

Κρυπτο Ψηφοφορίες

Παναγιώτης Γροντάς

ΕΜΠ - Κρυπτογραφία - (2017-2018)

19/12/2017

Περιεχόμενα

- Απαιτήσεις ηλεκτρονικών ψηφοφοριών
- Ομομορφικά συστήματα
- (Επαληθεύσιμα) Δίκτυα Μίξης
- Ψηφοφορίες με τυφλές υπογραφές
- Ανοιχτά Θέματα

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 τρέχουσες τεχνολογικές εξελίξεις κάθε εποχής

- Σήμερα: εκλογές με υπολογιστές
- Καλή ιδέα, κακή ιδέα ή κάτι αναπόφευκτο;
- Οι ψηφοφορίες περιέχουν εγγενείς δυσκολίες, λόγω πολλών αντικρουομένων απαιτήσεων
- Οι υπολογιστές τις επιτείνουν
- Όμως, υλοποιήσεις εκλογών με δεκάδες ελαττώματα επέζησαν αιώνες και χρησιμοποιούνται ακόμα
- Δεν έχουν όλες οι εκλογικές διαδικασίες τις ίδιες απαιτήσεις ασφάλειας
- Λύση που εξισορροπεί κινδύνους με απαιτήσεις ασφάλειας

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

Επιτυγχάνεται μέσω: *επαληθευσιμότητας*

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

Συνολικά: E2E (End To End) Verifiability

Απαιτεί: Παραγωγή Στοιχείων

Μυστικότητα

Ο ψηφοφόρος πρέπει να εκφράσει την πραγματική του επιλογή

- 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 πιο σημαντική;

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

Μυστικότητα πιο σημαντική;

- 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)

Εκλογές και Υπολογιστές

- Ψηφοφορία μέσω αντιπροσώπου
- Μη έμπιστου (κακόβουλο λογισμικό, προγραμματιστικά λάθη)
- Ανοιχτό λογισμικό, μεθοδολογίες πιστοποίησης δεν επαρκούν

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 επαληθευσσιμότητα
- Πρόσβαση από όλους τους εμπλεκόμενους
 - Authenticated: Κάθε καταχώρηση έχει ψηφιακή υπογραφή
 - Πρόσβαση: Read / Append
 - Θεωρητικά: Broadcast channel with memory

Συστατικά - Συμμετέχοντες II

Κανάλια επικοινωνίας

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

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

- Offline: Χρησιμοποιούν παραδοσιακή υποδομή
- Online: Αποκλειστικά ηλεκτρονικά
- Ομομορφικά συστήματα (Benaloh - 1985)
 - 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 $((e, n), d)$
 - $b = blind(m, r) = m \cdot r^e \pmod n$
 - $s = sign(d, b) = b^d \pmod n = m^d \cdot r \pmod n$
 - $\sigma = unblind(sb, r) = sb \cdot r^{-1} = m^d \pmod n$
 - $verify((e, n), m, \sigma) = \sigma^e = m \pmod n$

Ομομορφικά Συστήματα

Βασική ιδέα

- Οι ψήφοι:
 - κρυπτογραφούνται με το δημόσιο κλειδί των TA
 - 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:

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

- Αποκρυπτογραφείται **μόνο** το αποτέλεσμα

Ομομορφικά Συστήματα

Προβλήματα

- 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)

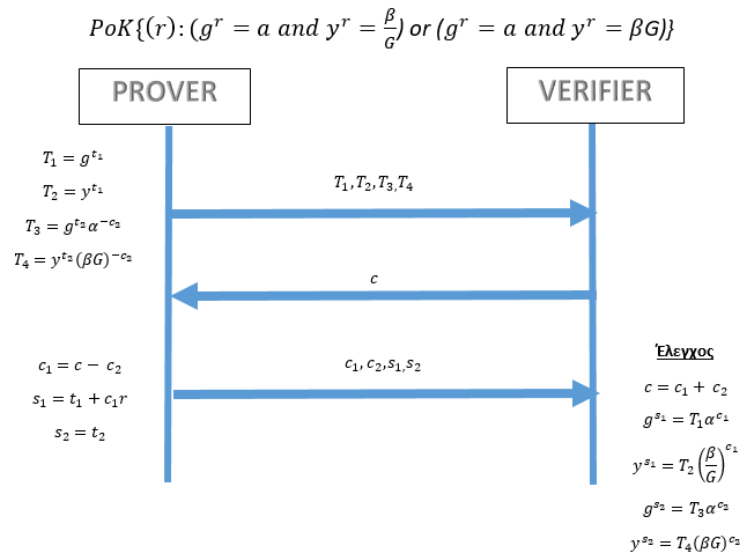
- Το βασικό πρωτόκολλο για ομομορφικά συστήματα
- Υλοποιείται στο σύστημα Helios
- Κρυπτογράφηση ψήφων με exponential el gamal
- Αποκρυπτογράφηση αποτελέσματος: Υπολογισμός μικρού διακριτού λογαρίθμου
- 3 αποδείξεις μηδενικής γνώσης:
 - Εγκυρότητα ψήφου
 - Γνώση ιδιωτικού κλειδιού που αντιστοιχεί σε 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:
 - $b = 1 : (\alpha, \beta) = (g^r, G \cdot y^r) \Rightarrow \log_g \alpha = \log_y (\beta / G)$
 - $b = -1 : (\alpha, \beta) = (g^r, y^r / G) \Rightarrow \log_g \alpha = \log_y (\beta \cdot G)$
 - 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 (άσκηση)
 - Επίλυση μικρού διακριτού λογαρίθμου δίνει το: $(\#yes - \#no)$

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

Έστω ότι ο ψηφοφόρος έχει ψηφίσει yes (απόδειξη για no άσκηση)

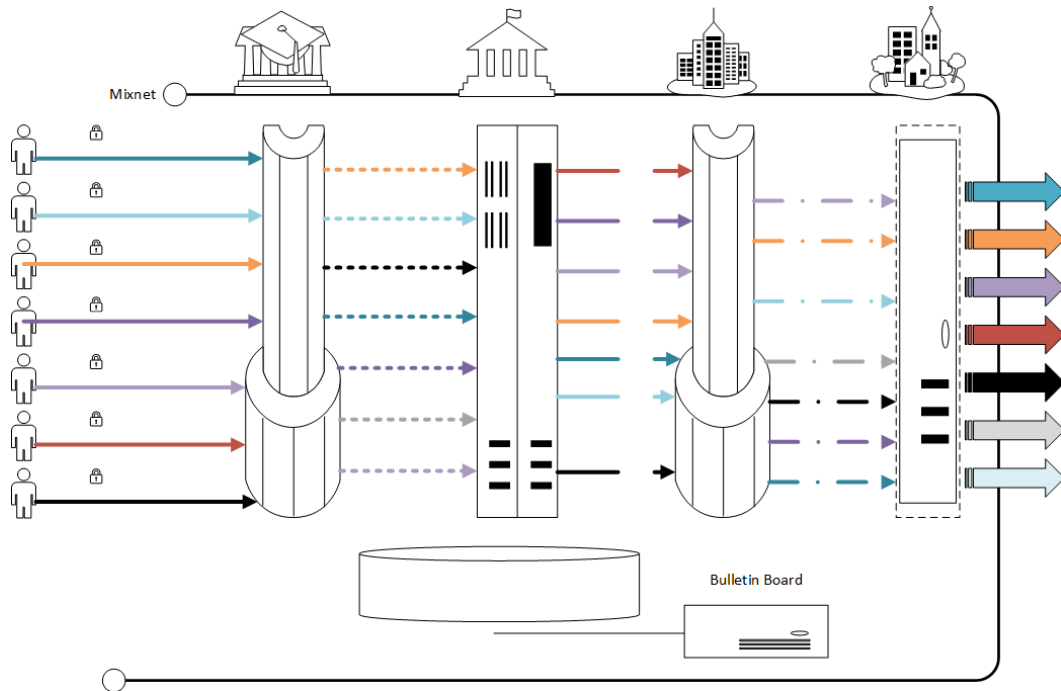


Στην πραγματικότητα: non interactive με Fiat-Shamir heuristic

Ψηφοφορίες με Δίκτυα Μίξης Εισαγωγή

- Γενικό δομικό στοιχείο 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 (ανακάτεμα)
- 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 (pk_i, sk_i)
- Ψηφοφόρος: κρυπτογράφηση ψήφου με δημόσια κλειδιά των μίκτων σε αντίστροφη σειρά.

$$L_0 = \{Enc_{pk_1}(Enc_{pk_2}(\dots Enc_{pk_m}(v_i, r_i) \dots, r_2), r_1)\}_{i=1}^n$$

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

$$L_1 = \{Enc_{pk_2}(\dots Enc_{pk_k}(v_i, r_i) \dots, r_2)\}_{i=\pi_1(1)}^{\pi_1(n)}$$

Decryption Mixnets (RSA)

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

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

- 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

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

Η μορφή των μηνυμάτων αλλάζει με reencryption
Δύο παραλλαγές:

- Reencryption και Permutation
- Decryption, Reencryption και Permutation

Reencryption Mixnets (ElGamal)

Reencryption

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:

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

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

Reencryption Mixnets (ElGamal)

Decryption and Reencryption

- Κάθε μίκτης $\{M_j\}_{j=1}^k$ έχει δημόσιο κλειδί y_j
- Αρχική κρυπτογράφηση με συνδυασμένο δημόσιο κλειδί $\prod_{j=1}^k y_j$

- Η είσοδος είναι:

$$L_0 = \{(g^{r_{0i}}, v_i (y_1 \cdots y_k)^{r_{0i}})\}_{i=1}^n$$

- Ο M_j αποκρυπτογραφεί μερικώς

$$L_{j-1} = \{(g^{\sum_{t=0}^{j-1} r_{ti}}, v_i \cdot (\prod_{t=j}^k y_t)^{\sum_{t=0}^{j-1} r_{ti}})\}_{i=1}^n$$

διαιρώντας με $g^{x_j \cdot \sum_{t=0}^{j-1} r_{ti}}$ και εφαρμόζει νέα τυχαιότητα r_{ji} :

$$L_j = \{(g^{\sum_{t=0}^{j-1} r_{ti} + r_{ji}}, v_i \cdot (\prod_{t=j+1}^k y_t)^{\sum_{t=0}^{j-1} r_{ti} + r_{ji}})\}_{i=1}^n$$

- 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

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

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

$$c'_{i0} = (t^x, u^x) = (g^{R'x}, v_i^x \cdot (y_1, \dots, y_k)^{R'x})$$

- 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 $v_{\pi(i)}^x = v_i^x$.

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

Προσθήκη επαληθευσιμότητας σε ένα απλό δίκτυο μίξης

- Έισοδος:
 - $C_1 = \text{Enc}(m_1, r_1)$
 - $C_2 = \text{Enc}(m_2, r_2)$.
- Reencryption
 - $C'_1 = \text{Reenc}(C_1) = \text{Enc}(m_1, r_1 + r'_1)$
 - $C'_2 = \text{Reenc}(C_2) = \text{Enc}(m_2, r_2 + r'_2)$
- 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

Προσθήκη επαληθευσιμότητας σε ένα απλό δίκτυο μίξης

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:

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

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

Χρήση non interactive Chaum Pedersen

Παράδειγμα III

Προσθήκη επαληθευσιμότητας σε ένα απλό δίκτυο μίξης

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:

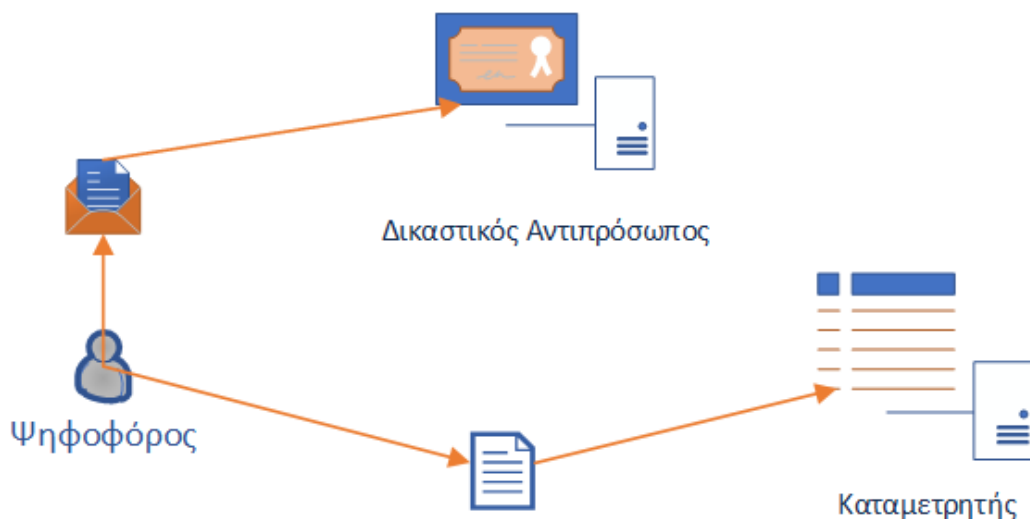
$$(C'_1 = Reenc(C_1) \wedge C'_2 = Reenc(C_2)) \vee (C'_1 = Reenc(C_2) \wedge C'_2 = Reenc(C_1))$$

Λύση: Σύνθεση 4 πρωτοκόλλων Chaum-Pedersen

Ψηφοφορίες με Τυφλές Υπογραφές

Fujioka, Okamoto και Ohta (FOO92)

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



- Ο ψηφοφόρος υποβάλλει μία 'τυφλωμένη' έκδοση του ψηφοδέλιου 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 τυφλωμένο ψηφοδέλτιο και το επιστρέφει στον ψηφοφόρο.
- Ο ψηφοφόρος αφού επαληθεύσει την υπογραφή της αρχής καταθέτει το ψηφοδέλτιο στο ΒΒ *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.

Αναλυτική περιγραφή FOO92 I

1 Ψηφοφόρος: Προετοιμασία

- Επιλογή ψήφου v_i
- Δέσμευση στην ψήφο με τυχειότητα rc_i .
- Το ψηφοδέλτιο είναι:

$$b_i = \text{commit}(v_i, rc_i) = g^{rc_i} h^{v_i}$$

- Τύφλωση του ψηφοδέλιου με rb_i και δημόσιο κλειδί της αρχής

$$bb_i = \text{blind}(b_i, rb_i) = b_i rb_i^{e_A}$$

- Υπογραφή τυφλωμένου ψηφοδέλιου:

$$sbb_i^V = \text{sign}_{d_i}(bb_i)$$

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

Αναλυτική περιγραφή FOO92 II

2 RA:Εξουσιοδότηση

- Έλεγχος 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 ψηφοδέλτιου $sbb_i^A = \text{sign}_{d_A}(bb_i) = b_i^{d_A} rb_i$.
- Τέλος επιστρέφει το sbb_i^A στον ψηφοφόρο i
- Ανακοίνωση από RA του συνολικού αριθμού ψηφοφόρων μέσω λίστας

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

Αναλυτική περιγραφή FOO92 III

3 Ψηφοφορία: Ενέργειες Ψηφοφόρου

- Αποτύφλωση υπογεγραμμένου ψηφοδέλτιου

$$sb_i^A = \text{unblind}(sbb_i^A) = b_i^{d_A}$$

- 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).

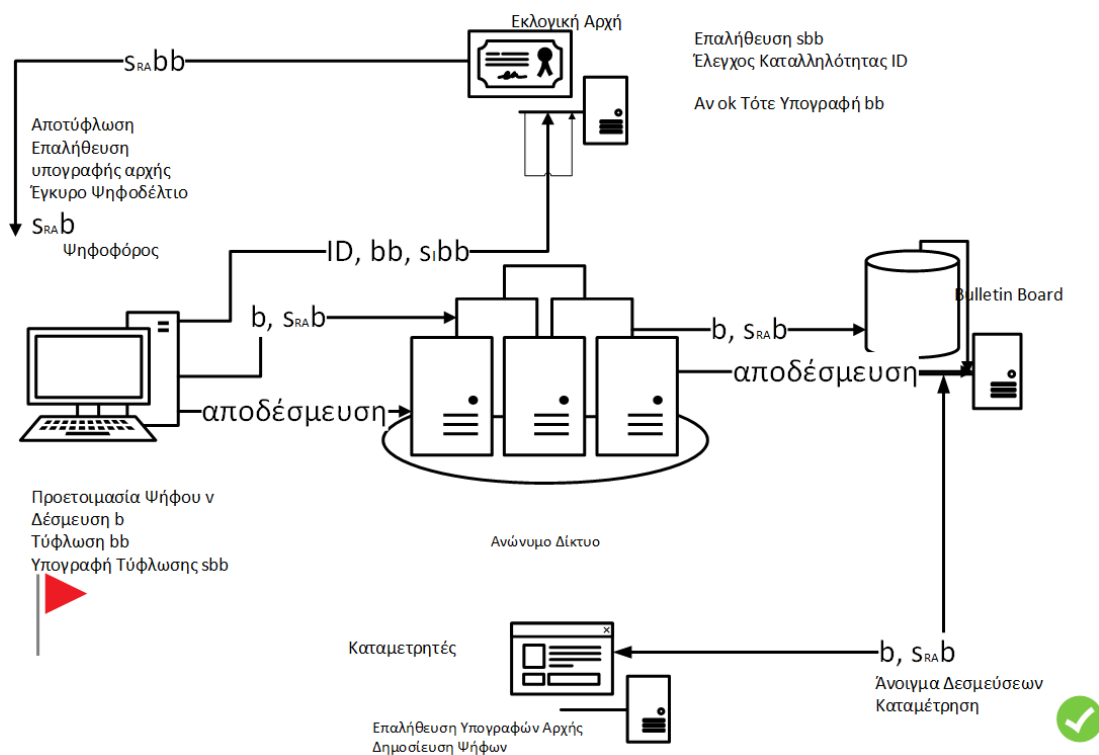
Αναλυτική περιγραφή FOO92 IV

- 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 AA

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

Το τελικό πρωτόκολλο



Συζήτηση FOO

- Privacy
 - Commitment scheme
 - Blindness
 - Anonymous Channel
- Verifiability: Δημόσια εκτελέσιμες ενέργειες
 - Individual: Υπαρξη $\{uid_i, b_i, sb_i^A\}$ 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 ΝΙΖΚΡ (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
- Εναλλακτικές μέθοδοι υπολογισμού αποτελέσματος
 - σε συνδυασμό με ομομορφικά συστήματα
- Coercion resistance
 - Απαραίτητο για internet voting
 - Κάθε ψηφοφόρος: Δυνατότητα πολλών επιλογών
 - Εκβιαστής: Δεν μπορεί να αποφανθεί αν πέτυχε η προσπάθειά του

Βιβλιογραφία I

- B. Adida. Advances in cryptographic voting systems. PhD thesis, Massachusetts Institute of Technology, 2006.
- David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Commun. ACM, 24(2):84–88, 1981.
- David Chaum. Blind signatures for untraceable payments. In D. Chaum, R.L. Rivest, and A.T.Sherman, editors, Advances in Cryptology Proceedings of Crypto 82, pages 199–203, 1983.
- Josh D. Cohen and Michael J. Fischer. A robust and verifiable cryptographically secure election scheme (extended abstract). In FOCS, pages 372–382, 1985.
- Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. A secure and optimally efficient multi-authority election scheme. pages 103–118. Springer-Verlag, 1997
- J. Alex Halderman. Securing digital democracy. Coursera Online Course, September 2012.
- Ari Juels, Dario Catalano, and Markus Jakobsson. Coercion-resistant electronic elections. In Proceedings of the 2005 ACM workshop on Privacy in the electronic society, pages 61–70. ACM, 2005.
- Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta. A practical secret voting scheme for large scale elections. In Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques: Advances in Cryptology, ASIACRYPT '92, pages 244–251, London, UK, UK, 1993. Springer-Verlag.
- ABE Masayuki. Mix-networks on permutation networks. In ASIACRYPT'99, page 258. Springer.
- Choonsik Park, Kazutomo Itoh, and Kaoru Kurosawa. Efficient anonymous channel and all/nothing election scheme. In EUROCRYPT, pages 248–259, 1993.
- B. Pfitzmann and A. Pfitzmann. How to break the direct rsa-implementation of mixes. In Advances in Cryptology—EUROCRYPT'89, pages 373–381. Springer, 1990
- Introduction to Electronic Voting, Filip Zagórski
- Cryptographic Voting — A Gentle Introduction, David Bernhard and Bogdan Warinschi