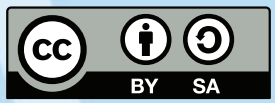
Ηλεκτρονικές Εκλογές με το Σύστημα Ζευς

Πάνος Λουρίδας
Ομάδα Ανάπτυξης Ζευς
louridas@grnet.gr

Εθνικό Δίκτυο Έρευνας και Τεχνολογίας

27 Νοεμβρίου 2013



Το Πρόβλημα

> *Θεωρώ εντελώς ασήμαντο ποιος από το κόμμα θα ψηφίσει, ή πώς· αλλά αυτό που είναι εξαιρετικά σημαντικό είναι το εξής—ποιος θα μετρήσει τις ψήφους, και πώς.*

Γιόζεφ Στάλιν

Στο πρωτότυπο: Я считаю, что совершенно неважно, кто и как будет в партии голосовать; но вот что чрезвычайно важно, это—кто и как будет считать голоса.

Ειπώθηκε το 1923, σύμφωνα με τα «Απομνημονεύματα του Πρώην Γραμματέα του Στάλιν» (1992), του Μπόρις Μπαζάνοφ [Αγία Πετρούπολη] (Борис Бажанов. Воспоминания бывшего секретаря Сталина).

Εναλλακτική (ελεύθερη) μετάφραση: Οι ψηφοφόροι δεν αποφασίζουν τίποτε. Αυτοί που μετράν τις ψήφους αποφασίζουν τα πάντα.

Quis Custodiet Ipsos Custodes?

Ποιος φυλάει τους φύλακες;

> *audio quid ueteres olim moneatis amici,*
> *“pone seram, cohibe.” sed quis custodiet ipsos*
> *custodes? cauta est et ab illis incipit uxor.*

Ιουβενάλιος Δέκιμος Ιούνιος (1ος αιώνας μ.Χ.), Σάτιρα VI, 346–348
Ή στα ελληνικά:

> *Ακούω πάντα την προειδοποίηση των φίλων μου,*
> *«δέσε την, συμμάζεψέ την». Αλλά ποιος μπορεί*
> *να φυλάξει τους φύλακες; Η γυναίκα προβλέπει*
> *και ξεκινάει απ’ αυτούς.*

Ποιος Φυλάει τους Φύλακες;

ἀλλὰ μὴν μέθη γε φύλαξιν ἀπρεπέστατον καὶ μαλακία καὶ ἀργία.

Πλάτων, Πολιτεία, Βιβλίο 3, 398e

γελοῖον γάρ, ἦ δ' ὅς, τόν γε φύλακα φύλακος δεῖσθαι.

Πλάτων, Πολιτεία, Βιβλίο 3, 403e

Η Πρόκληση

Μπορούμε να φτιάξουμε ένα σύστημα ηλεκτρονικής ψηφοφορίας στο οποίο να μην χρειάζεται να μας εμπιστεύονται οι χρήστες του;

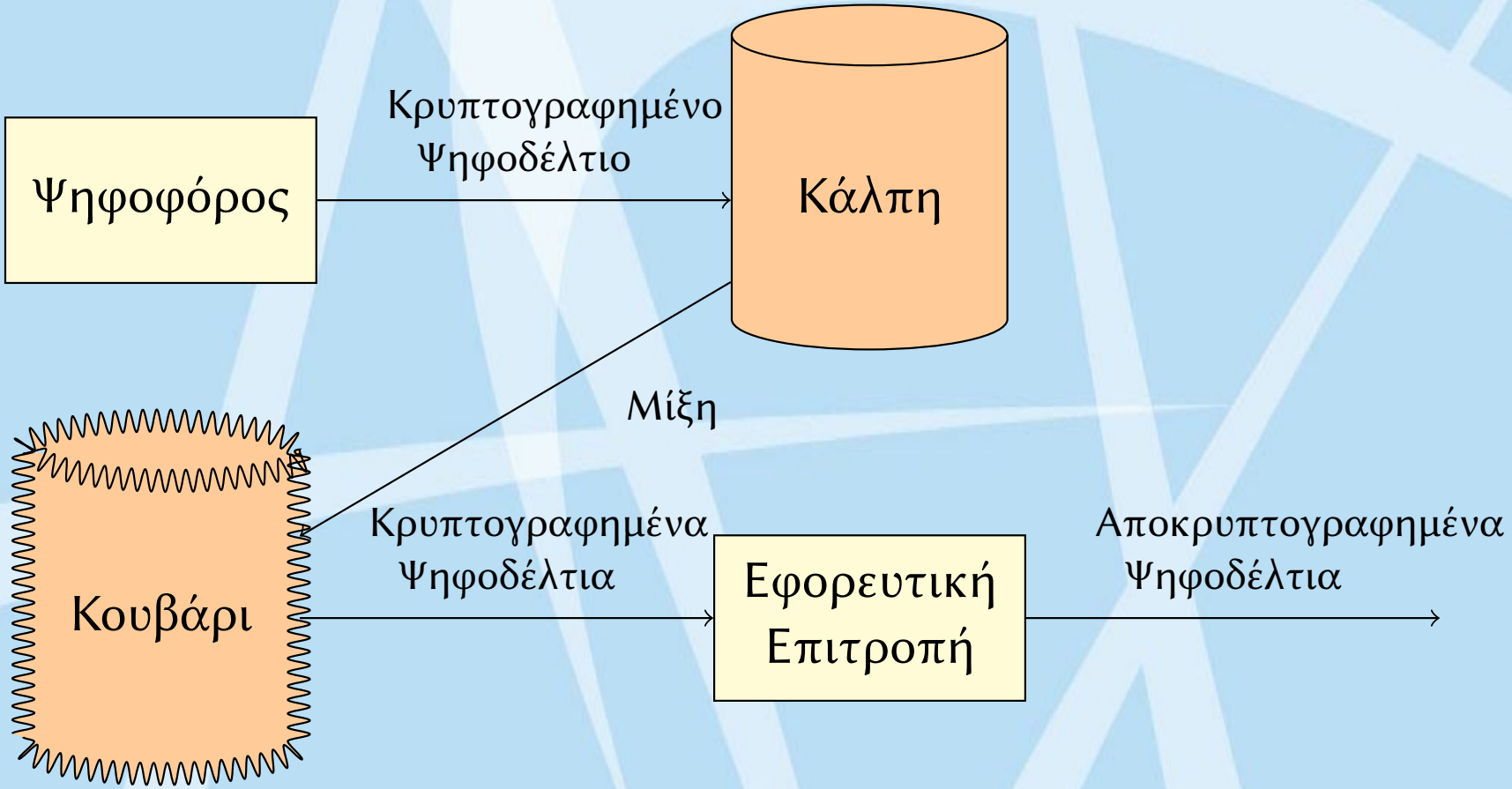
Δυνατότητες Συστήματος Ζευς

- Όλη η διαδικασία της ψηφοφορίας εκτελείται μέσω ενός τυπικού web browser (ακόμα και μέσω ταμπλέτας ή κινητού τηλεφώνου).
- Δεν απαιτούνται ιδιαίτερες δεξιότητες ούτε από τη μεριά του ψηφοφόρου ούτε από τη μεριά της εφορευτικής επιτροπής.
- Η εφορευτική επιτροπή, όπως και στις παραδοσιακές εκλογές, είναι υπεύθυνη για το σύνολο της διαδικασίας.
- Το σύστημα παρέχει μαθηματικές εγγυήσεις για την ανωνυμία της ψήφου και την επαλήθευση της καταμέτρησης.
- Το σύστημα μπορεί να υποστηρίξει κάθε είδους εκλογικό σύστημα, κάθε είδους ψηφοδελτία, ακόμα και write-in ballots (όπου δεν υπάρχουν μόνο προϋπάρχουσες επιλογές).

Helios

- Helios: Επαληθεύσιμες ηλεκτρονικές εκλογές από το 2008.
- Ανοικτός κώδικας `http://heliosvoting.org/`.
- Ο σχεδιασμός της έκδοσης 1 του Helios χρησιμοποιήθηκε ως βάση για το σχεδιασμό της εκλογικής διαδικασίας στο σύστημα Ζευς.
- Η έκδοση 3 του Helios χρησιμοποιήθηκε ως βάση για την υλοποίηση του συστήματος Ζευς.
- Αυτή τη στιγμή ο κώδικας του Helios στο Ζευς είναι λιγότερο από 50% του συνολικού κώδικα (και περιλαμβάνει κομμάτια που δεν χρησιμοποιούνται καθόλου).

Διαδικασία Εκλογών



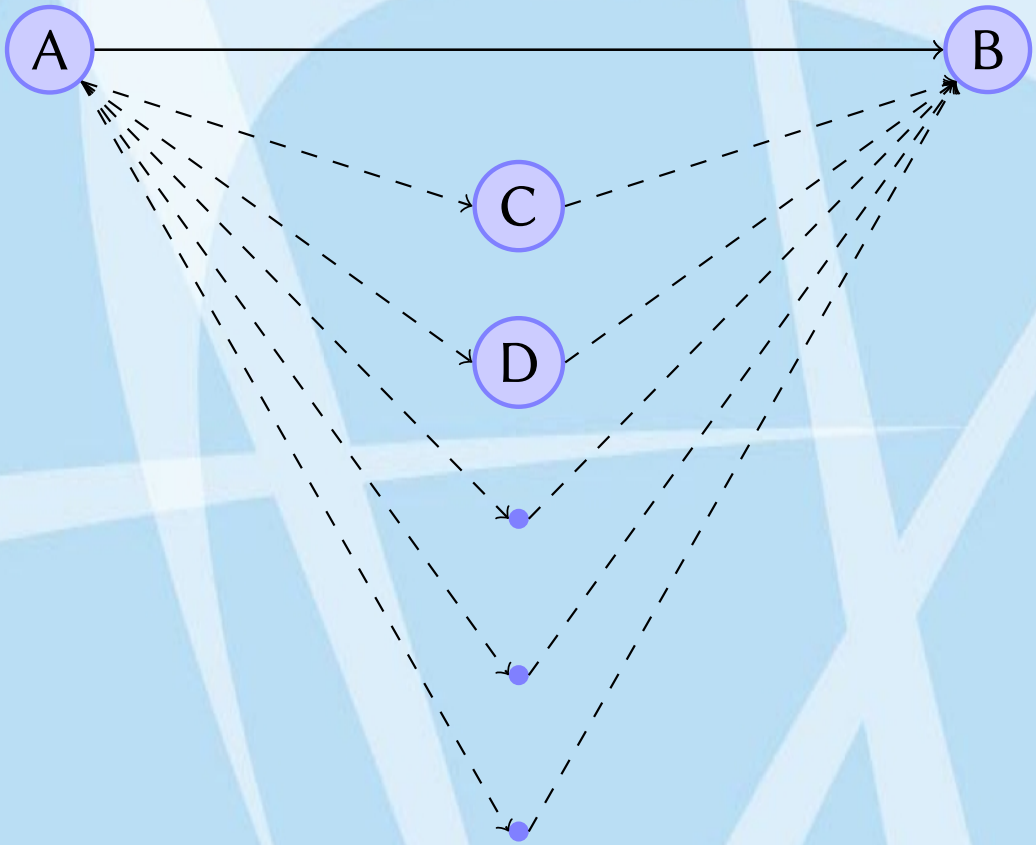
Βασικές Ιδέες

- Τα ψηφοδέλτια κρυπτογραφούνται στον υπολογιστή του ψηφοφόρου πριν σταλούν στο Ζευς.
- Τα ψηφοδέλτια αποθηκεύονται στο Ζευς κρυπτογραφημένα.
- Τα κλειδιά της αποκρυπτογράφησης κρατούνται από την Εφορευτική Επιτροπή + ένα κλειδί που κρατά το Ζευς.
- Τα κρυπτογραφημένα ψηφοδέλτια ανακατεύονται ώστε να χαθεί η συσχέτιση μεταξύ ψηφοδελτίων και ψηφοφόρων.
- Τα κρυπτογραφημένα ψηφοδέλτια αποκρυπτογραφούνται από την Εφορευτική Επιτροπή και το Ζευς.
- Η όλη διαδικασία μπορεί να επαληθευτεί μαθηματικά.

Συστατικά Στοιχεία

1. ElGamal για την παραγωγή των κλειδιών.
2. ElGamal για την κρυπτογράφηση, επανακρυπτογράφηση, αποκρυπτογράφηση.
3. Δίκτυα Μίξης (mixnets) για το ανακάτεμα των ψήφων.
4. Απόδειξη Μηδενικής Γνώσης (Zero Knowledge Proof) για την επαλήθευση της μίξης.

Απόδειξη Μηδενικής Γνώσης



Δίκτυα Μίξης

- Ένα Δίκτυο Μίξης είναι απλώς ένα σύνολο από μίξεις.
- Τα ψηφοδέλτια επανακρυπτογραφούνται και αναμιγνύονται.
- Αυτή η τυχαία μίξη καταστρέφει τη συσχέτιση μεταξύ των ψηφοφόρων και των φήφων τους.
- Εντούτοις, οι ψηφοφόροι μπορούν να επαληθεύσουν ότι η ψήφος τους μετρήθηκε, μέσω μιας Απόδειξης Μηδενικής Γνώσης!

Βασικές Παραδοχές

- Δεν χρειάζεται να εμπιστευτούμε τους διαχειριστές του Ζευς.
- Δεν χρειάζεται να εμπιστευτούμε κάθε μέλος της Εφορευτικής Επιτροπής.
- Πρέπει ένα τουλάχιστον μέλος της Εφορευτικής Επιτροπής ή οι διαχειριστές του Ζευς να είναι έντιμοι.
- Οι ψηφοφόροι δεν μπορούν να εξαναγκαστούν κατά την άσκηση του εκλογικού τους δικαιώματος γιατί μπορούν να ψηφίσουν όσες φορές θέλουν (αλλά μόνο η τελευταία φορά μετράει).

- Μέχρι σήμερα έχει χρησιμοποιηθεί σε περισσότερες από 120 εκλογές στην Ελλάδα.
- Οι μέχρι τώρα εκλογές αφορούσαν πάνω από 22.000 ψηφοφόρους.
- Εκλογές εξακολουθούν να διεξάγονται συνεχώς.
- Νέες εκλογές προγραμματίζονται τους επόμενους μήνες.

Σύνοψη

- Οι ηλεκτρονικές ψηφοφορίες δεν είναι κάτι τετριμμένο αλλά είναι εφικτές.
- Μπορούμε να υποστηρίξουμε κάθε είδους εκλογές, όπως και κάθε είδους εκλογικό σύστημα.
- Βασιστήκαμε σε υπάρχουσα, στιβαρή δουλειά όπου ήταν δυνατόν, αντί να ξανα-εφεύρουμε τον τροχό.
- Οι ηλεκτρονικές ψηφοφορίες απαιτούν εξίσου μεγάλη προσοχή στην οργάνωση της διαδικασίας, όσο και στην υλοποίηση.

- Το Ζευς ζει στο: `http://zeus.minedu.gov.gr`
- Ο κώδικας βρίσκεται στο: `https://github.com/grnet/zeus`