# Το Σύστημα Ζευς

Ομάδα Ανάπτυξης Ζευς

Εθνικό Δίκτυο Έρευνας και Τεχνολογίας

24 Μαΐου 2017

# Υπάρχουν Πλεονεκτήματα;

## Ναι, Υπάρχουν

- Μεγάλη εμπειρία—πόσο καιρό ψηφίζουμε με παραδοσιακά ψηφοφέλτια;
- Δεν χρειάζεται κάποια συγκεκριμένη τεχνολογία—βολεύει τους διοργανωτές.
- Δεν χρειάζονται κάποιες συγκεκριμένες δεξιότητες—αρκεί το πολύ η γραφή και η ανάγνωση.
- Υπάρχει μια χειροπιαστή απόδειξη—το ψηφοδέλτιο.
- Μπορεί στον κόσμο να αρέσει η διαδικασία της ψηφοφορίας.

# Αλλά...

## Αν κάτι πάει στραβά;

- Μπορώ να αποδείξω ότι ψήφισα; Ναι.
- Είναι η ψήφος μου ανώνυμη; Ναι.
- Έχουν μετρηθεί όλοι οι ψήφοι; Ναι.
- Έχει καταμετρηθεί η ψήφος μου; Ναι.
- Μπορούμε να προσθέσουμε ψήφους; Όχι.
- Μπορούμε να παραποιήσουμε ψήφους; Όχι.

# Αλλά...

## Αν κάτι πάει στραβά;

- Μπορώ να αποδείξω ότι ψήφισα; Ναι.
- Είναι η ψήφος μου ανώνυμη; Ναι.
- Έχουν μετρηθεί όλοι οι ψήφοι; Ναι.
- Έχει καταμετρηθεί η ψήφος μου; Ναι.
- Μπορούμε να προσθέσουμε ψήφους; Όχι.
- Μπορούμε να παραποιήσουμε ψήφους; Όχι.

# Αλλά...

## Αν κάτι πάει στραβά;

- Μπορώ να αποδείξω ότι ψήφισα; Ναι.
- Είναι η ψήφος μου ανώνυμη; Ναι.
- Έχουν μετρηθεί όλοι οι ψήφοι; Ναι.
- Έχει καταμετρηθεί η ψήφος μου; Ναι.
- Μπορούμε να προσθέσουμε ψήφους; Όχι.
- Μπορούμε να παραποιήσουμε ψήφους; Όχι.

# Αλλά...

## Αν κάτι πάει στραβά;

- Μπορώ να αποδείξω ότι ψήφισα; Ναι.
- Είναι η ψήφος μου ανώνυμη; Ναι.
- Έχουν μετρηθεί όλοι οι ψήφοι; Ναι.
- Έχει καταμετρηθεί η ψήφος μου; Ναι.
- Μπορούμε να προσθέσουμε ψήφους; Όχι.
- Μπορούμε να παραποιήσουμε ψήφους; Όχι.

# Αλλά...

## Αν κάτι πάει στραβά;

- Μπορώ να αποδείξω ότι ψήφισα; Ναι.
- Είναι η ψήφος μου ανώνυμη; Ναι.
- Έχουν μετρηθεί όλοι οι ψήφοι; Ναι.
- Έχει καταμετρηθεί η ψήφος μου; Ναι.
- Μπορούμε να προσθέσουμε ψήφους; Όχι.
- Μπορούμε να παραποιήσουμε ψήφους; Όχι.

# Αλλά...

## Αν κάτι πάει στραβά;

- Μπορώ να αποδείξω ότι ψήφισα; Ναι.
- Είναι η ψήφος μου ανώνυμη; Ναι.
- Έχουν μετρηθεί όλοι οι ψήφοι; Ναι.
- Έχει καταμετρηθεί η ψήφος μου; Ναι.
- Μπορούμε να προσθέσουμε ψήφους; Όχι.
- Μπορούμε να παραποιήσουμε ψήφους; Όχι.

# Αλλά...

## Αν κάτι πάει στραβά;

- Μπορώ να αποδείξω ότι ψήφισα; Ναι.
- Είναι η ψήφος μου ανώνυμη; Ναι.
- Έχουν μετρηθεί όλοι οι ψήφοι; Ναι.
- Έχει καταμετρηθεί η ψήφος μου; Ναι.
- Μπορούμε να προσθέσουμε ψήφους; Όχι.
- Μπορούμε να παραποιήσουμε ψήφους; Όχι.

# Παραδοχές

## Τι Θεωρούμε Δεδομένο

- Η εκλογική αρχή είναι έμπιστη και ανεξάρτητη.
- Το πολιτικό κλίμα ευνοεί τη διεξαγωγή των εκλογών.
- Έχουμε λύσει τα διαδικαστικά και οργανωτικά προβλήματα (ή πρέπει να φωνάξουμε διεθνείς παρατηρητές).

# Παραδοχές

## Τι Θεωρούμε Δεδομένο

- Η εκλογική αρχή είναι έμπιστη και ανεξάρτητη.
- Το πολιτικό κλίμα ευνοεί τη διεξαγωγή των εκλογών.
- Έχουμε λύσει τα διαδικαστικά και οργανωτικά προβλήματα (ή πρέπει να φωνάξουμε διεθνείς παρατηρητές).

# Παραδοχές

## Τι Θεωρούμε Δεδομένο

- Η εκλογική αρχή είναι έμπιστη και ανεξάρτητη.
- Το πολιτικό κλίμα ευνοεί τη διεξαγωγή των εκλογών.
- Έχουμε λύσει τα διαδικαστικά και οργανωτικά προβλήματα (ή πρέπει να φωνάξουμε διεθνείς παρατηρητές).

# Τότε Γιατί Ηλεκτρονική Ψήφο;

## Προβλήματα με την Παραδοσιακή

- Η διοργάνωση δεν είναι εύκολη.
- Κόστος.
- Δεν μπορούν όλοι να πάνε να ψηφίσουν.
- Η καταμέτρηση μπορεί να διαρκέσει πολύ και είναι βαρετή.
- Τα ψηφοδέλτια είναι ευαίσθητα σε καταστροφές (όπως φωτιά, νερό, κλοπή, βανδαλισμοί, ...).

# Δημοκρατικό

- Μόνο όσοι έχουν δικαίωμα ψήφου μπορούν να ψηφίσουν.
- Οι έχοντες το δικαίωμα ψήφου έχουν μία ψήφο (που να μετράει).

Πηγή: http://courses.csail.mit.edu/6.897/spring04/L17.pdf

# Ανωνυμία

- Κανείς δεν μπορεί να βρει τι ψήφισε ένας ψηφοφόρος (τουλάχιστον αν υπάρχουν αρκετοί ψηφοφόροι).
- Είναι OK (ίσως και υποχρεωτικό) να δημοσιεύεται η λίστα των ψηφισάντων (αλλά φυσικά όχι τι ψήφισε ο καθένας).

# Αδιάβλητο

- Ο ψηφοφόρος δεν μπορεί να εξαναγκαστεί ή να εξαγοραστεί ώστε να ψηφίσει με έναν συγκεκριμένο τρόπο.
- Ο ψηφοφόρος δεν μπορεί να αποδείξει σε έναν τρίτο τι ψήφισε.

# Ακρίβεια

Τα αποτελέσματα της καταμέτρησης είναι το ορθό άθροισμα των φήφων.

- Τα ψηφοδέλτια δεν μπορούν να αλλοιωθούν, να εξαφανιστούν, ή να αντικατασταθούν.
- Όλα τα ψηφοδέλτια καταμετρώνται· τυχόν άλλα (άκυρα) ψηφοδέλτια δεν μπορούν να προστεθούν σε αυτά.

# Επαληθευσιμότητα

> *Θεωρώ εντελώς ασήμαντο ποιος στο κόμμα θα ψηφίσει, ή τι θα ψηφίσει· αλλά αυτό που είναι εξαιρετικά σημαντικό είναι το εξής—ποιος θα καταμετρήσει τους ψήφους, και ποιος.*

Joseph Stalin
In Russian: 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, όπως αναφέρεται στα Απομνημονεύματα του Πρώην Γραμματέα του Στάλιν Μπόρις Μπαζάνοφ, Αγία Πετρούπολη, 1992. (Борис Бажанов. Воспоминания бывшего секретаря Сталина).
Ελεύθερη μετάφραση: Οι ψηφοφόροι δεν αποφασίζουν τίποτε. Οι καταμετρητές αποφασίζουν τα πάντα.

# Επαληθευσιμότητα

- Ατομική επαληθευσιμότητα: κάθε ψηφοφόρος μπορεί να επιβεβαίωση την ψήφο του.
- Αντιπροσωπευτική επαληθευσιμότητα: κάθε ψηφοφόρος μπορεί να αναθέσει σε έναν αντιπρόσωπό του να επιβεβαιώσει την ψήφο του (χωρίς να φανερώσει τι ψήφισε).
- Καθολική επαληθευσιμότητα: όλοι μπορούν να επιβεβαιώσουν το τελικό αποτέλεσμα.

# Αντοχή

- Οι εκλογές δεν μπορούν να παρακωλυθούν από μικρές ομάδες ανθρώπων (ηλεκτρονικές επιθέσεις, κατάχρηση ενστάσεων, ...).

# Ακεραιότητα

- Δεν γνωστοποιούνται μερικά αποτελέσματα πριν το τέλος των εκλογών.

# Ευχρηστία

- Εύκολη διεπαφή χρήστη.
- Υιοθέτηση βέλτιστων πρακτικών αλληλεπίδρασης.
- Προσβάσιμο από διαφορετικές συσκευές (υπολογιστής, ταμπλέτα, κινητό).

# Αποτελεσματικότητα

- Εύκολη διαδικασία ψηφοφορίας.
- Αποτελεσματική διαδικασία καταμέτρησης.

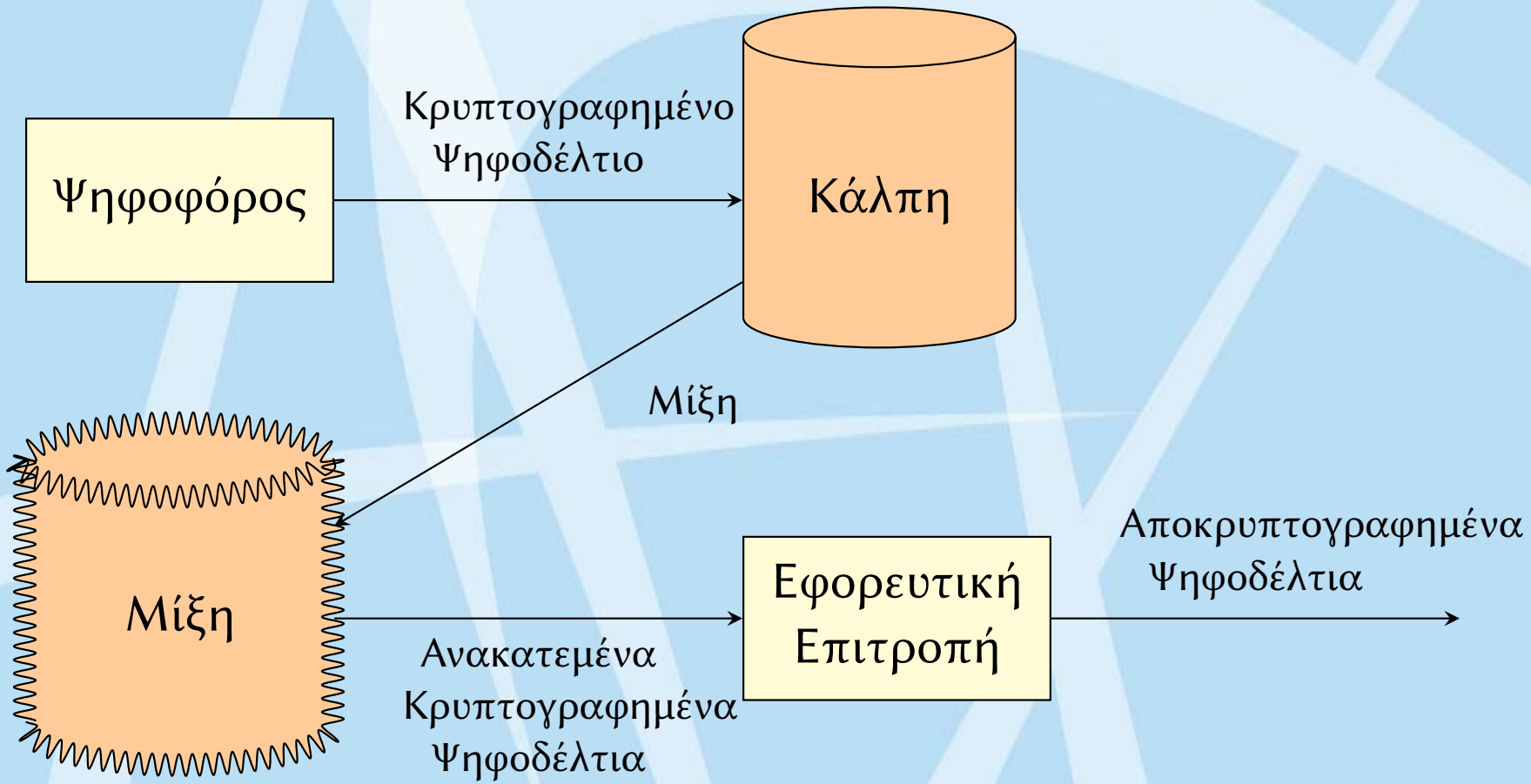
# Δυνατότητες Συστήματος Ζευς

- 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.

# 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

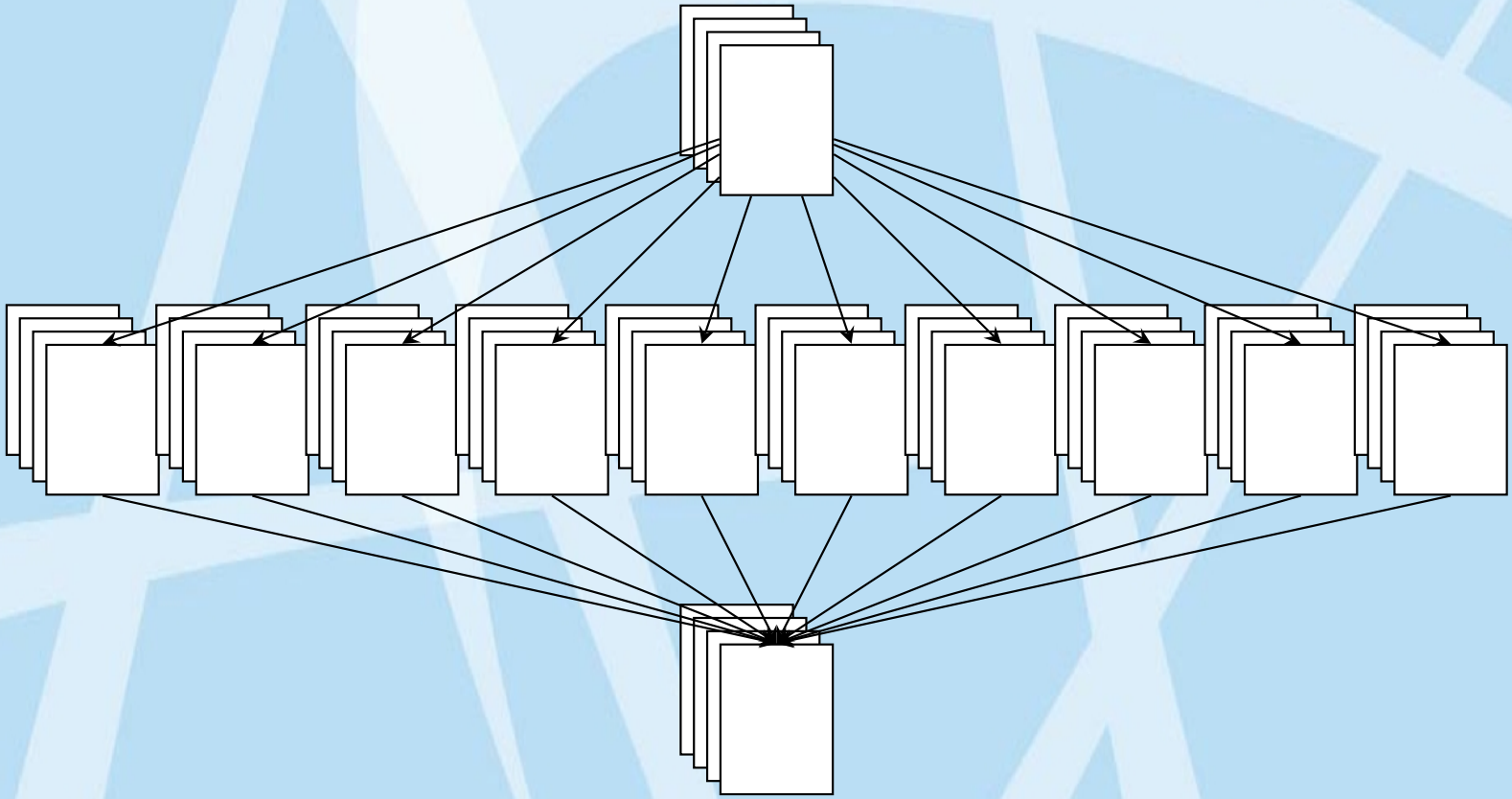
- Τα ψηφοδέλτια κρυπτογραφούνται στον υπολογιστή του ψηφοφόρου πριν σταλούν στο Ζευς.
- Τα ψηφοδέλτια αποθηκεύονται στο Ζευς κρυπτογραφημένα.
- Τα κλειδιά της αποκρυπτογράφησης κρατούνται από την Εφορευτική Επιτροπή + ένα κλειδί που κρατά το Ζευς.
- Τα κρυπτογραφημένα ψηφοδέλτια ανακατεύονται ώστε να 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.

# Επαληθευσιμότητα

Πώς επαληθεύουμε ότι το ανακάτεμα έγινε σωστά και δεν άλλαξαν τα ψηφοδέλτια;

- Στην πραγματικότητα κάνουμε παράλληλα πολλά ξεχωριστά ανακατέματα, εκτός του τελικού.
- Αν κάποιος θέλει να επαληθεύσει ότι η διαδικασία έγινε σωστά, μπορούμε να αποκαλύψουμε πώς από τα αρχικά ψηφοδέλτια πάμε σε ένα από τα παράλληλα ανακατέματα *ή* πώς από τα ενδιάμεσα πάμε στο τελικό (φυσικά όχι και τα δύο).
- Άρα αν έχουμε κάνει 100 ανακατέματα, η πιθανότητα να έχουμε αλλάξει τα ψηφοδέλτια είναι $2^{-100}$, που δεν μπορεί να συμβεί.

# Διαδικασία Μίξης



# 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).

# Εκλογές με το Ζευς

- Μέχρι σήμερα έχει χρησιμοποιηθεί σε περισσότερες από 500 εκλογές στην Ελλάδα.
- Οι μέχρι τώρα εκλογές αφορούσαν πάνω από 87.000 ψηφοφόρους και συμμετείχαν περισσότεροι από 57.000.
- Εκλογές εξακολουθούν να διεξάγονται συνεχώς.

# Επιπλέον Δυνατότητες

- Το Ζευς μπορεί να χρησιμοποιηθεί ως γενικός μηχανισμός επιβεβαιωμένης ανωνυμοποίησης.
- Εφαρμογές περιλαμβάνουν τη συλλογή δεδομένων, δημοσκοπήσεις, ανωνυμοποίηση μηνυμάτων, κ.λπ.
- Η υπηρεσία μπορεί να συνδέεται με οποιαδήποτε εξωτερική εφαρμογή ώστε να ενσωματώνεται σε υπηρεσίες τρίτων.

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