Ηλεκτρονικές Εκλογές με το Σύστημα Ζευς

Πάνος Λουρίδας, louridas@grnet.gr
Γιώργος Τσουκαλάς, gtsouk@grnet.gr
Κώστας Παπαδημητρίου, kpap@grnet.gr

Εθνικό Δίκτυο Έρευνας και Τεχνολογίας

20 & 21 Απριλίου 2013 / 6ο Συνέδριο Κοινοτήτων Ανοιχτού Λογισμικού
FOSSCOMM 2013

Outline

Επισκόπηση

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).

Επαλήθευση

> *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.

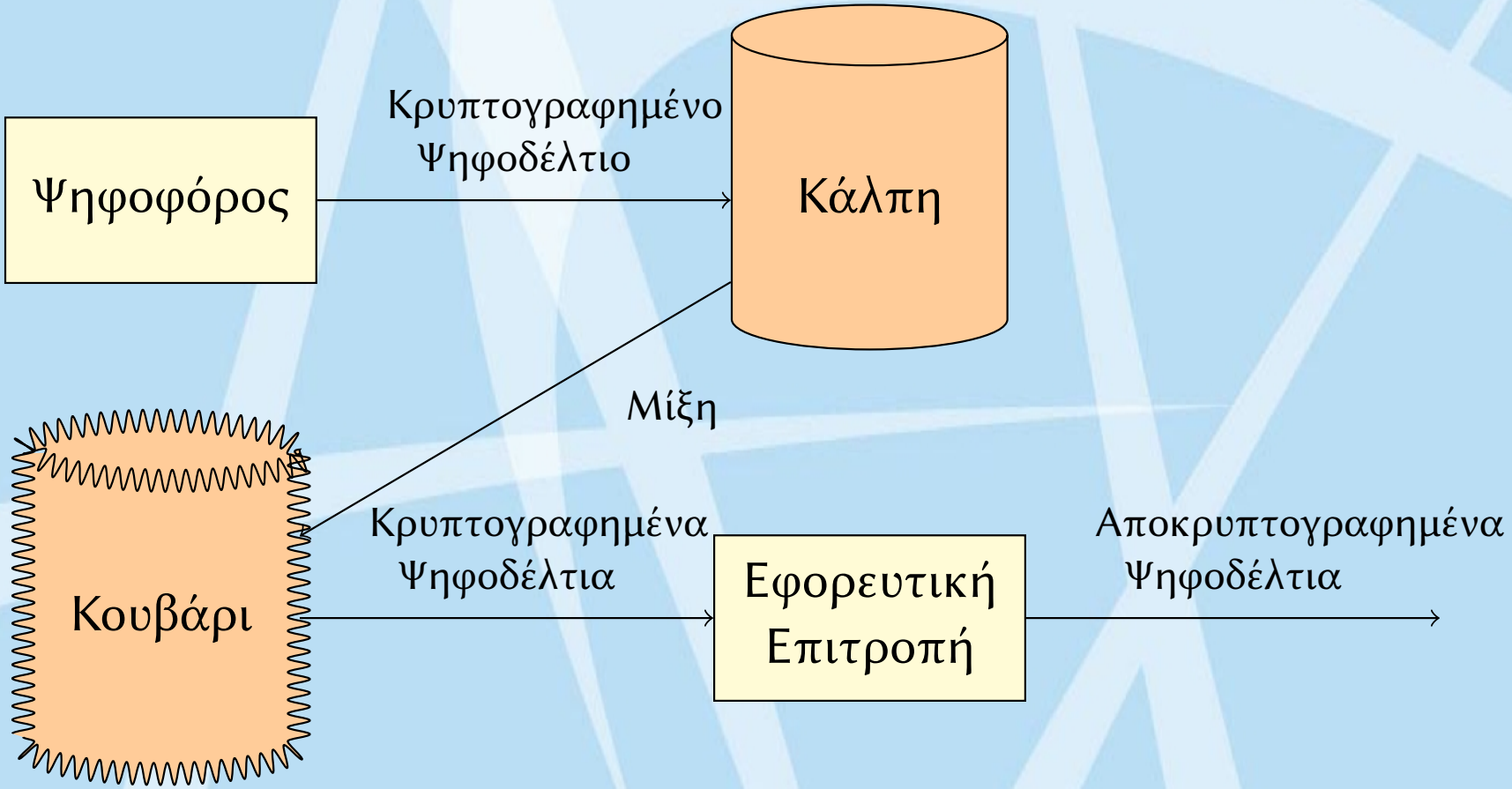
Ειπώθηκε το 1923, σύμφωνα με τα «Απομνημονεύματα του Πρώην Γραμματέα του Στάλιν» (1992), του Μπόρις Μπαζάνοφ [Αγία Πετρούπολη] (Борис Бажанов. Воспоминания бывшего секретаря Сталина).

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

Επαλήθευση

- Ατομική επαλήθευση: κάθε ψηφοφόρος μπορεί να επαληθεύσει την ψήφο του.
- Επαλήθευση μέσω εκπροσώπου: κάθε ψηφοφόρος μπορεί να αναθέσει σε έναν τρίτο την επαλήθεση της ψήφου του (χωρίς να αποκαλύπτει τι ψήφισε).
- Καθολική επαλήθεση: οποιοσδήποτε μπορεί να επαληθεύσει το τελικό αποτέλεσμα.

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.

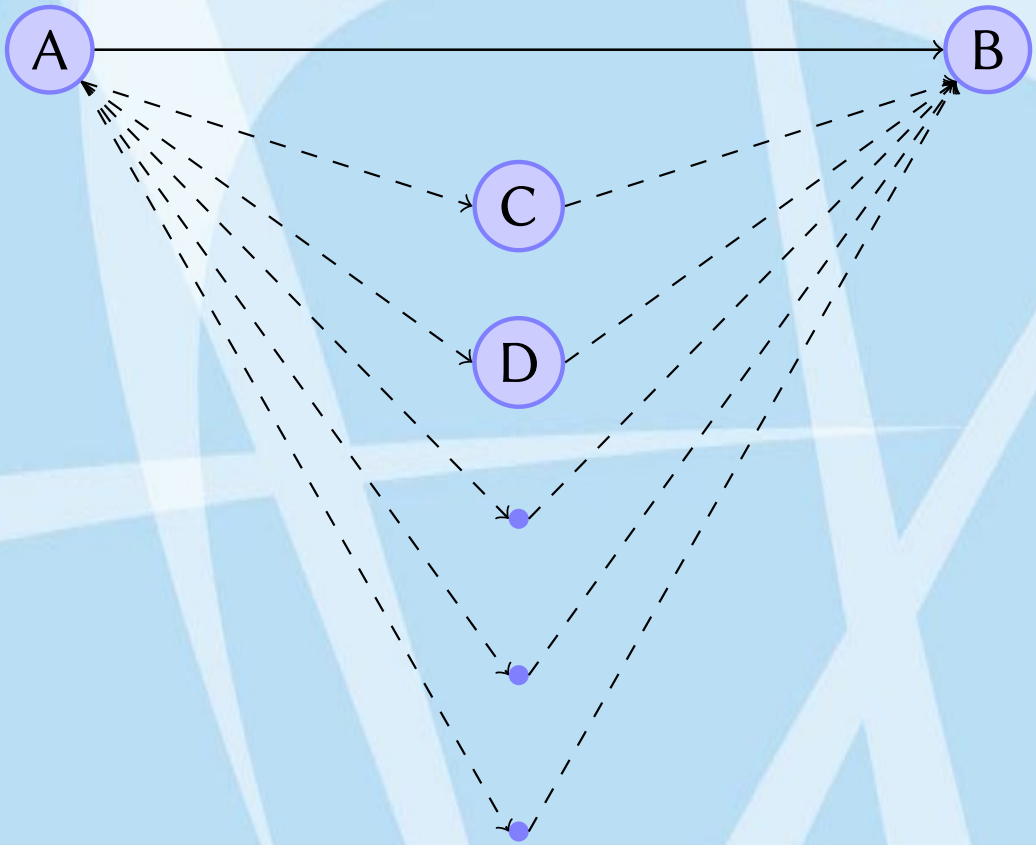
Βασικές Παραδοχές

- 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).

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!

Επισκόπηση

Γιατί όχι το Helios;

- Το Helios, μετά την έκδοση 1, συνδυάζει την καταμέτρηση με την εξαγωγή αποτελεσμάτων.
- Αυτό σημαίνει ότι δεν μπορεί να χρησιμοποιηθεί για εκλογικά συστήματα όπως η ταξινομική ψήφος (Singe Transferable Vote, STV), δηλαδή συστήματα όπου όλο το ψηφοδέλτιο, και όχι μόνο οι επιμέρους επιλογές σε αυτό, πρέπει να χρησιμοποιηθούν στην εξαγωγή των αποτελεσμάτων.
- Απαιτούνταν βελτιώσεις στη διεπαφή με τον χρήστη.

Το Ζευς Διαχωρίζει την Καταμέτρηση από την Εξαγωγή Αποτελεσμάτων

Θεώρημα

Μπορούμε να έχουμε ασφαλείς εκλογές ακόμα και αν διαχωρίσουμε την καταμέτρηση από την εξαγωγή των αποτελεσμάτων.

Απόδειξη.

1. Η καταμέτρηση μπορεί να επαληθευτεί, χρησιμοποιώντας τα ίδια μαθηματικά εργαλεία με το Helios.
2. Η παραγωγή των τελικών αποτελεσμάτων μπορεί να επαληθευτεί αφού γίνεται με ανοικτή διαδικασία. Έτσι το σύνολο της εκλογικής διαδικασίας μπορεί να επαληθευτεί. □

Το Ζευς Διαχωρίζει την Καταμέτρηση από την Εξαγωγή Αποτελεσμάτων

Θεώρημα

Μπορούμε να έχουμε ασφαλείς εκλογές ακόμα και αν διαχωρίσουμε την καταμέτρηση από την εξαγωγή των αποτελεσμάτων.

Απόδειξη.

1. Η καταμέτρηση μπορεί να επαληθευτεί, χρησιμοποιώντας τα ίδια μαθηματικά εργαλεία με το Helios.
2. Η παραγωγή των τελικών αποτελεσμάτων μπορεί να επαληθευτεί αφού γίνεται με ανοικτή διαδικασία. Έτσι το σύνολο της εκλογικής διαδικασίας μπορεί να επαληθευτεί. □

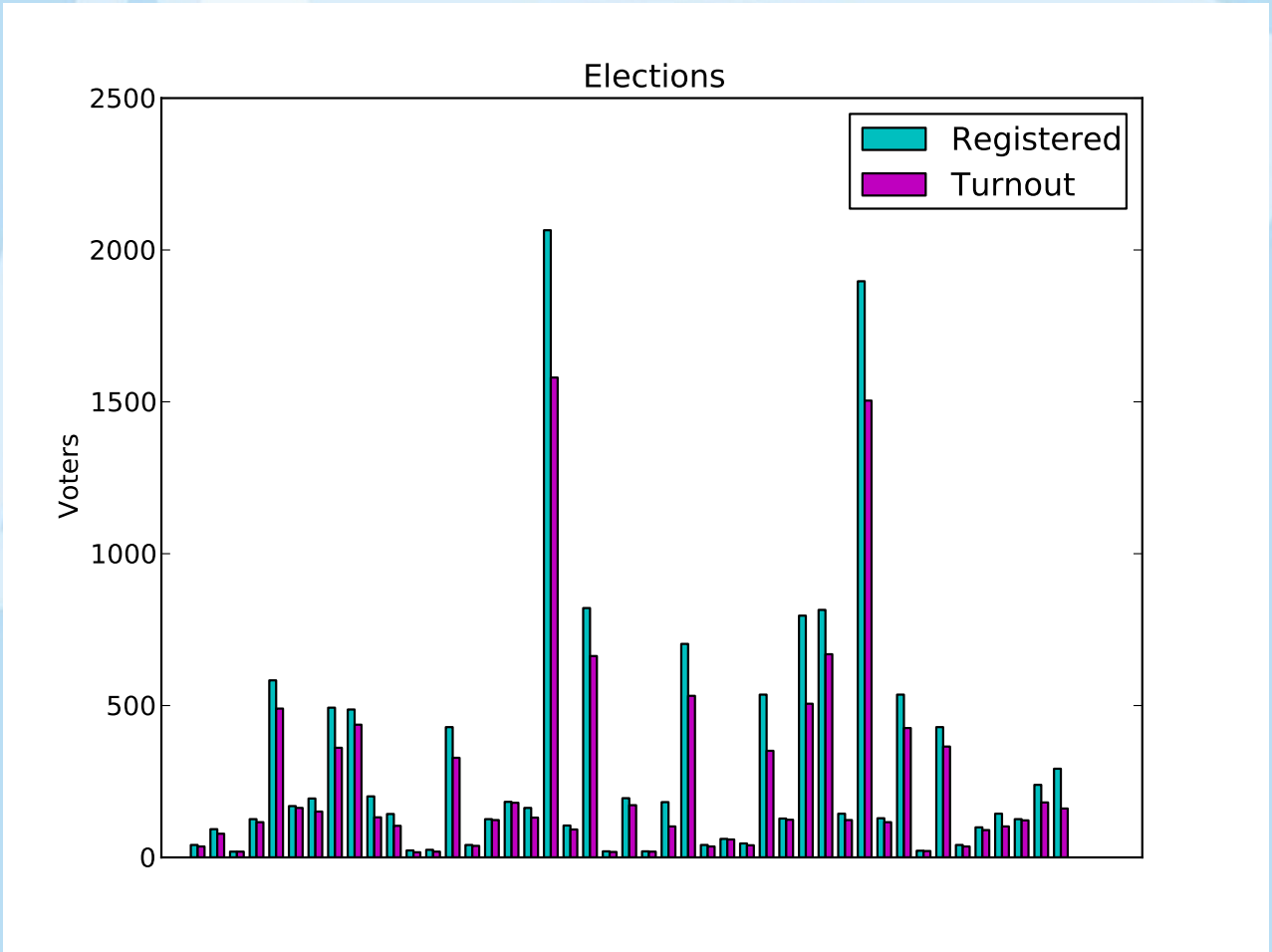
Η Γέννηση του Ζευς

- Χρησιμοποιεί τη βασική ιδέα του Helios, αλλά με σημαντικές προσθήκες και αλλαγές.
- Μπορεί να υποστηρίξει οποιοδήποτε τύπο εκλογών.
- Βελτιωμένη διεπαφή με τον χρήστη, τόσο για τους ψηφοφόρους όσο και για την Εφορευτική Επιτροπή, βάσει των σχολίων που λάβαμε από τους χρήστες.
- Έχει χρησιμοποιηθεί σε πολλές εκλογές, με χιλιάδες ψηφοφόρων, με διαφορετικά εκλογικά συστήματα.
- Η μίξη μπορεί να κλιμακωθεί εύκολα, γιατί είναι εντελώς παραλληλοποίησιμη (embarrassingly parallel).

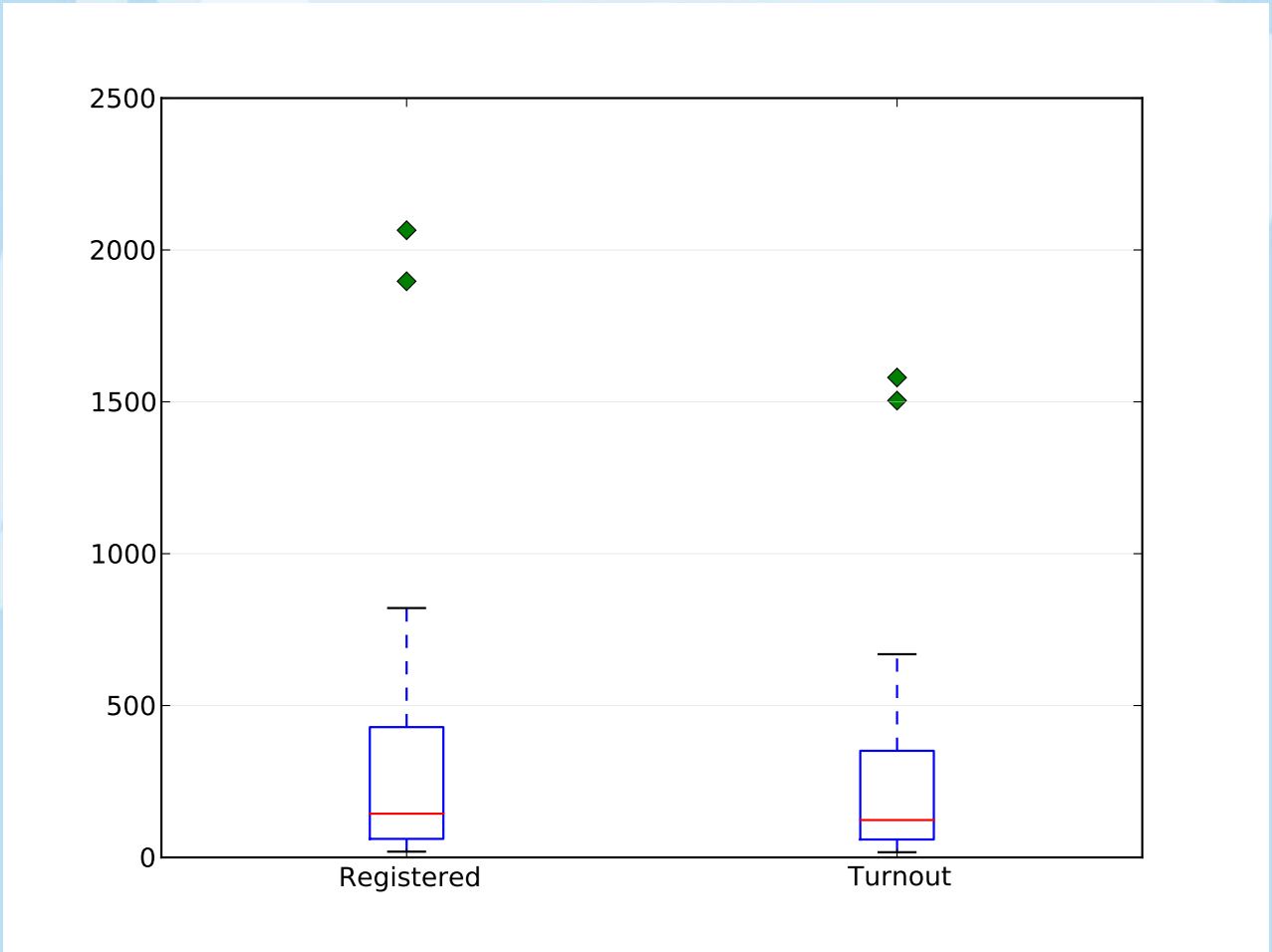
Επισκόπηση

- Μέχρι τις 18/04/2012 το σύστημα Ζευς είχε χρησιμοποιηθεί σε 45 εκλογές στην Ελλάδα.
- Το σύνολο των εγγεγραμμένων ψηφοφόρων ήταν 14.171, ενώ οι ψηφίσαντες ήταν 11.133.
- Στις πρώτες 23 ψηφοφορίες (όπου υπήρχαν αντιδράσεις) το ποσοστό συμμετοχής ήταν 80.76%.

Πραγματοποιηθήσες Εκλογές



Πραγματοποιηθήσες Εκλογές



Σύνοψη

- Οι ηλεκτρονικές ψηφοφορίες δεν είναι εύκολη υπόθεση αλλά είναι εφικτές.
- Βασιστήκαμε σε υπάρχουσα, στιβαρή δουλειά όπου ήταν δυνατόν, αντί να ξανα-εφεύρουμε τον τροχό.
- Ο όγκος της υλοποίησης είναι σημαντικός, όταν πρέπει να προχωρήσει κανείς πέρα από την υπάρχουσα κατάσταση.
- 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`

Ψάχνουμε κόσμο.

- Διαχειριστές συστημάτων Linux με γνώσεις προγραμματισμού.
- Αλλά και προγραμματιστές.
- Επικοινωνήστε με τον Ανδρέα Πολυράκη, apolyr@noc.grnet.gr.