Τυφλές υπογραφές και εφαρμογές

Παναγιώτης Γροντάς - Άρης Παγουρτζής - Αλέξανδρος Ζαχαράκης

15/01/2021

ΕΜΠ - Κρυπτογραφία (2020-2021)

Motivation

- Ψηφιακές Υπογραφές: Δημόσια επαληθεύσιμες
  - Ακεραιότητα
  - Αυθεντικότητα
  - Μη - Αποκήρυξη
- Χωρίς ιδιωτικότητα όμως...
- Ο $\mathcal{S}$ βλέπει το μήνυμά μας
- Επίσης μπορεί να συσχετίσει την υπογραφή με το αίτημα δημιουργίας της
- Κάτι τέτοιο δεν είναι πάντοτε επιθυμητό
  - Ηλεκτρονικό χρήμα
  - Ηλεκτρονικές ψηφοφορίες

Ηλεκτρονικό χρήμα

- Νόμισμα $c \leftarrow\!\!\$\, \{0,1\}^*$ με συγκεκριμένη αξία
- Για αποφυγή double-spending: υπογραφή από τράπεζα
- Διαφορετική υπογραφή για διαφορετικές αξίες

Διαδικασία αγοράς:

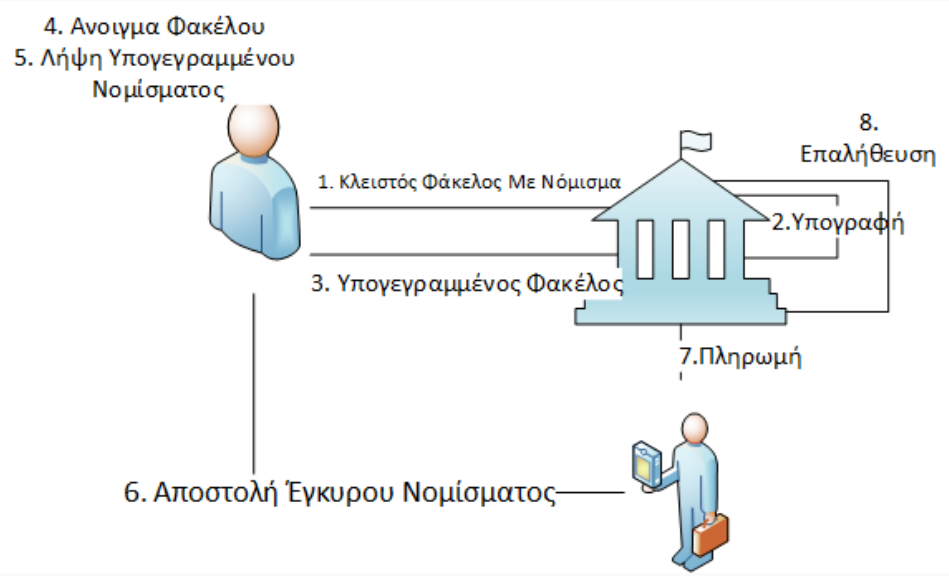
- Ο **Αγοραστής** ζητάει από την **Τράπεζα** ένα νόμισμα c.
- Ο **Αγοραστής** αγοράζει κάτι από τον **Πωλητή**.
- Ο **Πωλητής** επικοινωνεί με την τράπεζα για να βεβαιώσει ότι το νόμισμα δεν έχει ξαναξοδευτεί. Αν δεν έχει ξαναξοδευτεί το δέχεται και ολοκληρώνει τη συναλλαγή.
- Η **Τράπεζα** μαρκάρει το νόμισμα c ως ξοδεμένο.
- Αργότερα ο **Πωλητής** παίρνει από την τράπεζα την αξία ενός νομίσματος.

Όμως: Η **Τράπεζα** γνωρίζει πού ξοδεύτηκε το νόμισμα

Ανώνυμο Ηλεκτρονικό χρήμα

Λύση:

- Το νόμισμα μπαίνει σε ένα φάκελο
- Η **Τράπεζα** υπογράφει το φάκελο
- Η υπογραφή μεταφέρεται στο νόμισμα
- Το νόμισμα βγαίνει από τον φάκελο πριν ξοδευτεί
- Η **Τράπεζα** δεν μπορεί να συσχετίσει νόμισμα με φάκελο



RSA Blind Signatures

- $((N, e), d) \leftarrow \mathsf{KGen}(1^\lambda)$
- $(m', r) \leftarrow \mathsf{Blind}(m, (N, e))$
  $r \leftarrow\!\!\$\ \mathbb{Z}_N^*$
  $m' \leftarrow \mathsf{H}(m) \cdot r^e \bmod N$
- $\mathrm{Sig}' \leftarrow \mathsf{Sign}(m', d, (e, N))$
  $\mathrm{Sig}' \leftarrow m'^d \bmod N$
- $\mathrm{Sig} \leftarrow \mathsf{Unblind}(\mathrm{Sig}', r, (e, N))$
  $\mathrm{Sig} \leftarrow \mathrm{Sig}' \cdot r^{-1} \bmod N$
- $b \leftarrow \mathsf{Vf}(m, \sigma, (e, N))$
  $b \leftarrow \mathrm{Sig}^e \stackrel{?}{=} \mathsf{H}(m) \pmod N$

Ορθότητα

Ας υποθέσουμε ότι υπογράφηκε το μήνυμα m και πήραμε υπογραφή Sig. Τότε θα έχουμε

$$\begin{aligned}\mathrm{Sig}^e &\equiv (\mathrm{Sig}' \cdot r^{-1})^e \equiv (m'^d \cdot r^{-1})^e \\ &\equiv ((\mathsf{H}(m) \cdot r^e)^d \cdot r^{-1})^e \\ &\equiv (\mathsf{H}(m)^d \cdot r \cdot r^{-1})^e \\ &\equiv \mathsf{H}(m) \pmod N\end{aligned}$$

και ο $\mathcal{V}$ αποδέχεται.

Τυφλότητα (Διαισθητικά)

Κάθε υπογραφή εξαρτάται από m, r

Μία σχέση - δύο άγνωστοι

Σύνταξη τυφλών υπογραφών

Ορισμός
Ένα σχήμα τυφλών υπογραφών είναι μια τριάδα $\Pi = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vf})$:

- Δημιουργία δημοσίων κλειδιών και παραμέτρων:
  $(\mathsf{sk}, \mathsf{vk}, \mathsf{prms}) \leftarrow \mathsf{KGen}(1^\lambda)$
- Υπογραφή:
  $\mathsf{Sig} \leftarrow \mathsf{Sign}\langle \mathcal{S}(\mathsf{sk}), \mathcal{U}(m), \mathsf{vk} \rangle$
  Το Sign είναι πρωτόκολλο και όχι αλγόριθμος όπως στις ψηφιακές υπογραφές
  Περιλαμβάνει Blind, Sign, Unblind:
- Επαλήθευση:
  $\{0, 1\} \leftarrow \mathsf{Vf}(m, \mathsf{Sig}, \mathsf{vk})$

Ορθότητα:
$\mathsf{Vf}(m, \mathsf{Sign}\langle \mathcal{S}(\mathsf{sk}), \mathcal{U}(m), \mathsf{vk} \rangle, \mathsf{vk}) = 1$ για $(\mathsf{sk}, \mathsf{vk}, \mathsf{prms}) \leftarrow \mathsf{KGen}(1^\lambda)$

Ιδιωτικότητα

Ο αντίπαλος είναι ο υπογράφων $\mathcal{S}$

- Δεν πρέπει να μαθαίνει τίποτα για το μήνυμα που θα υπογράψει
- Βλέποντας μήνυμα και υπογραφή να μην μπορεί να το συσχετίσει με κάποια εκτέλεση του Sign.

Algorithm 1: $\mathsf{BlindGame}_{\Pi,\mathcal{A}}$

Input : λ

Output: $\{0,1\}$

$(\mathsf{prms}, \mathsf{vk}, \mathsf{sk}, m_0, m_1) \leftarrow \mathcal{A}(\textbf{find}, 1^\lambda)$

$b \leftarrow\!\!\$\ \{0,1\}$

$\mathsf{Sig}_b \leftarrow \mathsf{Sign}\langle \mathcal{A}(\textbf{issue}, \mathsf{sk}), \mathcal{U}(m_b), \mathsf{vk}\rangle$

$\mathsf{Sig}_{1-b} \leftarrow \mathsf{Sign}\langle \mathcal{A}(\textbf{issue}, \mathsf{sk}), \mathcal{U}(m_{1-b}), \mathsf{vk}\rangle$

if $\mathsf{Vf}(m_b, \mathsf{Sig}_b, \mathsf{vk}) = 1$ **AND** $\mathsf{Vf}(m_{1-b}, \mathsf{Sig}_{1-b}, \mathsf{vk}) = 1$ **then**

 | $b' \leftarrow \mathcal{A}(\textbf{guess}, \mathsf{Sig}_0, \mathsf{Sig}_1)$

end

return $b = b'$

Blindness

Perfect Blindness

Ένα σχήμα τυφλών υπογραφών Π είναι **τέλεια μυστικό** αν *για κάθε αντίπαλο* $\mathcal{A}$ ισχύει ότι

$$\mathsf{Pr}[\mathsf{BlindGame}_{\Pi,\mathcal{A}}(1^\lambda) = 1] = \frac{1}{2}$$

Computational Blindness

Ένα σχήμα τυφλών υπογραφών Π είναι **υπολογιστικά μυστικό** αν *για κάθε PPT αντίπαλο* $\mathcal{A}$ ισχύει ότι

$$\mathsf{Pr}[\mathsf{BlindGame}_{\Pi,\mathcal{A}}(1^\lambda) = 1] \leq \frac{1}{2} + \mathsf{negl}(\lambda)$$

Unforgeability

- Δεν δουλεύουν οι ορισμοί των απλών υπογραφών: γιατί το existential forgery είναι η ουσία των τυφλών υπογραφών.
- Αναλυτικά:
  - Ο $\mathcal{S}$ δημιούργησε (m', Sig')
  - Ο $\mathcal{U}$ από αυτό έφτιαξε (m, Sig)
  - ... για το οποίο $\text{Vf}(m, \text{Sig}, \text{vk}) = 1$

Ορίζουμε το unforgeability με βάση το σενάριο χρήσης του e-cash.

Ο χρήστης (αντίπαλος) δεν μπορεί να φτιάξει περισσότερα νομίσματα από αυτά που έδωσε η τράπεζα.

One-more unforgeability

One-more unforgeability

Algorithm 2: $\mathsf{OneMoreForge}_{\mathcal{A},\Pi}$

Input : λ

Output: $\{0,1\}$

$(\mathsf{sk},\mathsf{vk},\mathsf{prms}) \leftarrow \mathsf{KGen}(1^{\lambda})$

$\{(m_i,\mathsf{Sig}_i)\}_{i=1}^{l+1} \leftarrow \mathsf{Sign}\langle \mathcal{S}(\mathsf{sk}), \mathcal{A}(\cdot), \mathsf{vk}\rangle_{i=1}^{\mathsf{poly}(\lambda)}$

if $(\forall i,j \in [l+1]$ με $i \neq j \Rightarrow m_i \neq m_j)$ **AND** $(\forall i \in [l+1]\, \mathsf{Vf}(m_i,\mathsf{Sig}_i,\mathsf{vk}) = 1)$ **AND** $k \leq l$ **then**

  return 1

else

  return 0

end

One-more unforgeability

Definition
Ένα σχήμα τυφλών υπογραφών είναι **One-More Unforgeable** αν για κάθε PPT αντίπαλο $\mathcal{A}$ που εκτελεί το πολύ poly(λ) πρωτόκολλα Sign ισχύει ότι

$$\Pr[\text{OneMoreForge}_{\Pi,\mathcal{A}}(1^\lambda) = 1] \leq \text{negl}(\lambda)$$

Definition
Ένα σχήμα τυφλών υπογραφών είναι **Strongly One-More Unforgeable** αν για κάθε PPT αντίπαλο $\mathcal{A}$ που εκτελεί το πολύ poly$log(\lambda)$ πρωτόκολλα Sign ισχύει ότι

$$\Pr[\text{OneMoreForge}_{\Pi,\mathcal{A}}(1^\lambda) = 1] \leq \text{negl}(\lambda)$$

RSA Blind Signatures - Blindness

Θεώρημα
Οι υπογραφές RSA παρέχουν perfect blindness

Στο BlindGame ο αντίπαλος βλέπει:

$\text{view}_i = (m'_i, \text{Sig}'_i)$, Sig_j για $i, j \in \{0, 1\}$

Σε κάθε περίπτωση υπάρχει μοναδικό r ώστε view_i να αντιστοιχεί στο Sig_j

Συγκεκριμένα $r = \text{Sig}'_i \cdot \text{Sig}_j^{-1}$

Άρα η καλύτερη στρατηγική του $\mathcal{A}$ είναι να μαντέψει στην τύχη.

RSA Blind Signatures - Unforgeability

Algorithm 3: RSA-CTI πρόβλημα

Input : λ

Output: $\{0, 1\}$

$(d, (e, n)) \leftarrow \mathsf{KGen}(1^\lambda)$

for $i \leftarrow 1$ **to** $n(\lambda)$ **do**

  $y_i \leftarrow\!\!\$\ \mathbb{Z}_n^*$

end

$(\pi, \{x_i\}_{i=1}^{m(\lambda)+1}) \leftarrow \mathcal{A}^{(\cdot)^d}(n, e, \{y_i\}_{i=1}^{n(\lambda)})$

if $\pi : [m(\lambda) + 1] \mapsto [n(\lambda)]$ *είναι 1-1* **AND** $\forall i \in [m(\lambda) + 1] : x_i^e = y_{\pi(i)}$ **AND** *έγιναν το πολύ* $m(\lambda)$ *queries στο inversion oracle* **then**

  return 1

else

  return 0

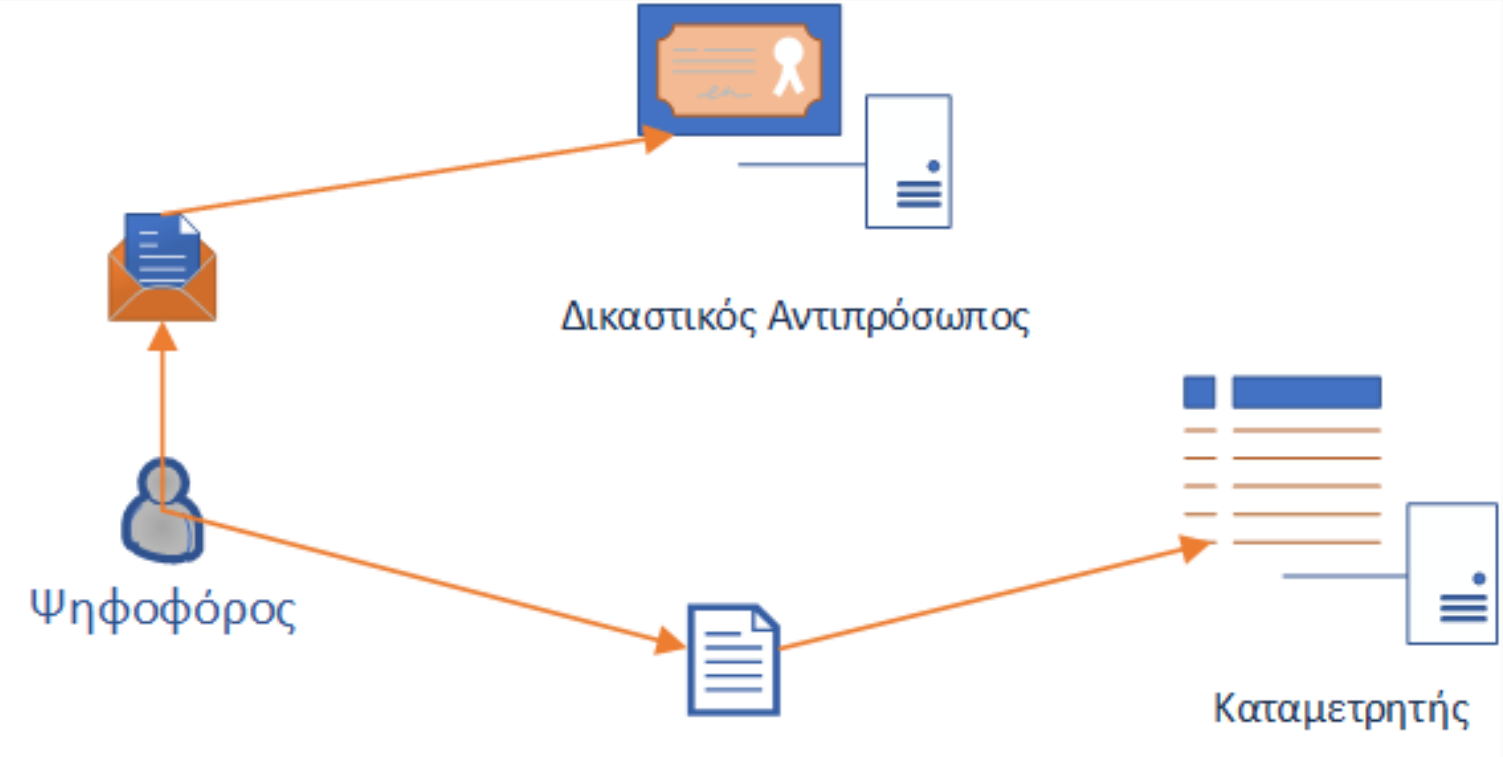
end

Θεώρημα

Οι υπογραφές RSA παρέχουν one-more forgery αν το πρόβλημα RSA-CTI είναι δύσκολο

Ψηφοφορίες με Τυφλές Υπογραφές

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

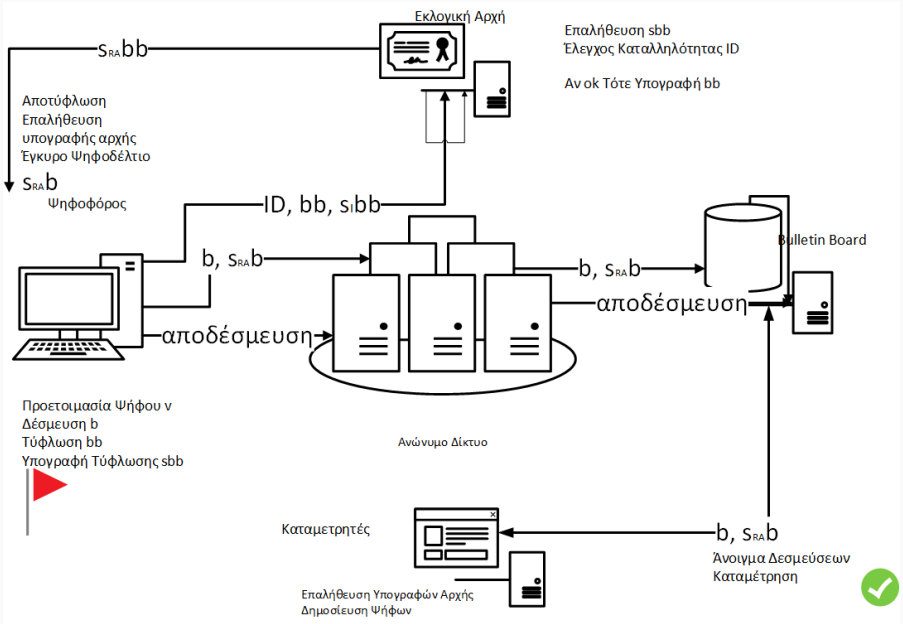


Ψηφοφορίες με Τυφλές Υπογραφές

- 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 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.

Ψηφοφόρος: Προετοιμασία

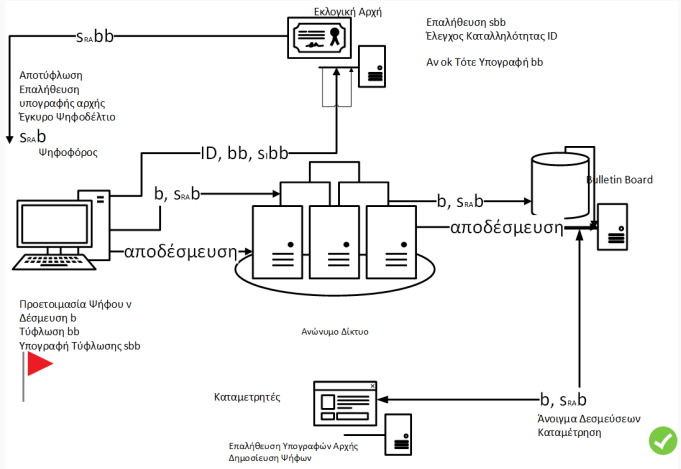
- Επιλογή ψήφου v_i
- Δέσμευση στην ψήφο με τυχαιότητα rc_i.
- Το ψηφοδέλτιο είναι: $b_i = commit(v_i, rc_i) = g^{rc_i} h^{v_i}$
- Τύφλωση του ψηφοδελτίου με rb_i και δημόσιο κλειδί της αρχής $bb_i = \text{Blind}(b_i, rb_i)$
- Υπογραφή τυφλωμένου ψηφοδέλτιου: $sbb_i^v = \text{Sign}_{d_i}(bb_i)$
- Αποστολή (id_i, bb_i, sbb_i^v) στην εκλογική αρχή (RA)



Αναλυτική περιγραφή FOO92 ii

RA:Εξουσιοδότηση

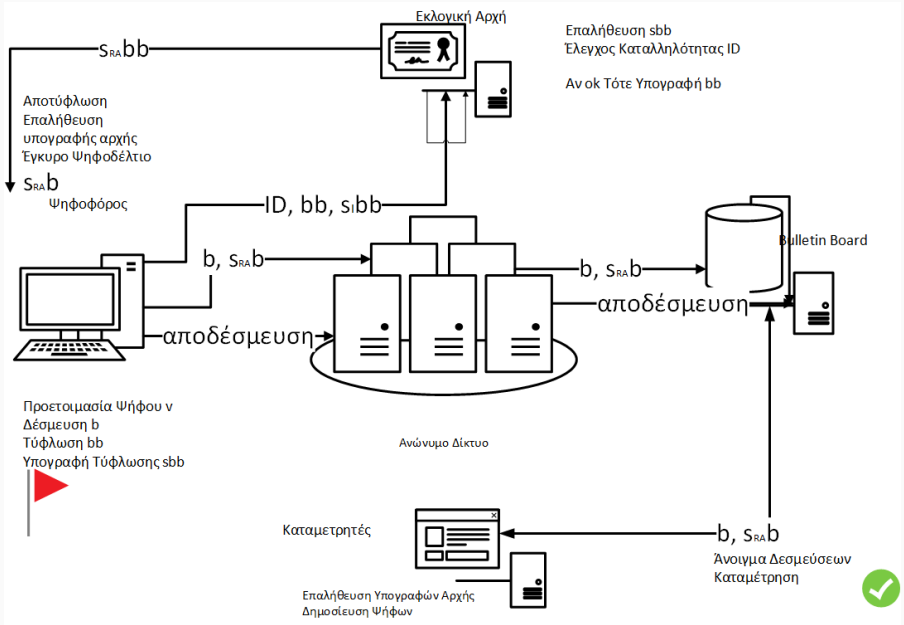
- Έλεγχοι με τη βοήθεια ενός πίνακα $T = \{id_i, e_i\}$ που περιέχει τις ταυτότητες και τα δημόσια κλειδιά των εγγεγραμμένων ψηφοφόρων:
  - το δικαίωμα του να ψηφίσει $id_i \in T$
  - υπογραφή του ψηφοφόρου με e_i
  - αν έχει ξαναψηφίσει
- Επιτυχείς έλεγχοι $\rightarrow$ έγκριση μέσω υπογραφής του τυφλωμένου ψηφοδελτίου $sbb_i^A = \mathrm{Sign}_{d_A}(bb_i)$.
- 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

Ψηφοφορία: Ενέργειες Ψηφοφόρου

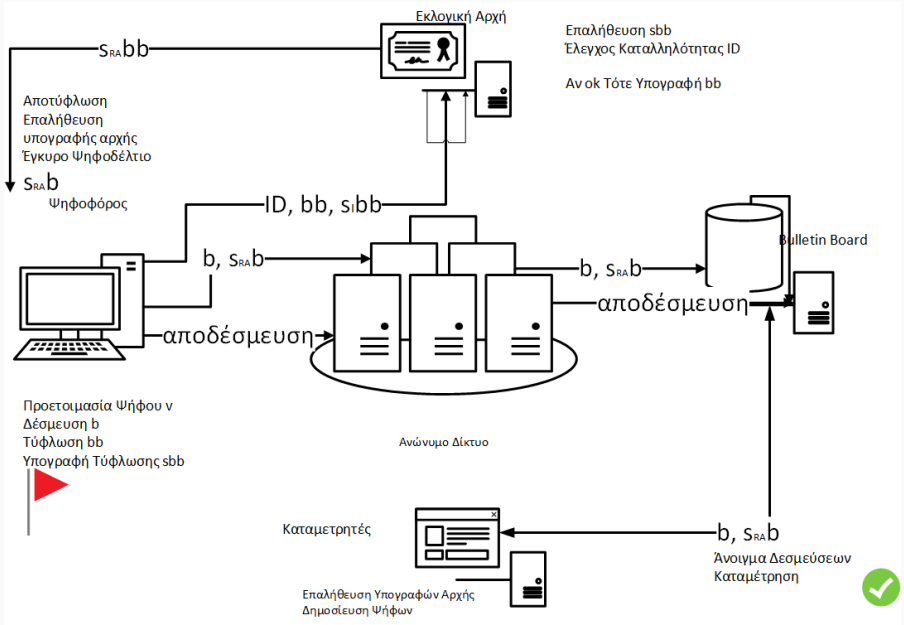
- Αποτύφλωση υπογεγραμμένου ψηφοδελτίου
  $sb_i^A = \text{Unblind}(sbb_A^i)$
- Προκύπτει υπογεγραμμένη η αρχική δέσμευση (επαληθεύσιμη από όλους)
- Κατάθεση ψήφου: Αποστολή των b_i, sb_i^A στην αρχή καταμέτρησης
- Χρήση ανώνυμου καναλιού (πχ. δίκτυο μίξης) για απόκρυψη στοιχείων που ίσως προδώσουν την ταυτότητα του ψηφοφόρου (πχ. δικτυακές διευθύνσεις).



Αναλυτική περιγραφή FOO92 iv

Καταμετρητές: Συλλογή

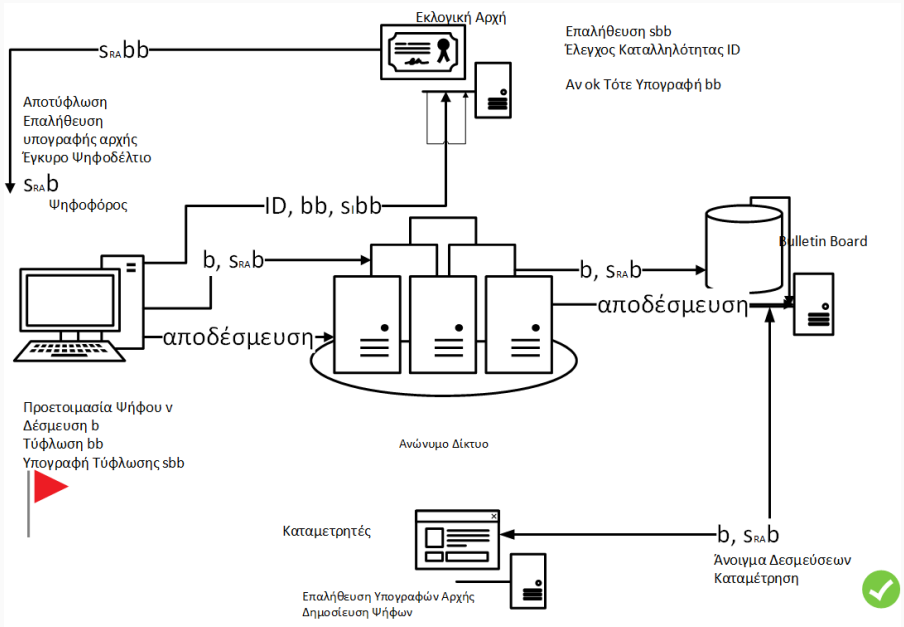
- Λαμβάνει ψηφοδέλτιο b_i, sb_i^A
- Η αρχή καταμέτρησης επαληθεύει την υπογραφή της αρχής σε κάθε ψηφοδέλτιο sb_i^A με το e_A
- Όσα ψηφοδέλτια πέρασαν τον έλεγχο δημοσιεύονται σε μια λίστα $\{uid_i, b_i, sb_i^A\}$, όπου uid_i είναι ένα τυχαίος αριθμός ή ένας ΑΑ



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



Αναλυτική περιγραφή FOO92 vi

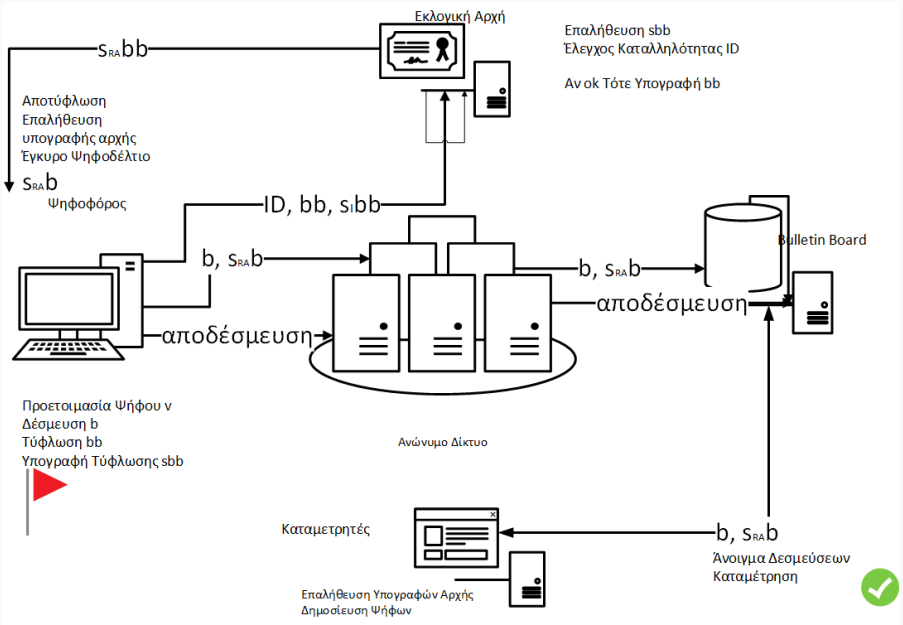
Καταμέτρηση

- Δημοσίευση 'ανώνυμων' ψηφοδελτίων
- Καταμέτρηση από κάθε ενδιαφερόμενο

Συζήτηση: Privacy

- Commitment scheme
- Blindness
- Anonymous Channel

Δεν χρειάζεται εμπιστοσύνη στους καταμετρητές



Τυφλές υπογραφές από Σ-πρωτόκολλα

Ισοδύναμη μορφή υπογραφής Schnorr

- Ιδιωτικό κλειδί: $x \leftarrow_{\$} \mathbb{Z}_q$, Δημόσιο: $h = g^x$
- Ο $\mathcal{S}$ στέλνει $y = g^t,\ t \leftarrow_{\$} \mathbb{Z}_q$
- Ο $\mathcal{U}$ στέλνει $c = \mathsf{H}(y||m)$
- Ο $\mathcal{S}$ στέλνει $s = t + cx$
- Δημόσια επαλήθευση $\mathsf{Sig} = (y, s)$:
  - Υπολογισμός $c = \mathsf{H}(y||m)$
  - Έλεγχος $g^s = yh^c$

Για τυφλότητα θα πρέπει:

- Το c να μην περιέχει καμία πληροφορία για το μήνυμα m.
- Το Sig να μην “προδίδει” μια συγκεκριμένη εκτέλεση του πρωτοκόλλου.
- Άρα πρέπει να τυφλωθούν (μετάθεση)

Τυφλές υπογραφές Schnorr

Sign

Signer		Recipient
input:x, h		input:m, h
Commit $t \leftarrow\$ \mathbb{Z}_q, y \leftarrow g^t$		
	$\xrightarrow{y}$	
		$\alpha, \beta \leftarrow\$ \mathbb{Z}_q$
		$y' \leftarrow y g^{\alpha} h^{\beta}$
		$c' = \mathrm{H}(y' \| \| m)$
		$c \leftarrow c' + \beta$
	$\xleftarrow{c}$	
$s = t + cx$		
	$\xrightarrow{s}$	
		$s' = s + \alpha$
		$\mathrm{Sig} = (y', s')$

Επαλήθευση: $c' = \mathrm{H}(y' || m)$

Πρώτο μέλος σχέσης επαλήθευσης

$g^{s'} = g^{s+\alpha} = g^{t+cx} g^{\alpha} = y h^{c} g^{\alpha}$

Δεύτερο μέλος σχέσης επαλήθευσης

$y' h^{c'} = y g^{\alpha} h^{\beta} h^{c-\beta} = y g^{\alpha} h^{c}$

Blindness

Θεώρημα
Οι υπογραφές Schnorr παρέχουν perfect blindness

Για κάθε $\text{view}_i = (y_i, c_i, s_i)$ και $m_j, \text{Sig}_j = (y'_j, s'_j)$
υπάρχει μοναδικό ζεύγος (α, β) τέτοιο ώστε το
view_i να αντιστοιχεί στο Sig_j

$\alpha = s'_j - s_i$
$\beta = c_i - c'_j = c_i - \text{H}(y'_j || m_j)$

Κατά συνέπεια ο αντίπαλος στο BlindGame πρέπει να μαντέψει στην τύχη

Unforgeability - One More Discrete Logarithm

Algorithm 4: OMDL πρόβλημα

Input : λ

Output: $\{0,1\}$

$(q, \mathbb{G}, g) \leftarrow \mathsf{KGen}(1^{\lambda})$

for $i \leftarrow 1$ **to** $n(\lambda)$ **do**

  $h_i \leftarrow\!\!\$\, \mathbb{G}$

end

$(\pi, \{x_i\}_{i=1}^{m(\lambda)+1}) \leftarrow \mathcal{A}^{DLOG()}(n, e, \{h_i\}_{i=1}^{n(\lambda)})$

if $\pi : [m(\lambda)+1] \mapsto [n(\lambda)]$ *είναι 1-1* **AND** $\forall i \in [m(\lambda)+1] : g^{x_i} = h_{\pi(i)}$ **AND** *έγιναν το πολύ* $m(\lambda)$ *queries στο DLOG oracle* **then**

  return 1

else

  return 0

end

Αναπαράσταση στοιχείου σε ομάδα

Ορισμός
Έστω $\mathbb{G}$ ομάδα τάξης q και $g_1, g_2 \in G$. Αναπαράσταση του $h \in \mathbb{G}$ ως προς g_1, g_2 ονομάζεται κάθε ζεύγος $x_1, x_2 \in \mathbb{Z}_q$ τέτοιο ώστε $h = g_1^{x_1} g_2^{x_2}$.

Αν ξέρω δύο αναπαραστάσεις του h ως προς g_1, g_2 τότε ξέρω διακριτό λογάριθμο w του g_2 ως προς g_1:

$$
\begin{aligned}
g_1^{x_1} g_2^{x_2} &= g_1^{x_1'} g_2^{x_2'} \Rightarrow \\
g_1^{x_1} g_1^{w x_2} &= g_1^{x_1'} g_1^{w x_2'} \Rightarrow \\
g_1^{x_1 + w x_2} &= g_1^{x_1' + w x_2'} \Rightarrow \\
x_1 + w x_2 &= x_1' + w x_2' \Rightarrow \\
w &= \frac{x_1' - x_1}{x_2 - x_2'}
\end{aligned}
$$

Πρωτόκολλο Okamoto Schnorr

PoK Representation

$$\left\{(\mathbb{G}, q, g_1, g_2, h), (x_1, x_2) : h = g_1^{x_1} g_2^{x_2}\right\}$$

$\Sigma - \mathit{Protocol}$:

1. $\mathcal{P}$: $t_1, t_2 \leftarrow_{\$} \mathbb{Z}_q$; $y \leftarrow g_1^{t_1} g_2^{t_2}$; **Στέλνει** y.
2. $\mathcal{V}$: $c \leftarrow_{\$} \mathbb{Z}_q$; **Στέλνει** c.
3. $\mathcal{P}$: $s_1 = t_1 + x_1 c$; $s_2 = t_2 + x_2 c$;
   Στέλνει s_1, s_2.
4. $\mathcal{P}$: **Αποδέχεται αν** $g_1^{s_1} g_2^{s_2} = y h^c$.

Τυφλές υπογραφές Okamoto Schnorr

KGen(1^λ)

- Επιλέγεται ομάδα $\mathbb{G}$ τάξης πρώτου q με δύσκολο DLOG.
- Επιλέγονται $g_1, g_2 \leftarrow_\$ \mathbb{G}$.
- Επιλέγονται $x_1, x_2 \leftarrow_\$ \mathbb{Z}_q$
- $h \leftarrow g_1^{x_1} g_2^{x_2}$
- Έξοδος
  - params $= (\mathbb{G}, q, g_1, g_2)$
  - sk $= (x_1, x_2)$
  - vk $= h$

Τυφλές υπογραφές Okamoto Schnorr

Sign

Signer		Recipient
input:(x_1, x_2)		input:m
$t_1, t_2 \leftarrow_R \mathbb{Z}, y = g_1^{t_1} g_2^{t_2}$		
	$\xrightarrow{y}$	
		$u_1, u_2, d \leftarrow\$ \mathbb{Z}_q$
		$y' \leftarrow y g_1^{u_1} g_2^{u_2} h^d$
		$c' \leftarrow \mathrm{H}(y', m)$
		$c \leftarrow c' + d$
	$\xleftarrow{c}$	
$s_1 = t_1 + x_1 c$		
$s_2 = t_2 + x_2 c$		
	$\xrightarrow{s_1, s_2}$	
		$\mathrm{Sig}_1 = s_1 + u_1$
		$\mathrm{Sig}_2 = s_2 + u_2$
		$g_1^{\mathrm{Sig}_1} g_2^{\mathrm{Sig}_2} \stackrel{?}{=} y h^c$

Ανάλυση ασφάλειας

Blindness: Με τρόπο ανάλογο ως προς το Schnorr
Unforgeability: Αν μπορούν να παραχθούν $l + 1$ υπογραφές με l (παράλληλες) συνόδους τότε ο μπορεί να λυθεί το DLOG
Χρησιμοποιείται και το RO
Pointcheval-Stern 2000: αμελητέα πιθανότητα επιτυχίας αν $l = \mathcal{O}(polylog(\lambda))$

Βιβλιογραφία

1. Chaum, D. (1983). ”Blind signatures for untraceable payments”. Advances in Cryptology Proceedings of Crypto. 82 (3): 199–203.
2. Chaum, D. (1985). ”Security without identification: transaction systems to make big brother obsolete”. Commun. ACM 28, 10 (Oct. 1985), 1030–1044.
3. Bellare M., Namprempre C., Pointcheval D., Semanko M. (2003). The One-More-RSA-Inversion Problems and the Security of Chaum’s Blind Signature Scheme . J. Cryptology 16, 185–215.
4. Claus-Peter Schnorr. “Efficient Signature Generation by Smart Cards”. In: J. Cryptology 4.3 (1991), pages 161–174.
5. David Chaum and Torben P. Pedersen. “Wallet Databases with Observers”. In: Advances in Cryptology - CRYPTO ’92.
6. Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta. “A Practical Secret Voting Scheme for Large Scale Elections”. In: Advances in Cryptology - AUSCRYPT ’92
7. Tatsuaki Okamoto. “Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes”. In: Advances in Cryptology - CRYPTO ’92
8. Pointcheval, D., Stern, J. Security Arguments for Digital Signatures and Blind Signatures . J. Cryptology 13, 361–396 (2000)
9. Claus-Peter Schnorr. “Security of Blind Discrete Log Signatures against Interactive Attacks”. In: Information and Communications Security, Third International Conference, ICICS 2001, Xian, China, November 13-16, 2001
10. Georg Fuchsbauer, Antoine Plouviez, and Yannick Seurin. “Blind Schnorr Signatures and Signed ElGamal Encryption in the Algebraic Group Model”. In: EUROCRYPT (2). Volume 12106. Lecture Notes in Computer Science. Springer, 2020, pages 63–95