Κρυπτό-Ψηφοφορίες

Παναγιώτης Γροντάς

22/12/2023

ΕΜΠ - Κρυπτογραφία

Περιεχόμενα

Εισαγωγή

Είπαν για τις (ηλεκτρονικές) ψηφοφορίες...

Joseph Stalin
It is enough that the people know there was an election. The people who cast the votes decide nothing. The people who count the votes decide everything.

Dick Tuck
The People have spoken.... the bastards!

Είπαν για τις (ηλεκτρονικές) ψηφοφορίες... (2)

David Dill (Stanford CS, From Hacking Democracy, 2006)
... The voting booth is separated by a curtain and there is a guy behind the curtain that would write down your vote. You dictate the vote and once you ‘re done you leave, without being able to look at the ballot. Most people in their right mind, would not trust this process. The guy behind the curtain could be incompetent, hear the votes wrong and register it incorrectly or it could be that he did not like your political affiliation and prefer your vote would go to another party ...

Ronald Rivest
Internet voting is like drunk driving

Το πρόβλημα της ψηφοφορίας

Εκλογές

Μία γενική κατανεμημένη διαδικασία λήψης απόφασης ... με ηλικία όση οι κοινωνίες ... που αλλάζει ακολουθώντας τις τεχνολογικές εξελίξεις κάθε εποχής

- Στόχος: εκλογές με υπολογιστές
- Παρατήρηση: Ακόμα και αν δεν το βλέπει ο ψηφοφόρος οι υπολογιστές εμπλέκονται στη διαδικασία (εγγραφή, υπολογισμός και μετάδοση ενδιάμεσων αποτελεσμάτων)
- Στόχος: εκλογές μόνο με υπολογιστές - Καλή ιδέα, κακή ιδέα ή κάτι αναπόφευκτο;
- Οι ψηφοφορίες περιέχουν εγγενείς δυσκολίες, λόγω πολλών αντικρουόμενων απαιτήσεων
- Οι υπολογιστές τις επιτείνουν
- Απαιτούνται ασφαλιστικές δικλείδες

Απαιτήσεις

Ακεραιότητα

Το αποτέλεσμα των εκλογών πρέπει να αντανακλά τη βούληση των ψηφοφόρων

- Cast as intended
  - Ακεραιότητα κατά την καταγραφή της ψήφου
- Recorded as cast
  - Ακεραιότητα κατά την μεταφορά της ψήφου στην διαδικασία καταμέτρησης
- Tallied as recorded
  - Ακεραιότητα κατά τον υπολογισμό του αποτελέσματος

Επαληθευσιμότητα

Ο ψηφοφόρος πρέπει να *πειστεί* για την ακεραιότητα:
Επαληθευσιμότητα

- Ατομική (individual)
- Καθολική (universal)
- Διαχειριστική (administrative)

Συνολικά: E2E (End To End) Verifiability
Απαιτεί: Παραγωγή Στοιχείων

Ιδιωτικότητα

Ο ψηφοφόρος πρέπει να εκφράσει την πραγματική του επιλογή

- Μυστικότητα: Μη αποκάλυψη περιεχομένου ψήφου
- Ανωνυμία: Αδυναμία σύνδεσης ψήφου - ψηφοφόρου
- Εναντίον:
  - Των καταμετρητών (privacy)
  - Άλλων ψηφοφόρων (coercion)
  - Του ίδιου του ψηφοφόρου (vote selling)
- Το ίδιο το αποτέλεσμα διαρρέει πληροφορία

Σύγκριση

Ακεραιότητα χωρίς μυστικότητα;

- Εύκολη - Ψηφοφορία δι' ανατάσεως της χειρός
- Έχει νόημα; η έλλειψη μυστικότητας ακυρώνει την ακεραιότητα πριν καν κατατεθεί η ψήφος

Μυστικότητα χωρίς ακεραιότητα;

- Άχρηστη, αφού η ψήφος μπορεί να μην μετρηθεί σωστά
- Οδηγεί σε αποχή

Άλλες απαιτήσεις

- Δικαιοσύνη: Δεν είναι γνωστά ενδιάμεσα αποτελέσματα
- Eligibility: Ψηφίζουν μόνο όσοι έχουν δικαίωμα
  - Προϋποθέτει αυθεντικοποίηση
  - Μυστικότητα (;)
- Enfranchisement: Ώθηση για συμμετοχή
  - Η διαδικασία είναι διαφανής
  - και εύκολα κατανοητή (κρυπτογραφία;)
- Διαθεσιμότητα
  - Η επανάληψη δεν είναι δίκαιη
- Αποδοτικότητα (χρόνος, χρήμα)

Κρυπτογραφία και Ψηφοφορίες

Εκλογές και Υπολογιστές

- Ψηφοφορία μέσω αντιπροσώπου
- Μη έμπιστου (κακόβουλο λογισμικό, προγραμματιστικά λάθη)
- Ανοιχτό λογισμικό, μεθοδολογίες πιστοποίησης δεν επαρκούν
    - Αναγκαίες αλλά όχι ικανές συνθήκες

Software/System Independence (Rivest)

- Τα σφάλματα του συστήματος δεν πρέπει να επηρεάζουν τα αποτελέσματα
- Επαλήθευση: και αυτή μέρος του συστήματος
- VVPAT (Voter Verifiable Paper Trail)
- Κρυπτογραφία: Επαλήθευση με μαθηματικά

Κρυπτογραφία και Εκλογές: Μυστικότητα αλλά κυρίως **εμπιστοσύνη**

Συστατικά - Συμμετέχοντες i

Bulletin Board

- Αποθετήριο **όλων** των δεδομένων που παράγονται σε κάθε φάση μιας ψηφοφορίας για επαληθευσιμότητα
- Πρόσβαση από όλους τους εμπλεκόμενους
  - Authenticated: Κάθε καταχώρηση έχει ψηφιακή υπογραφή
  - Πρόσβαση: Read / Append

Συστατικά - Συμμετέχοντες ii

Κανάλια επικοινωνίας

- Private: Κρυπτογραφημένα - Υπολογιστική ασφάλεια
- Anonymous: Αφαίρεση πληροφορίας ταυτότητας (χωρίς να θυσιαστεί η ακεραιότητα)
- Untappable: Πληροφοριοθεωρητική ασφάλεια (συνήθως φυσική παρουσία)

Συστατικά - Συμμετέχοντες iii

Οντότητες - Ρόλοι

- Ψηφοφόροι
- Registration authorities: καταχωρούν στοιχεία των ψηφοφόρων και δίνουν τα αντίστοιχα tokens
- Counters: Εξάγουν μερικά ή πλήρη αποτελέσματα
- Verifiers: Επαλήθευση της διαδικασίας (ολόκληρης ή τμηματικά)

Οικογένειες κρυπτογραφικών συστημάτων ψηφοφοριών

- Offline: Χρησιμοποιούν παραδοσιακή υποδομή
- Online: Αποκλειστικά ηλεκτρονικά
- Ομομορφικά συστήματα (Benaloh (1985) - Cramer, Gennaro, Schoenmakers (1997))
  - Με βάση κρυπτογραφία
  - Με βάση διαμοιρασμό απορρήτων
- Δίκτυα Μίξης (Chaum (1981) - Park, Itoh, Kurosawa (1993))
- Τυφλές Υπογραφές (Chaum 1983 - Fujioka, Okamoto, Ohta (1992))

Κρυπτογραφικά Δομικά στοιχεία i

- Κρυπτοσυστήματα δημοσίου κλειδιού
  - ElGamal, Lifted El Gamal
  - Κρυπτογράφηση ψήφου - δημόσιο κλειδί αρχής
  - Υπογραφές ψήφων - MAC στο BB
- Διαμοιρασμός Απορρήτων
  - Threshold El Gamal
  - Αποκρυπτογράφηση ψήφων και αποτελέσματος
  - Σε ομάδες με σύγκρουση συμφερόντων (αντίπαλα κόμματα)
- Σχήματα δέσμευσης

Κρυπτογραφικά Δομικά στοιχεία ii

- Μη διαλογικές αποδείξεις γνώσης (NIZK)
  - Απόδειξη εγκυρότητας της ψήφου
  - Απόδειξη ορθής εκτέλεσης πρωτοκόλλου
  - Απόδειξη σωστής αποκρυπτογράφησης
- Τυφλές υπογραφές - για ανωνυμία

  Αποστολέας: Μήνυμα m, $r \in_R \mathbb{Z}_n^*$

  Υπογράφων: Ζεύγος κλειδιών $((e, n), d)$
  - $b = \text{Blind}(m, r) = m \cdot r^e \bmod n$
  - $s = \text{Sign}(d, b) = b^d \bmod n = m^d \cdot r \bmod n$
  - $\sigma = \text{Unblind}(sb, r) = sb \cdot r^{-1} = m^d \bmod n$
  - $\text{Vf}((e, n), m, \sigma) = \sigma^e = m \pmod n$

Ομομορφικά Συστήματα

Ομομορφικά Συστήματα

- Οι ψήφοι:
  - κρυπτογραφούνται με το δημόσιο κλειδί των ΤΑ
  - εισάγονται στο BB
  - διατηρούνται μυστικοί καθ' όλη τη διάρκεια της διαδικασίας
- Το αποτέλεσμα υπολογίζεται στα κρυπτοκείμενα με βάση τις ομομορφικές ιδιότητες του κρυπτοσυστήματος
- Για παράδειγμα στο Lifted El Gamal:

$$\begin{aligned} \mathrm{Enc}(v_1) \cdot \mathrm{Enc}(v_2) = \\ (g^{r_1}, g^{v_1} \cdot y^{r_1}) \cdot (g^{r_2}, g^{v_2} \cdot y^{r_2}) = \\ (g^{r_1+r_2}, g^{v_1+v_2} \cdot y^{r_1+r_2}) \end{aligned}$$

- Αποκρυπτογραφείται **μόνο** το αποτέλεσμα

Ομομορφικά Συστήματα

- Ακεραιότητα - Εγκυρότητα της ψήφου:
  Πώς επαληθεύεις μία κρυπτογραφημένη ψήφο
  Λύση: Απόδειξη μηδενικής γνώσης *(non interactive)* για την εγκυρότητα
  Κατάθεση μαζί με την ψήφο
  Επαλήθευση από όλους
- Μυστικότητα / Δικαιοσύνη
  Αποκρυπτογράφηση μεμονωμένων ψήφων - ενδιάμεσων αποτελεσμάτων
  Λύση: Threshold cryptosystems

Cramer, Genaro, Schoenmakers (CGS97)

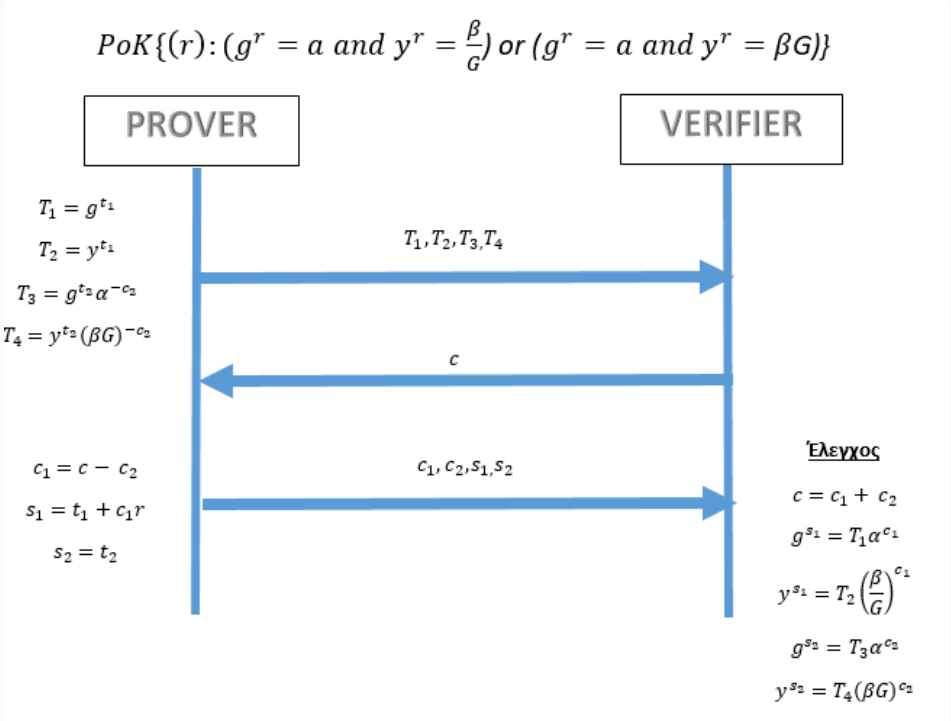
- Το βασικό πρωτόκολλο για ομομορφικά συστήματα
- Υλοποιείται στο σύστημα Helios
- Κρυπτογράφηση ψήφων με εκθετικό ElGamal
- Αποκρυπτογράφηση αποτελέσματος: Υπολογισμός *μικρού* διακριτού λογαρίθμου
- 3 αποδείξεις μηδενικής γνώσης:
  - Εγκυρότητα ψήφου
  - Γνώση ιδιωτικού κλειδιού που αντιστοιχεί σε δημόσιο (Schnorr)
  - Έγκυρη Αποκρυπτογράφηση (Chaum - Pedersen)

Cramer, Genaro, Schoenmakers (CGS97):Λεπτομέρειες

- Ψήφος $b \in \{1, -1\}$ (yes-no)
- Κρυπτογράφηση: $(g^r, G^b \cdot y^r)$
- Απόδειξη εγκυρότητας:
  - $b = 1 : (\alpha, \beta) = (g^r, G \cdot y^r) \Rightarrow log_g \alpha = log_y(\beta / G)$
  - $b = -1 : (\alpha, \beta) = (g^r, \frac{y^r}{G}) \Rightarrow log_g \alpha = log_y(\beta \cdot G)$
  - Παραλλαγή OR πρωτοκόλλου Chaum - Pedersen
- Στο BB: ψήφος με μη διαλογική απόδειξη
- Καταμέτρηση
  - Επαλήθευση αποδείξεων
  - Πολλαπλασιασμός ψηφοδελτίων με έγκυρες αποδείξεις
  - $(A, B) = (\prod_{i=1}^{n} g^{r_i}, \prod_{i=1}^{n} g^{b_i} y^{r_i})$
  - Threshold Decryption δίνει το $g^{(\#yes - \#no)}$
  - Απόδειξη ορθής αποκρυπτογράφησης (Chaum Pedersen πάλι)
  - Επίλυση μικρού διακριτού λογαρίθμου δίνει το: $(\#yes - \#no)$

Cramer, Genaro, Schoenmakers (CGS97):Η απόδειξη μηδενικής γνώσης

Έστω ότι ο ψηφοφόρος έχει ψηφίσει yes



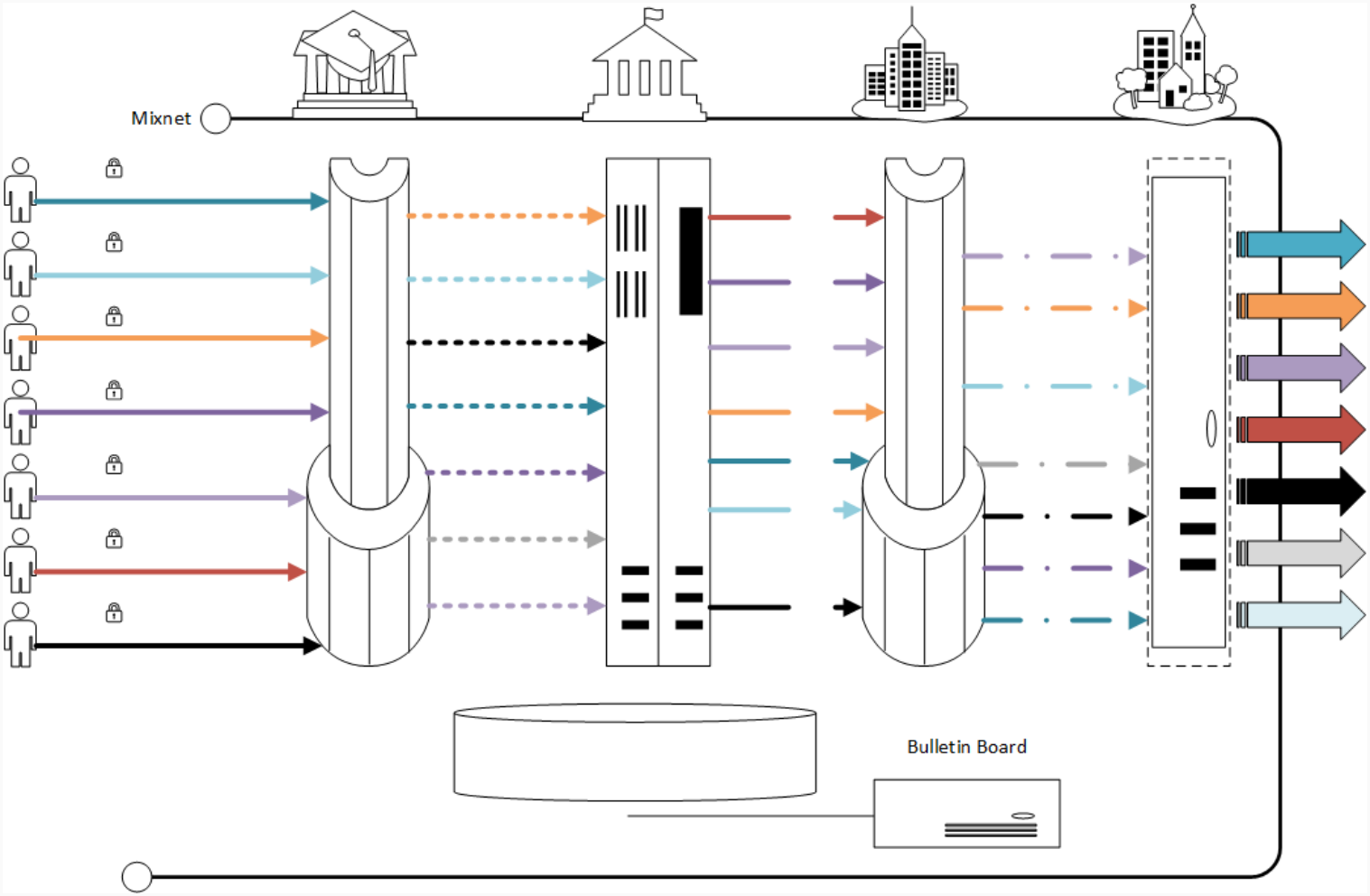
Στην πραγματικότητα: non interactive με Fiat-Shamir heuristic

Δίκτυα Μίξης

Ψηφοφορίες με Δίκτυα Μίξης

- Γενικό δομικό στοιχεία για εφαρμογές ανωνυμίας
- Προτάθηκε από τον David Chaum (1981)
- Αποτελείται από ένα σύνολο από **μίκτες**. Κάθε ένας:
  - λαμβάνει ένα σύνολο από μηνύματα (BB)
  - αλλάζει τη μορφή τους
  - εφαρμόζει μια τυχαία μετάθεση
- Δύο μορφές λειτουργίας
  - Σειριακά (κάθε μίκτης σε όλα τα μηνύματα)
  - Παράλληλα (κάθε μίκτης σε ένα υποσύνολο από τα μηνύματα)
- Στις ψηφοφορίες: τα μηνύματα είναι οι ψήφοι (ανακάτεμα της κάλπης)
- BB: παρέχει είσοδο και λαμβάνει έξοδο από κάθε μίκτη

Γενική Μορφή Δίκτυου Μίξης



Decryption Mixnets (RSA)

- Κάθε μίκτης i έχει ένα ζεύγος κλειδιών RSA $(\mathsf{pk}_i, \mathsf{sk}_i)$
- Ψηφοφόρος: κρυπτογράφηση ψήφου με δημόσια κλειδιά των μικτών $(\mathsf{Enc}_i = \mathsf{Enc}_{pk_i})$ *σε αντίστροφη σειρά.*

$$L_0 = \{\mathsf{Enc}_1(\mathsf{Enc}_2(\cdots \mathsf{Enc}_m(v_i, r_{mi}) \cdots, r_{2i}), r_{1i})\}_{i=1}^{n}$$

- Μίκτης: Αλλαγή Μορφής
  - αφαιρεί ένα επίπεδο κρυπτογράφησης χρησιμοποιώντας με το ιδιωτικό του κλειδί (ξεφλούδισμα)
  - αφαιρεί την τυχαιότητα που περιέχει
- Μίκτης: Ανακάτεμα
  - Επιλογή τυχαίας μετάθεσης και εφαρμογή στα μηνύματα
  - Το αποτέλεσμα γράφεται στο BB
  - Για παράδειγμα ο πρώτος μίκτης θα γράψει:

$$L_1 = \{\mathsf{Enc}_2(\cdots \mathsf{Enc}_k(v_i, r_{mi}) \cdots, r_{2i})\}_{i=\pi_1^{-1}(1)}^{\pi_1^{-1}(n)}$$

Decryption Mixnets (RSA)

- Η διαδικασία επαναλαμβάνεται.
- Τελικά στην έξοδο του δικτύου μίξης:

$$L_k = \{v_i\}_{i=\pi_k^{-1}\circ\cdots\circ\pi_1^{-1}(1)}^{\pi_k^{-1}\circ\cdots\circ\pi_1^{-1}(n)}$$

- Ακολουθεί η καταμέτρηση
- Παρατηρήσεις:
  - Αρκεί ένας 'τίμιος' μίκτης απέναντι σε παθητικό αντίπαλο
  - Ο τελευταίος μίκτης έχει πρόσβαση στο plaintext
  - Το πλήθος των κρυπτογραφήσεων και το μέγεθος του κρυπτοκειμένου είναι ανάλογο του αριθμού των μικτών.

Reencryption Mixnets (ElGamal)

Ιδιότητα El Gamal: Reencryption

$$\mathrm{Enc}(v, r_1) \cdot \mathrm{Enc}(1, r_2) = \mathrm{Enc}(v, r_1 + r_2)$$

Μπορεί να χρησιμοποιηθεί για αλλαγή της μορφής των μηνυμάτων
Δύο παραλλαγές:

- Reencryption και Permutation
- Decryption, Reencryption και Permutation

Reencryption Mixnets (ElGamal)

Ο μίκτης M_j:

- Λαμβάνει από το BB την είσοδο

$$L_{j-1} = \{\text{Enc}(v_i, r_{j-1,i})\}_{i=1}^{n} = \{(g^{r_{j-1,i}}, v_i \cdot y^{r_{j-1,i}})\}_{i=1}^{n}$$

- Εισάγει νέα τυχαιότητα με reencryption:

$$L'_{j-1} = \{\text{Enc}(v_i, r_{j-1,i}) \cdot \text{Enc}(1, r_{j,i})\}_{i=1}^{n} = \{(g^{r_{j-1,i}+r_{j,i}}, v_i \cdot y^{r_{j-1,i}+r_{j,i}})\}_{i=1}^{n}$$

- Εφαρμόζει μία τυχαία μετάθεση π_j
- Γράφει τα αποτελέσματα στο BB

Reencryption - Decryption Mixnets (ElGamal)

- Κάθε μίκτης $\{M_j\}_{j=1}^k$ έχει δημόσιο κλειδί $y_j = g^{x_j}$
- Συνδυασμένο δημόσιο κλειδί $Y = \prod_{j=1}^k y_j = g^{\sum_j x_j}$
- Αρχική κρυπτογράφηση με Y
  - Η είσοδος είναι:
    $$L_0 = \{(g^{r_{i0}}, v_i(y_1 \cdots y_k)^{r_{i0}})\}_{i=1}^n$$
  - Ο M_j λαμβάνει ως είσοδο:
    $$L_{j-1} = \{(g^{\sum_{t=0}^{j-1} r_{it}}, v_i \cdot (\prod_{t=j}^k y_t)^{\sum_{t=0}^{j-1} r_{it}})\}_{i=1}^n$$
    Αποκρυπτογραφεί μερικώς διαιρώντας με $g^{x_j \cdot \sum_{t=0}^{j-1} r_{it}}$ και εφαρμόζει νέα τυχαιότητα r_{ij}:
    $$L_j = \{(g^{\sum_{t=0}^{j-1} r_{it}} \cdot g^{r_{ij}}, v_i \cdot (\prod_{t=j+1}^k y_t)^{\sum_{t=0}^{j-1} r_{it}} \cdot (\prod_{t=j+1}^k y_t)^{r_{ij}})\}_{i=1}^n$$
  - Εφαρμόζει μία τυχαία μετάθεση π_j

Ενεργή επίθεση (Pfitzmann)

- Στόχος $\mathcal{A}$: αποκάλυψη v_i για συμμετέχοντα P_i
- Μέσο: Συνεργασία με κάποιο 'κακό' ψηφοφόρο
- Ανάκτηση αρχικής ψήφου από το BB

$$c_{i0} = (t, u) = (g^R, v_i \cdot (y_1, \cdots, y_k)^R)$$

- Ο $\mathcal{A}$ επιλέγει τυχαίο x και παράγει

$$c'_{i0} = (t^x, u^x) = (g^{R'}, v_i^x \cdot (y_j, \cdots, y_k)^{R'})$$

- Αντικατάσταση ψήφου του συνεργάτη του.
- Η έξοδος του δικτύου μίξης θα περιέχει το v_i^x και v_i
- Ο $\mathcal{A}$ ανακτά όλα τα μηνύματα εξόδου και τα υψώνει στην x.
- Στην συνέχεια ελέγχει τις δύο λίστες για κοινά στοιχεία.
- Όταν βρει έμαθε το μήνυμα που έψαχνε καθώς $v^x_{\pi(i)} = v_i^x$.

Λύσεις για ψηφοφορίες

Επαληθευσιμότητα των ενεργειών ψηφοφόρων και μικτών

- Ψηφοφόρος: Απόδειξη γνώσης της ψήφου ώστε
  - να **μην** βάλει ετικέτα σε κάποια ψήφο
  - να **μην** αντιγράψει μια ψήφο
  - ... όπως στα ομομορφικά συστήματα
- Μίκτης: Απόδειξη μετάθεσης (proof of shuffle)
  - Η μετάθεση είναι έγκυρη
  - χωρίς να αλλάξει κάποια ψήφο
  - χωρίς να παραλείψει κάποια ψήφο

Παράδειγμα i

- Έισοδος:
  - $C_1 = \mathrm{Enc}(m_1, r_1)$
  - $C_2 = \mathrm{Enc}(m_2, r_2)$.
- Reencryption
  - $C'_1 = Reenc(C_1) = \mathrm{Enc}(m_1, r_1 + r'_1)$
  - $C'_2 = Reenc(C_2) = \mathrm{Enc}(m_2, r_2 + r'_2)$
- Τυχαία επιλογή bit $b \in_R \{0, 1\}$.
- Αν $b = 0$ έξοδος (C'_1, C'_2)
- Αν $b = 1$ έξοδος (C'_2, C'_1)

Παράδειγμα ii

Βήμα 1 Απόδειξη ορθότητας reencryption

Δηλαδή
Το κρυπτογράφημα $C' = (G', M') = (g^u, m' \cdot y^u)$ είναι reencryption του $C = (G, M) = (g^t, m \cdot y^t)$

Βασική ιδέα: Το C' είναι reencryption του C ανν και τα δύο κρυπτογραφούν το ίδιο μήνυμα, δηλ. $m' = m$.

Διαιρούμε τα δύο μέρη και έχουμε:

$$\frac{G'}{G} = \frac{g^u}{g^t} = g^{u-t} \text{ και } \frac{M'}{M} = \frac{m'y^u}{my^t} = y^{u-t}$$

Αρκεί νδο ότι $log_g \frac{G'}{G} = log_y \frac{M'}{M}$

Χρήση non interactive Chaum Pedersen

Παράδειγμα iii

Βήμα 2 Απόδειξη ορθότητας μετάθεσης
Πρέπει νδο $\{C'_1, C'_2\}$ είναι reencryption μια μετάθεσης του $\{C_1, C_2\}$ χωρίς να την φανερώσουμε την αντιστοιχία.

Ισοδύναμα:

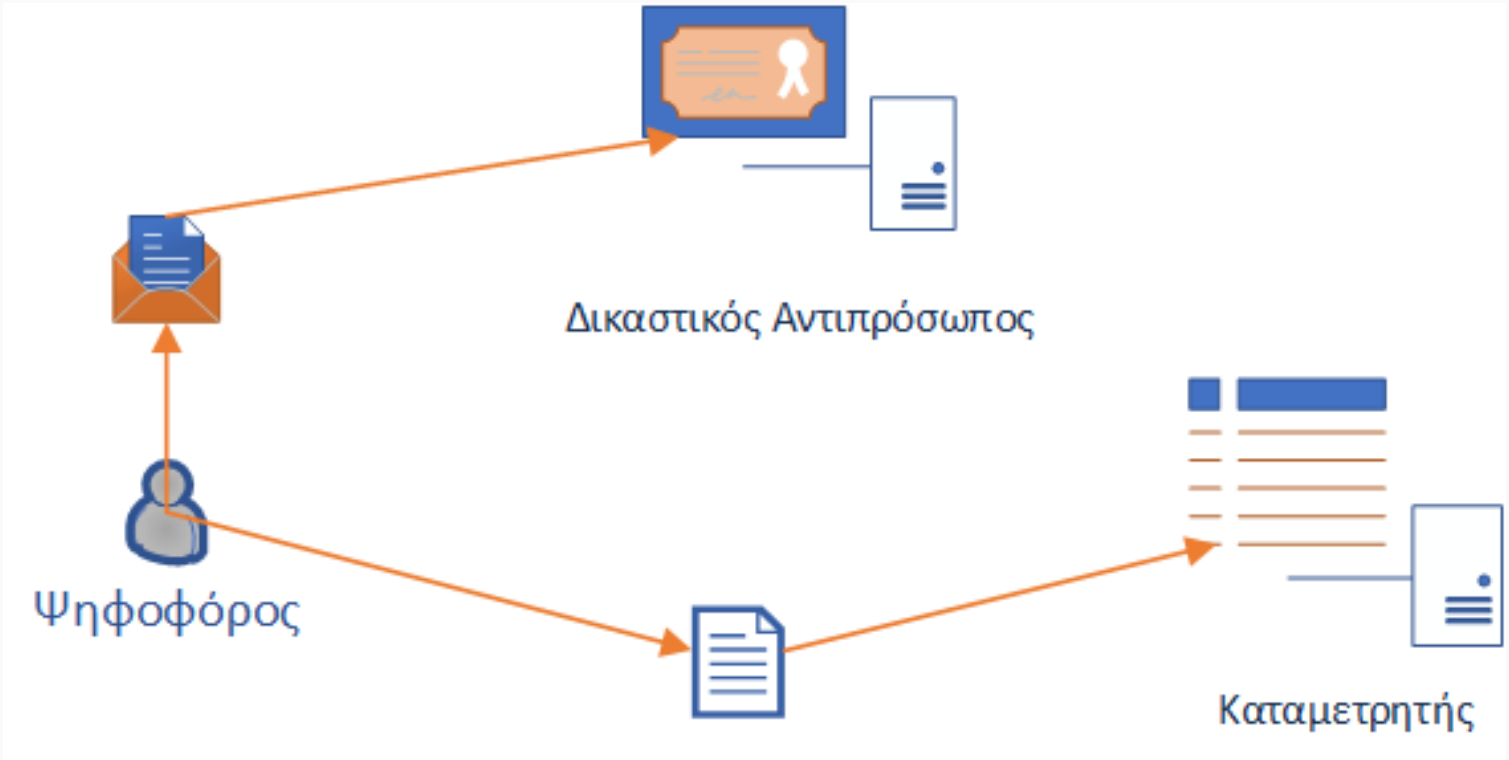
$$(C'_1 = Reenc(C_1) \wedge C'_2 = Reenc(C_2)) \bigvee (C'_1 = Reenc(C_2) \wedge C'_2 = Reenc(C_1))$$

Λύση: Σύνθεση 4 πρωτοκόλλων Chaum-Pedersen

Ψηφοφορίες με Τυφλές Υπογραφές

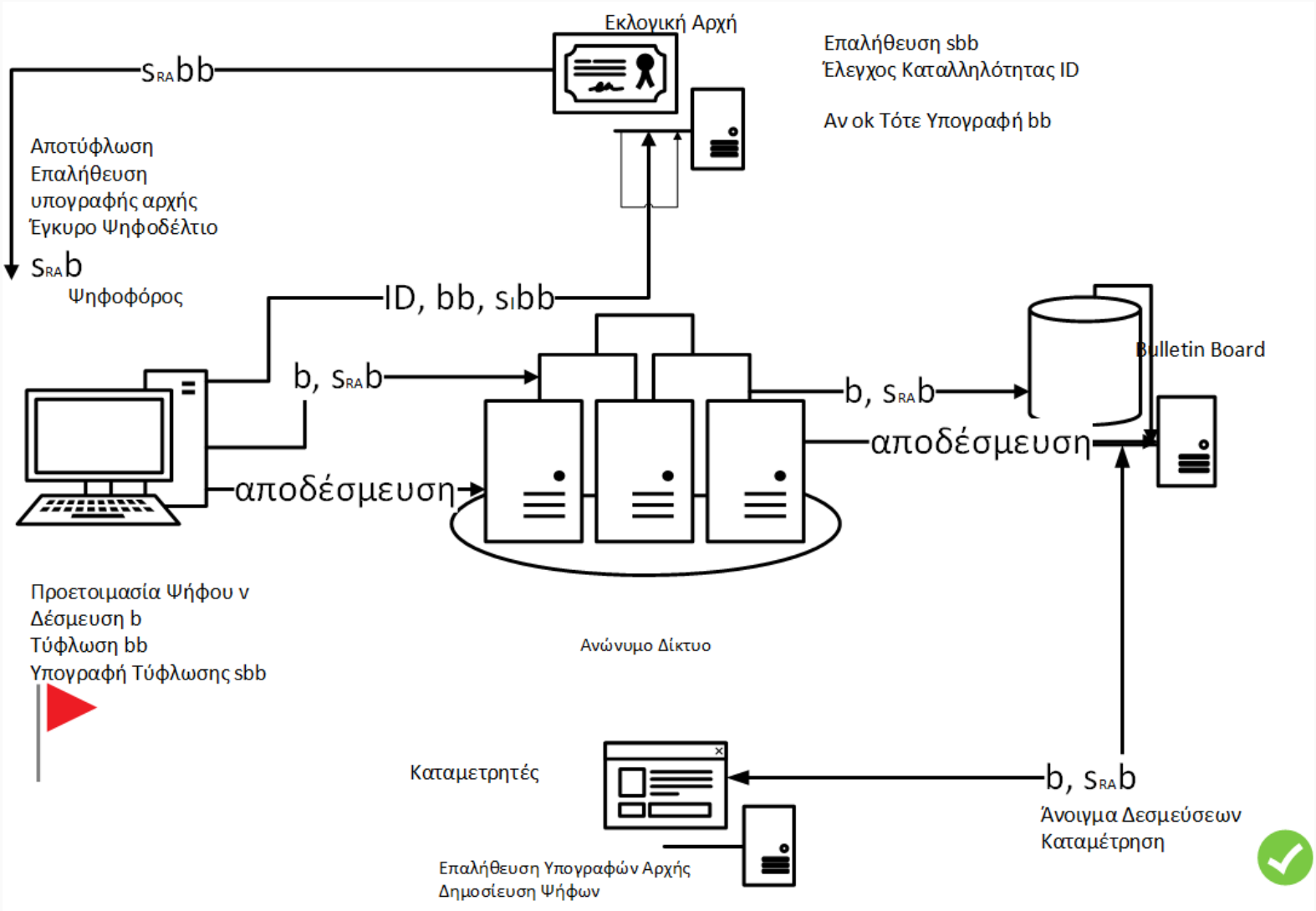
Ψηφοφορίες με Τυφλές Υπογραφές

Βασική ιδέα: Πώς θα δούλευαν οι παραδοσιακές ψηφοφορίες αν οι δικαστικοί αντιπρόσωποι ήταν σε διαφορετικό φυσικό χώρο από τους καταμετρητές



Ψηφοφορίες με Τυφλές Υπογραφές

- Ο ψηφοφόρος υποβάλλει μία ‘τυφλωμένη’ έκδοση του ψηφοδελτίου μαζί με πληροφορίες ταυτότητας.
- Η εκλογική αρχή επαληθεύει την ταυτότητα του υποψηφίου και ελέγχει αν έχει δικαίωμα ψήφου. Αν η απάντηση είναι θετική υπογράφει ψηφιακά το υπογεγραμμένο και τυφλωμένο ψηφοδέλτιο και το επιστρέφει στον ψηφοφόρο.
- Ο ψηφοφόρος αφού επαληθεύσει την υπογραφή της αρχής καταθέτει το ψηφοδέλτιο στο BB *ανώνυμα*.
- Η αρχή λαμβάνει τα υπογεγραμμένα ψηφοδέλτια και επαληθεύει την υπογραφή της.
- Ο ψηφοφόρος μπορεί να επαληθεύσει το ψηφοδέλτιο του εισάγοντας σε αυτό ένα τυχαίο αριθμό που μόνο αυτός γνωρίζει.


Εκλογική Αρχή
Επαλήθευση sbb
Έλεγχος Καταλληλότητας ID
Αν ok Τότε Υπογραφή bb
sRAbb
Αποτύφλωση
Επαλήθευση
υπογραφής αρχής
Έγκυρο Ψηφοδέλτιο
sRAb
Ψηφοφόρος
ID, bb, sibb
b, sRAb
αποδέσμευση
b, sRAb
αποδέσμευση
Bulletin Board
Προετοιμασία Ψήφου v
Δέσμευση b
Τύφλωση bb
Υπογραφή Τύφλωσης sbb
Ανώνυμο Δίκτυο
Καταμετρητές
b, sRAb
Άνοιγμα Δεσμεύσεων
Καταμέτρηση
Επαλήθευση Υπογραφών Αρχής
Δημοσίευση Ψήφων

Αναλυτική περιγραφή FOO92 i

1. **Ψηφοφόρος: Προετοιμασία**
   - Επιλογή ψήφου v_i
   - Δέσμευση στην ψήφο με τυχαιότητα r_{c_i}.
   - Το ψηφοδέλτιο είναι:

$$b_i = \text{Commit}(v_i, r_{c_i}) = g^{r_{c_i}} h^{v_i}$$

   - Τύφλωση του ψηφοδελτίου με r_{b_i} και δημόσιο κλειδί της αρχής

$$bb_i = \text{Blind}(b_i, r_{b_i}) = b_i r_{b_i}^{e_A}$$

   - Υπογραφή τυφλωμένου ψηφοδέλτιο:

$$sbb_i^v = \text{Sign}_{d_i}(bb_i)$$

   - Αποστολή (id_i, bb_i, sbb_i^v) στην εκλογική αρχή (RA)

2. **RA:Εξουσιοδότηση**
   - Έλεγχοι με τη βοήθεια ενός πίνακα $T = \{id_i, e_i\}$ που περιέχει τις ταυτότητες και τα δημόσια κλειδιά των εγγεγραμμένων ψηφοφόρων:
     - το δικαίωμα του να ψηφίσει $id_i \in T$
     - υπογραφή του ψηφοφόρου με e_i
     - αν έχει ξαναψηφίσει
   - Επιτυχείς έλεγχοι $\rightarrow$ έγκριση μέσω υπογραφής του τυφλωμένου ψηφοδελτίου $sbb_i^A = \mathrm{Sign}_{d_A}(bb_i) = b_i^{d_A} r_{b_i}$.
   - Τέλος επιστρέφει το sbb_i^A στον ψηφοφόρο i
   - Ανακοίνωση από RA του συνολικού αριθμού ψηφοφόρων μέσω λίστας

$$(id_i, bb_i, sbb_i^V)$$

3. **Ψηφοφορία: Ενέργειες Ψηφοφόρου**
   - Αποτύφλωση υπογεγραμμένου ψηφοδελτίου

$$sb_i^A = \text{Unblind}(sbb_A^i) = b_i^{d_A}$$

   - Προκύπτει υπογεγραμμένη η αρχική δέσμευση (επαληθεύσιμη από όλους)
   - Κατάθεση ψήφου: Αποστολή των b_i, sb_i^A στην αρχή καταμέτρησης
   - Χρήση ανώνυμου καναλιού (πχ. δίκτυο μίξης) για απόκρυψη στοιχείων που ίσως προδώσουν την ταυτότητα του ψηφοφόρου (πχ. δικτυακές διευθύνσεις).

Αναλυτική περιγραφή FOO92 iv

4. **Καταμετρητές: Συλλογή** Όλες οι ενέργειες έχουν δημόσιες εισόδους και άρα είναι επαληθεύσιμες
   - Λαμβάνει ψηφοδέλτιο b_i, sb_i^A
   - Η αρχή καταμέτρησης επαληθεύει την υπογραφή της αρχής σε κάθε ψηφοδέλτιο sb_i^A με το e_A
   - Όσα ψηφοδέλτια πέρασαν τον έλεγχο δημοσιεύονται σε μια λίστα $\{uid_i, b_i, sb_i^A\}$,
     όπου uid_i είναι ένα τυχαίος αριθμός ή ένας ΑΑ

Αναλυτική περιγραφή FOO92 v

5. **Αποδεσμεύσεις - Επαληθεύσεις** Μετά τη λήξη της προθεσμίας ψηφοφορίας:
   κάθε ψηφοφόρος (και λοιποί ενδιαφερόμενοι) επαληθεύουν:
   - το ψηφοδέλτιο καθενός βρίσκεται στο BB.
   - το πλήθος των ψηφοφόρων που δημοσίευσε η εκλογική αρχή = πλήθος των ψηφοδελτίων που δημοσίευσε η αρχή καταμέτρησης.
   - Επιτυχείς έλεγχοι ανάκτηση uid_i από το *BB*
   - Αποστολή decommitment values uid_i, v_i, rc_i μέσω ανώνυμου καναλιού
   - Επαλήθευση δεσμεύσεων από καταμετρητές
6. **Καταμέτρηση**
   - Δημοσίευση 'ανώνυμων' ψηφοδελτίων
   - Καταμέτρηση από κάθε ενδιαφερόμενο

Συζήτηση FOO

- Privacy
  - Commitment scheme
  - Blindness
  - Anonymous Channel
- Verifiability: Δημόσια εκτελέσιμες ενέργειες
  - Individual: Ύπαρξη $\{uid_i, b_i, sb_i^A\}$ και uid_i, v_i, rc_i
  - Universal: Οποιοσδήποτε μπορεί να επαναλάβει τις ενέργειες του καταμετρητή
  - Eligibility: Βασίζεται στο unforgeability του σχήματος υπογραφών

Ανοιχτά Θέματα

- Θέματα υλοποίησης
  - Κωδικοποίηση πολλών υποψηφίων
  - Απόδοση NIZK (μέγεθος, ταχύτητα δημιουργίας και επαλήθευσης)
- Everlasting privacy
  - Adi Shamir: Όλα τα κρυπτογραφικά κλειδιά που χρησιμοποιούνται σήμερα θα είναι άχρηστα σε 30 χρόνια
  - Quantum Computing
  - Λόγω verifiability οι ψήφοι είναι εν δυνάμει διαθέσιμοι σε πολλές οντότητες
- Τυπικοί ορισμοί για ιδιότητες
- Εναλλακτικές μέθοδοι υπολογισμού αποτελέσματος
- Coercion resistance
  - Απαραίτητο για internet voting
  - Κάθε ψηφοφόρος: Δυνατότητα πολλών επιλογών
  - Εκβιαστής: Δεν μπορεί να αποφανθεί αν πέτυχε η προσπάθειά του