ΧΑΡΗΣ Β. ΓΕΩΡΓΙΟΥ
Ερευνητής Πληροφορικής, M.Sc., Ph.D.

Ηλεκτρονική ψηφοφορία

Αναβιώνοντας την «Εκκλησία του Δήμου» στον 21ο αιώνα

εξ αποστάσεως

Η ψηφιακή τεχνολογία και οι δυνατότητες των σύγχρονων τηλεπικοινωνιακών δικτύων συχνά δίνουν μια νέα οπτική σε μερικά από τα σημαντικότερα ζητήματα των σύγχρονων κοινωνιών. Μπορεί η «συμμετοχική Δημοκρατία» της Εκκλησίας του Δήμου στην αρχαία Αθήνα να αποτελεί σήμερα ουτοπία στις σύγχρονες πόλεις των πολλών εκατομμυρίων κατοίκων, όμως ο εκμηδενισμός των αποστάσεων μέσω του διαδικτύου και η ευρεία διαθεσιμότητα κρυπτογραφικών μεθόδων εξαιρετικά υψηλής αξιοπιστίας και ασφάλειας καθιστούν σήμερα τις διαδικασίες αυτές τεχνικά εφικτές. Αν η τεχνολογία μπορεί να προσφέρει τα μέσα για τη ριζική αναμόρφωση του τρόπου οργάνωσης και διεξαγωγής των πιο σημαντικών διαδικασιών στις σύγχρονες κοινωνίες, όπως είναι η εκλογή εκπροσώπων και η ίδια η διακυβέρνηση σε μια χώρα, τότε σίγουρα θα άξιζε τα ζητήματα αυτά να τεθούν στη σωστή τους βάση και με τις κατάλληλες προδιαγραφές για το μέλλον.

Ένα από τα βασικά συστατικά μιας Δημοκρατίας αποτελεί η ελεύθερη έκφραση της βούλησης των πολιτών μέσα από εκλογικές διαδικασίες για την επιλογή των εκπροσώπων που επωμίζονται την ευθύνη διακυβέρνησης μιας χώρας. Για να είναι αξιόπιστες και αποτελεσματικές, οι διαδικασίες αυτές πρέπει να βασίζονται σε συγκεκριμένους κανόνες, συνταγματικά κατοχυρωμένους και εφαρμόσιμους στην πράξη, αλλά κυρίως στην έννοια της εμπιστοσύνης. Οι ψηφοφόροι πρέπει να εμπιστεύονται, όχι μόνο τους υποψηφίους που υποστηρίζουν και που θέλουν να επιλέξουν με την ψήφο τους, αλλά και την ίδια τη διαδικασία εκλογής τους, το δίκαιο του συστήματος – διαφορετικά το τελικό αποτέλεσμα δεν θα μπορέσει να λάβει ουσιαστική νομιμοποίηση από το εκλογικό σώμα. Συνεπώς, μια παράμετρος μείζονος σημασίας σε οποιοδήποτε εκλογικό σύστημα, ηλεκτρονικό ή μη, είναι η έννοια της εμπιστοσύνης σε αυτό, που αφορά το αδιάβλητο της λειτουργίας και της εφαρμογής του.

Παραδοσιακά, μια τυπική εκλογική διαδικασία περιλαμβάνει δύο βασικές ομάδες συμμετεχόντων, τους ψηφοφόρους και τους υποψηφίους, οι οποίες, λόγω της αρχής της ελεύθερης συμμετοχής στα κοινά και της ανάδειξης εκπροσώπων (όταν φυσικά αυτό υφίσταται ως αρχή) επικαλύπτονται σε κάποιο ποσοστό. Ένας ψηφοφόρος μπορεί γενικά να είναι και υποψήφιος, συνεπώς πρέπει κάποιος τρίτος, «αυξέτερος», να αναλάβει το διαδικαστικό μέρος της εκλογής, ώστε αυτή να είναι αξιόπιστη και αδιάβλητη σε κάθε περίπτωση. Τον ρόλο αυτό αναλαμβάνει η εφορευτική επιτροπή που απαρτίζεται από (συνήθως τυχαία επιλεγμένα) μέλη του εκλογικού σώματος αλλά όχι υποψηφίων

προς εκλογή. Έτσι, η τρίτη αυτή ομάδα αναλαμβάνει τον ρόλο του «φύλακα» της ακεραιότητας της εκλογικής διαδικασίας, διασφαλίζοντας μεταξύ άλλων ότι ο κάθε ψηφοφόρος ψηφίζει μόνο μία φορά, ότι ψηφίζουν μόνο όσοι και όπου έχουν δικαίωμα, ότι στην κάλπη δεν ρίπτονται πλαστές ψήφοι, ότι στο τέλος καταμετρώνται όλες σωστά (μόνο οι έγκυρες), κλπ.

Στην παραπάνω τυπική διαδικασία, η απαραίτητη υποδομή για τη διεξαγωγή της ψηφοφορίας περιλαμβάνει μια σειρά από μηχανισμούς και μέσα (υλικό) που είναι απαραίτητα για τη διασφάλιση των απαιτούμενων προδιαγραφών. Για παράδειγμα, η μορφή και ο τρόπος συμπλήρωσης των ψηφοδελτίων είναι σαφέστατα καθορισμένα, η κάλπη στην οποία συλλέγονται είναι επίσης συγκεκριμένων προδιαγραφών (κλειδωμένη, συνήθως διαφανής), κάθε συμπληρωμένο ψηφοδέλτιο πρέπει να τοποθετείται σε κλειστό σφραγισμένο φάκελο μέχρι την τελική καταμέτρηση, ενώ τα ψηφοδέλτια διατηρούνται και δεν καταστρέφονται για ένα συγκεκριμένο (σχετικά μενάλο) χρονικό διάστημα μετά το πέρας της διαδικασίας.

Οι παραπάνω προδιαγραφές δεν είναι καθόλου τυχαίες. Αντίθετα, έχουν προκύψει ώς μια πρακτική υλοποίηση κάποιων πολύ βασικών και απαραίτητων κανόνων για μια αξιόπιστη εκλογική διαδικασία οποιασδήποτε μορφής. Αν και οι ακριβείς κανόνες και προδιαγραφές καθορίζονται κάθε φορά από διαφορετικούς παράγοντες, μια αξιόπιστη και ελεύθερη εκλογική διαδικασία πρέπει να βασίζεται στις εξής δέκα κύριες προϋποθέσεις:

1. **Καθολικότητα:** Οποιοσδήποτε πολίτης έχει κατοχυρωμένο δικαίωμα ψήφου, δηλαδή θα πρέπει να μπορεί να συμμετάσχει στη διαδικασία χωρίς κανένα πρόβλημα ή δυσκολία.
2. **Μοναδικότητα:** Κάθε ψήφος προσμε-

Συχνά οι εκλογικές διαδικασίες πρέπει να βασιστούν σε ελάχιστα διαθέσιμα μέσα και να υλοποιηθούν με τον απλούστερο και φθηνότερο τρόπο, χωρίς φυσικά να παραβιαστεί η αξιοπιστία και η εγκυρότητα. Σε χώρες με τεράστιο πληθυσμό ήκαι ελάχιστη υποδομή, όπως η Ινδία και το Αφγανιστάν, η ταυτοποίηση των ψηφοφόρων γίνεται μέσω οποιουδήποτε επίσημου εγγράφου (αντί εκλογικού βιβλιαρίου ή μόνο ταυτότητας), ενώ η διασφάλιση της μοναδικότητας της ψήφου εφαρμόζεται με τη βαφή ενός συγκεκριμένου κόβε φορά δακτύλου με ειδικό μελάνι.

τράται, ακριβώς μία φορά, και αντιστοιχεί σε ακριβώς έναν ψηφοφόρο (αντιστοιχία 1 προς 1).

3. Μυστικότητα-Ανωνυμία: Οταν και όπου απαιτείται, εφαρμόζεται μυστική ή/και ανώνυμη ψηφοφορία.

4. Ακρίβεια: Η καταμέτρηση πραγματοποιείται σωστά (επισημαίνοντας άκυρα, λευκά, κλπ.), επικυρώνεται με δεύτερη (τυλάχιστον) καταμέτρηση, ενώ είναι δυνατή και επιτυχόν καταμέτρηση αργότερα, αν αυτό κριθεί αναγκαίο.

5. Δικαιοσύνη: Κανείς δεν πληροφορείται επιλεκτικά για τα αποτελέσματα νωρίτερα από άλλους, ειδικά κατά τη διάρκεια διεξαγωγής της ψηφοφορίας.

6. Διαφάνεια: Κάθε μηχανισμός, υλικό και αποτέλεσμα είναι δυνατό να ελεγχθεί πριν, κατά τη διάρκεια και μετά το πέρας της διαδικασίας.

7. Ανθεκτικότητα: Κανένα επιμέρους λάθος ή παράλειψη, εσκεμμένο ή μη, δεν πρέπει να είναι καταστροφικό για την εκλογική διαδικασία (πρέπει να υπάρχουν εναλλακτικές λύσεις).

8. Μη Εξαναγκασμός: Πρέπει να προστατεύεται η ελευθερία της έκφρασης των ψηφοφόρων ως προς το τι θα επιλέξουν στην κάλπη.

9. Επιβεβαιωσιμότητα: Κάθε ψηφοφόρος πρέπει να είναι σε θέση (ο ίδιος) να επιβεβαιώσει ότι η ψήφος του καταχωρήθηκε και καταμετρήθηκε σωστά.

10. Μη Λογοδοσία: Στην επιβεβαιωσιμότητα θα πρέπει να προστατεύεται η μυστικότητα της ψήφου (μη αποκάλυψη περιεχομένου).

Οι παραπάνω δέκα παράγοντες αποτελούν ουσιαστικά έναν κατάλογο κριτηρίων βάσει των οποίων μια εκλογική διαδικασία μπορεί να χαρακτηριστεί ως ελεύθερη και δημοκρατική ή όχι. Σε αυτούς τους παράγοντες προστίθενται φυσικά και μερικοί ακόμα, περισσότερο συνταγματικής φύσης, όπως για παράδειγμα το αν μπορεί να θέσει υποψηφιότητα οποιοσδήποτε από το εκλογικό σώμα, το πώς και από ποιον γίνεται η ταυτοποίηση των στοιχείων κάθε ψηφοφόρου πριν ψηφίσει, κλπ. Επιπλέον, κάποιοι από τους παραπάνω παράγοντες, σε μικρό ή μεγάλο βαθμό, αλληλοεπικαλύπτονται. Για παράδειγμα, η έννοια της μυστικότητας και της ανωνυμίας της κάθε ψήφου φαίνονται ταυτόσημες έννοιες, όμως στην πράξη αφορούν διαφορετικό στάδια της εκλογικής διαδικασίας (κατά τη διάρκεια ή μετά την ψηφοφορία, αντίστοιχα).

Σήμερα μια τυπική διαδικασία ψηφοφορίας σε μεγάλη κλίμακα, όπως για παράδειγμα σε κάποιο εθνικό δημοψήφισμα ή σε εθνικές βουλευτικές εκλογές, καλύπτει αρκετές από τις παραπάνω απαιτήσεις αλλά απανίως το σύνολό τους. Η πιο συνηθισμένη μορφή τέτοιας εκλογικής διαδικασίας περιλαμβάνει τυπωμένα ψηφοδέλτια συγκεκριμένης μορφής, φακέλους σφραγισμένους (από την εφορευτική επιτροπή) στους οποίους αναγράφονται και συγκεκριμένες τοποθεσίες (εκλογικά κέντρα) όπου πραγματοποιείται η ψηφοφορία. Το πρότυπο αυτό καλύπτει κατά κύριο λόγο τους παράγοντες 1-6 και σε μεγάλο βαθμό και τον 7 (ανθεκτικότητα) με την προσθήκη εναλλακτικών, έστω και αναχρονιστικών, διαδικασιών σε περίπτωση εμφάνισης κάποιου προβλήματος, όπως για παράδειγμα στη μετάδοση των αποτελεσμάτων κατά την καταμέτρηση. Οι παράγοντες 8-10 αποτελούν εγγενές πρόβλημα όλων ουσιαστικά των τύπων και μεθόδων ψηφοφορίας, καθώς θεωρητικά δεν μπορούν ποτέ να διασφαλιστούν πλήρως.

Στην περίπτωση που επιτρέπεται ψηφοφορία εξ' αποστάσεως, αυτό κατά κανόνα πραγματοποιείται με τη μορφή επιστολικής ψήφου: η ταυτοποίηση του ψηφοφόρου και η δόκηση του εκλογικού διακώματος πραγματοποιείται από κάποια αρμόδια (πιστοποιημένη) αρχή, όπως για παράδειγμα από την αντίστοιχη πρεσβεία σε κάποια άλλη χώρα, ενώ το ψηφοδέλτιο τοποθετείται και πάλι σε σφραγισμένο φάκελο και αποστέλλεται προς καταμέτρηση, κατά κανόνα νωρίτερα από τη διεξαγωγή της κανονικής (τοπικής) ψηφοφορίας. Παρ' ότι ως διαδικασία δεν φαίνεται να διαφέρει σημαντικά, εν τούτοις σε πρακτικό-τεχνικό επίπεδο δημιουργούνται νέες απαιτήσεις και προδιαγραφές, από τις οποίες οι τρεις πιο σημαντικές είναι η πιστοποίηση κάποιας εναλλακτικής, σε σχέση με την κεντρική, αρχής, η ασφαλής (μυστικότητα, ακεραιότητα) μεταφορά των ψήφων προς καταμέτρηση και ο ασύγχρονος (όχι ταυτόχρονος) χαρακτήρας της ψηφοφορίας σε αυτή την περίπτωση.

Πώς, όμως, συνδέονται τα παραπάνω με την έννοια της ηλεκτρονικής ψηφοφορίας (e-Voting) και ειδικά της εξ αποστάσεως ηλεκτρονικής ψηφοφορίας (Remote e-Voting); Μπορεί άραγε η σύγχρονη τεχνολογία να προσφέρει κάτι ουσιαστικό για τη βελτίωση των παραπάνω διαδικασιών σε ότι αφορά την ποιότητα μιας τυπικής εκλογικής διαδικασίας;

ΗΛΕΚΤΡΟΝΙΚΗ ΚΑΙ ΕΞ ΑΠΟΣΤΑΣΕΩΣ ΗΛΕΚΤΡΟΝΙΚΗ ΨΗΦΟΦΟΡΙΑ

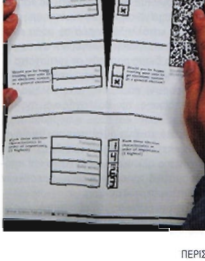
Μια πρώτη διάκριση που πρέπει να γίνει εδώ είναι μεταξύ των δύο αυτών εννοιών, της απλής ηλεκτρονικής και της εξ αποστάσεως ηλεκτρονικής ψηφοφορίας. Η πρώτη αναφέρεται στις γνωστές και τυπικές εκλογικές διαδικασίες που όμως θασίζονται εν μέρει ή εξ ολοκλήρου σε ηλεκτρονικά μέσα. Για παράδειγμα, τα ψηφοδέλτια μπορεί να είναι τυπωμένα αλλά η συμπλήρωσή τους να γίνεται με τέτοιον τρόπο ώστε να επιτρέπει την καταμέτρησή τους μέσω υπολογιστή – εναλλακτικά μπορεί και το ίδιο το «ψηφοδέλτιο» να έχει ηλεκτρονική μορφή στην οθόνη ενός υπολογιστή και η όλη διαδικασία να διεξάγεται με ηλεκτρονικό τρόπο. Παρόμοιες διαδικασίες εφαρμόζονται εδώ και πολλά χρόνια σε χώρες με μεγάλο εκλογικό σώμα (όπως στις ΗΠΑ), όπου η γρήγορη και έγκυρη καταμέτρηση είναι ζήτημα μείζονος σημασίας για την εκλογική διαδικασία. Συνήθως τα συστήματα αυτού του τύπου επιτρέπουν την εφαρμογή κρυπτογραφικών μεθόδων κατάλληλων για την κάλυψη επιπρόσθετων απαιτήσεων, όπως για παράδειγμα κάποιο ανώνυμο αποδεικτικό «κουπόνι» το οποίο παραλαμβάνει ο ψηφοφόρος και που μπορεί να χρησιμοποιηθεί αργότερα, αν χρειαστεί, για να επιβεβαιωθεί (διατηρώντας πάντα την μυστικότητα της ψήφου του) ότι η επιλογή του καταμετρήθηκε σωστά και συμπεριελήφθη στα συγκεντρωτικά αποτελέσματα.

Η έννοια της εξ αποστάσεως ηλεκτρονικής ψηφοφορίας προσομοιάζει περισσότερο στη διαδικασία της επιστολικής ψήφου: η εκλογική διαδικασία όχι μόνα περιλαμβάνει ένα ή περισσότερα στάδια «αυτοματοποίησης» μέσω κατάλληλων ηλεκτρονικών διατάξεων, αλλά ένας υπολογιστής καθίσταται ο ίδιος αρχή πιστοποίησης, εκλογικό κέντρο και μεταφοράς της ψήφου, για κάθε μεμονωμένο ψηφοφόρο, χρησιμοποιώντας τα παγκόσμια τηλεπικοινωνιακά δίκτυα. Οι βασικές προδιαγραφές και οι απαιτήσεις παραμένουν οι ίδιες, όμως στην προκειμένη περίπτωση κάποιες από αυτές είναι αρκετά πιο δύσκολο να ικανοποιηθούν με αξιόπιστο και ολοκληρωμένο τρόπο. Ενώ σε μια τυπική ψηφοφορία, ηλεκτρονική ή μη, η εκλογική διαδικασία είναι απόλυτα ελεγχόμενη και η εγκυρότητά της διασφαλίζεται σε φυσικό επίπεδο από την εφορευτική επιτροπή και την αρμόδια αρχή, στην εξ αποστάσεως ψηφοφορία αυτή η δυνατότητα μετατρέπεται σε μείζον ζήτημα ασφάλειας και αξιοπιστίας. Κάθε ψηφοφόρος, ακόμη και αν διαθέτει τον κατάλληλο ηλεκτρονικό εξοπλισμό (υπολογιστή κλπ.), πρέπει να μπορεί να ψηφίσει εξίσου ανώνυμα, έγκυρα, ελεύθερα, αλλά και μοναδικά, με ταυτοποίηση και διαφάνεια, όπως ακριβώς στις τυπικές εκλογικές διαδικασίες με τυπωμένα ψηφοδέλτια, εκλογικά κέντρα και σφραγισμένες κάλπες.

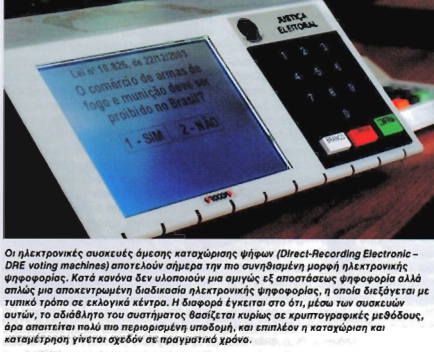
Τα ερωτήματα που προκύπτουν σχετικά με την ηλεκτρονική, και ειδικότερα την εξ αποστάσεως ψηφοφορία, είναι αρκετά και δύσκολο να απαντηθούν. Φυσικά, το πρώτο και κύριο ερώτημα είναι: Μπορεί η τεχναλογία να διασφαλίσει τουλάχιστον τον ίδιο θαθμό αξιοπιστίας, εγκυρότητας και διαφάνειας με αυτόν των παραδοσιακών «φυσικών» τρόπων ψηφοφορίας; Δηλαδή, μπορεί ένα τέτοιο σύστημα να αντικατασταθεί, μερικώς ή καθολικά, μια αντίστοιχη τυπική διαδικασία ψηφοφορίας, όπως για παράδειγμα σε εθνικές δημοτικές ή θουλευτικές εκλογές; Αν η απάντηση στο παραπάνω ερώτημα είναι θετική, το επόμενο λογικό ζήτημα που προκύπτει είναι κατά πόσον κάτι τέτοιο είναι σκόπιμο και θεμιτό, δηλαδή αν και ποια πλεονεκτήματα προσφέρει μια τέτοια επιλογή, πάντα με γνώμονα τη θελτίωση της ίδιας της εκλογικής διαδικασίας και όχι απλά να διεξαχθεί η ψηφοφορία μέσω υπολογιστή, ως «πείραμα».

Οπως σε κάθε άλλη δραστηριότητα, έτσι και εδώ, η εφαρμογή των νέων τεχνολογικών εξελίξεων σε ήδη τυποποιημένες διαδικασίες επιλύει ορισμένα προθλήματα, χωρίς όμως να αποφεύγει να δημιουργήσει κάποια νέα. Αν αυτά τα νέα ζητήματα μπορούν να αντιμετωπιστούν με αποτελεσματικό και πρακτικό τρόπο, καθώς και με χαμηλό κόστος, τότε οι νέες αυτές λύσεις ενσωματώνονται επιτυχώς στις διαδικασίες και αποτελούν το νέο πρότυπο.

Το ζήτημα της ηλεκτρονικής ψηφοφορίας αποτελεί ουσιαστικά μια εξαιρετικά θετική εξέλιξη σε ό,τι αφορά την ακεραιότητα και την ταχύτητα επεξεργασίας των δεδομένων που παράγονται από μια τυπική εκλογική διαδικασία. Αν είναι δυνατό να αυτοματοποιηθεί η διαδικασία ψηφοφορίας από το πρώτο στάδιο, δηλαδή αυτό της συλλογής των ψήφων, τότε όλα τα επόμενα στάδια μπορούν να επιταχυνθούν σε εξαιρετικά υψηλό θαθμό, καθώς οι υπολογιστές είναι κατασκευασμένοι ακριβώς για τη γρήγορη και σωστή επεξεργασία δεδομένων. Επιπλέον, η ψηφιοποίηση των δεδομένων αυτών κατά το πρώτο στάδιο επιτρέπει, όπως αναφέρθηκε πιο πάνω, την υλοποίηση πρόσθετων μηχανισμών που μέχρι σήμερα δεν υπήρχαν. Για παράδειγμα, σε κάποιες Πολιτείες των ΗΠΑ εφαρμόζεται η τεχνική των «τμηματοποιημένων κουπονιών» (splitted e-Ballots), κατά την οποία ο ψηφοφόρος χρησιμοποιεί ένα (πιστοποιημένο) ηλεκτρονικό μηχάνημα για να σημειώσει την ψήφο του και εκτυπώνει το αντίστοιχο συμπληρωμένο ψηφοδέλτιο, το οποίο αποτελείται από ένα κωδικό ανωνυμίας (anonymity ID) και δύο ή περισσότερα τμήματα. Ο ψηφοφόρος επιλέγει ένα τμήμα (split) για να ρίξει στην κάλπη και ένα για να κρατήσει ο ίδιος ως αποδεικτικό – το ψηφοδέλτιο στην κάλπη έχει ήδη σήμανση γνησιότητας αλλά ταυτόχρονα κανείς άλλος, παρά μόνο ο ίδιος, δεν μπορεί να αντιστοιχίσει πλήρως τις καταχωρημένες επιλογές με



Ενας από τους απλούστερους τρόπους «επιβεβαίωσης ψηφοφορίας» (verifiable voting) είναι αυτή κατά την οποία ο κάθε ψηφοφόρος μπορεί να ελέγξει, αν χρειαστεί, ότι οι επιλογές του καταχωρήθηκαν και καταμετρήθηκαν κανονικά. Το ψηφοδέλτιο αποτελείται από δύο μέρη (splits) εκ των οποίων το ένα περιλαμβάνει τις διαθέσιμες επιλογές και το άλλο αυτές που επιλέγει ο ψηφοφόρος. Και τα δύο μέρη σημειώνονται με τον ίδιο μοναδικό κωδικό, αλλά χωρίς περισσότερα στοιχεία ταυτοποίησης, και μάλιστα με τρόπο που είναι εύκολο να εντοπιστεί αργότερα (audit trail). Το απαντητικό δελτίο δεν φανερώνει τίποτα για την ταυτότητα του ψηφοφόρου και ταυτόχρονα ο ψηφοφόρος, αν χρειαστεί, μπορεί να αντιπαραβάλλει το πρώτο μισό, το οποίο κρατά ως απόδειξη, και να διαπιστώσει ότι η ψήφος του βρίσκεται χωρίς καμία αλλοίωση στο σύστημα προς καταμέτρηση.



Οι ηλεκτρονικές συσκευές άμεσης καταχώρισης ψήφων (Direct-Recording Electronic – DRE voting machines) αποτελούν σήμερα την πιο συνηθισμένη μορφή ηλεκτρονικής ψηφοφορίας. Κατά κανόνα δεν υλοποιούν μια αμιγώς εξ αποστάσεως ψηφοφορία αλλά απλώς μια αποκεντρωμένη διαδικασία ηλεκτρονικής ψηφοφορίας, η οποία διεξάγεται με τυπικό τρόπο σε εκλογικά κέντρα. Η διαφορά έγκειται στο ότι, μέσω των συσκευών αυτών, το αποδέλτιο του συστήματος βασίζεται κυρίως σε κρυπτογραφικές μεθόδους, όρα απαιτείται πολύ πιο περιορισμένη υποδομή, και επιπλέον η καταχώριση και καταμέτρηση γίνεται σχεδόν σε πραγματικό χρόνο.

κάποιον συγκεκριμένο ψηφοφόρο. Παρόμοιες μέθοδοι, όχι απαραίτητα ηλεκτρονικές, ονομάζονται «επιδεδειγμένα ψηφοφορία» (verifiable voting).

Στην εξ αποστάσεως ηλεκτρονική ψηφοφορία τίθεται επιπλέον το ζήτημα της ασφαλούς (εμπιστευτικής) και έγκυρης (μη τροποποίησιμης) μετάδοσης της ψήφου μέσω ενός δικτύου υπολογιστών, καθώς επίσης και της επιδεδειγμένης της ίδιας της ταυτότητας του ψηφοφόρου. Σήμερα, τα ζητήματα αυτά μπορούν να επιλυθούν σε πρακτικό επίπεδο μέσω ειδικών κρυπτογραφικών μεθόδων και ασφαλών πρωτοκόλλων επικοινωνίας, τόσο σε επίπεδο ταυτοποίησης όσο και σε επίπεδο κρυπτασφάλειας.

ΠΟΣΟ ΑΞΙΟΠΙΣΤΗ ΕΙΝΑΙ ΜΙΑ ΕΞ ΑΠΟΣΤΑΣΕΩΣ ΗΛΕΚΤΡΟΝΙΚΗ ΨΗΦΟΦΟΡΙΑ;

Μια διαδικασία ψηφοφορίας δεν είναι τίποτα άλλο παρά ένα τυπικό σύστημα μετάδοσης και επεξεργασίας δεδομένων, με κάποιες συγκεκριμένες προδιαγραφές ασφάλειας και αξιοπιστίας. Σε οποιοδήποτε τέτοιο σύστημα, το ενδιαφέρον εστιάζεται σε τρεις κύριους παράγοντες: (α) τον αποστολέα του μηνύματος, (β) τον παραλήπτη του μηνύματος και (γ) τον δίαυλο/μέσο μετάδοσης. Σε μια τυπική «φυσική» ψηφοφορία, τα τρία αυτά μέρη «συγχωνεύονται» σε ένα σημείο, απόλυτα ελεγχόμενο, που δεν είναι άλλο από το εκάστοτε εκλογικό κέντρο. Προκτικά, η διαχείριση της διαδικασίας, τόσο κατά τη διάρκεια της ψηφοφορίας όσο και κατά την καταμέτρηση, μπορεί να ελεγχθεί απόλυτα και μάλιστα τοπικά. Φυσικά απαιτούνται αντίστοιχες προβλέψεις σε ό,τι αφορά τη μετάδοση των επιμέρους αποτελεσμάτων για την έκδοση των γενικών αποτελεσμάτων και την προσωρινή αποθήκευση των καταμετρημένων ψηφοδελτίων, αλλά και πάλι αυτά είναι ζητήματα που διασφαλίζονται σχετικά εύκολα από την αρμόδια αρχή. Στην περίπτωση της επιστολικής ψήφου, η «τοπικότητα» της ψηφοφορίας δεν ισχύει πλέον: κάποια ψηφοδέλτια πρέπει να συλλεχούν και να ταξερθούν (σε φυσική μορφή) σε κάποιο πιστοποιημένο σημείο καταμέτρησης από κάποιον κατάλληλο φορέα σε ρόλο εφορευτικής επιτροπής. Ακόμη και αν τα ψηφοδέλτια διαμοιραστούν σε αντίστοιχα εκλογικά κέντρα (π.χ. βάσει καταγωγής των ψηφοφόρων), παρομένει το πρόβλημα της ταυτοποίησης, της συλλογής και της μεταφοράς τους. Και πάλι, η αρμόδια αρχή είναι κατά κανόνα αυτή που αναλαμβάνει τη διεκπεραίωση αυτών των διαδικασιών με τον πιο αξιόπιστο, αδιάβλητο και αποτελεσματικό τρόπο (π.χ. μέσω προσθέτων και διπλωματικών σάκων).

Στην περίπτωση της εξ αποστάσεως ηλεκτρονικής ψηφοφορίας, τα πράγματα είναι αρκετά διαφορετικά. Η διαχείριση ψηφοδελτίων δεν αφορά πλέον φυσικά εκτυπωμένα κουπόνια, τα οποία μπορούν να σφραγιστούν και να υπογραφούν, αλλά ψηφιακά δεδομένα χωρίς ιδιαίτερα εγγενή «φυσικά» χαρακτηριστικά, ενώ ταυτόχρονα μπορούν να αντιγραφούν και να μεταδοθούν πολύ εύκολα. Οι ίδιες οι έννοιες της ταυτοποίησης και της γνησιότητας δεν θαείζονται πλέον στα φυσικά χαρακτηριστικά π.χ. μιας υπογραφής, αλλά σε κρυπτογραφικές μεθόδους και ειδικούς αλγορίθμους ελέγχου πρόσβασης και ακεραιότητας σε επίπεδο ψηφιακών δεδομένων. Πρακτικά, οι ηλεκτρονικές αυτές διαδικασίες διαφέρουν ελάχιστα από τον τρόπο που λειτουργούν οι ηλεκτρονικές συναλλαγές σε εμπορικό επίπεδο: ο κάτοχος μιας πιστωτικής ή χρεωστικής κάρτας, αφού ταϋτοποιηθούν τα στοιχεία του ως νόμιμου κατόχου της, μπορεί να τη χρησιμοποιήσει προκειμένου να «χρεώσει» ψηφιακά τον τραπεζικό του λογαριασμό για μια αγορά που πραγματοποιεί. Προχωρώντας ένα βήμα πιο πέρα, η ίδια πιστωτική κάρτα μπορεί να χρησιμοποιηθεί, με κατάλληλες διαδικασίες πιστοποίησης και ασφαλούς μετάδοσης των δεδομένων, σε μια ηλεκτρονική αγορά μέσω διαδικτύου. Στην περίπτωση αυτή, η ταυτοποίηση δεν γίνεται μέσω φυσικών χαρακτηριστικών (π.χ. σύγκριση αστυνομικής ταυτότητας με στοιχεία κάρτας και οπτική αναγνώριση σε σχέση με μία φωτογραφία) αλλά μέσω ειδικών κωδικών πρόσβασης και ψηφιακών κρυπτογραφικών πιστοποιητικών που αντικαθιστούν την απλή φυσική υπογραφή του «κατόχου».

Εξετάζοντας τον κατάλογο που αναφέρθηκε στην αρχή του άρθρου με τα επιθυμητά χαρακτηριστικά μιας αξιόπιστης και ελεύθερης εκλογικής διαδικασίας (παράγοντες 1-10), θα πρέπει κάποιος να αναλύσει πώς μπορεί να υλοποιηθεί κάθε ένας από τους παράγοντες αυτούς σε τεχνικό επίπεδο, μέσω της σύγχρονης ψηφιακής τεχνολογίας, των υπολογιστών και των τηλεπικοινωνιακών δικτύων που είναι διαθέσιμα σήμερα. Θεωρώντας ως δεδομένο ότι κάθε ψηφοφόρος μπορεί να κατέχει ήδη ή να προμηθευτεί προσωρινό ψηφιακό πιστοποιητικό από κάποια αρμόδια αρχή, αντίστοιχης αξιοπιστίας και χρησιμότητας με την αστυνομική ταυτότητα ή το εκλογικό βιβλιάριο, οι απαιτήσεις σχετικά με την ταυτοποίηση του εκάστοτε ψηφοφόρου (καθολικότητα, μοναδικότητα, κλπ.) μπορούν να ικανοποιηθούν στο ακέραιο. Επιπλέον, λόγω της ψηφιακής επεξεργασίας των δεδομένων, η αξιοπιστία σε

επίπεδο μεμονωμένων ψήφων (ακρίβεια, μυστικότητα, ανωνυμία, κλπ.) είναι σχετικά εύκολο να επιτευχθεί με τη χρήση κατάλληλων κρυπτογραφιών μεθόδων και πρωτοκόλλων μετάδοσης. Σε ό,τι αφορά κάποιες ειδικές απαιτήσεις, που σε μια τυπική «φυσική» ψηφοφορία δεν είναι δυνατό να υλοποιηθούν, στο πλαίσιο της ηλεκτρονικής ψηφοφορίας μπορούν να ενσωματωθούν διαδικασίες επικύρωσης της κάθε ψήφου όχι μόνο από τον ίδιο τον ψηφοφόρο (ηλεκτρονική «απόδειξη» - e-Receipt) αλλά και από την εφορευτική επιτροπή (ηλεκτρονικό «έγχος» - audit trail) σε όλα τα επίπεδα.

Υπάρχουν, όμως, και κάποια χαρακτηριστικά που ακόμη και στην ηλεκτρονική ψηφοφορία εξακολουθούν να αποτελούν σημαντικά ζήτημα, λόγω μάλιστα σε σοβαρότερα βαθμό. Οσον αφορά τον μη εξαναγκασμό και τη μη λογοδοσία, η μυστικότητα της εκλογικής διαδικασίας (όταν υπάρχει) μέσω ενός παραβάν και ενός κλειστού αφραγισμένου φακέλου όπου τοποθετείται το συμπληρωμένο (ανώνυμο) ψηφοδέλτιο, θεωρείται επαρκής μηχανισμός, τουλάχιστον σε σχέση με το άμεσο τοπικό περιβάλλον της διεξαγωγής της ψηφοφορίας αλλά και της μη ηχνηλασιμότητας του κάθε ψηφοφόρου. Στην εξ αποστάσεως ηλεκτρονική ψηφοφορία, η μυστικότητα φαίνεται να ενισχύεται, όμως ο τρόπος δημιουργίας και χρήσης των αντίστοιχων ψηφιακών πιστοποιητικών καθιστά τα ζητήματα της ανωνυμίας και της μη ηχνηλασιμότητος αρκετά δυσκολότερο να ικανοποιηθούν. Συγκεκριμένα, εκτός από την εφορευτική επιτροπή, είναι απαραίτητη πλέον μια πρόσθετη αρμόδια αρχή, αυτή της προσθήκης ενός σταδίου ανωνυμίας (anonymizer), η οποία αποσυνδέει την ταυτότητα/ψηφιότητα της ψηφιακής ψήφου (e-Ballot) από τη διαδικασία συμπλήρωσης του αντίστοιχου δελτίου και άρα του ψηφοφόρου-χρήστη του συστήματος. Με άλλα λόγια, επειδή λόγω της διαδικασίας που υλοποιούν τα πρωτόκολλα ασφαλείας η ταυτότητα του χρήστη πρέπει να επικυρώνεται τη στιγμή που συμπληρώνει το κάθε μεμονωμένο (πλέον) ψηφοδέλτιο, αυτό θα πρέπει με κάποιον τρόπο να διατηρεί την εγκυρότητά του αλλά να «χάνει» την προέλευσή του. Ετσι, ο κάθε πιστοποιημένος ψηφοφόρος συνήθως προμηθεύεται (μετά την ταυτοποίησή του) από την αρχή αυτή ένα μοναδικό ηλεκτρονικό «κουπόνι» μιας χρήσης (e-Token), το οποίο μεταδίδεται χωρίς άλλα στοιχεία στην εφορευτική επιτροπή και το οποίο αυτή χρησιμοποιεί ως μηχανι-

ΧΩΡΕΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΑ ΣΥΣΤΗΜΑΤΑ ΨΗΦΟΦΟΡΙΑΣ

e-Voting	Remote e-Voting	Μελλοντικά σχέδια
Αυστραλία, Βραζιλία, Καναδάς, Γαλλία, Ινδία, Ιαπωνία, Καζακστάν, Περού, Ρωσία, ΗΠΑ, ΗΑΕ, Βενεζουέλα	Αυστρία, Αυστραλία, Καναδάς, Εσθονία, Γαλλία, Ιαπωνία, Ελβετία	Αργεντινή, Αζερμπαϊτζάν, Λευκορωσία, Βουλγαρία, Χιλή, Τσεχία, Φινλανδία, Ελλάδα, Ιταλία, Λετονία, Λιθουανία, Μεξικό, Νεπάλ, Νιγηρία, Νορβηγία, Πολωνία, Πορτογαλία, Ρουμανία, Σλοβακία, Σλοβενία, Ισπανία, Ν. Αφρική, Ν. Κορέα, Σουηδία

Στον συνοδευτικό πίνακα παρουσιάζεται συνοπτικά η διείσδυση των τεχνολογιών ηλεκτρονικής ψηφοφορίας ανά χώρα παγκοσμίως. Η πρώτη στήλη (e-Voting) αφορά χώρες που ήδη εφαρμόζουν συστήματα ηλεκτρονικής ψηφοφορίας σε επίπεδο καταχώρισης σε τυπικά εκλογικά κέντρα ή «σταθμούς» ηλεκτρονικής ψηφοφορίας (polling stations). Στις περισσότερες περιπτώσεις τα συστήματα αυτά αποτελούνται από ειδικά τερματικά ηλεκτρονικής συμπλήρωσης και εκτύπωσης των συμπληρωμένων ψηφοδελτίων. Αξίζει να σημειωθεί ότι το νομοθετικό πλαίσιο που ισχύει στις ΗΠΑ επιτρέπει διαφορετικές προβλέψεις και προδιαγραφές ανά Πολιτεία, με αποτέλεσμα τα αντίστοιχα συστήματα να εμφανίζουν σημαντικότατες διαφορές μεταξύ τους.

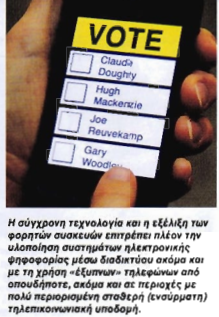
Στη δεύτερη στήλη παρουσιάζονται χώρες που έχουν ήδη υλοποιήσει σε επίπεδο πραγματικών εκλογών (περιφερειακών, κοινοβουλευτικών ή ευρωεκλογών) συστήματα εξ αποστάσεως ηλεκτρονικής ψηφοφορίας μέσω διαδικτύου ή μέσω τηλεφώνου. Από τις χώρες αυτές, η Αυστραλία και η Εσθονία είναι ίσως αυτές με τη μεγαλύτερη εμπειρία και τεχνογνωσία, καθώς έχουν εφαρμόσει παρόμοια συστήματα σε μεγάλη έκταση εδώ και αρκετά χρόνια. Η Εσθονία αποτελεί ίσως το πιο επιτυχημένο παράδειγμα στην Ευρώπη μιας ψηφοφορίας εξ αποστάσεως σε εθνικό επίπεδο (όχι μόνο αντί επιστολικής ψήφου), καθώς ήδη από το 2002 διαθέτει το κατάλληλο νομοθετικό πλαίσιο, και παρά τα προβλήματα που φαίνεται πως το σύστημα λειτουργεί αρκετά αξιόπιστα, με τη χρήση «έξυπνων» καρτών (smartcards) και ψηφιακών υπογραφών (digital signatures). Το 2005 κατέστη η πρώτη χώρα παγκοσμίως που προσέφερε τη δυνατότητα ηλεκτρονικής ψηφοφορίας μέσω διαδικτύου σε εθνικό επίπεδο (περιφερειακές εκλογές).

Στην τρίτη ομάδα ανήκουν οι χώρες που διαθέτουν συστήματα ηλεκτρονικής ψηφοφορίας υπό δοκιμή, καθώς και χώρες που τώρα δημιουργούν την αντίστοιχη νομοθεσία και σχεδιάζουν σύντομα να αποκτήσουν παρόμοια συστήματα. Αξίζει να σημειωθεί ότι στην πλειονότητά τους οι χώρες αυτές χαρακτηρίζονται από το μέγεθος του εκλογικού σώματος ή/και από τη γεωγραφική τους έκταση: είτε είναι πολύ μικρές, οπότε είναι εύκολη η σχεδίαση και η πιλοτική εφαρμογή ηλεκτρονικής ψηφοφορίας, είτε είναι πολύ μεγάλες, οπότε ένα τέτοιο σύστημα διευκολύνει ιδιαίτερα τη διαδικασία.

Στην Ελλάδα, το εκλογικό σώμα είναι της τάξης των 10 εκατομμυρίων πολιτών, με μεγάλο και συνεχώς αυξανόμενο ποσοστό αποχής από την εκλογική διαδικασία (29,1% στις εθνικές εκλογές του 2009). Μεταξύ αυτών, η διείσδυση του διαδικτύου ανέρχεται σήμερα περίπου στα 4 εκατομμύρια κατοίκους, με σημαντικές, όμως, αποκλίσεις ως προς το επίπεδο ψηφιακής Παιδείας. Σήμερα, η ελληνική νομοθεσία προβλέπει ψήφο επιστολική ή με «άλλο πρόσφορο μέσο» μόνο για τους μόνιμους κατοίκους Ελλάδας. Βάσει των τελευταίων εκλογικών αποτελεσμάτων, το μεγαλύτερο ποσοστό των ψηφοφόρων που δεν ψήφισαν ήταν κυρίως νέοι με μέσο ή ανώτερο επίπεδο γνώσεων σε δ,τι αφορά τη χρήση νέων τεχνολογιών. Κατά συνέπεια, η υλοποίηση ενός συστήματος εξ αποστάσεως ηλεκτρονικής ψηφοφορίας στην Ελλάδα ίσως προσφέρει σημαντικότατα οφέλη όσον αφορά το ποσοστό συμμετοχής σε μελλοντικές εκλογικές διαδικασίες.

σμό πιστοποίησης της ψήφου, αλλά όχι του ίδιου. Ο λόγος που η αρχή έκδοσης αυτών των ηλεκτρονικών κουπονιών μιας χρήσης πρέπει να είναι διαφορετική από την εφορευτική επιτροπή που διαχειρίζεται τις ψήφους, είναι ακριβώς για να μη μπορεί κανένα από τα δύο αυτά μέρη να προδεί σε πλήρη ταυτοποίηση ψηφοφόρων-ψήφων, χωρίς όμως να υποβαθμίζεται η αξιοπιστία του συστήματος.

Αν και παρόμοιοι μηχανισμοί ενισχύουν σε μεγάλο βαθμό τη δυνατότητα επιβεβαίωσης από την πλευρά του ψηφοφόρου, άρα και την εμπιστοσύνη του στο σύστημα και στη διαδικασία, εν τούτοις η δυνατότητα πλήρους αποσύνδεσης του ψηφοφόρου από την «τοπικότητα» του εκλογικού κέντρου καθιστά, σύμφωνα με αρκετούς μηχανικούς Πληροφορικής αλλά και πολιτικούς αναλυτές, σημαντικά αυξημένο τον κίνδυνο έναντι της απαίτησης για μη εξαναγκασμό και μη λογοδοσία. Εφόσον η ψηφοφορία δεν διεξάγεται πλέον σε περιορισμένο, απόλυτα ελεγχόμενο φυσικό χώρο (εκλογικά κέντρα), υπάρχει σαφέστατος κίνδυνος ως προς το κατά πόσον ο ψηφοφόρος εκφράζεται ελεύθερα ή/και αν το αποδεικτικό που θα λάβει, εφόσον είναι πλήρες ως προς το περιεχόμενο του ψηφοδελτίου (όχι απλά κωδικός επιβεβαίωσης), δεν ενισχύει τον κίνδυνο εξαγοράς ψήφων. Πρακτικά, υπάρχει πραγματικό δίλημμα μεταξύ της εφαρμογής κρυπτογραφικών μεθόδων για τη διασφάλιση της εμπιστευτικότητας και ταυτόχρονα της ανάγκης διατήρησης της ανωνυμίας, ακριβώς λόγω της ίδιας της φύσης των τεχνικών λύσεων που υφίστανται σήμερα. Κάποιοι μάλιστα ισχυρίζονται ότι οι δυσκολίες αυτές είναι τέτοιες που «...ποτέ ένα ηλεκτρονικό σύστημα ψηφοφορίας δεν θα μπορεί να είναι αρκούντως ασφαλές», ειδικότερα όταν τα αντίστοιχα συστήματα υλικού (hardware) και λογισμικού (software) που χρησιμοποιούνται είναι απλώς «πιστοποιημένα» αλλά όχι πλήρως βασισμένα σε ανοικτά πρότυπα (open standards). Η αλήθεια βρίσκεται μάλλον κάπου στη μέση. Σίγουρα κανένα ηλεκτρονικό σύστημα δεν μπορεί να ικανοποιήσει πλήρως όλες τις απαιτήσεις ασφάλειας, αξιοπιστίας, ακεραιότητας, κλπ. Από την άλλη πλευρά, κανένα παραδοσιακό σύστημα ψηφοφορίας, με τυπωμένα ψηφοδέλτια, κανονικά εκλογικά κέντρα και σφραγίδες μελανιού δεν είναι εν γένει περισσότερο ασφαλές ή αξιόπιστο, καθώς τα προβλήματα είναι μεν διαφορετικά αλλά εξίσου σημαντικά.



Η σύγχρονη τεχνολογία και η εξέλιξη των φορητών συσκευών επιτρέπει πλέον την υλοποίηση συστημάτων ηλεκτρονικής ψηφοφορίας μέσω διαδικτύου ακόμα και με τη χρήση «έξυπνων» τηλεφώνων από οποιδήποτε, ακόμα και σε περιοχές με πολύ περιορισμένη σταθερή (ενσύρματη) τηλεπικοινωνιακή υποδομή.

ΗΛΕΚΤΡΟΝΙΚΑ ΣΥΣΤΗΜΑΤΑ ΨΗΦΟΦΟΡΙΑΣ ΚΑΙ ΚΡΥΠΤΑΣΦΑΛΕΙΑ

Ενας από τους πιο σημαντικούς παράγοντες κατά τη σχεδίαση και την υλοποίηση των συστημάτων ηλεκτρονικής ψηφοφορίας, ειδικά όταν πρόκειται για εξ αποστάσεως ψηφοφορία, αποτελεί η ασφάλεια. Πιο συγκεκριμένα, σε παρόμοια συστήματα το ενδιαφέρον επικεντρώνεται και στους τρεις βασικούς άξονες ενός τηλεπικοινωνιακού μοντέλου, δηλαδή τον πομπό (ψηφοφόρος), τον παραλήπτη (κάλπη) και το μέσο μετάδοσης. Ως προς το τελευταίο, όταν πρόκειται για εξ αποστάσεως ψηφοφορία μέσω διαδικτύου, υπάρχει σαφέστατη ανάγκη για αδιαβλητότητα, ακεραιότητα, αλλά και μυστικότητα-ανωνυμία της κάθε ψήφου. Στο πλαίσιο αυτό, εφόσον πρόκειται για μη ελεγχόμενα δίκτυα εξαιρετικά μεγάλης έκτασης και χωρίς καμία διασφάλιση εμπιστευτικότητας, η μοναδική μέθοδος διασφάλισης των παραπάνω απαιτήσεων είναι μέσω κατάλληλων κρυπτογραφικών μεθόδων.

Πρακτικά, αυτό που απαιτείται είναι ένα σύστημα το οποίο να προσφέρει (α) αξιόπιστη πιστοποίηση του κάθε μέρους στα άκρα του διαύλου επικοινωνίας και (β) προστασία των μηνυμάτων που ανταλλάσονται τόσο σε επίπεδο ακεραιότητας (να μη μπορούν να τροποποιηθούν από τρίτο) όσο και σε επίπεδο εμπιστευτικότητας (προστασία μυστικότητας). Τα θέματα αυτά εν γένει δεν είναι διόλου απλά – ειδικότερα το ζήτημα της απόλυτα ασφαλούς ανταλλαγής του κλειδιού σε ένα τυπικό μοντέλο ανταλλαγής κρυπτογραφημένων μηνυμάτων αποτελεί ένα θεωρητικά άλυτο μαθηματικό πρόβλημα. Παρ' όλα αυτά, εδώ και μερικές δεκαετίες οι δυνατότητες των υπολογιστών επιτρέπουν την υλοποίηση μεθόδων που επιλύουν το πρόβλημα αυτό με «πρακτικά επαρκή» τρόπο.

Υπάρχουν δύο κατηγορίες κρυπτογραφικών συστημάτων: (α) τα συμμετρικά, όπου τα δύο μέρη που επικοινωνούν χρησιμοποιούν ένα κοινό προσυμφωνημένο κλειδί για την κρυπτογράφηση και αποκρυπτογράφηση των μηνυμάτων τους, και (β) τα ασύμμετρα, όπου κάθε μέρος χρησιμοποιεί ένα ζεύγος κλειδιών το οποίο περιλαμβάνει ένα κλειδί μόνο για κρυπτογράφηση («δημόσιο») και ένα μόνο για αποκρυπτογράφηση («ιδιωτικό»). Το πλεονέκτημα της δεύτερης αυτής κατηγορίας κρυπτοσυστημάτων είναι ο διαχωρισμός των δύο ενεργειών – εφόσον η κρυπτογράφηση πραγματοποιείται με «ασύμμετρο» (όχι απλά ταυτόσημα αντίστροφο) τρόπο, το ίδιο συμβαίνει και με τα δύο μέρη του ζεύγους των κλειδιών. Στην πράξη, είναι σαν να κατασκευάζεται μια πόρτα η οποία κλειδώνει μόνο με το πρώτο «δημόσιο» κλειδί και ξεκλειδώνει μόνο με το δεύτερο «ιδιωτικό» κλειδί. Έτσι, αν το δύο κλειδιά είναι «αρκούντως ασύνδετα» μεταξύ τους, δηλαδή η γνώση του ενός δεν υποδηλώνει τίποτα για το άλλο, η διαρροή του πρώτου κλειδιού δεν συνιστά κανέναν κίνδυνο και συνεπώς μπορεί να μεταδοθεί ελεύθερα χωρίς κανένα πρόβλημα.

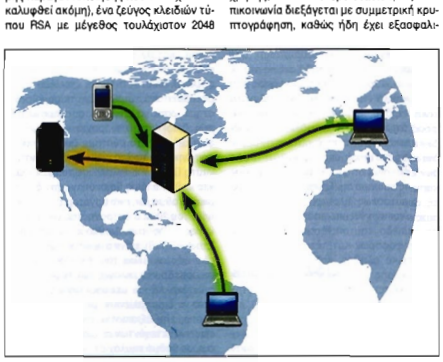
Το 1977, οι Ron Rivest, Adi Shamir και Leonard Adleman του MIT δημοσίευσαν μια ιστορική πλέον εργασία τους ακριβώς για την επίλυση του παραπάνω προβλήματος, αυτό της δημιουργίας ενός (τυχαίου) ζεύγους κλειδιών με τα παραπάνω χαρακτηριστικά, δηλαδή να είναι «συμπληρωματικά» ως προς την κρυπτογράφηση-αποκρυπτογράφηση, να μη μπορεί να τα «μαντέψει» κάποιος εύκολα και επιπλέον να είναι τέτοια ώστε η γνώση του ενός να μη υποβαθμίζει τη μυστικότητα του άλλου κλειδιού. Ο αλγόριθμος RSA, όπως τον αποκάλεσαν από τα αρχικά των ονομάτων τους, βασίστηκε στην εγγενή δυσκολία της παραγοντοποίησης πολύ μεγάλων ακεραίων αριθμών σε πρώτους παράγοντες και επιπλέον στους πάρα πολλούς συνδυασμούς που προκύπτουν για την ομαδοποίηση των παραγόντων αυτών σε δύο «ομάδες». Χρησιμοποιώντας μαθηματικές μεθόδους και θεωρήματα από τη Θεωρία Αριθμών, κατάφεραν να αποδείξουν ότι η

κάθε τέτοια (εν γένει τυχαία) ομάδα πρώτων παραγόντων μπορεί να δημιουργήσει ένα από τα δύο κλειδιά του ζεύγους, και μάλιστα, βάσει του περίφημου «Κινεζικού θεωρήματος των υπολοίπων», είναι δυνατό να υλοποιηθούν με αποδοτικό τρόπο οι αντίστοιχες διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης μηνυμάτων. Σχεδόν ταυτόσημο αλγόριθμο είχε διατυπώσει νωρίτερα το 1973 ο Βρετανός μαθηματικός Clifford Cocks, σε διαδιαθημισμένο όμως έγγραφο, το οποίο δεν δημοσιεύτηκε παρά μόλις το 1997.

Η ασφάλεια ενός τέτοιου συστήματος βασίζεται στο γεγονός ότι αν το γινόμενο των δύο ομάδων πρώτων αριθμών είναι «αρκούντως μεγάλο» και η ακριβής σύσταση τους είναι «αρκούντως τυχαία», πρακτικά είναι αδύνατο από το πρώτο (δημόσια διαθέσιμο) κλειδί κρυπτογράφησης και μια σειρά κρυπτογραφημένων μηνυμάτων να εικάσει κάποιος το δεύτερο (μυστικό) κλειδί αποκρυπτογράφησης. Η έννοια «αρκούντως τυχαία» αφορά το πώς ακριβώς διαμοιράζονται οι πρώτοι παράγοντες του αρχικού γινομένου στις δύο ομάδες, ενώ το «αρκούντως μεγάλο» ως προς το μέγεθος των κλειδιών εξαρτάται από τις εκάστοτε τεχνικές δυνατότητες των υπολογιστών που πιθανώς να αναλάβουν το έργο της κρυπτανάλυσης. Με βάση τις σημερινές προβλέψεις για τις επόμενες γενιές υπολογιστών και με βάση τις σημερινές μαθηματικές μας γνώσεις (αν δεν υπάρχει κάποιο θεώρημα ευκολότερης παραγοντοποίησης που δεν έχει ανακαλυφθεί ακόμη), ένα ζεύγος κλειδιών τύπου RSA με μέγεθος τουλάχιστον 2048 bits ($2^{2048} \approx 3{,}16 \times 10^{616}$ συνδυασμοί) είναι ασφαλές από επιθέσεις κρυπτανάλυσης τύπου «brute force attacks» για πολλές χιλιάδες χρόνια.

Εκτός από τη βασική διατύπωση του αλγορίθμου RSA, παρόμοιες τεχνικές έχουν διατυπωθεί για αντίστοιχα ή ισοδύναμα ασύμμετρα κρυπτοσυστήματα, όπου ένα ζεύγος κλειδιών «τύπου RSA» κατασκευάζεται βάσει ενός εξαιρετικά δύσκολου μαθηματικού (συνήθως συνδυαστικού) προβλήματος και στη συνέχεια τα δύο κλειδιά χρησιμοποιούνται ως συμπληρωματικά για κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων. Οι τεχνικές αυτές αποτέλεσαν πραγματική επανάσταση στα ψηφιακά δίκτυα τηλεπικοινωνιών και ιδιαίτερα κατά τα πρώτα στάδια του διαδικτύου τις δεκαετίες του 70 και του 80, αφού κατέστησαν δυνατή την ασφαλή μετάδοση πληροφοριών χωρίς την ανάγκη κανενός άλλου πρόσθετου μέσου μετάδοσης κλειδιών και πιστοποιητικών ασφαλείας. Κατά κανόνα οι ασύμμετρες μέθοδοι κρυπτογράφησης, όπως ο RSA, είναι πολύ πιο απαιτητικές και αργές σε σύγκριση με τις περισσότερες συμμετρικές μεθόδους (κοινού μυστικού κλειδιού) που προσφέρουν ανάλογο επίπεδο ασφάλειας. Έτσι, η ασύμμετρη κρυπτογράφηση συνήθως εφαρμόζεται κατά το πρώτο στάδιο της επικοινωνίας, όπου το «δημόσιο» κλειδί κάθε μέρους μεταδίδεται ελεύθερα και μέσω αυτού κρυπτογραφείται ένα νέο, μυστικό κλειδί από κοινού χρήσης, και σε δεύτερο στάδιο η κύρια επικοινωνία διεξάγεται με συμμετρική κρυπτογράφηση, καθώς ήδη έχει εξασφαλιστεί η ασφαλής «συμφωνία» ενός τυχαίου κλειδιού για αυτόν τον σκοπό. Η διαδικασία αυτή αποτελεί εδώ και αρκετές δεκαετίες το βασικό μοντέλο ασφαλούς επικοινωνίας στο διαδίκτυο και εφαρμόζεται με διάφορες παραλλαγές και υλοποιήσεις σε όλες σχεδόν τις περιπτώσεις όπου απαιτείται υψηλό επίπεδο ασφάλειας κατά τη μετάδοση μηνυμάτων (πρωτόκολλα SSL/TLS για ηλεκτρονική τραπεζική, ηλεκτρονικές αγορές, ιδιωτικά δίκτυα τύπου VPN, κ.ά.).

Είναι φανερό πως οι παραπάνω έννοιες, ιδιαίτερα αυτή ενός «δημόσιου» κλειδιού που μπορεί να μεταδοθεί ελεύθερα και που συνδέεται εγγενώς με ένα άλλο «ιδιωτικό» κλειδί, σχετίζονται άμεσα με τις απαιτήσεις ασφάλειας σε ένα σύστημα εξ αποστάσεως ηλεκτρονικής ψηφοφορίας. Αληθοφανή όπως ο RSA διασφαλίζουν ότι κάθε μέρος της διαδικασίας, τόσο ο εκάστοτε ψηφοφόρος όσο και η διοργανώτρια αρχή (ως ηλεκτρονική «κάλπη»), μπορεί να κατασκευάσει ένα μοναδικό, τυχαίο ζεύγος κλειδιών, να δημοσιοποιήσει ένα εκ των δύο και τελικά να εγκαθιδρύσει έναν ασφαλή δίαυλο επικοινωνίας τύπου σημείο-προς-σημείο (point-to-point), μέσω του οποίου μπορεί με αξιόπιστο και ασφαλή τρόπο να καταχωρήσει την ψήφο του. Ενα εξίσου σημαντικό, όμως, πλεονέκτημα των ασύμμετρων κρυπτοσυστημάτων τύπου RSA είναι το γεγονός ότι, εν γένει, τα δύο κλειδιά μπορούν να χρησιμοποιηθούν και με «αντίστροφη» σειρά (καθώς είναι συμπληρωματικά), εφόσον κάτι τέτοιο απαιτείται. Με άλλα λόγια, η έννοια του «δημόσιου» και του «ιδιωτικού» κλειδιού μπορεί να αντιστραφεί, αν κάτι πρέπει να μπορεί να κρυπτογραφηθεί μοναδικά από τον κάτοχο του μυστικού κλειδιού και να μπορεί να αποκρυπτογραφηθεί από οποιονδήποτε βάσει του δημόσια διαθέσιμου αντίστοιχου

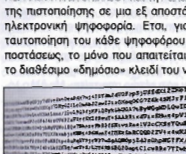


Η χρήση εξελιγμένων κρυπτογραφικών μεθόδων όπως οι αλγόριθμοι ασύμμετρης κρυπτασφάλειας τύπου RSA καθιστούν δυνατή τη δημιουργία «εικονικών» ιδιωτικών δικτύων υψηλού επιπέδου ασφαλείας (Virtual Private Network – VPN), ακόμα και διαμέσου ενός εντελώς «ανοικτού» δικτύου διαμεσολάβησης όπως είναι το Internet. Στην περίπτωση ηλεκτρονικής ψηφοφορίας εξ αποστάσεως, παρόμοια δίκτυα εγκαθίστανται είτε μόνιμα, μεταξύ εκλογικών κέντρων και αρμόδιας αρχής, είτε ακόμα και προσωρινά, με σκοπό τη διασύνδεση ενός μεμονωμένου ψηφοφόρου με κάποιο εικονικό εκλογικό κέντρο για την καταχώριση της ψήφου του/της.

Από τεχνική άποψη, η δυνατότητα ασφαλούς, αξιόπιστης, ελεύθερης εκλογικής διαδικασίας, με προστασία των ατομικών δικαιωμάτων και του αδιαβλήτου του αποτελέσματος, σαφέστατα υπάρχει εδώ και μερικές δεκαετίες.

κλειδιού. Ισως αυτό να φαίνεται κάπως αντιφατικό, όμως αποτελεί τη βάση της έννοιας της ψηφιακής υπογραφής και του ψηφιακού πιστοποιητικού: αν κάτι μπορεί να «σημανθεί» με μοναδικό τρόπο από κάποιον και στη συνέχεια να «ελεγχθεί» από οποιονδήποτε άλλον, αυτή ακριβώς η διαδικασία έχει την έννοια της υπογραφής, με ψηφιακά όμως τρόπο, η ασφάλεια της οποίας βασίζεται εξ ολοκλήρου σε κρυπτογραφικούς αντί για βιομετρικούς παράγοντες (ψραφικός χαρακτήρας).

Αν κάτι μπορεί να «υπογραφεί» ψηφιακά μόνο από τον κάτοχο του «ιδιωτικού» κλειδιού και στη συνέχεια να μεταδοθεί ελεύθερα ως «γνήσιο», με τη δυνατότητα ελέγχου του οποιαδήποτε στιγμή μέσω του αντίστοιχου «δημόσιου» κλειδιού, ένα τέτοιο ασύμμετρο κρυπτοσύστημα τύπου RSA ικανοποιεί επιπλέον και την απαίτηση της πιστοποίησης σε μια εξ αποστάσεως ηλεκτρονική ψηφοφορία. Έτσι, για την ταυτοποίηση του κάθε ψηφοφόρου εξ αποστάσεως, το μόνο που απαιτείται είναι το διαθέσιμο «δημόσιο» κλειδί του να φέρει την ψηφιακή υπογραφή (πιστοποίηση εγκυρότητας) από την εκάστοτε αρμόδια ανώτατη αρχή πιστοποίησης-ταυτοποίησης των ψηφοφόρων. Η απαραίτητη υποδομή για την αποθήκευση και τη διαθεσιμότητα των «δημόσιων» κλειδιών όλων των χρηστών του συστήματος συνήθως αναφέρεται ως «Υποδομή Δημόσιων Κλειδιών» (Public Key Infrastructure – PKI) και μπορεί να είναι είτε δημόσια είτε ιδιωτική, επίσημα θεσμοθετημένη ή ανεπίσημη ως ένα απλό συνεργατικό δίκτυο (π.χ. η ελεύθερα προσβάσιμη υπηρεσία PKI του MIT).



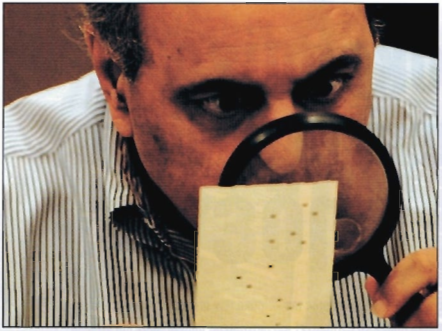
Η πλειοψηφία των πρωτοκόλλων επικοινωνίας στο διαδίκτυο, σήμερα, διατηρεί τη μορφή «βασισμένη σε κείμενο» (plaintext format) για τη μεταφορά δεδομένων, κυρίως για λόγους συμβατότητας με παλαιότερα συστήματα. Ακόμη και έτσι, με τη χρήση κατάλληλων κρυπτογραφικών πρωτοκόλλων, τα περιεχόμενα των μηνυμάτων είναι «αναγνώσιμα» ως εκτυπώσιμο κείμενο, όμως τα δεδομένα που μεταφέρουν είναι δισσοφαλισμένα με τους ισχυρότερους αλγορίθμους κρυπτογράφησης. Στον παγκόσμιο ιστό (World Wide Web – WWW) οι ηλεκτρονικές αγορές ή οι ηλεκτρονικές τραπεζικές συναλλαγές διεξάγονται με αυτόν τον τρόπο, μέσω ασφαλών πρωτοκόλλων και μηχανισμών (SSL/TLS, πρωτόκολλο «https» αντί «http»).

Αξίζει επιπλέον να σημειωθεί ότι η αρμόδια αρχή πιστοποίησης έχει πρόσβαση μόνο στο «δημόσιο» κλειδί κάποιου προς πιστοποίηση χρήστη του συστήματος – το «ιδιωτικό» κλειδί δημιουργείται και παραμένει πάντοτε μυστικό και γνωστό μόνο στον κάτοχό του. Πρακτικά, η έννοια της πιστοποίησης ενός ψηφοφόρου στις τυπικές (μη ηλεκτρονικές) διαδικασίες ψηφοφορίας περιλαμβάνει αντίστοιχο «δημόσιο κλειδί», δηλαδή βιομετρικά και μη βιομετρικά χαρακτηριστικά του ατόμου που (ειδικά τα πρώτα) είναι αρκετά δύσκολο να αντιγραφούν και να χρησιμοποιηθούν από τρίτο, καθώς και «υπογραφή» (πιστοποίηση εγκυρότητας-αξιοπιστίας) από την αρμόδια αρχή, δηλαδή ειδικά χαρτί, σήμανση, σφραγίδες, κλπ. Ο τρόπος που λειτουργούν τα ψηφιακά πιστοποιητικά είναι παρόμοιος, με τη βασική όμως διαφορά ότι το αντίστοιχο «ιδιωτικό» κλειδί δεν αποκαλύπτεται ποτέ, ούτε στην αρμόδια αρχή πιστοποίησης, αφού κάτι τέτοιο δεν είναι απαραίτητο. Επίσι, θα μπορούσε κάποιος να υποστηρίξει πως ένα σύστημα εξ αποστάσεως ηλεκτρονικής ψηφοφορίας είναι εν γένει περισσότερο ασφαλές σε επίπεδο ταυτοποίησης-πιστοποίησης των ψηφοφόρων. Κάτι τέτοιο όμως δεν είναι γενικά αληθές, καθώς η αξιοπιστία της έγκυρης ταυτοποίησης του ψηφοφόρου έγκειται αποκλειστικά και μόνο στην ασφαλή αποθήκευση (μη διαρροή) και χρήση (όχι από τρίτους) του αντίστοιχου «ιδιωτικού» κλειδιού, που άλλωστε ως ψηφιακό δεδομένο μπορεί εύκολα να αντιγραφεί και να μεταδοθεί αν δεν έχει προστατευθεί σωστά σε τεχνικό επίπεδο. Το γεγονός αυτό καταδεικνύει πάσο η ψηφιακή Παιδεία αποτελεί ίσως τον πιο καθοριστικό παράγοντα σε συστήματα ηλεκτρονικής ψηφοφορίας, εξίσου ή περισσότερο σημαντικό από το επίπεδο ασφάλειας του ίδιου του συστήματος σε καθαρά τεχνικό επίπεδο.

ΕΠΙΛΟΓΟΣ

Είναι, άραγε, η ηλεκτρονική ψηφοφορία πανάκεια στα προβλήματα της συμμετοχικότητας και της αποτελεσματικής διακυβέρνησης στις σύγχρονες κοινωνίες; Μπορεί η εξ αποστάσεως ψηφοφορία μέσω διαδικτύου να θελτιώσει την ποιότητα της δημοκρατίας και του σεοβήματος δικαιοσύνης, πολύ περισσότερο και με σαφώς καθοριστικότερο τρόπο απ' ότι οι λεγόμενες «επαναστάσεις του διαδικτύου» όπως στην Αίγυπτο και στην Τυνησία; Η απάντηση δεν είναι καθόλου εύκολη και απαιτεί μεγάλη προσοχή, καθώς υπάρχει ο κίνδυνος η τεχνολογία να αναδομήσει ως αυτοσκοπός και στον όρο «ηλεκτρονική ψηφοφορία» να δοθεί βάση αποκλειστικά στο πρώτο, παραβλέποντας το δεύτερο (πολύ πιο σημαντικό) συνθετικό.

Από τεχνική άποψη, η δυνατότητα ασφαλούς, αξιόπιστης, ελεύθερης εκλογικής διαδικασίας, με προστασία των ατομικών δικαιωμάτων και του αδιαβλήτου του αποτελέσματος, σαφέστατα υπάρχει εδώ και μερικές δεκαετίες. Με τη χρήση κατάλληλων κρυπτογραφικών μεθόδων, το διαδίκτυο μπορεί να μεταπραπεί σε ανθεκτικά και αδιάβλητα μέσο ασφαλούς μετάδοσης, κατάλληλο για οποιονδήποτε τύπου εξ αποστάσεως ηλεκτρονική ψηφοφορία. Μάλιστα, η NASA έχει ήδη κατασκευάσει από το 1997 ένα παρόμοιο σύστημα ώστε να μπορούν οι αστροναύτες που βρίσκονται σε τροχιά να ψηφίζουν στις εκλογές. Το σύστημα αυτό χρησιμοποιήθηκε για πρώτη φορά από τον αστροναύτη David Wolf το 1997 σε τοπικές εκλογές καθώς ο ίδιος βρισκόταν στον διαστημικό σταθμό Mir, ενώ αργότερα, τον Νοέμβριο του 2004, ο αστροναύτης Leroy Chiao, κυβερνήτης του ΔιεΘνούς Διαστημικού Σταθμού (ISS), έγινε ο πρώτος Αμερικανός που ψήφισε μέσω του ίδιου συστήματος σε προεδρικές εκλογές των ΗΠΑ. Ασφαλή πρωτόκολλα και μέθοδοι μπορούν πράγματι να διασφαλίσουν, με κρυπτογραφικό τρόπο, την αξιοπιστία της πιστοποίησης των συμμετεχόντων σε μια τέτοια διαδικασία, σε βαθμό ταυλάχιστον παρόμοιο ή κα-



Τον Νοέμβριο του 2000, στις προεδρικές εκλογές των ΗΠΑ, η Πολιτεία της Florida υπήρξε το πρώτο ίσως τόσο σημαντικό παράδειγμα εγγενούς δυσκολίας που εμπεριέχει το εγχείρημα της πλήρους αυτοματοποίησης της εκλογικής διαδικασίας με τεχνικά μέσα. Μετά από καταγγελίες για εσφαλμένη καταχώριση ψήφων και σημαντικότατες αστοχίες όσον αφορά τη λειτουργία των μηχανών DRE που χρησιμοποιήθηκαν στα εκλογικά κέντρα, δόθηκε εντολή επανακαταμέτρησης των ψήφων από τα στελέχη των εφορευτικών επιτροπών. Σύντομα διαπιστώθηκε ότι οι προδιαγραφές της μηχανογράφησης, κυρίως το μέγεθος και ο τρόπος σήμανσης των δελτίων με τις καταχωρημένες ψήφους, καθιστούσαν το εγχείρημα αυτό εξαιρετικά δύσκολο και αμφίβολο. Μετά από μία σχεδόν εβδομάδα και με καταμετρημένες μόλις 175.037 από συνολικά 6.000.000 περίπου ψήφους, το ανώτατο δικαστήριο έδωσε εντολή να διακοπεί η επανακαταμέτρηση, επικυρώνοντας ταυτόχρονα τα αρχικά αποτελέσματα, παρότι ήταν βέβαιο ότι η έκβαση στη συγκεκριμένη Πολιτεία ήταν καθοριστική για την εκλογή του επόμενου προέδρου των ΗΠΑ.

Λύτερο απ' ότι τα σημερινά «παραδοσιακά» μέσα ταυτοποίησης.

Παρ' όλα αυτά, είναι εξαιρετικά σημαντικό να μη παραβλέπεται το γεγονός ότι κανένα τεχνολογικό μέσα ή επίτευγμα δεν είναι απόλυτα αξιόπιστο, ούτε απόλυτα προσθάσιμο ή κατανοητό από το σύνολο των ατόμων που εν γένει αφορά. Για τη διεξαγωγή μιας διαδικασίας ψηφοφορίας με τον «παραδοσιακό» τρόπο απαιτούνται κάποια ελάχιστα φυσικά μέσα, όπως για παράδειγμα ψηφοδέλτια, κάλπες, παραβάν (αν πρόκειται για μυστική ψηφοφορία), κλπ., ενώ σε αυτήν μπορεί να συμμετάσχει ουσιαστικά το σύνολο του πληθυσμού. Αντίθετα, σε μια εξ αποστάσεως ηλεκτρονική ψηφοφορία απαιτείται η ύπαρξη υπολογιστών και τηλεπικοινωνιακών δικτύων, ηλεκτρικό ρεύμα (όχι αυτονόητο αγαθό παγκοσμίως) και κυρίως ψηφιακή Παιδεία και ικανότητα χρήσης της αντίστοιχης τεχνολογίας από κάθε ψηφοφόρο. Οι περιορισμοί αυτοί είναι καθοριστικοί, μερικές φορές απαγορευτικοί, τόσο σε πρακτικό όσο και σε νομικό-συνταγματικό επίπεδο, βάσει της αρχής της ισονομίας και της δικαιοσύνης. Για τον λόγο αυτόν, κυρίως, η εξ αποστάσεως ηλεκτρονική ψηφοφορία εξακολουθεί να αποτελεί ένα σημαντικό μεν, αλλά συμπληρωματικό μέσο διεξαγωγής εκλογικών διαδικασιών, ακόμα και στις πιο προηγμένες χώρες του πλανήτη. Άλλωστε, δεν είναι λίγοι αυτοί που υποστηρίζουν την άποψη ότι οι εκλογές ανέκαθεν ήταν και πρέπει να παραμείνουν μια εξόχως «συμμετοχική» διαδικασία, κάτι παραπάνω από την απλή «τεχνική» διαδικασία συλλογής και καταμέτρησης ψήφων, κάθε φορά με τον πιο αποτελεσματικό τρόπο. ■

ΒΙΒΛΙΟΓΡΑΦΙΑ

(1) T. Buchsbaum: E-VOTING: INTERNATION::AL DEVELOPMENTS AND LESSONS LEARNT, Proc. Elec. Voting in Europe Technology, Law, Politics and Society, 2004.

(2) ELECTRONIC VOTING (article), Wikipedia, 15 Apr 2013.

(3) L. H. Nestas, K. J. Hole: BUILDING AND MAINTAINING TRUST IN INTERNET VOTING, IEEE Computer, May 2012, pp. 74-80.

(4) M. Volkamer: EVALUATION OF ELECTRONIC VOTING, Springer, 2009.

(5) R. Celeste, D. Thornburgh, H. Lin: ASKING THE RIGHT QUESTIONS ABOUT ELECTRONIC VOTING, National Academies Press, 2006.

(6) J. Elkiit, P. Svensson: WHAT MAKES ELECTIONS FREE AND FAIR?, J. Democracy, vol.8, no.3, 1997, pp. 32-46.

(7) S. March, M. R. Dibban: THE ROLE OF TRUST IN INFORMATION SCIENCE AND TECHNOLOGY, Ann. Rev. Information Science and Technology, vol.37, no.1, 2003, pp. 465-498.

(8) Q. Feng, L. Sun, L. Liu, Y. Yang, Y. Dai: VOTING SYSTEMS WITH TRUST MECHANISMS IN CYBERSPACE: VULNERABILITIES AND DEFENSES, IEEE Trans. Knowledge and Data Eng., vol.22, no.12, pp. 1766-1779 (Dec 2010).

(9) R. Farquharson: THEORY OF VOTING, Oxford, 1961.

(10) L. F. Cranor, R. K. Cytron: SENSUS: A SECURITY-CONSCIOUS ELECTRONIC POLLING SYSTEM FOR THE INTERNET, Proc. 13th Int. Conf. on System Sci., vol.3, pp. 561-570 (Jan 1997).

(11) O. Cetinkaya, M. L. Koc: PRACTICAL ASPECTS OF DYNAVOTE E-VOTING PROTOCOL, Elec. J. of e-Gov., vol.7, no.4, pp. 327-338 (2009).

(12) M. A. Herschberg: SECURE ELECTRONIC VOTING OVER THE WORLD WIDE WEB, MSc thesis, MIT, 1997.

(13) R. Sampigethaya, R. Poovendran: A FRAMEWORK AND TAXONOMY FOR COMPARISON OF ELECTRONIC VOTING SCHEMES, Elsevier Computers & Security, vol.25, no.2, pp. 137-153.

(14) D. Zissis, D. Lekkas: SECURING E-GOVERNMENT AND E-VOTING WITH AN OPEN CLOUD COMPUTING ARCHITECTURE, Gov. Inf. Quart., vol.28, no.2, pp. 239-251 (Apr 2011).

(15) D. Chaum, P. A. Ryan, S. Schneider: A PRACTICAL VOTER-VERIFIABLE ELECTION SCHEME, 10th European Symposium On Research In Computer Security (ESORICS '05), LNCS 3679: pp. 118-139.

(16) C. Thompson: CAN YOU COUNT ON VOTING MACHINES?, The New York Times, 6 Jan 2008.

(17) S. Kremer, M. Ryan, B. Smyth: ELECTION VERIFIABILITY IN ELECTRONIC VOTING PROTOCOLS, 15th European Symposium on Research in Computer Security (ESORICS '10), LNCS 6345: pp. 389-404.

(18) (2000) FLORIDA ELECTION RECOUNT (article), Wikipedia, 5 Jun 2013.

(19) M. Shamos, A. Yasinsac: REALITIES OF E-VOTING SECURITY, IEEE Security & Privacy, vol.10, no.5, pp. 16-17 (Sept/Oct 2012).

(20) ELECTRONIC VOTING IN ESTONIA (article), Wikipedia, 27 Mar 2013.

www.gnomonpublications.gr

ΤΕΥΧΟΣ 379 • ΟΚΤΩΒΡΙΟΣ 2013 • €7,00

ΠΕΡΙΣΚΟΠΙΟ ΤΗΣ ΕΠΙΣΤΗΜΗΣ

Κοσμική σκόνη

Η αγνοημένη ύλη του γαλαξία

Βιονικός οφθαλμός

Η τεχνολογία που υπόσχεται επαναφορά της όρασης

Τα οφέλη της νηστείας

Το μυστικό της σωματικής και ψυχικής υγείας;

Θερμοκρασίες κάτω από το απόλυτο μηδέν;

Και όμως είναι δυνατόν!

Γιάννης Νίκολης

Ο πρωτοπόρος Έλληνας ερευνητής της Πολυπλοκότητας και του Χάους

Ηλεκτρονική ψηφοφορία εξ αποστάσεως

Αναβιώνοντας την «Εκκλησία του Δήμου» στον 21ο αιώνα