρυπτογράφησης*. Ο αποστολέας κρυπτογραφεί πρώτα το μήνυμα με ένα μη ελεγχόμενο σύστημα κρυπτογράφησης, και στη συνέχεια με τον κρυπτογραφικό αλγόριθμο του συστήματος ανάκτησης κλειδιού [Blaz94]. Αυτή η επίθεση είναι δύσκολο να αντιμετωπιστεί, εκτός και αν υποθέσουμε ότι δεν υπάρχουν μη ελεγχόμενα συστήματα κρυπτογράφησης, κάτι που είναι μια μη ρεαλιστική υπόθεση.

- *Η Επίθεση των Pfitzmann-Waidner*. Κατά την επίθεση αυτή ο επιτιθέμενος χρησιμοποιεί τον μηχανισμό ανάκτησης κλειδιού για τη διπλή κρυπτογράφηση [Pfi97_1]. Έτσι, το σύστημα μπορεί να νικηθεί χωρίς την ανάγκη χρήσης ενός μη ελεγχόμενου συστήματος κρυπτογράφησης. Η επίθεση περιγράφεται ξεχωριστά στην Ενότητα 5.3.1.

Όλα τα συστήματα ανάκτησης κλειδιού που έχουν προταθεί έως σήμερα είναι ευάλωτα στις επιθέσεις διπλής κρυπτογράφησης. Στην Ενότητα 5.5 προτείνουμε ένα *υβριδικό* μοντέλο ανάκτησης κλειδιού που απευθύνεται κυρίως στο εταιρικό περιβάλλον και υπό προϋποθέσεις μπορεί να αντιμετωπίσει την επίθεση των Pfitzmann-Waidner.

---

[47] Πρόκειται για μια κρυπτογραφική μέθοδο της οποίας η ασφάλεια θεωρείται (και είναι) απόλυτη, όμως στην πράξη χρησιμοποιείται ελάχιστα (π.χ. για ανταλλαγή μηνυμάτων ύψιστης ασφάλειας μεταξύ κρατικών μυστικών υπηρεσιών) αφού απαιτεί το κλειδί κρυπτογράφησης να έχει το ίδιο μήκος με το μήνυμα που ανταλλάσσεται, και επίσης το κλειδί να χρησιμοποιείται μόνον μια φορά.

5.3.1 Η Επίθεση των Pfitzmann-Waidner

Η επίθεση αυτή [Pfi97_1] αφορά το μοντέλο των Verheul-Henk-Tilborg [Ver97] για συστήματα *εικονικής διευθυνσιοδότησης* κλειδιών συνόδου. Περιγράφουμε συνοπτικά τον μηχανισμό ανάκτησης: ο αποστολέας, έστω η Alice, επιλέγει ένα κλειδί συνόδου S και κρυπτογραφεί με αυτό το μήνυμα M, στα πλαίσια ενός συμμετρικού αλγόριθμου κρυπτογράφησης. Στη συνέχεια, η Alice κρυπτογραφεί το S με το δημόσιο κλειδί του παραλήπτη, έστω του Bob, PK_{Bob}, καθώς επίσης και με το δημόσιο κλειδί PK_A της Αρχής Ανάκτησης Κλειδιού. Η Alice αποστέλλει στον Bob το κρυπτογράφημα:

$$C = [M]_S \parallel [S]_{PK_{Bob}} \parallel [S]_{PK_A} \parallel proof \quad (1)$$

όπου *proof* είναι μία μη αλληλεπιδραστική (non-interactive) απόδειξη με μηδενική γνώση (zero knowledge), ότι τα κλειδιά συνόδου που περιέχονται στο δεύτερο και το τρίτο τμήμα του C είναι τα ίδια [Cha92]. Η ορθότητα της απόδειξης αυτής μπορεί να επαληθευτεί από οποιονδήποτε εξωτερικό παρατηρητή (οικουμενική επαληθευσιμότητα).

Η Επίθεση. Εάν δεχθούμε ότι οι χρήστες μπορούν να κάνουν μικρές παρεμβάσεις στο λογισμικό κρυπτογράφησης/αποκρυπτογράφησης [Pfi97_1], τότε η Alice μπορεί να αποστείλει στον Bob το κρυπτογράφημα:

$$C = [M_1]_{S_1} \parallel [S_1]_{PK_{Bob}} \parallel [S_1]_{PK_A} \parallel proof$$

όπου

$$M_1 = info \parallel [M_2]_{S_2} \parallel [S_2]_{PK_{Bob}}$$

όπου το τμήμα *info* περιέχει οδηγίες για το πώς ο Bob θα χειριστεί το κρυπτογράφημα. Σε αυτό το σημείο πρέπει ξανά να τονιστεί πως θεωρούμε ότι οι Bob και Alice δεν μοιράζονται εκ των προτέρων κάποια μυστική πληροφορία, επομένως το τμήμα *info* είναι απαραίτητο για να είναι επιτυχής η επίθεση.

5.4 Ανάκτηση Κλειδιού με Ισχυρή Χρονική Ασφάλεια

Τα συστήματα ανάκτησης κλειδιού αρχικά προτάθηκαν ως ένα μέσο προστασίας της κοινωνίας από άτομα που χρησιμοποιούν ένα κρυπτογραφικό σύστημα επικοινωνίας για να σχεδιάσουν ή να τελέσουν εγκληματικές πράξεις. Εντούτοις, από τη σκοπιά του ατόμου, τα συστήματα αυτά μπορούν να δώσουν μεγάλη δύναμη στην κοινωνία (Big Brother [Cha85]), την οποία δύναμη σε αρκετές περιπτώσεις η κοινωνία μπορεί να καταχραστεί. Σε ένα *«δίκαιο»* (equitable) σύστημα, [Bur98,Mic92,Mag00], η δύναμη αυτή μοιράζεται εξίσου στο άτομο και στην κοινωνία.

Ένα αποτελεσματικό μέτρο για την άσκηση ελέγχου στη δύναμη που μπορεί να έχει η κοινωνία, προβλέπει τα κλειδιά που ανακτώνται (υποθηκεύονται) να έχουν περιορισμένη χρονική διάρκεια ισχύος. Κατά αυτόν τον τρόπο παρέχεται *χρονική ασφάλεια* (forward security) [Bur98,Gun89, Bel99] για τα κλειδιά που αφορούν περιόδους που *προηγούνται* της περιόδου κατά την οποία ασκείται το δικαίωμα της ανάκτησης των μηνυμάτων.

Ωστόσο η κρυπτογραφική προστασία της *χρονικής ασφάλειας* δεν είναι αρκετή. Τα συστήματα με χρονική ασφάλεια δεν παρέχουν επαρκή προστασία στα κρυπτογραφημένα μηνύματα του χρήστη που αφορούν περιόδους που *έπονται* της περιόδου ανάκτησης (ή υπεξαίρεσης ή κλοπής) του ιδιωτικού κλειδιού [Bur_Mag01]. Στη συνέχεια ορίζουμε την έννοια της *ισχυρής χρονικής ασφάλειας* και περιγράφουμε το μηχανισμό με τον οποίο αυτή μπορεί να επιτευχθεί.

5.4.1 Ισχυρή Χρονική Ασφάλεια

Στην Ενότητα αυτή προτείνουμε την ισχυρή χρονική ασφάλεια (strong forward security) ως μια μέθοδο για την ελαχιστοποίηση των συνεπειών της εξουσιοδοτημένης (π.χ. στην περίπτωση της νόμιμης ανάκτησης κλειδιού από τις Αρχές Επιβολής Νόμου) ή μη εξουσιοδοτημένης (π.χ. hacking) αποκάλυψης ενός ιδιωτικού κλειδιού, στα πλαίσια ενός κρυπτογραφικού συστήματος δημοσίου κλειδιού [Bur_Mag01]. Σύμφωνα με τη μέθοδο αυτή, η οποία μπορεί να αξιοποιηθεί και για την προστασία ιδιωτικών κλειδιών ψηφιακής υπογραφής [Bur_Mag01,You00], το ζεύγος ιδιωτικού/δημόσιου κλειδιού ενός χρήστη ανανεώνεται ανά τακτά χρονικά διαστήματα. Ο μηχανισμός ανανέωσης επεκτείνει την έννοια της *χρονικής ασφάλειας* [Gun89,Bel99] καθώς εξασφαλίζει ότι η αποκάλυψη του ιδιωτικού κλειδιού ενός χρήστη κατά τη διάρκεια μιας συγκεκριμένης περιόδου, δε θα υπονομεύσει την ιδιωτικότητα του χρήστη κατά τις περιόδους που *προηγήθηκαν* (χρονική ασφάλεια) αλλά και κατά τις περιόδους που *έπονται* της αποκάλυψης (ισχυρή χρονική ασφάλεια).

Ο μηχανισμός ανανέωσης που προτείνουμε *δεν* απαιτεί φυσικές (out-of-band) μεθόδους αυθεντικοποίησης, αλλά επιτυγχάνεται αυθεντικοποιώντας το ανανεωμένο ιδιωτικό κλειδί με το προηγούμενο ιδιωτικό κλειδί, και υποβάλλοντας το αντίστοιχο δημόσιο κλειδί σε μια Αρχή Πιστοποίησης (Certification Authority – CA). Εάν υπάρξει και δεύτερη οντότητα, π.χ. ένας εισβολέας (hacker) ή μια κακόβουλη Αρχή Επιβολής Νόμου *LEA* που υποβάλλει ένα (πιθανότατα διαφορετικό) κλειδί εκ μέρους του ίδιου χρήστη για πιστοποίηση, τότε η Αρχή *CA* θα ανακαλέσει το δημόσιο κλειδί του χρήστη.

5.4.2 Ένα «Δίκαιο» Κρυπτογραφικό Σχήμα Ανάκτησης Κλειδιού με Ισχυρή Χρονική Ασφάλεια

Σε αυτήν την Ενότητα προτείνουμε ένα σχήμα ανάκτησης κλειδιού με ισχυρή χρονική ασφάλεια, βασισμένο στην παραδοσιακή προσέγγιση (Ενότητα 5.2), όπου η διαμοίραση κλειδιών στους πράκτορες ανάκτησης (recovery agents) καθώς και η ανανέωση του ιδιωτικού κλειδιού του χρήστη γίνεται κατά τρόπο πρακτικό και ασφαλή [Bur_Mag01].

Για απλότητα περιγράφουμε ένα σχήμα με δύο πράκτορες ανάκτησης κλειδιού, RA_1, RA_2. Οι πράκτορες υπεισέρχονται επίσης στη διαδικασία ανανέωσης των ιδιωτικών κλειδιών των χρηστών, κατά τρόπο ανεξάρτητο του αριθμού των χρηστών του συστήματος. Μια Αρχή Πιστοποίησης *CA* είναι υπεύθυνη για την πιστοποίηση των κλειδιών που ανανεώνονται, ενώ η Αρχή Επιβολής Νόμου *LEA* έχει τη δυνατότητα, κατόπιν εντάλματος, να ζητήσει τη συμβολή των πρακτόρων στην ανάκτηση των μηνυμάτων ενός χρήστη που αφορούν μια συγκεκριμένη χρονική περίοδο.

Κάθε χρήστης, π.χ. η Alice, κατά τη διάρκεια της εγγραφής του στο σύστημα, επιλέγει ένα ιδιωτικό κλειδί *μακράς διάρκειας* x_A και το υποθηκεύει στους πράκτορες κατά τρόπο, όπως θα δούμε, επαληθεύσιμο. Έπειτα, στην αρχή κάθε περιόδου i, οι πράκτορες κατασκευάζουν μια *παράμετρο ελέγχου χρόνου* (time control identifier) h_i, η οποία αναμεταδίδεται από την *CA* και θα χρησιμοποιηθεί από όλους τους χρήστες του συστήματος κατά την ανανέωση του ιδιωτικού κλειδιού τους. Συγκεκριμένα, το ανανεωμένο κλειδί της Alice SK_i θα προκύψει ως συνάρτηση του προηγούμενου κλειδιού SK_{i-1}, του κλειδιού μακράς διαρκείας x_A, κάποιας επιπλέον τυχαιότητας (που επιλέγει η Alice) και της παραμέτρου h_i. Μετά από την ανανέωση, η Alice και οι πράκτορες διαγράφουν κάθε πληροφορία που θα μπορούσε να είναι χρήσιμη σε έναν εχθρό που επιθυμεί την πρόσβαση σε κλειδιά προηγούμενων περιόδων (*χρονική ασφάλεια*). Το ρόλο του εχθρού θα μπορούσε να διαδραματίσει:

- Ένας εισβολέας (hacker).
- Μια κακόβουλη Αρχή *LEA*.

Επιπλέον, η Alice ανανεώνει το δημόσιο της κλειδί σε PK_t, και αποδεικνύει στην *CA* με ένα πρωτόκολλο απόδειξης με *μηδενική γνώση* [Gol85], το οποίο θα παρουσιάζουμε ξεχωριστά στο τέλος του Κεφαλαίου (Παράρτημα Β), ότι το κλειδί έχει κατασκευαστεί ακολουθώντας την προβλεπόμενη διαδικασία. Η *CA* τότε πιστοποιεί το ανανεωμένο κλειδί PK_t και επιστρέφει το πιστοποιητικό στον χρήστη.

Το σύστημα που προτείνουμε είναι «δίκαιο»: εάν όλα τα μυστικά της Alice περιέλθουν στην κατοχή του εχθρού, ο εχθρός θα επιχειρήσει να ανανεώσει το κλεμμένο ιδιωτικό κλειδί της και εν συνεχεία να πιστοποιήσει το αντίστοιχο δημόσιο κλειδί στην *CA*. Εφόσον και η Alice θα υποβάλλει το ανανεωμένο κλειδί της για ανανέωση, η *CA* θα παρατηρήσει ότι δυο διαφορετικά (με μεγάλη πιθανότητα) κλειδιά υποβάλλονται για πιστοποίηση και θα ανακαλέσει το δημόσιο κλειδί της Alice για την τρέχουσα περίοδο (*ισχυρή χρονική ασφάλεια*). Σε αυτήν την περίπτωση η επόμενη ανανέωση του κλειδιού της Alice θα πρέπει να γίνει με φυσικές (out-of-band) μεθόδους.

Το Πρωτόκολλο

Χρησιμοποιούμε ως βάση το σύστημα κρυπτογράφησης ElGamal [ElG85]. Έστω r, p, q μεγάλοι πρώτοι αριθμοί με $q = 2r + 1$, $p = 2q + 1$, και έστω H μια υποομάδα του Z_q^* τάξης r με γεννήτορα h, και G μια υποομάδα του Z_p^* τάξης q με γεννήτορα g. Για απλότητα, και όπου δεν υπάρχουν αμφιβολίες, θα παραλείπουμε τους *modulus* τελεστές. Ο τελεστής *DH* (Diffie-Hellman [Dif76]) ορίζεται ως $DH(g^a, g^b) = g^{ab}$. Θυμίζουμε ότι δεδομένων των αριθμών g^a, g^b, το πρόβλημα του υπολογισμού του $DH(g^a, g^b)$ αποκαλείται και ως

πρόβλημα Diffie-Hellman. Δεδομένου ενός $z \in Z_p$, το πρόβλημα της απόφασης για το εάν ισχύει η ισότητα $z = DH(g^a, g^b)$ αποκαλείται και ως *πρόβλημα απόφασης Diffie-Hellman* [Dif76].

Αρχικοποίηση (Setup). Η Alice επιλέγει τυχαία ένα ιδιωτικό κλειδί μακράς διαρκείας $x_A \in_R Z_q^*$ και υπολογίζει $y_A = g^{x_A}$. Η Alice αυθεντικοποιεί το δημόσιο κλειδί της $PK_A =< p, q, g, y_A >$ στην *CA* με μη κρυπτογραφικές (out of band) μεθόδους, και λαμβάνει ένα πιστοποιητικό $Cert(ID_A, PK_A)$. Τότε,

1. Η Alice επιλέγει μερίδια $x_1 \in_R Z_q^*$ και $x_2 = x_A(x_1)^{-1}$. Η Alice αποστέλλει τα μερίδια x_1, x_2 στους πράκτορες RA_1, RA_2, αντίστοιχα.

2. Οι πράκτορες ελέγχουν εάν $y_A = DH(g^{x_1}, g^{x_2})$. Εάν όχι, η Alice αναφέρεται στην *LEA*.

Ανανέωση Κλειδιού (περίοδος $t = 1.2....$). Οι πράκτορες RA_1, RA_2, επιλέγουν τυχαίους αριθμούς $r_{1,t}, r_{2,t} \in_R Z_r^*$ αντιστοίχως, και κατασκευάζουν από κοινού την παράμετρο ελέγχου χρόνου $h^{r_t} = h^{r_{1,t} \cdot r_{2,t}}$ χρησιμοποιώντας το πρωτόκολλο ανταλλαγής κλειδιών[48] των Diffie-Hellman [Dif76]. Οι πράκτορες στέλνουν το h^{r_t} στην *CA* η οποία το δημοσιεύει. Αυτός ο αριθμός αναφέρεται στην τρέχουσα περίοδο t και θα πρέπει να χρησιμοποιηθεί από όλους τους χρήστες του συστήματος για την ανανέωση των κλειδιών τους. Οι πράκτορες στη συνέχεια διαγράφουν τους εκθέτες $r_{1,t-1}, r_{2,t-1}$ της προηγούμενης περιόδου (στην περίπτωση όπου $t > 1$). Τότε,

---

[48] Κατά το πρωτόκολλο ανταλλαγής κλειδιών των Diffie-Hellman, είναι δυνατό για τους δύο πράκτορες RA_1, RA_2, με εισόδους τα $r_{1,t}$ και $r_{2,t}$ αντίστοιχα, να κατασκευάσουν τον αριθμό $h^{r_t} = DH(h^{r_{1,t}}, h^{r_{2,t}})$ ως κοινή έξοδο, χωρίς ο RA_1 να αποκτήσει γνώση της μυστικής εισόδου $r_{2,t}$ του RA_2, ή ο RA_2 να αποκτήσει γνώση της μυστικής εισόδου $r_{1,t}$ του RA_1.

1. Η Alice επιλέγει έναν τυχαίο αριθμό $r_{A,t} \in_R Z_r^*$, υπολογίζει $h^{r_{A,t}}$ και το αποστέλλει στην *CA*. Επίσης υπολογίζει το Diffie-Hellman κλειδί $h_t = h^{r_t r_{A,t}}$.

2. Η Alice ανανεώνει το ιδιωτικό της κλειδί για την περίοδο t σε $SK_{A,t} = h_t x_A$. Στη συνέχεια υπολογίζει $y_{A,t} = g^{h_t x_A}$ και στέλνει στην CA το δημόσιο κλειδί για την περίοδο t, $PK_{A,t} = < p, q, r, g, h, y_{A,t} >$. Η Alice στη συνέχεια αποδεικνύει στην *CA*, με ένα πρωτόκολλο μηδενικής γνώσης (η απόδειξη περιγράφεται στο Παράρτημα Β), ότι $y_{A,t} = g^{DH(h^{r_t}, h^{r_{A,t}}) DL(g^{x_A})}$, όπου $DL(g^{x_A})$ είναι ο διάκριτος λογάριθμος του g^{x_A}. Εάν η απόδειξη είναι ορθή, η *CA* πιστοποιεί το ανανεωμένο δημόσιο κλειδί $PK_{A,t}$ και εκδίδει για την Alice ένα πιστοποιητικό $Cert(ID_A, PK_{A,t})$. Η Alice τότε διαγράφει το $r_{A,t}$ καθώς και το ιδιωτικό κλειδί $SK_{A,t-1}$ της προηγούμενης περιόδου $t-1$ (στην περίπτωση όπου $t > 1$).

Σημείωση: Η αλληλεπιδραστική απόδειξη μηδενικής γνώσης στο Βήμα 2, μπορεί να αντικατασταθεί με μια υπογραφή, δηλαδή με μια μη αλληλεπιδραστική απόδειξη μηδενικής γνώσης, χρησιμοποιώντας την «ευριστική» προσέγγιση των Fiat-Shamir [Fia86]. Εντούτοις, η ασφάλεια των υπογραφών αυτών αποδεικνύεται μόνον στο μοντέλο Random Oracle[11] *[Bel93].*

Ανάκτηση Κλειδιού. Ας υποθέσουμε πως η *LEA* έχει στην κατοχή της ένα ένταλμα για την αποκρυπτογράφηση όλων των μηνυμάτων που προορίζονται για την Alice κατά τη διάρκεια της περιόδου t. Έστω $(g^k, m(y_{A,t})^k)$ μια ElGamal κρυπτογράφηση ενός μηνύματος m που στάλθηκε στην Alice την περίοδο αυτή. Η *LEA* επιδεικνύει το ένταλμα στην *CA*, λαμβάνει την παράμετρο $h^{r_{A,t}}$ που αντιστοιχεί στην Alice και στέλνει τα g^k,

$h^{r_{A,t}}$ στους πράκτορες. Οι πράκτορες υπολογίζουν το Diffie-Hellman κλειδί $h_i = h^{r_i r_{A,t}}$ και στη συνέχεια το $(y_{A,t})^k = (((g^k)^{h_i})^{x_1})^{x_2}$ το οποίο και επιστρέφουν στην *LEA*. Τέλος η *LEA* χρησιμοποιεί το $(y_{A,t})^k$ για να ανακτήσει το m.

Θεώρημα. *Αν το πρόβλημα απόφασης Diffie-Hellman [Dif76] είναι υπολογιστικά δύσκολο, τότε το προτεινόμενο σχήμα ανάκτησης κλειδιού παρέχει ισχυρή χρονική ασφάλεια.*

Απόδειξη. Ας υποθέσουμε πως υπάρχει ένας αλγόριθμος πολυωνυμικού χρόνου A, που παραβιάζει την ασφάλεια του προτεινόμενου σχήματος ανάκτησης κλειδιού. Έστω $z, h^a, h^b \in_R Z_q^*$ μια είσοδος για το πρόβλημα απόφασης Diffie Hellman. Τότε, θα δείξουμε ότι ο πολυωνυμικός αλσγόριθμος A μπορεί να χρησιμοποιηθεί για την επίλυση του προβλήματος απόφασης Diffie Hellman.

Επιλέγονται τυχαία $k, x_A \in_R Z_q^*$, $m \in_R Z_p^*$ και ετοιμάζεται ένα ιστορικό για ζεύγη κρυπτογραφημάτων – μηνυμάτων (c, m) για τον αλγόριθμο A, επιλέγοντας $r_i, r_{A,t} \in_R Z_p^*$ και λαμβάνοντας $c = (g^k, mg^{kx_A} h^{r_i r_{A,t}})$. Στη συνέχεια δίνεται ως είσοδος στον αλγόριθμο A: το x_A, το μακράς διαρκείας δημόσιο κλειδί $y_A = g^{x_A}$ και τα z, h^a, h^b αντί των $h_j, h^{r_{A,j}}, h^{r_j}$, το δημόσιο κλειδί της περιόδου j, $y_{A,j} = g^{zx_A}$, και το «κρυπτογράφημα»: (g^k, mg^{kzx_A}). Έστω ότι το αποτέλεσμα στην έξοδο του A είναι m'. Αν $m = m'$ τότε η απόφαση είναι πως $z = h^{ab}$, αλλιώς $z \neq h^{ab}$.

Σημείωση: Οι πράκτορες ανάκτησης αποτελούν ουσιαστικά μια ασφαλή αποθήκη για τα ιδιωτικά κλειδιά μακράς διαρκείας των χρηστών του συστήματος. Στο πρωτόκολλο μας οι πράκτορες επίσης δημιουργούν από κοινού έναν τυχαίο αριθμό h^{r_t}. Ο αριθμός αυτός, τον οποίο ονομάσαμε παράμετρο ελέγχου χρόνου, αντιστοιχεί σε συγκεκριμένη χρονική

περίοδο και είναι ίδιος για όλους τους χρήστες του συστήματος. Σε επόμενες περιόδους δημιουργούνται καινούριοι αριθμοί, ενώ όλα τα δεδομένα που αφορούν την προηγούμενη περίοδο διαγράφονται. Πρέπει επίσης να τονιστεί ότι η πρόσθεση ή διαγραφή χρηστών από το σύστημα δεν επηρεάζει τη λειτουργικότητα των πρακτόρων ανάκτησης.

Γενικεύσεις

1. Με τη χρήση των τεχνικών που περιγράφονται στις εργασίες [Ped92,Fran96,Oka97_1], το σχήμα μας μπορεί εύκολα να επεκταθεί σε ένα (t,ℓ) threshold σχήμα ανάκτησης κλειδιών, όπου t σε σύνολο ℓ πρακτόρων συνεργάζονται για την αποκρυπτογράφηση των μηνυμάτων. Σε αυτήν την περίπτωση το σχήμα θα προσφέρει προστασία ενάντια σε (μέχρι και) $t-1$ πράκτορες που συμπεριφέρονται κακόβουλα, π.χ. συνεργάζονται με μια κακόβουλη *LEA* για την αποκρυπτογράφηση μηνυμάτων της Alice σε προηγούμενες ή επόμενες περιόδους.

2. Είναι γνωστό πως το σχήμα κρυπτογράφησης ElGamal [ElG85], το οποίο χρησιμοποιήσαμε λόγω της απλότητας στην υλοποίηση του, δεν προσφέρει *σημειολογική ασφάλεια*[49] (semantic security) [Sch96]. Για σημειολογική ασφάλεια, θα μπορούσε να χρησιμοποιηθεί η επέκταση των Cramer-Shoup [Cra97_1] στο σχήμα ElGamal.

[49] Ένα σχήμα κρυπτογράφησης δημοσίου κλειδιού ονομάζεται *σημειολογικά ασφαλές* όταν είναι αδύνατον για έναν παθητικό εχθρό (passive adversary) που υποκλέπτει ένα κρυπτογράφημα να εξάγει οποιαδήποτε πληροφορία σχετικά με το κείμενο που περιέχεται στο κρυπτογράφημα.

5.5 Ένα Υβριδικό Μοντέλο Ανάκτησης Κλειδιού

Στην Ενότητα αυτή προτείνουμε ένα μοντέλο ανάκτησης κλειδιού για την αντιμετώπιση, υπό προϋποθέσεις, των επιθέσεων διπλής κρυπτογράφησης των Pfitzmann-Waidner (Ενότητα 5.3.1) [Pfi97_1]. Οι προϋποθέσεις εφαρμογής του μοντέλου μας είναι οι εξής [Mag03]:

- Ο αποστολέας και ο παραλήπτης δεν μοιράζονται εκ των προτέρων μυστική πληροφορία, και

- Όλα τα ιδιωτικά κλειδιά αποκρυπτογράφησης μακράς διαρκείας είναι υποθηκευμένα. Αυτή η υπόθεση είναι άρρηκτα συνδεδεμένη με την υπόθεση ύπαρξης μιας καλά ορισμένης και ασφαλούς Υποδομής Δημοσίου Κλειδιού (Public Key Infrastructure) [You97].

Σημείωση: Στο περιβάλλον του Διαδικτύου οι προϋποθέσεις αυτές δεν είναι ρεαλιστικές, επειδή ο έλεγχος που μπορούν να ασκήσουν οι Υπηρεσίες Επιβολής του Νόμου (Law Enforcement Agencies) στους χρήστες είναι εκ των πραγμάτων περιορισμένος. Ωστόσο, στο εταιρικό περιβάλλον οι παραπάνω προϋποθέσεις θα μπορούσαν να αποτελούν σημαντικό κομμάτι της πολιτικής ασφάλειας για τη διαχείριση των κλειδιών των χρηστών της επιχείρησης. Επομένως, το μοντέλο ανάκτησης κλειδιού που προτείνουμε μπορεί να εφαρμοστεί κυρίως για την προστασία των κρίσιμων δεδομένων μιας επιχείρησης που αρχειοθετούνται ή ανταλλάσσονται μεταξύ των χρηστών του ενδοδικτύου (intranet) της επιχείρησης.

Το μοντέλο μας είναι *υβριδικό*:

- Για την ανάκτηση των ιδιωτικών κλειδιών μακράς διαρκείας επικαλούμαστε *παραδοσιακούς μηχανισμούς* υποθήκευσης [Den96,Mic92, Fran95], όπου ένας αριθμός πρακτόρων ανάκτησης κλειδιών επιφορτίζονται με την ασφαλή φύλαξη των ιδιωτικών κλειδιών του

χρήστη μέχρις ότου τους ζητηθεί από μια Αρχή η συνδρομή τους στην ανάκτηση ενός κρυπτογραφημένου μηνύματος. Για ανθεκτικότητα (robustness), προτείνεται εναλλακτικά η χρησιμοποίηση τεχνικών threshold ανάκτησης κλειδιού [Desm89], βασισμένων είτε στο *διακριτό λογάριθμο* [Ped92] είτε στην *παραγοντοποίηση* μεγάλων πρώτων αριθμών [Oka97_1,Pou98].

- Για την ανάκτηση των κλειδιών συνόδου που κρυπτογραφούν συμμετρικά τα μηνύματα που αρχειοθετούν ή ανταλλάσσουν οι χρήστες, προτείνουμε τον μηχανισμό *εικονικής διευθυνσιοδότησης* κλειδιών συνόδου των Verheul-Henk-Tilborg (Ενότητα 5.3.1) [Ver97].

Η αρχιτεκτονική αυτή που προτείνουμε δεν συνιστά μεγάλη πολυπλοκότητα. καθώς τα κλειδιά μακράς διαρκείας ανακτώνται μόνον όταν ανιχνευτεί επίθεση *διπλής κρυπτογράφησης* στο σύστημα.

Οι Συμμετέχοντες. Οι συμμετέχοντες στο μοντέλο μας (Σχήμα 14) είναι οι χρήστες, ο *Παροχέας Υπηρεσιών* (Π.Υ), η *Αρχή Επιβολής Πολιτικής Ασφάλειας* (Α.Ε.Π.Α), η *Αρχή Έκδοσης Εισιτηρίων* (Α.Ε.Ε), η *Αρχή Ανάκτησης Κλειδιού* (Α.Α.Κ) και η *Αρχή Υποθήκευσης Κλειδιού* (Α.Υ.Κ).

- *Χρήστες* (π.χ. Alice, Bob). Στην περίπτωση αρχειοθετημένων δεδομένων (archived data) μπορούμε να θεωρήσουμε ότι η Alice και ο Bob είναι το ίδιο πρόσωπο.

- *Παροχέας Υπηρεσιών*. Ο Π.Υ είναι ο διανομέας (hub) του μοντέλου μας. Υλοποιεί έναν μηχανισμό φιλτραρίσματος και ελέγχει αν τα κρυπτογραφήματα που αποθηκεύονται ή διακινούνται μεταξύ των χρηστών έχουν το κατάλληλο format (ωστόσο, ο Π.Υ δεν μπορεί να τα

αποκρυπτογραφήσει). Ο Π.Υ διατηρεί αντίγραφα (logs) των δεδομένων που διέρχονται από αυτόν[50].

- *Αρχή Επιβολής Πολιτικής Ασφάλειας*. Η Α.Ε.Π.Α είναι υπεύθυνη για την έναρξη του μηχανισμού ανάκτησης.

- *Αρχή Έκδοσης Εισιτηρίων*. Η Α.Ε.Ε[51] είναι μια offline υπηρεσία που εκδίδει «εισιτήρια» περιορισμένης χρονικής ισχύος τα οποία εξουσιοδοτούν την αποκρυπτογράφηση των συνομιλιών μεταξύ δύο χρηστών του συστήματος.

- *Αρχή Ανάκτησης Κλειδιού*. Για κάθε κρυπτογράφημα που συνοδεύεται από το αντίστοιχο εισιτήριο εξουσιοδότησης, η Α.Α.Κ ανακτά την αντίστοιχη αποκρυπτογραφημένη πληροφορία.

- *Αρχή Υποθήκευσης Κλειδιού*. Η Α.Υ.Κ φυλάσσει τα ιδιωτικά κλειδιά μακράς διαρκείας όλων των χρηστών του συστήματος.

Το Πρωτόκολλο

α) Η Alice στέλνει ένα κρυπτογράφημα στον Bob μέσω του Παροχέα Υπηρεσιών. Ο Π.Υ ελέγχει για ορθότητα την απόδειξη *proof* (εξίσωση (1) - Ενότητα 5.3.1), καταγράφει το κρυπτογράφημα C και το προωθεί στον Bob.

[50] Ο Π.Υ θα μπορούσε να είναι για παράδειγμα ένα module εκτελούμενο σε ένα σύστημα Windows 2000 server που ταυτόχρονα είναι και Ελεγκτής (domain controller) του Τομέα δικτύου της επιχείρησης, ενώ οι χρήστες είναι συστήματα Windows 2000 clients – μέλη του Τομέα. Σε αυτήν την περίπτωση, η πρόσβαση στους πόρους του δικτύου ακολουθεί την στρατηγική client-server και τα αρχειοθετημένα ή διακινούμενα δεδομένα μπορούν να φιλτραριστούν στον Ελεγκτή του Τομέα.

[51] Η ονομασία αυτή είναι ίδια με την ονομασία της γνωστής Αρχής Έκδοσης Εισητηρίων (Ticket Granting Service) του συστήματος Kerberos [Mil87], λόγω της ομοιότητας που παρουσιάζουν ως προς τη λειτουργία τους.

Σχήμα 14. Ένα υβριδικό μοντέλο ανάκτησης κλειδιού

β) Σε περίπτωση απώλειας κλειδιών ή εάν η Αρχή Επιβολής Πολιτικής Ασφάλειας θεωρεί ότι η ροή μηνυμάτων προς τον Bob για μια δεδομένη χρονική περίοδο είναι ύποπτη, υποβάλλει στην Αρχή Έκδοσης Εισιτηρίων αίτημα για την ανάκτηση των μηνυμάτων που στέλνονται στον Bob και λαμβάνει ένα εισιτήριο (περιορισμένης χρονικής διαρκείας). Το εισιτήριο εσωκλείει το αναγνωριστικό ID_{Bob}. Πρέπει να τονιστεί, ότι στην περίπτωση της απώλειας κλειδιών, μπορεί και η ίδια η Alice να ζητήσει ένα εισιτήριο από την Α.Ε.Ε για να αποκρυπτογραφήσει τα αρχειοθετημένα δεδομένα της (σε αυτήν την περίπτωση, όπως είδαμε, η Alice και ο Bob είναι το ίδιο πρόσωπο).

γ) Η Α.Ε.Π.Α παρουσιάζει το εισιτήριο στον Π.Υ και λαμβάνει τα κρυπτογραφήματα που έχουν καταγραφεί και απευθύνονται στον Bob για την χρονική περίοδο που αναγράφεται στο εισιτήριο.

δ) Η Α.Ε.Π.Α προωθεί το κρυπτογράφημα C (καθώς και όλα τα κρυπτογραφήματα που εστάλησαν στον Bob κατά τη συγκεκριμένη χρονική περίοδο) στην Αρχή Ανάκτησης Κλειδιού. Η Α.Α.Κ χρησιμοποιεί το ιδιωτικό της κλειδί αποκρυπτογράφησης ώστε να ανακτήσει το συμμετρικό κλειδί S_1 και κατ' επέκταση το μήνυμα M_1, στα πλαίσια του μηχανισμού εικονικής

διευθυνσιοδότησης (Ενότητα 5.3.1). Η Α.Α.Κ. στέλνει τα (M_1, ID_{Bob}) στην Α.Ε.Π.Α.

ε) Αν η Α.Ε.Π.Α θεωρήσει ότι το M_1 αποτελεί το μοναδικό αποκρυπτογράφημα που απευθύνεται στον Bob, τότε η διαδικασία ανάκτησης κλειδιού ολοκληρώνεται. Εάν όμως υποπτευθεί ότι το M_1 περιέχει επιπλέον δεδομένα, κρυπτογραφημένα διπλά με το δημόσιο κλειδί του Bob (επίθεση των Pfitzmann-Waidner), στέλνει τα (M_1, ID_{Bob}) στην Αρχή Υποθήκευσης Κλειδιού.

στ) Η Α.Υ.Κ χρησιμοποιεί το υποθηκευμένο κλειδί του Bob για να εξάγει το διπλά κρυπτογραφημένο μήνυμα M_2, και στέλνει τα (M_2, ID_{Bob}) στην Α.Ε.Π.Α.

Πρακτικότητα. Στο μοντέλο μας απαιτήσαμε όλα τα δημόσια κλειδιά μακράς διαρκείας να είναι υποθηκευμένα, σύμφωνα με την παραδοσιακή προσέγγιση, σε μια Αρχή Υποθήκευσης Κλειδιού (Α.Υ.Κ). Για επιπλέον ασφάλεια στην προστασία της ιδιωτικότητας των χρηστών, και προκειμένου η Α.Υ.Κ να μη θεωρηθεί ως ένα μοναδικό σημείο αποτυχίας, προτείναμε την υλοποίηση της Α.Υ.Κ ως ένα σύνολο από ανεξάρτητες Α.Υ.Κ [Mic92]. Αυτό συνεπάγεται ένα επιπλέον κόστος για τα στάδια της δημιουργίας και ανάκτησης των κλειδιών. Ωστόσο, οι Α.Υ.Κ δεν υπεισέρχονται στην κανονική λειτουργία του συστήματος, παρά μόνον όταν όλες οι απόπειρες ανάκτησης του μηνύματος αποτυγχάνουν (π.χ. στην περίπτωση της επίθεσης Pfitzmann-Waidner). Κατά την κανονική λειτουργία του συστήματος, η ανάκτηση των μηνυμάτων γίνεται γρήγορα και αποδοτικά βάσει του μοντέλου εικονικής διευθυνσιοδότησης κλειδιών συνόδου, όπως αυτό προτάθηκε από τους Verheul-Henk-Tilborg [Ver97] και περιγράφτηκε στην Ενότητα 5.3.1. Επομένως θεωρούμε ότι το υβριδικό μοντέλο που προτείνουμε θα μπορούσε να οδηγήσει, υπό προϋποθέσεις, στην υλοποίηση ασφαλών και πρακτικών

συστημάτων ανάκτησης κλειδιού, στα πλαίσια μιας πολιτικής ασφάλειας για τη διαχείριση των κλειδιών των χρηστών και την πρόσβαση στα κρίσιμα εταιρικά δεδομένα.

5.6 Συζήτηση

Η ιδέα της ανάκτησης κλειδιού στα συστήματα επικοινωνιών έχει αποτελέσει κατά καιρούς πεδίο σύγκρουσης μεταξύ των πολιτών και των επιχειρήσεων ή των Αρχών Επιβολής Νόμου. Ιδιαίτερα τα συστήματα που βρίσκουν εφαρμογή στο πλαίσιο της παρακολούθησης συνομιλιών των πολιτών μέσω Διαδικτύου, λόγω των ιδιαιτεροτήτων που παρουσιάζουν, συγκεντρώνουν και το μεγαλύτερο ενδιαφέρον από τη σκοπιά της ασφάλειας.

Αρκετοί συγγραφείς έχουν καταδείξει τους κινδύνους που ελλοχεύουν στα συστήματα ανάκτησης κλειδιού, όταν η εξουσία περιέλθει σε (ή ασκείται από) ολοκληρωτικά ή εξτρεμιστικά καθεστώτα [Abel98]. Σε αυτήν την περίπτωση, ένα σύστημα ανάκτησης κλειδιού χωρίς χρονική ασφάλεια μπορεί να αποδειχτεί ισχυρό όπλο κατά της ιδιωτικότητας των πολιτών. Πρέπει να τονιστεί βέβαια ότι η χρονική ασφάλεια στα πλαίσια ενός τέτοιου καθεστώτος είναι δύσκολο (αν όχι ακατόρθωτο) να επιτευχθεί, αφού το καθεστώς, με μεγάλη πιθανότητα, θα ελέγχει πλήρως όλα τα επιμέρους τμήματα του συστήματος.

Στην Ενότητα 5.4 ορίσαμε την έννοια της *ισχυρής χρονικής ασφάλειας* η οποία επεκτείνει την έννοια της χρονικής ασφάλειας [Gun89] για την προστασία κρυπτογραφικών κλειδιών. Έτσι, ενώ σε ένα σύστημα με απλή χρονική ασφάλεια, μια κακόβουλη Αρχή Επιβολής Νόμου που κατέχει με νόμιμους (π.χ. ανάκτηση ή δήμευση κλειδιού) ή παράνομους τρόπους (π.χ. καταναγκασμός πολιτών [Bur_Mag02a]) το ιδιωτικό κλειδί του χρήστη για την περίοδο t δε μπορεί να αποκρυπτογραφήσει μηνύματα προηγούμενων περιόδων, σε ένα σύστημα με ισχυρή χρονική ασφάλεια η Αρχή δε μπορεί να αποκρυπτογραφήσει ούτε τα μηνύματα των επόμενων περιόδων. Θεωρούμε

πως ένα *«δίκαιο»* (equitable) σύστημα ανάκτησης κλειδιού πρέπει να παρέχει την επιπλέον αυτή προστασία. Στην Ενότητα 5.4 παρουσιάσαμε ένα πρακτικό σύστημα ανάκτησης κλειδιού με ισχυρή χρονική ασφάλεια [Bur_Mag01]. Το σύστημα αυτό εμπίπτει στην κατηγορία των «δίκαιων» ηλεκτρονικών συστημάτων συναλλαγών (Κεφάλαιο 1) υπό την έννοια ότι εξασφαλίζεται η ορθότητα της ανάκτησης κατόπιν εντάλματος, από την Αρχή Επιβολής Νόμου, των αποκρυπτογραφημένων μηνυμάτων που αφορούν μια συγκεκριμένη χρονική περίοδο, προστατεύοντας παράλληλα την ιδιωτικότητα των πολιτών για περιόδους πριν ή μετά την περίοδο ανάκτησης.

Στη διεθνή βιβλιογραφία έχει επίσης καταδειχθεί η δυσκολία υλοποίησης συστημάτων ανάκτησης κλειδιού, ιδίως στα πλαίσια των υπηρεσιών επιβολής νόμου. Τα περισσότερα συστήματα ανάκτησης κλειδιού είναι ευάλωτα σε επιθέσεις *διπλής κρυπτογράφησης*, όπου τα μηνύματα κρυπτογραφούνται πρώτα με ένα μη ελεγχόμενο κρυπτοσύστημα, και στη συνέχεια το κρυπτογράφημα που προκύπτει κρυπτογραφείται με τον αλγόριθμο που προβλέπει το μοντέλο ανάκτησης. Οι Pfitzmann και Waidner [Pfi97_1] μάλιστα περιέγραψαν μια επίθεση στα συστήματα εικονικής διευθυνσιοδότησης [Ver97], όπου ο επιτιθέμενος χρησιμοποιεί το ίδιο το σύστημα ανάκτησης κλειδιού για να παρεμποδίσει την πρόσβαση στις συνομιλίες του. Βέβαια, εκτός από την επίθεση των Pfitzmann και Waidner, οι επιτιθέμενοι μπορεί να χρησιμοποιήσουν *στεγανογραφία* ή ακόμη να σχεδιάσουν και να υλοποιήσουν από την αρχή μυστικούς κρυπτογραφικούς αλγόριθμους [Kil95]. Εντούτοις, πιστεύεται ότι

εάν κάποτε υπάρξει μια καλά ορισμένη Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure – PKI) με εγγενή υποστήριξη ανάκτησης κλειδιού, οι επιτιθέμενοι που παρακάμπτουν την υποδομή αυτή θα έχουν σημαντικές δυσκολίες στη διανομή των κλειδιών τους [Mic92].

Μια τέτοια Υποδομή μπορεί να έχει πρακτική εφαρμογή κυρίως στο περιβάλλον μιας επιχείρησης, στα πλαίσια μιας καλά ορισμένης πολιτικής ασφάλειας.

Η ύπαρξη Υποδομής Δημόσιου Κλειδιού αποτέλεσε τη βάση στην κατασκευή ενός μοντέλου για την αντιμετώπιση, υπό προϋποθέσεις, της επίθεσης διπλής κρυπτογράφησης των Pfitzmann-Waidner. Το μοντέλο μας είναι *υβριδικό* [Mag03]: τα κλειδιά αποκρυπτογράφησης μακράς διαρκείας (που χρήζουν αυξημένης προστασίας) είναι υποθηκευμένα, χρησιμοποιώντας την *Παραδοσιακή Προσέγγιση*, σε μια Αρχή Υποθήκευσης Κλειδιού η οποία για προστασία της ιδιωτικότητας των χρηστών μπορεί να υλοποιηθεί ως ένας αριθμός από ανεξάρτητες τρίτες οντότητες [Mic92], ενώ τα κλειδιά συνόδου μπορούν να ανακτηθούν από μια Αρχή Ανάκτησης Κλειδιού, βάσει του (πιο) ευέλικτου μηχανισμού της *εικονικής διευθυνσιοδότησης* [Ver97]. Η αρχιτεκτονική αυτή δεν συνιστά μεγάλη πολυπλοκότητα, καθώς τα κλειδιά μακράς διαρκείας ανακτώνται μόνον όταν ανιχνευτεί επίθεση *διπλής κρυπτογράφησης* στο σύστημα.

Πέραν των προσπαθειών για εγκαθίδρυση μιας υποδομής δημόσιου κλειδιού στα συστήματα ηλεκτρονικών επικοινωνιών, η μελλοντική έρευνα στο χώρο της ανάκτησης κλειδιού αναμένεται να στραφεί:

- Στην εύρεση κρυπτογραφικών αλγορίθμων αποκλειστικών για τη δημιουργία ψηφιακών υπογραφών, ώστε τα συστήματα ανάκτησης κλειδιών να αφορούν αποκλειστικά και μόνο κλειδιά κρυπτογράφησης.

- Στην αντιμετώπιση των γενικευμένων επιθέσεων διπλής κρυπτογράφησης, όπου ο αποστολέας κρυπτογραφεί πρώτα το μήνυμα με ένα μη ελεγχόμενο σύστημα κρυπτογράφησης, και στη συνέχεια με τον κρυπτογραφικό αλγόριθμο του συστήματος ανάκτησης κλειδιού.

- Στην εύρεση αλγορίθμων για την αντιμετώπιση επιθέσεων που βασίζονται σε στεγανογραφικές μεθόδους.

Παράρτημα Β - Ορθότητα Ανανέωσης Δημόσιου Κλειδιού (περίοδος t) στην Ανάκτηση Κλειδιού με Ισχυρή Χρονική Ασφάλεια

Έστω

$L = \{(p,q,r,g,g^a,h^b,h^c,z) \mid p,q,r$ πρώτοι αριθμοί, όπου $p = 2q+1$, $q = 2r+1$, g γεννήτορας του Z_p^*, h γεννήτορας του Z_q^*, $a \in Z_q^*$, $b,c \in Z_r^*$, και $z \in Z_p^*$ με $z = g^{a(h^{bc})} \bmod p\}$.

Μία Αλληλεπιδραστική Απόδειξη Μηδενικής Γνώσης για τη Συμμετοχή στην Ομάδα L

Είσοδος: $x = (p,q,r,g,g^a,h^b,h^c,z)$. **Επανάλαβε** ℓ **φορές** ($\ell = \Theta(\log p)$):

1. Ο Αποδεικνύων επιλέγει $k \in_R Z_q^*$, $t \in_R Z_r^*$, υπολογίζει $u = ka \bmod q$, $v = c + t \bmod r$, και στέλνει στον Επαληθευτή:

$$X = g^{uh^{bv}}, \quad Y = g^u, \quad Z = h^v.$$

2. Ο Επαληθευτής στέλνει στον Αποδεικνύοντα ένα ψηφίο ερώτησης $e \in \{0,1\}$.

3. Ο Αποδεικνύων στέλνει στον Επαληθευτή:

(u,v), εάν $e = 0$.

(k,t), εάν $e = 1$.

Επαλήθευση: Ο Επαληθευτής ελέγχει εάν:

$$\text{όταν } e=0,\quad X=g^{u(h^b)^v},\quad Y=g^u,\quad Z=h^v$$

$$\text{όταν } e=1,\quad X=z^{k(h^b)^t},\quad Y=(g^a)^k,\quad Z=h^c h^t.$$

Ο Επαληθευτής αποδέχεται ότι $x\in L$ εάν η επαλήθευση ικανοποιείται σε σύνολο ℓ επαναλήψεων.

Απόδειξη Ορθότητας

Πληρότητα (Completeness): Εάν $x\in L$ τότε ο Επαληθευτής πάντοτε θα αποδέχεται την απόδειξη ως αληθή.

Ανθεκτικότητα (Soundness): Εάν ο Επαληθευτής αποδέχεται με μη αμελητέα πιθανότητα $(\geq 1/poly(\log p))$, τότε ο Αποδεικνύων πρέπει να απαντά σωστά τόσο στην περίπτωση όπου $e=0$, όσο και για $e=1$, για κάποια τριάδα X,Y,Z. Συνεπώς:

$$Z=h^v=h^c h^t \;\Rightarrow\; v=c+t \bmod r$$

$$Y=g^u=(g^a)^k \;\Rightarrow\; u=ka \bmod q$$

$$X=g^{u(h^b)^v}=g^{ka(h^b)^{(c+t)}}=z^{k(h^b)^t} \;\Rightarrow\; z=g^{ah^{bc}}.$$

Συνεπάγεται ότι $x\in L$.

Προσομοίωση (μηδενική γνώση):

Όταν $e=0$, επίλεξε τυχαία u,v και κατασκεύασε X,Y,Z όπως στο βήμα 1.

Όταν $e=1$, επίλεξε τυχαία k,t και κατασκεύασε $X=z^{k(h^b)^t}$, $Y=(g^a)^k$, και

$$Z=h^c h^t.$$

Κεφάλαιο 6

Συμπεράσματα της Διατριβής

Στη σημερινή εποχή όπου η καθολικότητα του Διαδικτύου είναι αδιαμφισβήτητη, πολλές από τις δραστηριότητες που έως σήμερα διενεργούνταν με φυσικό τρόπο αποκτούν ηλεκτρονική μορφή. Η μετάβαση αυτή έχει ως στόχο την εύκολη πρόσβαση των χρηστών σε υπηρεσίες και αγαθά, στα πλαίσια ενός πολυμεσικού περιβάλλοντος όπως το Web. Η συνεχής εξέλιξη τεχνολογιών και προτύπων για την αύξηση του ρυθμού διαμεταγωγής δεδομένων (ATM over IP, IPv6) καθώς και η υιοθέτηση εναλλακτικών τρόπων διασύνδεσης (ασύρματη δικτύωση, κινητή τηλεφωνία τρίτης γενιάς), καθιστούν το Διαδίκτυο ως το πλέον ελκυστικό περιβάλλον για την παροχή υπηρεσιών, τη διεξαγωγή συναλλαγών, καθώς και εν γένει τη συμμετοχή των πολιτών στην κοινωνία της πληροφορίας.

Η βιωσιμότητα των ηλεκτρονικών δικτυακών εφαρμογών εξαρτάται καταρχάς από παράγοντες όπως *πρακτικότητα* και *ευκολία υλοποίησης*. Ωστόσο, ο πλέον σημαντικός παράγοντας για την αποδοχή ενός ηλεκτρονικού συστήματος είναι η *ασφάλεια* του περιβάλλοντος στο οποίο εκτελείται. Ο επιστημονικός κλάδος της «ασφάλειας των πληροφοριών» ασχολείται, εκτός των άλλων, με την ασφαλή υλοποίηση ηλεκτρονικών συστημάτων που διενεργούνται μέσω του Διαδικτύου. Προς την κατεύθυνση αυτή, ο κλάδος της *κρυπτογραφίας* συνεισφέρει στην παροχή υπηρεσιών ασφάλειας όπως αυθεντικότητα, εμπιστευτικότητα, ακεραιότητα. Στα πλαίσια αυτά η παρούσα Διδακτορική Διατριβή πραγματεύτηκε ζητήματα που σχετίζονται με ιδιαίτερα σημαντικές και επίκαιρες εφαρμογές όπως *ηλεκτρονικές εκλογές, ηλεκτρονικές δημοπρασίες, συστήματα αναμετάδοσης κρυπτογραφημένου υλικού*, και *συστήματα ανάκτησης κλειδιού*. Οι εφαρμογές αυτές εμπίπτουν, στο μοντέλο *ηλεκτρονικών συστημάτων συναλλαγών* που περιγράψαμε στο Κεφάλαιο 1.

Οι στόχοι και τα προαπαιτούμενα των χρηστών και των τρίτων οντοτήτων που εμπλέκονται σε ηλεκτρονικά συστήματα συναλλαγών είναι ενίοτε αντίθετα: οι χρήστες επιθυμούν να διασφαλίσουν την ιδιωτικότητα των επιλογών τους, ενώ η «κοινωνία» (χρήστες, τρίτες οντότητες, εξωτερικοί παρατηρητές, άλλες οντότητες με έννομο συμφέρον) αποσκοπεί στην εξασφάλιση της ορθότητας και ακρίβειας των αποτελεσμάτων, καθώς και της διαθεσιμότητας του συστήματος. Στην παρούσα Διατριβή θεωρήσαμε ότι τόσο οι τρίτες οντότητες όσο και οι χρήστες ενδέχεται να συμπεριφερθούν κακόβουλα. Έτσι, οι χρήστες ενδέχεται να καταχραστούν την ιδιωτικότητα που τους παρέχεται και να συμβάλουν στην δυσλειτουργία του συστήματος, ενώ οι τρίτες οντότητες να καταχραστούν την εξουσία που τους δίνεται για να παραβιάσουν την ιδιωτικότητα των χρηστών.

Το αντικείμενο της Διδακτορικής Διατριβής ήταν η αναζήτηση κρυπτογραφικών μηχανισμών για την εκπλήρωση, στα ηλεκτρονικά συστήματα συναλλαγών, απαιτήσεων ασφαλείας όπως:

- **Αυθεντικοποίηση** (authentication), στην οποία υπάγονται οι επιμέρους απαιτήσεις του *καταλογισμού ευθύνης* (non-repudiation) και της ασφαλούς *ταυτοποίησης* (identification) των χρηστών του συστήματος.

- **Ιδιωτικότητα** (privacy), στην οποία υπάγονται οι επιμέρους απαιτήσεις της ανωνυμίας (anonymity) και της μυστικότητας (secrecy) των επιλογών των χρηστών.

- **Προστασία από Καταναγκασμό** (uncoercibility), στην οποία περιλαμβάνονται οι απαιτήσεις τόσο για προστασία του χρήστη από *εξωτερικό καταναγκασμό* (external coercion), όσο και από επιθέσεις *αυτό-καταναγκασμού* (self-coercing), όπου ο χρήστης παραβιάζει την ιδιωτικότητα του για ίδιον όφελος (π.χ. πώληση προσφοράς). Γενικά, η απαίτηση για προστασία από καταναγκασμό μπορεί να θεωρηθεί ότι υπάγεται στην απαίτηση για ιδιωτικότητα, ωστόσο στην παρούσα

Διατριβή αξιολογήθηκε ξεχωριστά, λόγω του ιδιαίτερου ενδιαφέροντος που παρουσιάζει σε εφαρμογές συστημάτων ηλεκτρονικών συναλλαγών (π.χ. συστήματα ηλεκτρονικής ψηφοφορίας, ηλεκτρονικές δημοπρασίες), αλλά και γενικότερα στο ηλεκτρονικό εμπόριο [Bur_Mag02a] (Κεφάλαιο 1).

- **Επαληθευσιμότητα** (verifiability), στην οποία υπάγονται τόσο η *ατομική* (atomic) όσο και η *οικουμενική* (universal) επαληθευσιμότητα.

- **Ανθεκτικότητα** (robustness) του συστήματος παρά την δυσλειτουργία, τυχαία ή σκόπιμη, κάποιας ή κάποιων οντοτήτων που λαμβάνουν μέρος στο σύστημα, είτε αυτές οι οντότητες είναι χρήστες είτε Αρχές του συστήματος.

Στην προσπάθεια αυτή δόθηκε έμφαση στο σχεδιασμό «*δίκαιων*» (equitable) συστημάτων, δηλαδή συστημάτων στα οποία διατηρείται μια ισορροπία μεταξύ της ανάγκης των χρηστών για ιδιωτικότητα και της ανάγκης της «κοινωνίας» για ακρίβεια και ορθότητα των αποτελεσμάτων.

Συστήματα Ηλεκτρονικής Ψηφοφορίας

Η αποτροπή επιθέσεων *καταναγκασμού* στις ηλεκτρονικές εκλογές αποτέλεσε σημαντικό κομμάτι της έρευνας μας για ασφαλή συστήματα ηλεκτρονικής ψηφοφορίας μέσω Διαδικτύου. 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 [Mag01].

Αναλύσαμε το πρόβλημα της *απόσυρσης ψήφου* στις ηλεκτρονικές εκλογές κεντρικής διαχείρισης που βασίζονται 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 όσων ψηφοφόρων αποφασίζουν να απόσχουν. Προτείναμε «Δίκαιες» 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 ψηφοφόρους [Mag02].

Όταν τα συστήματα ηλεκτρονικής ψηφοφορίας μέσω Διαδικτύου εκπληρώσουν τις εύλογες απαιτήσεις ασφάλειας και πρακτικότητας, αναμένεται να υιοθετηθούν και να υλοποιηθούν σε εκλογές μεγάλης κλίμακας. Προς αυτήν την κατεύθυνση, αναμένονται προσπάθειες σε ερευνητικό επίπεδο για την εύρεση κρυπτογραφικών αλγορίθμων δημοσίου κλειδιού με εγγενή προστασία από καταναγκασμό, αλλά και την ασφαλή ταυτοποίηση των ψηφοφόρων με βιομετρικές τεχνικές. Παράλληλα, η χρήση φορητών συσκευών με δυνατότητες εκτέλεσης κρυπτογραφικών πράξεων, αλλά και η αξιοποίηση εναλλακτικών συστημάτων-πελατών (π.χ. ATM, κινητά τηλέφωνα) αναμένεται να δώσουν έμφαση στο σχεδιασμό τεχνολογικώς ουδέτερων συστημάτων, με χαμηλή πολυπλοκότητα και υψηλή επεκτασιμότητα.

Ηλεκτρονικές Δημοπρασίες

Παρουσιάσαμε ένα «Δίκαιο» κρυπτογραφικό πρωτόκολλο για Κλειστές ηλεκτρονικές Δημοπρασίες στο Διαδίκτυο, χωρίς τη χρήση έμπιστων τρίτων οντοτήτων: το πρωτόκολλο προσφέρει ανωνυμία και μυστικότητα για όλους τους χρήστες, χωρίς όμως να επιτρέπει την *απόσυρση μιας προσφοράς*. Οι χρήστες χρησιμοποιούν ψευδώνυμα μιας χρήσης και οι προσφορές τους συνδέονται μοναδικά με την αληθινή τους ταυτότητα μέσω ενός Γρίφου Συγκεκριμένου Χρόνου Επίλυσης που υποβάλλουν στο Δημοπράτη, και ο

οποίος απαιτεί συγκεκριμένο χρόνο επίλυσης [Mag00]. Θέτουμε, ως στόχο την επέκταση του πρωτοκόλλου ώστε να υποστηρίζει Ανοικτές Δημοπρασίες καθώς και Διπλές Δημοπρασίες όπου συμμετέχουν περισσότεροι του ενός πωλητές και αγοραστές.

Επίσης εισαγάγαμε την έννοια της *προστασίας από καταναγκασμό* στις ηλεκτρονικές δημοπρασίες, ως μέσο για την καταπολέμηση των Δακτυλίων, δηλαδή συμπαιγνιών μεταξύ υποψήφιων αγοραστών που προσπαθούν να πετύχουν με αθέμιτα μέσα την πτώση της τιμής πώλησης του αγαθού που δημοπρατείται. Προτείναμε ένα ασφαλές κρυπτογραφικό πρωτόκολλο Κλειστών ηλεκτρονικών Δημοπρασιών στο οποίο επιτυγχάνεται προστασία από καταναγκασμό για τους χρήστες καθώς και οικουμενική επαληθευσιμότητα για τα τελικά αποτελέσματα της δημοπρασίας [Bur_Mag02a].

Οι ηλεκτρονικές δημοπρασίες παρέχουν σημαντικά επιχειρησιακά πλεονεκτήματα στον πωλητή αλλά και υπηρεσίες στον υποψήφιο αγοραστή. Η διείσδυση τους στο ηλεκτρονικό εμπόριο καθιστά σημαντική την σχεδίαση μηχανισμών ασφάλειας για τη διασφάλιση των συναλλαγών που πραγματοποιούνται. Στο μέλλον, αναμένεται να δοθεί έμφαση στο σχεδιασμό ασφαλών συστημάτων με ιδιαίτερα χαμηλή πολυπλοκότητα, για δημοπρασίες αγαθών μικρής αξίας, καθώς και στην κατασκευή μοντέλων ασφάλειας υλοποιήσιμων σε κάθε τύπο δημοπρασίας (Ανοικτές ή Κλειστές δημοπρασίες, Απλές ή Διπλές δημοπρασίες).

Συστήματα Αναμετάδοσης Κρυπτογραφημένου Υλικού

Στην παρούσα Διατριβή ασχοληθήκαμε με συστήματα *ανίχνευσης «προδοτών»*, δηλαδή με συστήματα που ανιχνεύουν όσους αναδιανέμουν σε τρίτους τα κλειδιά που απέκτησαν νόμιμα στα πλαίσια μιας εφαρμογής αναμετάδοσης κρυπτογραφημένης πληροφορίας. Η εφαρμογή αυτή μπορεί να είναι μετάδοση εικόνας συνδρομητικής τηλεόρασης, παροχή ηλεκτρονικών

υπηρεσιών σε πραγματικό χρόνο μέσω Web, διανομή CD-ROM με εμπορικό software, κ.λ.π. Στο πλαίσιο αυτό, παρουσιάσαμε ένα ασύμμετρο σχήμα ανίχνευσης «προδοτών» χωρίς τρίτη έμπιστη οντότητα [Mag01_1]. Για αυτόν το λόγο, τροποποιήσαμε το στάδιο της εκχώρησης κλειδιών ενός πρακτικού και ασφαλούς συμμετρικού σχήματος [Kur98,Kur00] ώστε ο παροχέας του υλικού να μη γνωρίζει το αποτύπωμα που αποδίδεται σε έναν εξουσιοδοτημένο χρήστη του συστήματος. Εάν ένας ή περισσότεροι «προδότες» συνδυάσουν τα αποτυπώματα τους και κατασκευάσουν έναν «πειρατικό» αποκωδικοποιητή, τότε ο αποκωδικοποιητής θα περιέχει πληροφορίες που οδηγούν στην ταυτότητα τουλάχιστον ενός εκ των «προδοτών». Περιγράψαμε επίσης τρόπους με τους οποίους οι χρήστες μπορούν να εξασφαλίσουν ότι τα κλειδιά που τοποθετούνται από τον παροχέα στην είσοδο του αλγορίθμου εκχώρησης είναι διαφορετικά μεταξύ τους, αλλά και ότι δεν πρόκειται να εκχωρηθούν σε κάποιον άλλον εξουσιοδοτημένο χρήστη. Ως στόχο θέτουμε την επέκταση του πρωτοκόλλου ώστε να προσφέρει ανωνυμία στους εξουσιοδοτημένους χρήστες του συστήματος.

Η μελλοντική έρευνα στο χώρο της προστασίας των πνευματικών δικαιωμάτων για ηλεκτρονικά αγαθά, αναμένεται να στραφεί στην εύρεση μηχανισμών ανεξάρτητων της εφαρμογής ή του αγαθού που προφυλάσσεται, οι οποίοι θα βασίζονται σε λύσεις ασφαλούς υλικού (hardware) χαμηλού επιπέδου και θα υποστηρίζονται και σε επίπεδο λειτουργικού συστήματος. Οι μηχανισμοί αυτοί θα στοχεύουν στην αποτροπή, και όχι απλά αποθάρρυνση, της αντιγραφής και της αναδιανομής ψηφιακών αγαθών. Παράλληλα, αναμένεται να συνεχιστεί η έρευνα για την αναζήτηση ασφαλών στεγανογραφικών μεθόδων εισαγωγής υδατογραφημάτων σε αρχεία πολυμέσων.

Συστήματα Ανάκτησης Κλειδιού

Τα συστήματα ανάκτησης κλειδιού εμπίπτουν στην κατηγορία των συστημάτων διαχείρισης κλειδιού και επιτρέπουν την πρόσβαση σε αποκρυπτογραφημένο υλικό, υπό ορισμένες προϋποθέσεις, όπως επιβολή του νόμου, απώλεια κλειδιών πρόσβασης σε αρχειοθετημένα δεδομένα, ανάκτηση συνομιλιών ή κρυπτογραφημένων αρχείων στο περιβάλλον των επιχειρήσεων κ.λ.π.

Ορίσαμε την έννοια της *ισχυρής χρονικής ασφάλειας* που επεκτείνει την έννοια της χρονικής ασφάλειας για την προστασία κρυπτογραφικών κλειδιών στα συστήματα ανάκτησης κλειδιού [Bur_Mag01]. Έτσι, σε ένα σύστημα με ισχυρή χρονική ασφάλεια, η Αρχή Επιβολής Νόμου (Law Enforcement Agency) μπορεί να αποκρυπτογραφήσει τις κρυπτογραφημένες συνομιλίες ενός χρήστη που αφορούν μία περίοδο t, χωρίς να είναι δυνατή η πρόσβαση σε συνομιλίες που αφορούν προγενέστερες ή μεταγενέστερες περιόδους. Θεωρούμε πως ένα «Δίκαιο» σύστημα ανάκτησης κλειδιού πρέπει να παρέχει την επιπλέον αυτή προστασία.

Τα συστήματα ανάκτησης κλειδιού είναι ευάλωτα σε επιθέσεις *διπλής κρυπτογράφησης*. Η υπόθεση ύπαρξης μιας καλά ορισμένης Υποδομής Δημόσιου Κλειδιού αποτέλεσε την αφετηρία στην κατασκευή ενός *υβριδικού* μοντέλου για την αντιμετώπιση επιθέσεων διπλής κρυπτογράφησης [Pfi97_1] στο περιβάλλον των επιχειρήσεων. Το μοντέλο προβλέπει την υποθήκευση κλειδιών μακράς διαρκείας, αλλά και την χρήση τεχνικών *εικονικής διευθυνσιοδότησης* για την ανάκτηση των κλειδιών συνόδου των χρηστών [Mag03]. Η αρχιτεκτονική του μοντέλου δεν συνιστά μεγάλη πολυπλοκότητα, καθώς τα κλειδιά μακράς διαρκείας ανακτώνται μόνον όταν ανιχνευτεί επίθεση διπλής κρυπτογράφησης στο σύστημα.

Προϋπόθεση για όλα τα συστήματα ανάκτησης κλειδιού αποτελεί η εγκαθίδρυση μιας καλά ορισμένης Υποδομής Δημοσίου Κλειδιού. Μια τέτοια υποδομή με εγγενή υποστήριξη ανάκτησης κλειδιού θα έχει ως αποτέλεσμα οι επιτιθέμενοι που παρακάμπτουν την υποδομή να έχουν σημαντικές δυσκολίες

στη διανομή των κλειδιών τους [Mic92]. Εξάλλου, η έρευνα στο χώρο της ανάκτησης κλειδιού αναμένεται να στραφεί στην εύρεση κρυπτογραφικών αλγορίθμων αποκλειστικών για τη δημιουργία ψηφιακών υπογραφών, ώστε τα συστήματα ανάκτησης κλειδιών να αφορούν αποκλειστικά και μόνο κλειδιά κρυπτογράφησης, καθώς και στην εύρεση αλγορίθμων για την αντιμετώπιση επιθέσεων που βασίζονται σε στεγανογραφικές μεθόδους.

Βιβλιογραφικές Αναφορές

[Abe98] Abe, M: Universally Verifiable Mix-net with Verification Work Independent of the Number of Mix-servers. In: Advances in Cryptology - EUROCRYPT '98, Lecture Notes in Computer Sciences, Vol. 1403, Springer-Verlag, pp. 437-447, 1998.

[Abel98] Abelson, H. et al: The Risks of Key Recovery, Key Escrow, Trusted Third Party & Encryption. In: Digital Issues, No. 3, pp. 1-18, 1998.

[Adl00] Adler, J., Dai, W., Green, R., and Neff, A.: Computational Details of the VoteHere Homomorphic Election System. November 2000, at: http://www.votehere.net/ada_compliant

[Alp98] Alpert, D., Ellard, D., Kavazovic, O., and Scheff, M.: Receipt-free Secure Elections 6.857 Final Project. 6.857 Network and Computer Security, 1998, at: http://www.eecs.harvard.edu/~ellard/6.857/final.ps

[And01] Andersson, R.: Security Engineering, a Guide to Building Dependable Distributed Systems. John Wiley and Sons, 2001.

[And96] Anderson, R., and Kuhn, M.: Tamper Resistance – A Cautionary Note. In: Proceedings of Usenix Electronic Commerce Workshop, Usenix Press, pp. 1-11, 1996.

[And98] Anderson, R., and Peticolas, F.: On the Limits of Steganography. In: IEEE Journal of Selected Areas in Communications, Special Issue on Copyright & Privacy Protection, Vol. 16(4), pp. 474-481, 1998.

[And97] Anderson, R., and Roe, M.: The GCHQ Protocol and Its Problems. In: Advances in Cryptology - EUROCRYPT '97, Lecture Notes in Computer Sciences, Vol. 1233, Springer-Verlag, pp. 134-148, 1997.

[Aso98] Asokan, N., Shoup, V., and Waidner, M.: Asynchronous Protocols for Optimistic Fair Exchange. In: Proceedings of 1998 IEEE Symposium on Security and Privacy, IEEE CS Press, pp. 86-99, 1998.

[Auc02] www.auctioninsider.com/every.html (Λίστα με περίπου 300 Ηλεκτρονικούς Οίκους Δημοπρασιών).

[Bau01] Baudron, O., Fouque, P., Pointcheval, D., Poupard, G., and Stern, J.: Practical Multi-Candidate Election System. In: Proceedings of the 20th ACM Symposium on Principles of Distributed Computing, ACM Press, pp. 274-283, 2001.

[Bel89] Bellare, M., and Micali, S.: Non-Interactive Oblivious Transfer and Applications. In: Advances in Cryptology – CRYPTO '89, Lecture Notes in Computer Sciences, Vol. 435, Springer-Verlag, pp. 544-557, 1990.

[Bel93] Bellare, M., and Rogaway, P.: Random Oracles are Practical. In: Proceedings of the 1st Annual Conference on Computer and Communications Security, ACM Press, pp. 154-164, 1993.

[Bel96] Bellare, M., and Goldwasser, S.: Encapsulated Key-Escrow. MIT Laboratory for Computer Science, Report No. 688, April 1996, at: http://www.cse.ucsd.edu/users/mihir

[Bel97] Bellare, M., and Goldwasser, S.: Verfiable Partial Key Escrow. In: Proceedings of the 4th ACM Conference on Computer and Communications Security, ACM Press, pp. 78-91, 1997.

[Bel99] Bellare, M., and Miner, S.: A Forward-Secure Digital Signature Scheme. In: Advances in Cryptology – CRYPTO '99 Lecture Notes in Computer Sciences, Vol. 1666, Springer-Verlag, pp. 197-207, 1999.

[Ben87] Benaloh, J.: Verifiable Secret-Ballot Elections. PhD Thesis, Yale University, 1987.

[Ben88] Ben-Or, M., Goldwasser, S., and Wigderson, A.: Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computing. In: Proceedings of the 20th Annual ACM Symposium on Theory of Computing, ACM Press, pp. 1-10, 1998.

[Ben94] Benaloh, J., and Tuinstra, D.: Receipt-Free Secret-Ballot Elections. In: Proceedings of the 26th Annual ACM Symposium on Theory of Computing, ACM Press, pp. 544-553, 1994.

[Bie97] Biehl, I., and Meyer, B.: Protocols for Collusion – Secure Asymmetric Fingerprinting. In: Proceedings of the 14th Symposium on Theoretical Aspects of Coputer Sciences - STACS '97, pp. 399-412, 1997.

[Bih97] Biham, E., and Shamir, A.: Differential Fault Analysis of Secret Key Cryptosystems. In: Advances in Cryptology – CRYPTO '97, Lecture Notes in Computer Sciences, Vol. 1294, Springer-Verlag, pp. 513-525, 1997.

[Blaz94] Blaze, M.: Protocol Failure in the Escrowed Encryption Standard. In: Proceedings of the 2nd ACM Conference on Computer and Communications Security, ACM Press, pp. 59-67, 1994.

[Bon97] Boneh, D., Demillo, R., and Lipton, R.: On the Importance of Checking Computations. In: Advances in Cryptology - EUROCRYPT '97, Lecture Notes in Computer Sciences, Vol. 1233, Springer-Verlag, pp. 37-51, 1997.

[Bon99] Boneh, D., and Franklin, M.: An Efficient Public Key Traitor Tracing Scheme. In: Advances in Cryptology - EUROCRYPT '99, Lecture Notes in Computer Sciences, Vol. 1666, Springer-Verlag, pp. 338-353, 1999.

[Bon00] Boneh, D., and Naor, M.: Timed Commitments. In: Advances in Cryptology - CRYPTO '2000, Lecture Notes in Computer Sciences, Vol. 1880, Springer-Verlag, pp. 236-254, 2000.

[Bon95] Boneh, D., and Shaw, J.: Collusion Secure Fingerprinting For Digital Data. In: Advances in Cryptology - CRYPTO '95, Lecture Notes in Computer Sciences, Vol. 963, Springer-Verlag, pp. 452-465, 1995.

[Bra87] Brassard, G., Crepeau, C., and Robert, J.: All-or-Nothing Disclosure of Secrets. In: Advances in Cryptology - CRYPTO '86, Lecture Notes in Computer Sciences, Vol. 263, Springer-Verlag, pp. 234-238, 1995.

[Bur_Mag01] Burmester, M., Chrissikopoulos, V., Kotzanikolaou, P., and Magkos, E.: Strong Forward Security. In: Proceedings of the International Information Security Conference IFIP-SEC '01, Kluwer Academic Publishers, pp. 109-119, 2001.

[Bur_Mag02a] Burmester, M., Magkos, E., and Chrissikopoulos, V.: Uncoercible e-bidding Games. In: Electronic Commerce Research Journal, Special Issue on Security Aspects in E-Commerce, Kluwer Academic Publishers. To be published, 2002.

[Bur_Mag02b] Burmester, M., and Magkos, E.: Towards Secure and Practical e-Elections in the New Era. In: Secure Electronic Voting, Kluwer Academic Publishers. To be published, 2002.

[Bur98] Burmester, M., Desmedt, Y., and Seberry, J.: Equitable Key Escrow with Limited Time Span (or How to Enforce Time Expiration Cryptographically). In: Advances in Cryptology - ASIACRYPT '98, Lecture Notes in Computer Sciences, Vol. 1514, Springer-Verlag, pp. 380-391, 1998.

[Cac99] Cachin, C.: Efficient Private Bidding and Auctions with an Oblivious Third Party. In: Proceedings of the 6th ACM Conference in Computer and Communications Security, ACM Press, pp. 120-127, 1999.

[Cal00] California Internet Voting Task Force: A Report on the Feasibility of Internet Voting, Jan 2000, at: http://www.ss.ca.gov/executive/ivote/

[Cal01] CALTEC/MIT: Voting Technology Project, 2001, at: http://www.vote.caltech.edu/reports/index.html

[Cam96] Camp, J., Harkavy, M., Tygar, K., and Yee, B.: Anonymous Atomic Transactions. In: Proceedings of the 2nd USENIX Workshop on Electronic Commerce, USENIX Press, pp. 123-133, 1996.

[Can97] Canetti, R., Dwork, C., Naor, M., and Ostrovsky, R.: Deniable Encryption.' In: Advances in Cryptology - CRYPTO '97, Lecture Notes in Computer Sciences, Vol. 1294, Springer-Verlag, pp. 90-104, 1997.

[Can96] Canetti, R. and Gennaro, R.: Uncoercible Multiparty Computation. In: Proceedings of the 37th IEEE Symposium on the Foundations of Computer Science – FOCS '96, IEEE Press, pp. 462-471, 1996.

[Cer02] Certmail: The Certified Electronic Mail System, at: http://www.certifiedmail.com

[Cha82] Chaum, D.: Blind Signatures for Untraceable Payments. In: CRYPTO '82, Plenum Press, pp. 199-203, 1982.

[Cha85] Chaum, D.: Security Without Identification: Transaction Systems to Make Big Brother Obsolete. In: Communications of the ACM, Vol. 28(10), pp. 1030-1044, 1985.

[Cha88_1] Chaum, D.: The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. In: Journal of Cryptology, Vol. 1(1), pp. 65-75, 1988.

[Cha81] Chaum, D.: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. In: Communications of the ACM, Vol. 24(2), pp. 84-88, 1981.

[Cha87] Chaum, D., Damgard, I., and Graaf, J.: Multiparty Computations Ensuring Privacy of Each Party's Input and Correctness of the Result. In: Advances in Cryptology - CRYPTO '87, Lecture Notes in Computer Sciences, Vol. 293, Springer-Verlag, pp. 87-119, 1988.

[Cha88] Chaum, D., Fiat, A., and Naor, M.: Untraceable Electronic Cash. In: Advances in Cryptology – CRYPTO '88, Lecture Notes in Computer Science, Vol. 1440, Springer-Verlag, pp. 319-327, 1988.

[Cha92] Chaum, D. and Pedersen, T.: Wallet Databases with Observers. In: Advances in Cryptology - Crypto '92, Lecture Notes in Computer Sciences, Vol. 740, Springer-Verlag, pp. 89-105, 1993.

[Cho94] Chor, B., Fiat, A., and Naor, M.: Tracing Traitors. Advances in Cryptology - CRYPTO '94, Lecture Notes in Computer Science, Vol. 293, Springer-Verlag, pp. 257-270, 1994.

[Chu00] Chui, K., and Zwick, R.: Auctions on the Internet – A preliminary study. Manuscript, 2000, at: http://home.ust.hk/~mkzwick/Internet_Auction.html

[Coc97] Cocks, K.: Split Knowledge Generation of RSA Parameters. In: Proceedings of the 6th IMA Conference on Cryptography and Coding, Springer-Verlag, pp. 89-95, 1997.

[Coh85] Cohen, J., and Fisher, M.: A Robust and Verifiable Cryptographically Secure Election Scheme. In: Proceedings of the 26th IEEE Symposium on Foundations of Computer Science, IEEE Computer Society, pp. 372-382, 1985.

[Col02] Coleman, S.: Elections in the 21st Century: From Paper Ballot to E-Voting. Report by the Independent Commission on Alternative Voting Methods, London, Electoral Reform Society, February 2002.

[Com02] Community ConneXion, Inc., at: http://www.anonymizer.com

[Cot02] Cottrell, L.: Mixmaster and Remailer Attacks, 1999, at: http://obscura.obscura.com/~loki/remailer/remailer-essay.html

[Cra96] Cramer, R., Franklin, M., Schoenmakers, B., and Yung, M. : Multi-Authority Secret Ballot with Linear Work. In: Advances in Cryptology – EUROCRYPT '96, Lecture Notes in Computer Science, Vol. 1070, Springer-Verlag, pp. 72-83, 1996.

[Cra97] Cramer, R., Gennaro, R., and Schoenmakers, B.: A Secure and Optimally Efficient Multi-Authority Election Scheme. In: Advances in Cryptology - EUROCRYPT '97, Lecture Notes in Computer Science, Vol. 1233, Springer-Verlag, pp. 103-118, 1997.

[Cra97_1] Cramer, R., and Shoup, V.: A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attacks. In: Advances in Cryptology - Crypto '98, Lecture Notes in Computer Science, Vol. 1462, Springer-Verlag, pp. 1-18, 1997.

[Cramp98] Crampton, P.: Ascending Auctions. In : European Economic Review, Vol. 42, pp. 745-756, 1998.

[Cramp98_1] Crampton P., and Ausubel L.M.: Demand Reduction and Inefficiency in Multi-Unit Auctions. Working Paper, University of Maryland, 1998, at: www.cramton.umd.edu/papers1995-1999/98wp-demand-reduction.pdf

[Cramp97] Crampton P., Cameron L.J., and Wilson R.: Using Auctions to Divest Generation Assets. In: Electricity Journal, Vol. 10(10), pp. 22-31, 1997.

[Cran97] Cranor, L., and Cytron, R.: Sensus: A Security-Conscious Electronic Polling System for the Internet. In: Proceedings of the Hawaii International Conference on System Sciences, 1997, at: http://lorrie.cranor.org/pubs/hicss/

[Cry99] Cryptography Research Inc., Differential Power Analysis, 2000, at: http://www.cryptography.com/dpa/index.html

[Dam01] Damgard, I., and Juric, M.: A Generalization, a Simplification and Some Applications of Pallier's Probabilistic Public-Key System. In: Advances in Cryptology - PKC '01, Lecture Notes in Computer Science, Vol. 1992, Springer-Verlag, pp. 119-136, 2001.

[Dav96] Davenport, B., Newberger, A., and Woodard, J.: Creating a Secure Digital Voting Protocol for Campus Elections. Princeton University, 1996, at: http://www.princeton.edu/

[Dav94] Davis, D., Ihaka, R., and Fenstermacher, P..: Cryptographic Randomness from Air Turbulence in Disk Drives. In: Advances in Cryptology – CRYPTO '94, Lecture Notes in Computer Science, Vol. 839, Springer-Verlag, pp. 114-120, 1994.

[Den96] Denning, D., and Branstad, D.: A Taxonomy of Key Escrow Encryption Systems. In: Communications of the ACM, Vol. 39(3), pp. 34-40, 1996.

[Des94] De Santis, A., Desmedt, Y., Frankel, Y., and Yung, M.: How to Share a Function Securely. In: Proceedings of the 25th Annual Symposium on Theory of Computing, ACM Press, pp. 522-533, 1994.

[Desm94] Desmedt, Y.: Threshold Cryptography. In: European Transactions on Telecommunications, Vol. 5(4), pp. 449-457, 1994.

[Des01] Desmedt, Y., Burmester, M., and Seberry, J.: Equitability in Retroactive Data Confiscation Versus Proactive Key Escrow. In: Advances in Cryptology - PKC '01, Lecture Notes in Computer Science, Vol. 1992, Springer-Verlag, pp. 277-286, 2001.

[Desm89] Desmedt, Y., and Frankel, Y.: Threshold Cryptosystems. In: Advances in Cryptology - CRYPTO '89, Lecture Notes in Computer Science, Vol. 435, Springer-Verlag, pp. 307-315, 1989.

[Dic00] Dictson, D., and Ray, D.: The Modern Democratic Revolution: An Objective Survey of Internet-based Elections. White Paper, January 2000, at: www.securepoll.com

[Dif76] Diffie, W., and Hellman, M.: New Directions in Cryptography. In: IEEE Transactions on Information Theory, Vol. 22(6), pp. 644-654, 1976.

[Dom98] Domingo-Ferrer, J.: Anonymous Fingerprinting of Electronic Information with Automatic Identification of Redistributors. In: IEE Electronic Letters, Vol. 34(13), pp. 1303-1304, 1998.

[Dom99] Domingo-Ferrer, J.: Anonymous Fingerprinting Based on Committed Oblivious Transfer. In: Proceedings of PKC '99, Lecture Notes in Computer Science, Vol. 1560, Springer-Verlag, pp. 43-52, 1999.

[Dtl02] DTLR News Release: May Elections to Trial Online Voting, 2002, at: http://www.press.dtlr.gov.uk/pns/DisplayPN.cgi?pi_id=2002_0033

[Dur99] Durette, B. W.: Multiple Administrators for Electronic Voting. Bachelor's Thesis, Massachusetts Institute of Technology, May 1999.

[ElG85] ElGamal, T.: A Public-key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. In: IEEE Transactions on Information Theory, Vol. 31(4), pp. 469-472, 1985.

[Ell99] Elliot, D.: Examining Internet Voting in Washington. White paper, 1999, at: http://www.electioncenter.org/voting/InetVotingWhitePaper.html

[Eve85] Even, S., Goldreich, O., and Lempel, A.: A Randomized Protocol for Signing Contracts. In: Communications of the ACM, Vol. 28, pp. 637-647, 1985.

[Fed00] Federal Voting Assistance Program: Voting Over the Internet Project. 2000, at: www.fvap.ncr.gov/voireport.pdf

[Fia93] Fiat, A., and Naor, M.: Broadcast Encryption. In: Advances in Cryptology - CRYPTO '93, Lecture Notes in Computer Science, Vol. 773, Springer-Verlag, pp. 480-491, 1993.

[Fia86] Fiat, A., and Shamir, A.: How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In: Advances in Cryptology – CRYPTO '86, Lecture Notes in Computer Science, Vol. 263, Springer-Verlag, pp. pp. 186-194, 1986.

[Fia99] Fiat, A., and Tassa, T.: Dynamic Traitor Tracing. In: Advances in Cryptology – CRYPTO '99, Lecture Notes in Computer Science, Vol. 1666, Springer-Verlag, pp. 354-371, 1999.

[Fip94] FIPS PUB 185 Escrowed Encryption Standard. US Department of Commerce, February 1994, at: http://www.itl.nist.gov/fipspubs/fip185.htm

[Fou99] Fouque, P., Poupard, G., and Stern, J.: Recovering Keys in Open Networks. In: Proceedings of the Information Theory Workshop '99, IEEE Press, 1999, at: http://guillaume.poupard.free.fr/Publi/ps/FoPoSt99.ps

[Fran96] Frankel, Y., Gemmel, P., and Yung, M.: Witness Based Cryptographic Program Checking and Robust Function Sharing. In: Proceedings of the 28th Annual ACM Symposium on Theory of Computing, ACM Press, pp. 499-508, 1996.

[Fran95] Frankel, Y., and Yung, M.: Escrow Encryption Systems Visited: Attacks, Analysis and Designs. In: Advances in Cryptology - CRYPTO '95, Lecture Notes in Computer Science, Vol. 963, Springer-Verlag, pp. 222-235, 1995.

[Fra96] Franklin, M., and Reiter, M.: The Design and Implementation of a Secure Auction Service. In: IEEE Transactions on Software Engineering, Vol. 22(5), pp. 302-311, 1996.

[Fra00] Franklin, M., and Sander, T.: Commital Deniable Proofs and Electronic Campaign Finance. In: Advances in Cryptology - ASIACRYPT '2000, Lecture Notes in Computer Science, Vol. 1976, Springer-Verlag, pp. 373-387, 2000.

[Fri93] Friedman, D., and Rust, J.: The Double Auction Market Institutions, Theories and Evidence. Addison-Wesley, MA, 1993.

[Fuj93] Fujioka, A., Okamoto, T., and Ohta, K.: A Practical Secret Voting Scheme for Large Scale Elections. In: Proceedings of AUSCRYPT '92, Lecture Notes in Computer Science, Vol. 718, Springer-Verlag, pp. 244-251, 1993.

[Gaf99] Gafni, E., Staddon, J., and Yin, L.: Efficient Methods for Integrating Traceability and Broadcast Encryption. In: Advances in Cryptology – CRYPTO '99, Lecture Notes in Computer Science, Vol. 1666, Springer-Verlag, pp. 372-387, 1999.

[Gen97] Gennaro, R., Karger, P., Matyas, S., Peyravian, M., Roginsky, A., Safford, D., Zollet M., and Zunic, N.: Two-Phase Cryptographic Key Recovery System. In: Computers & Security, Elsevier Sciences Ltd, pp. 481-506, 1997.

[Gol87] Goldreich, O., Micali, S., and Wigderson, A.: How to Play any Mental Game – or – a Completeness Theorem for Protocols with Honest Majority. In: Proceedings of the 19th ACM Symposium on the Theory of Computing – STOC '87, ACM Press, pp. 218-229, 1987.

[Gol91] Goldreich, O., Micali, S., and Widgerson. A.: Proofs that Yield Nothing but their Validity, or All Languages in NP have Zero-Knowledge Proof Systems. In: Journal of the ACM, Vol. 38, pp. 691-729, 1991.

[Gol99] Goldschlag, D., Reed, M., and Syverson, P.: Onion Routing for Anonymous and Private Communications. In: Communications of the ACM, Vol. 42(2), 39-41, 1999.

[Gol85] Goldwasser, S., Micali, S., and Rackoff, C.: The Knowledge Complexity of Interactive Proof Systems. In: Proceedings of the 17th ACM Symposium on the Theory of Computing – STOC '85, ACM Press, pp. 291-304, 1985.

[Gol94] Goldwasser, S. and Micali, S.: Probabilistic Encryption. In: Journal of Computer and System Sciences, Vol. 28, pp. 270-299, 1984.

[Gud01] Gudmundsson, O.: DNSSEC and IPv6 A6 Aware Server/Resolver Message Size Requirements. In: RFC 3226, at: ftp://ftp.isi.edu/in-notes/rfc3226.txt

[Gun89] Gunther, C.: An Identity-based Key Exchange Protocol. In: Advances in Cryptology – EUROCRYPT '89, Lecture Notes in Computer Science, Vol. 434, Springer-Verlag, pp. 29-37, 1989.

[Hac00] Hachez, G., Koeune, F., and Quisquater, J.: Biometrics, Access Control, Smart Cards, a Not so Simple Combination. In: Proceedings of the 4th Working Conference on Smart Card Research and Advanced Applications – CARDIS '00, Kluwer Academic Publishers, pp. 273-288, 2000.

[Har98] Harkavy, M., Kikuchi, H., and Tygar, J.: Electronic Auctions with Private Bids. In: Proceedings of the 3rd USENIX Workshop on Electronic Commerce. USENIX Press, pp. 61-74, 1998.

[Har99] Harkavy, M., Kikuchi, H., and Tygar, J.: Multi-Round Anonymous Auction Protocols. In: Proceedings of the 1st IEEE Workshop on Dependable and Real-Time E-Commerce Systems - DARE '99, IEEE Press, pp. 62-69, 1999.

[He98] He, Q., and Su, Z.: A New Practical Secure e-Voting Scheme. In: Proceedings of the 14th International Information Security Conference - IFIP/SEC '98, Kluwer Academic Publishers, 1998, at: http://tsinghua.ece.cmu.edu/projects/e-voting/e-voting.ps

[Hers97] Herschberg, M.: Secure Electronic Voting Using the World Wide Web. Master's Thesis, MIT, June 1997, at: http://theory.lcs.mit.edu/~cis/theses/herschberg-masters.pdf

[Herz97] Herzberg, A., Jakobsson, M., Jarecki, S., Krawczyk H. and Yung, M.: Proactive Public-key and Signature Schemes. In: Proceedings of the 4th ACM Annual Conference on Computer and Communications Security, ACM Press, pp. 100-110, 1997.

[Hirt00] Hirt, M., and Sako, K.: Efficient Receipt-Free Voting Based on Homomorphic Encryption. In: Advances in Cryptology - EUROCRYPT '2000, Lecture Notes in Computer Science, Vol. 1807, Springer-Verlag, pp. 539-556, 2000.

[Iet99] IETF Org.: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC 2459, 1999, at: http://www.ietf.org/rfc/rfc2459.txt?number=2459

[Int01] Internet Policy Institute: Report of the National Workshop on Internet Voting, March 2001, at: http://www.internetpolicy.org

[Jak98] Jakobsson, M.: A Practical Mix. In: Advances in Cryptology – EUROCRYPT '98, Lecture Notes in Computer Science, Vol. 1403, Springer-Verlag, pp. 448-461, 1998.

[Jak99] Jakobsson, M.: Flash Mixing. In: Proceedings of the 18th ACM Symposium on Principles of Distributed Computing - PODC '99, ACM Press, pp. 83-89, 1999.

[Jak02] Jakobsson, M., Juels, A., and Rivest, R.: Making Mix Nets Robust for Electronic Voting by Randomized Partial Checking. 2002, at: http://theory.lcs.mit.edu/~rivest

[Jak96] Jakobsson, M., Sako, K., and Impagliazzo, R.: Designated Verifier Proofs and their Applications. In: Advances in Cryptology - EUROCRYPT '96, Lecture Notes in Computer Science, Vol. 1070, Springer-Verlag, pp. 143-154, 1996.

[Jef95] Jefferies, N., Mitchell, C., and Walker, M.: Trusted Third Party based Key Management Allowing Warranted Interception. In: Proceedings of the Public Key Infrastructure Invitational Workshop, MITRE McLean. 1995, at: http://isg.rhbnc.ac.uk/cjm/TTPBKM.zip

[Jef00] Jefferson, D.: ATM Network Voting: A non-Starter. In: The Risks Digest, Vol. 21(15), 2000, at: http://catless.ncl.ac.uk/Risks/21.15.html#subj2

[Jua96] Juang, W. and Lei, C.: A Collision-free Secret Ballot Protocol for Computerized General Elections. In: Journal of Computers & Security, Vol. 15(4), pp. 339-348, 1996.

[Jua97] Juang, W. and Lei, C.: A Secure and Practical Electronic Voting Scheme for Real World Environments. In: Journal of IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E80(1), pp. 64-71, 1997.

[Kil95] Killian, J., and Leighton, T.: Fair Cryptosystems, Revisited. In: Advances in Cryptology - EUROCRYPT '95, Lecture Notes in Computer Science, Vol. 963, Springer-Verlag, pp. 208-220, 1995.

[Kil98] Kilian, J., and Petrank, E.: Identity Escrow. In: Advances in Cryptology - CRYPTO 98, Lecture Notes in Computer Science, Vol. 1462, Springer-Verlag, pp. 169-185, 1998.

[Kim99] Kim, S., Lee, I., Mambo, M., and Park, S.: On the Difficulty of Key Recovery Systems. In: Proceedings of the Information Security Workshop - ISW '99, Lecture Notes in Computer Science, Vol. 1729, Springer-Verlag, pp. 207-224, 1999.

[Kle99] Klemperer, P.: Auction Theory: A Guide to the Literature. In: Journal of Economic Surveys, Vol. 13, 1999, at: http://econwpa.wustl.edu:8089/eps/mic/papers/9903/9903002.pdf

[Knu98] Knudsen, L., and Martin, K.: In Search of Multiple Domain Key Recovery. In: Journal of Computer Security, Vol. 6(4), pp. 219-235, 1998.

[Koo02] Koops, B.: Crypto Law Survey - Overview per Country. Version 20.0, March 2002, at: http://cwis.kub.nl/~frw/people/koops/cls2.htm

[Kud98] Kudo, M.: Secure Electronic Sealed-bid Auction Protocol with Public Key Cryptography. In: Journal of IEICE Transactions on Fundamentals, Vol. E81-A(1), pp. 20-27, 1998.

[Kum98] Kumar, M., and Feldman, S.: Internet Auctions. In: Proceedings of the 3rd USENIX Workshop on Electronic Commerce, USENIX Press, pp. 49-60, 1998.

[Kur00] Kurosawa, K., Burmester, M., and Demedt, Y.: The Failure of the Boneh-Franklin/Stinson-Wei Attack Against Optimal Traitor Tracing. DIMACS 2000, 2000.

[Kur98] Kurosawa, K., and Demedt, Y.: Optimum Traitor Tracing. In: Advances in Cryptology - EUROCRYPT '98, Lecture Notes in Computer Science, Vol. 1403, Springer-Verlag, pp. 145-157, 1999.

[Luc02] The Lucent Personalized Web Assistant, at: http://lpwa.com

[Mag03] Magkos, E.: A Hybrid Key Recovery Scheme. Cyprus Computer Society Journal "Pliroforiki", Issue 3, to appear, 2003.

[Mag00] Magkos, E. Burmester, M., and Chrissikopoulos, V.: An Equitably Fair On-line Auction Scheme. In: Proceedings of the 1st International Conference on Electronic Commerce and Web technologies – ECWEB '2000, Lecture Notes in Computer Science, Vol. 1875, Springer-Verlag, pp. 72-84, 2000.

[Mag01] Magkos, E., Burmester, M., and Chrissikopoulos V.: Receipt-Freeness in Large-scale Elections without Untappable Channels. In: Proceedings of the 1st IFIP Conference on E-Commerce/E-business/E-Government, Kluwer Academic Publishers, pp. 683-693, 2001.

[Mag01_1] Magkos, E., Kotzanikolaou, P., and Chrissikopoulos, V.: An Asymmetric Traceability Scheme for Copyright Protection without Trust Assumptions. In: Proceedings of the 2nd International Conference on Electronic Commerce and Web technologies - ECWEB '2001, Lecture Notes in Computer Science, Vol. 2115, Springer-Verlag, pp. 186-195, 2001.

[Mag02] Magkos, E., and Chrissikopoulos, V., Equitably Fair Internet Voting. In: Journal of Internet Technology, Vol. 3(3), Special Issue on Network Security, pp. 187-193, 2002.

[Mag02_1] Magkos, E., Chrissikopoulos, V., and Alexandris, N.: A Common Security Model for Conducting e-Auctions and e-Elections. In: Proceedings of the 6th WSEAS International Conference on Communications, WSEAS Press, pp. 463-467, 2002.

[Mag01_2] Magkos, E., Chrissikopoulos, V., and Alexandris, N.: Software-based Receipt-Freeness in On-line Elections. In: Proceedings of the IFIP TG11-WG11.4 1st Annual Working Conference on Network Security, Kluwer Academic Publishers, pp. 33-43, 2001.

[Mah96] Maher, D.: Crypto Backup and Key Escrow. In: Communications of the ACM, Vol. 39(3), pp. 41-47, March 1996.

[Mao01] Mao, W.: Timed-Release Cryptography. Hewlett-Packard Laboratories, Report HPL-2001-37, United Kingdom, 2001.

[Mao01_1] Mao, W.: Verifiable Partial Escrow of Integer Factors. In: Design, Codes and Cryptography, Vol 24(3), Kluwer Academic Publishers, pp. 327-342, 2001.

[May00] May, P.: Alaskan Voters are Pioneers. Mercury News, Jan 25, 2000, at: http://www.mercurycenter.com/svtech/news/indepth/docs/vote012600.htm

[McC90] McCabe, K., Rassenti, S., and Smith, V.: Auction Institutional Design: Theory and Behavior of Simultaneous Multiple-Unit Generalizations of the Dutch and English Auctions. In: American Economic Review, Vol. 80(5), pp. 1276-1283, 1990.

[Mea87] Mead, W.: Natural Resource Disposal Policy: Oral Auction Versus Sealed Bids. In: Natural Resources Journal, Vol. 7, pp. 195-224, 1987.

[Men97] Menezes, A., Van Oorschot, P., and Vanstone, S.: Handbook of Applied Cryptography, CRC Press, 1997.

[Mer01] Mercuri R., and Neumann, P.: System Integrity Revisited. In: Communication of the ACM, Vol. 44(1), 2001, at: http://www.notablesoftware.com/Papers/Integrisk.html.

[Mic92] Micali, S.: Fair Public Key Cryptosystems. In: Advances in Cryptology - CRYPTO '92, Lecture Notes in Computer Science, Vol. 740, Springer-Verlag, pp. 113-138, 1993.

[Mic95] Micali, S., and Sidney, R.: A Simple Method for Generating and Sharing Pseudo-Random Functions, with Applications to Clipper-like Key Escrow Systems. In: Advances in Cryptology - CRYPTO '95, Lecture Notes in Computer Science, Vol. 963, Springer-Verlag, pp. 185-196, 1995.

[Mil87] Miller, S., Neuman, B., Schiller, J., and Saltzer, J.: Kerberos Authentication and Authorization System. M.I.T. Project Athena, Cambridge, Massachusetts, December 21, 1987.

[Mil89] Milgrom P.: Auctions and Bidding - A Primer. In: Journal of Economic Perspectives, Vol. 3, pp. 3-22, 1989.

[Moh01] Mohen, J., and Glidden, J.: The Case for Internet Voting. In: Communications of the ACM, Vol. 44(1), pp. 72-82, 2001.

[Nao99] Naor, M., and Pinkas, B.: Oblivious Transfer and Polynomial Evaluation. In: Proceedings of the 31th ACM Symposium on Theory Of Computing - STOC '99, ACM Press, pp. 245-254, 1999.

[Nao00] Naor, M., Pinkas, B., and Sumner, R.: Privacy Preserving Auctions and Mechanism Design. In: Proceedings of the 1st ACM Conference on Electronic Commerce, ACM Press, 2000, at: http://www.cs.ucsb.edu/~suri/ecommerceq/privacy.ps.

[Nef01] Neff, A.: A Verifiable Secret Shuffle and its Application to E-voting. In: Proceedings of the 8th ACM Conference on Computer and Communications Security, Philadelphia, 2001, at: http://www.votehere.net

[Neu96] Neuman, M., and Moore, D.: Computer Security Past and Future. In: ACM Crossroads Student Magazine, 1996, at: http://www.acm.org/crossroads/xrds2-4/intro.html

[Nie94] Niemi V, and Renvall A.: How to Prevent Buying of Votes in Computer Elections. In: Proceedings of ASIACRYPT '94, Lecture Notes in Computer Science, Vol. 917, Springer-Verlag, pp. 141-148, 1994.

[Ois98] Oishi, K., Mambo, M., and Okamoto, E.: Anonymous Public Key Certificates and the Applications. In: Journal of IEICE Transactions on Fundamentals of Electronics, Communications, and Computer Sciences, Vol. E81-A(1), pp. 56-64, 1998.

[Oka96] Okamoto T.: An Electronic Voting Scheme. In: Proceedings of the IFIP '96 Conference, Advanced IT Tools, Chapman & Hall, pp. 21-30, 1996.

[Oka97] Okamoto, T.: Receipt-Free Electronic Voting Schemes for Large Scale Elections. In: Proceedings of the 5th Security Protocols Workshop '97, Lecture Notes in Computer Science, Vol. 1163, pp. 125-132, 1997.

[Oka97_1] Okamoto, T.: Threshold Key-Recovery Systems for RSA. In: Proceedings of the 5th Security Protocols Workshop, Lecture Notes in Computer Science, Vol. 1361, Springer-Verlag, pp. 191-200, 1997.

[Pal99] Pallier, P.: Public-Key Cryptosystems Based on Discrete Logarithm Residues. In: Advances in Cryptology - EUROCRYPT '99, Lecture Notes in Computer Science, Vol. 1592, Springer-Verlag, pp. 223-238, 1999.

[Par94] Park, C., Itoh, K., and Kurosawa, K.: Efficient Anonymous Channel and All or Nothing Election Scheme. In: Advances in Cryptology – EUROCRYPT '93, Lecture Notes in Computer Science, Vol. 765, Springer-Verlag, pp. 248-259, 1994.

[Ped91] Pedersen, T.: A Threshold Cryptosystem Without a Trusted Party. In: Advances in Cryptology - EUROCRYPT '91, Lecture Notes in Computer Science, Vol. 547, Springer-Verlag, pp. 522-526, 1991.

[Ped92] Pedersen, T.: Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing. In: Advances in Cryptology - CRYPTO '91, Lecture Notes in Computer Science, Vol. 576, Springer-Verlag, pp. 129-140, 1992.

[Pet95] Petersen, H., Horster, P., and Michels, M.: Blind Multisignature Schemes and their Relevance to Electronic Voting. In: Proceedings of the 11th Annual Computer Security Applications Conference, IEEE Press, pp. 149-155, 1995.

[Pet99] Peticolas, F., Anderson, R., and Kuhn, M.: Information Hiding - A Survey. In: Proceedings of the IEEE Special Issue on Protection of Multimedia Content, Vol. 87(7), pp. 1062-1078, 1999.

[Pfi96] Pfitzmann, B.: Trials of Traced Traitors. Information Hiding Workshop, LNCS 1174, Springer-Verlag, 1996, pp. 49-64.

[Pfi96_1] Pfitzmann, B., Schunter, M.: Asymmetric Fingerprinting. In: Advances in Cryptology – EUROCRYPT '96, Lecture Notes in Computer Science, Vol. 1070, Springer-Verlag, pp. 84-95, 1996.

[Pfi97] Pfitzmann, B., and Waidner, M.: Anonymous Fingerprinting. In: Advances in Cryptology – EUROCRYPT '97, Lecture Notes in Computer Science, Vol. 1233, Springer-Verlag, pp. 88-102, 1997.

[Pfi97_2] Pfitzmann, B., and Waidner, M.: Asymmetric Fingerprinting for Larger Collusions, In: Proceedings of the ACM Conference on Computer and Communication Security, ACM Press, pp. 151-160, 1997.

[Pfi97_1] Pfitzmann, B., and Waidner, M.: How to Break Fraud-Detectable Key Recovery. In: EUROCRYPT '97, Rump Session, Konstanz, Germany, May 13, 1997.

[Phi01] Philips, D., and Spakovsky, H.: Gauging the Risks of Internet Elections. In: Communication of the ACM, Vol. 44(1), pp. 72-85, 2001.

[Pou98] Poupard, G., and Stern, J.: Generation of Shared RSA Keys by Two Parties. In: Advances in Cryptology - AsiaCrypt '98, Lecture Notes in Computer Science, Vol. 1514, Springer-Verlag, pp. 11-24, 1998.

[Rab81] Rabin, M.: How to Exchange Secrets by Oblivious Transfer. Technical Memo TR-81, Aiken Computation Laboratory, 1981.

[Rab83] Rabin, M.: Transaction Protection by Beacons. In: Journal of Computer and System Sciences, Vol. 27(2), pp.256-267, 1983.

[Reg00] Regulation of Investigatory Powers Act 2000, at: http://www.homeoffice.gov.uk/ripa/

[Rei95] Reiter, M.: The Rampart Toolkit for Building High-Integrity Services. In: Theory and Practice in Distributed Systems, Lecture Notes in Computer Science, Vol. 938, Springer-Verlag, pp. 99-110, 1995.

[Rei97] Reiter M., and Rubin, A.: Crowds, Anonymity for Web Transactions. DIMACS Technical Report 97-15, April 1997, at: http://www.research.att.com/projects/crowds/

[Rie98] Riera, A.: An Introduction to Electronic Voting Schemes. University of Barcelona, Report PIRDI-9/98, Barcelona, Spain, at: http://pirdi.uab.es/document/pirdi9.ps

[Rie98_1] Riera, A., Borrell, J., and Rifa, J.: An Uncoercible Verifiable Electronic Voting Protocol. In: Proceedings of the 14th International Information Security Conference IFIP/SEC '98, Kluwer Academic Publishers, pp. 206-215, 1998.

[Riv01] Rivest, R.: Electronic Voting. In: Financial Cryptography '01, at: http://theory.lcs.mit.edu/~rivest/Rivest-ElectronicVoting-ppt.pdf

[Riv01_1] Rivest, R.: Security in Voting Technology. At: http://theory.lcs.mit.edu/~rivest/rivest-may-24-01-testimony.txt

[Riv91] Rivest, R.: The MD4 Message Digest Algorithm. In: Advances in Cryptology - CRYPTO '90, Lecture Notes in Computer Science, Vol. 537, Springer-Verlag, pp. 303-311, 1991.

[Rsa78] Rivest, R., Shamir, A., and Adleman, L.: A Method for Obtaining Digital Signatures and Public Key Cryptosystems. In: Communications of the ACM, Vol.21, pp. 120-126, 1978.

[Riv96] Rivest, R., Shamir, A., and Wagner, D.: Time-Lock Puzzles and Timed-Release Crypto. LCS Tech. Memo MIT/LCS/TR-684, 1996, at: http://theory.lcs.mit.edu/~rivest/RivestShamirWagner-timelock.ps

[Rob85] Robinson, M.: Collusion and the Choice of Auction. In: Rand Journal of Economics, Vol. 16, pp. 141-145, 1985.

[Rub01] Rubin, A.: Security Considerations for Remote E-Voting over the Internet. AT&T Labs-Research, June 2001, at: http://avirubin.com/e-voting.security.html

[Sak93] Sako, K.: Electronic Voting Scheme Allowing Open Objection to the Tally. In: Journal of IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol E77-A (1), pp.24-30, 1993.

[Sak99] Sako, K.: Universally Verifiable Auction Protocol which Hides Losing Bids. In: Proceedings of the Symposium on Cryptography and Information Security - SCSI '99, pp. 35-39, 1999.

[Sak95] Sako K. and Killian J.: Receipt-Free Mix-type Voting Schemes - A Practical Solution to the Implementation of Voting Booth. In: Advances in Cryptology - EUROCRYPT '95, Lecture Notes in Computer Science, Vol. 921, Springer-Verlag, pp. 393-403, 1995.

[Saku00] Sakurai, K. and Miyazaki, S.: An Anonymous Electronic Bidding Protocol Based on New Convertible Group Signature Scheme. In: Proceedings of the 5th Australasian Conference for Information Security and Privacy - ACISP '2000, Lecture Notes in Computer Science, Vol. 1841, Springer-Verlag, pp. 385-399, 2000.

[Sch96] Schneier, B.: Applied Cryptography, Second Edition - Protocols, Algorithm and Source Code in C. John Wiley and Sons, 1996.

[Sch99] Schoenmakers, B.: A Simple Publicly Verifiable Secret Sharing Scheme and its Application to Electronic Voting. In: Advances in Cryptology - CRYPTO '99, Lecture Notes in Computer Science, Vol. 1666, Springer-Verlag, pp. 148-164, 1999.

[Sha79] Shamir, A.: How to Share a Secret. In: Communications of the ACM, Vol. 22(11), pp. 612-613, 1979.

[Sha95] Shamir, A.: Partial key Escrow - A New Approach to Software Key Escrow. The Weizmann Institute, Presentation at NIST Key Escrow Standards meeting, Sept. 15, 1995.

[Sta02] Stajano, F.: Security for Ubiquitous Computing. John Wiley and Sons, Wiley Series in Communications Networking & Distributed Systems, 2002.

[Sta99] Stajano, F., and Anderson, R.: The Cocaine Auction Protocol - On the Power of Anonymous Broadcast. In: Proceedings of the 3rd International Workshop on Information Hiding, Lecture Notes in Computer Science, Vol. 1768, Springer-Verlag, pp. 434-448, 1999.

[Sti95] Stinson, D.: Cryptography Theory and Practice. CRC Press LLC, 1995.

[Sti98] Stinson, D., and Wei, R.: Combinatorial Properties and Constructions for Traceability Schemes. In: SIAM Journal on Discrete Mathematics, Vol. 11(1), pp. 41-53, 1998.

[Stu99] Stubblebine, S., and Syverson, P.: Fair On-line Auctions Without Special Trusted Parties. In: Financial Cryptography '99, Lecture Notes in Computer Science, Vol. 1468, Springer-Verlag, pp. 231-241, 1999.

[Sur02] Surety Technologies, Inc., at: http://www.e-timestamp.com/

[Tem02] The Complete, unofficial TEMPFST Information Page. 2002, at: http://www.eskimo.com/~joelm/tempestintro.html#What is

[Tyg96] Tygar, S.: Atomicity in Electronic Commerce. In: Proceedings of the 15th Annual Symposium on Principles of Distributed Computing. ACM Press, pp. 8-26, 1996.

[Ung98] Ungar, L., Parkes, D., and Foster, D.: Cost and Trust Issues in On-line Auctions. In: Proceedings of the Agents-98 Workshop on Agent-Mediated Electronic Trading, pp. 161-172, 1998.

[Ver97] Verheulm, E., Henk, C., and Van Tilborg, C.: Binding ElGamal - A Fraud-Detectable Alternative to Key-Escrow Proposals. In: Advances in Cryptology - EUROCRYPT '97, Lecture Notes in Computer Science, Vol. 1233, Springer-Verlag, pp. 119-133, 1997.

[Vic61] Vickrey, W.: Counterspeculation, Auctions, and Competitive Sealed Tenders. In: Journal of Finance, Vol. 16(8), pp. 8-37, 1961.

[Wag83] Wagner, N.: Fingerprinting. In: Proceedings of the 1983 Symposium on Security and Privacy, IEEE Computer Society, pp. 18-22, 1983.

[Wal96] Walker, S., Lipner, S., Ellison, C., and Balenson, D.: Commercial Key Recovery. In: Communications of the ACM, Vol. 39(3), pp. 41-47, 1996.

[Wan02] Wang, W., Hidvegi, Z., and Whinston, A.: Shill Bidding in English Auctions. Paper under review, 2002, at: http://www.goizueta.emory.edu/upload/108/Shill.pdf

[Wel98] Wellman, M., and Wurman, P.: Real time Issues for Internet Auctions. In: Proceedings of the 1st IEEE Workshop - DARE '98, 1998, at: http://ftp.eecs.umich.edu/people/wellman/dare98.ps

[Wra66] Wraight, R.: The Art Game. New York: Simon and Schuster, pp. 110-111, 1966.

[Wur98] Wurman P., Walsh W., and Wellman M.: Flexible Double Auctions for Electronic Commerce: Theory and Implementation. In: Decision Support Systems, Vol. 24, pp. 17-27, 1998.

[You00] Young, A., and Yung, M.: Towards Signature-Only Signature Schemes. In: Advances in Cryptology - ASIACRYPT '2000, Lecture Notes in Computer Science, Vol. 1976, Springer-Verlag, pp. 97-115, 2000.

[You97] You, C., Zhou, J., and Lam, K.: On the Efficient Implementation of Fair Non-Repudiation. In: Proceedings of the 1997 IEEE Computer Security Foundations Workshop, IEEE Press, pp. 126-132, 1997.

[You98] Young, A., and Yung, M.: Auto-Recoverable and Auto-Certifiable Cryptosystems. In: Advances in Cryptology - EUROCRYPT '98, Lecture Notes in Computer Science, Vol. 1403, Springer-Verlag, pp. 17-31, 1998.