Τυφλές Υπογραφές

Μοντέλα Ασφάλειας - Κατασκευές - Εφαρμογές - Επιθέσεις

Παναγιώτης Γροντάς

01/06/2023

ΕΜΠ - Advanced Crypto (2022-2023)

Εισαγωγή

Motivation

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

Ηλεκτρονικό χρήμα με TTP

- Νόμισμα $c \leftarrow\$ \{0,1\}^*$ με συγκεκριμένη αξία (πχ. 1)
- Για ασφάλεια (αποφυγή double, overspending): υπογραφή από τράπεζα

Διαδικασία αγοράς:

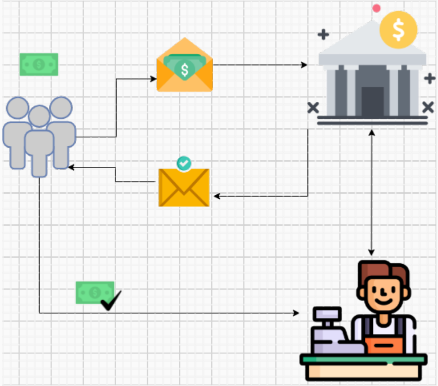
- Ο **Αγοραστής** ζητάει από την **Τράπεζα** ένα νόμισμα c.
- Ο **Αγοραστής** αγοράζει κάτι από τον **Πωλητή** με το c.
- Ο **Πωλητής** επικοινωνεί με την τράπεζα για να βεβαιώσει ότι το c δεν έχει ξαναξοδευτεί.
  Αν δεν έχει ξαναξοδευτεί το δέχεται και ολοκληρώνει τη συναλλαγή.
- Η **Τράπεζα** μαρκάρει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

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

Ανώνυμο Ηλεκτρονικό χρήμα (με TTP)

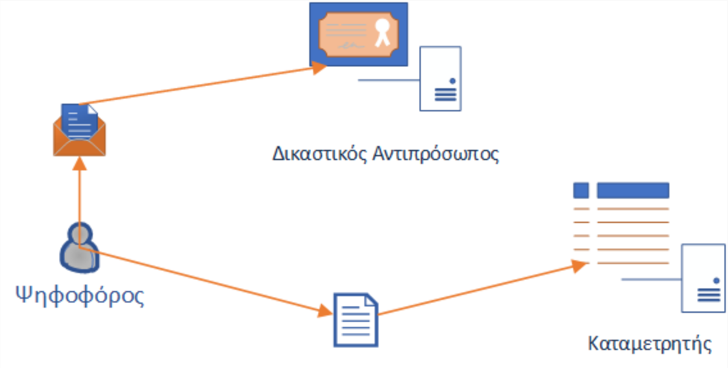
Λύση: Φάκελος με καρμπόν [?]

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



Η υπογραφή είναι τυφλή.

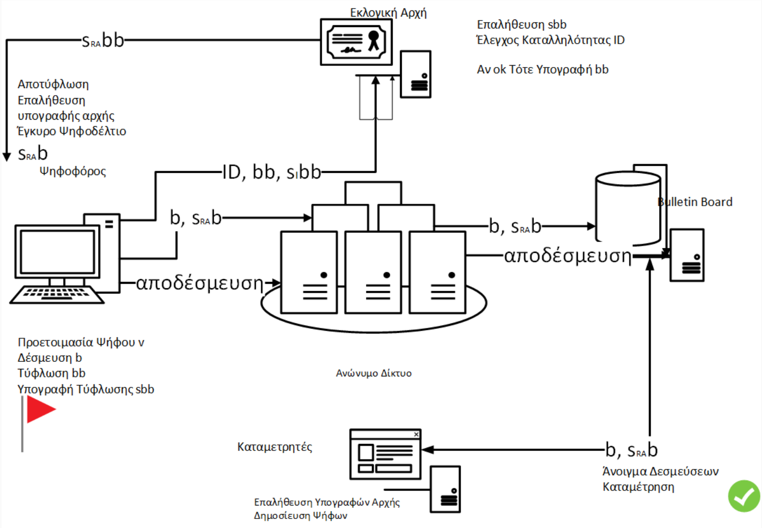
Βασική ιδέα [?]: Πώς θα δούλευαν οι παραδοσιακές ψηφοφορίες αν οι δικαστικοί αντιπρόσωποι ήταν σε διαφορετικό φυσικό χώρο από τους καταμετρητές



Ψηφοφορίες με Τυφλές Υπογραφές ii

- 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.

Ψηφοφορίες με Τυφλές Υπογραφές iii



Ψηφοφορίες με Τυφλές Υπογραφές iv

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

$$b_i = \mathsf{Commit}(v_i, r_{c_i})$$

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

$$bb_i = \mathsf{Blind}_{\mathsf{pk}_{EA}}(b_i, r_{b_i})$$

   - Υπογραφή τυφλωμένου ψηφοδέλτιου:

$$sbb_i = \mathsf{Sign}_{\mathsf{sk}_i}(bb_i)$$

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

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

$$(id_i, bb_i, sbb_i)$$

Ψηφοφορίες με Τυφλές Υπογραφές vi

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

$$sb_i = \mathsf{Unblind}(sbb_i)$$

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

Ψηφοφορίες με Τυφλές Υπογραφές vii

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

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

Ιδιότητες

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

Μοντελοποίηση

Σύνταξη τυφλών υπογραφών

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

- $(\mathsf{sk}, \mathsf{vk}, \mathsf{prms}) \leftarrow \mathsf{KGen}(1^\lambda)$
  Δημιουργία κλειδιών και κρυπτογραφικών παραμέτρων
- $\sigma \leftarrow \mathsf{Sign}\langle \mathcal{S}(\mathsf{sk}), \mathcal{U}(m), \mathsf{vk} \rangle$
  Το Sign είναι *πρωτόκολλο* και όχι αλγόριθμος. Συνήθως:
    - $m' := \mathsf{Blind}(m, \mathsf{vk})$ εκτελείται από τον $\mathcal{U}$
    - $\sigma' := \mathsf{Sign}(m', \mathsf{sk})$ όπου ο $\mathcal{S}$ εκτελεί τον *αλγόριθμο* Sign
    - $\sigma := \mathsf{Unblind}(\sigma', \mathsf{vk})$ εκτελείται από τον $\mathcal{U}$
- Επαλήθευση:
  $\{0, 1\} \leftarrow \mathsf{Vf}(m, \sigma, \mathsf{vk})$

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 μάθει τίποτα για το μήνυμα που υπογράφει
- 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: $\{0,1\}$

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

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

$\sigma_b \leftarrow \mathsf{Sign}\langle \mathcal{A}(\mathbf{issue}, \mathsf{sk}), \mathcal{U}(m_b), \mathsf{vk}\rangle$

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

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

    $b' \leftarrow \mathcal{A}(\mathbf{guess}, \sigma_0, \sigma_1)$

end

return $b = b'$

Ο αντίπαλος πρέπει να μαντέψει τη σειρά υπογραφής.

Blindness

Perfect Blindness

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

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

Computational Blindness

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

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

Unforgeability για τυφλές υπογραφές

- Δεν έχει νόημα το μοντέλο των κλασικών υπογραφών (EUF-CMA).
- Εξήγηση:
  - Ο $\mathcal{S}$ δημιούργησε (m', σ')
  - Ο $\mathcal{U}$ από αυτό έφτιαξε (m, σ)
  - ... για το οποίο $\mathsf{Vf}(m, \sigma, \mathsf{vk}) = 1$
  - Δηλ. ο $\mathcal{U}$ έφτιαξε έγκυρη υπογραφή χωρίς να έχει ιδιωτικό κλειδί (έκανε πλαστογράφηση)

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

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

Νέα έννοια unforgeability: **One-more unforgeability**

One-more unforgeability

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

Input : λ

Output: $\{0,1\}$

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

$\{(m_i, \sigma_i)\}_{i=1}^{l+1} \leftarrow \mathsf{Sign}\langle \mathcal{S}(\mathsf{sk}), \mathcal{A}(m_j), \mathsf{vk}\rangle_{j=1}^{k}$

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

  return 1

else

  return 0

end

l: Το μέγιστο πλήθος των sessions $\langle \mathcal{S}, \mathcal{A} \rangle$

Μπορούν να είναι σειριακά ή παράλληλα!

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

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

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

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

Κατασκευές

RSA [?] - με FDH

- $((n, e), d) \leftarrow \mathsf{KGen}(1^\lambda)$
- $(m', r) := \mathsf{Blind}(m, (n, e))$
  $r \leftarrow\$ \mathbb{Z}_n^*$
  $m' \leftarrow \mathsf{H}(m) \cdot r^e \bmod n$
- $\sigma' \leftarrow \mathsf{Sign}(m', d, (n, e))$
  $\sigma' \leftarrow m'^d \bmod N$
- $\sigma \leftarrow \mathsf{Unblind}(\sigma', r, (n, e))$
  $\sigma \leftarrow \sigma' \cdot r^{-1} \bmod N$
- $\mathsf{Vf}(m, \sigma, (n, e)) = 1 \Leftrightarrow \sigma^e \equiv \mathsf{H}(m) \pmod n$

Ορθότητα

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

και ο $\mathcal{V}$ αποδέχεται.

RSA - Blindness

Τυφλότητα (Διαισθητικά)

Κάθε υπογραφή εξαρτάται από m, r - Μία σχέση - δύο άγνωστοι!

Ισχύει ότι $m' \equiv \mathsf{H}(m) r^e \mod n$ δηλαδή $r^e \equiv m' \mathsf{H}(m)^{-1} \pmod n$
Έγκυρη σ για κάθε m με κατάλληλη επιλογή r!

Θεώρημα

Οι υπογραφές RSA παρέχουν perfect blindness

Στο BlindGame ο αντίπαλος βλέπει:

$\mathsf{view}_i = (m'_i, \sigma'_i), \sigma_j$ για $i, j \in \{0, 1\}$

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

Συγκεκριμένα $r = \sigma'_i \cdot \sigma_j^{-1}$

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

RSA - Unforgeability

Algorithm 3: RSA-CTI πρόβλημα

Input : λ

Output: $\{0,1\}$

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

for $i := 1$ **to** m **do**

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

end

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

if $\pi : [l+1] \rightarrow [n]$ *είναι 1-1* **AND** $\forall i \in [l+1] : x_i^e = y_{\pi(i)}$ **AND** $k \leq l$ **then**

  return 1

else

  return 0

end

Θεώρημα

Οι υπογραφές RSA παρέχουν one-more forgeability στο μοντέλο του τυχαίου μαντείου αν το πρόβλημα RSA-CTI είναι δύσκολο.[**?**]

Τυφλές υπογραφές από Σ-πρωτόκολλα

Ισοδύναμη μορφή υπογραφής Schnorr

- Ιδιωτικό κλειδί: $x \leftarrow\$ \mathbb{Z}_q$, Δημόσιο: $Y = g^x$
- Ο $\mathcal{S}$ στέλνει $T = g^t,\ t \leftarrow\$ \mathbb{Z}_q$
- Ο $\mathcal{U}$ στέλνει $c = \mathsf{H}(T, Y, m)$
- Ο $\mathcal{S}$ στέλνει $s = t + cx$
- Δημόσια επαλήθευση $\sigma = (T, s)$:
  - Υπολογισμός $c = \mathsf{H}(T, Y, m)$
  - Έλεγχος $g^s = TY^c$

Διαίσθηση για τυφλότητα

- Ο $\mathcal{S}$ γνωρίζει (T, c, s)
- Η τελική μορφή της υπογραφής πρέπει να τα 'κρύψει'
- Μετατόπιση s κατά α
- Μετατόπιση c κατά β
- Αντίστοιχη μετατόπιση T ώστε να επαληθεύεται η υπογραφή αλλά και να κρύβεται το T

Τυφλές υπογραφές Schnorr

Sign

Signer(x, Y) — User(m, Y)

$t \leftarrow\!\$\, \mathbb{Z}_q, T \leftarrow g^t$

$\xrightarrow{\quad T \quad}$

Blind

$\alpha, \beta \leftarrow\!\$\, \mathbb{Z}_q$

$T' \leftarrow T g^{\alpha} Y^{\beta}$

$c' = \mathsf{H}(T', Y, m)$

$c \leftarrow c' + \beta$

$\xleftarrow{\quad c \quad}$

$s = t + cx$

$\xrightarrow{\quad s \quad}$

Unblind

$s' = s + \alpha$

$\sigma = (T', c', s')$

Επαλήθευση:

$c' = \mathsf{H}(T', Y, m)$

Πρέπει: $g^{s'} = T'Y^{c'}$

Πράγματι:

$$g^{s'} = g^{s+\alpha} = g^{t+cx} g^{\alpha} =$$
$$= TY^c g^{\alpha} = TY^{c'+\beta} g^{\alpha} =$$
$$= Tg^{\alpha}Y^{\beta}Y^{c'} = T'Y^{c'}$$

Blindness

Θεώρημα

Οι υπογραφές Schnorr παρέχουν perfect blindness

Για κάθε $\text{view}_i = (T_i, c_i, s_i)$ και $m_j, \sigma_j = (T'_j, c'_j, s'_j)$ υπάρχει (μοναδικό) ζεύγος (α, β) τέτοιο ώστε το view_i να αντιστοιχεί στο σ_j

$$\alpha = s'_j - s_i$$
$$\beta = c_i - c'_j = c_i - \mathsf{H}(T'_j, Y, m_j)$$

Κατά συνέπεια ο αντίπαλος στο BlindGame πρέπει να μαντέψει στην τύχη

One More Discrete Logarithm

Algorithm 4: OMDL πρόβλημα

Input : λ
Output: $\{0, 1\}$

$(\mathbb{G}, q, g) \leftarrow \mathsf{Pgen}(1^\lambda)$
$\{x_i\}_{i=1}^{m} \leftarrow \mathbb{Z}_q$
for $i \leftarrow 1$ **to** m **do**
  $Y_i := g^{x_i}$
end
$(\pi, \{z_i\}_{i=1}^{l+1}) \leftarrow \mathcal{A}^{\mathsf{DL}}(\mathbb{G}, q, g, (Y_i)_{i=1}^{n})$
if $\forall i \in l+1 : \ y_i = g^{z_{\pi(i)}} \wedge l \leq m$ **then**
  return 1
else
  return 0
end

Blind Schorr Unforgeability ii

Αποτελέσματα Unforgeability

Αναγκαίες συνθήκες:

- Η ασφάλεια του DLP
- Η ασφάλεια του Schnorr identification scheme (Active adversaries: OMDL)

Ικανές συνθήκες σε Standard ή Random Oracle Model:

- Impossibility Results [**?**]
- Το πρόβλημα ROS (συνέχεια)

Δεν μπορεί να χρησιμοποιηθεί το Random Oracle Programmability όπως στις υπογραφές Schnorr ($\mathcal{RO}(T, Y, m) = c$) λόγω του blinding.

Blind Schorr Unforgeability iii

Δεν μπορεί να προσομοιωθεί το $\mathcal{SO}$ χωρίς το ιδιωτικό κλειδί. Πρέπει να του δοθεί το ιδιωτικό κλειδί από τον αντίπαλο (αδύνατο αφού αυτό πρέπει να υπολογίσει ο αντίπαλος)

Αποδείξιμη ασφάλεια: Παραλλαγή Okamoto [**?**] με ικανή συνθήκη το DLP στο μοντέλο του τυχαίου μαντείου.

Βασίζεται σε witness indistinguishability. Ο αντίπαλος θα δημιουργήσει τα κλειδιά και θα προσομοιώσει το με αυτά

Αναπαράσταση στοιχείου σε ομάδα

Ορισμός

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

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

$$\begin{aligned} g_1^{x_1} g_2^{x_2} = g_1^{x'_1} g_2^{x'_2} &\Rightarrow \\ g_1^{x_1} g_1^{wx_2} = g_1^{x'_1} g_1^{wx'_2} &\Rightarrow \\ g_1^{x_1+wx_2} = g_1^{x'_1+wx'_2} &\Rightarrow \\ x_1 + wx_2 = x'_1 + wx'_2 &\Rightarrow \\ w = \frac{x'_1 - x_1}{x_2 - x'_2} & \end{aligned}$$

Τυφλές υπογραφές Okamoto Schnorr [?]

Βασίζονται στο παρακάτω Σ-πρωτόκολλο απόδειξης γνώσης αναπαράστασης $Y \in \mathbb{G}$ δηλ.
PoK$\Big\{(\mathbb{G}, q, g_1, g_2, Y), (x_1, x_2) : Y = g_1^{x_1} g_2^{x_2}\Big\}$

- $\mathcal{P}$: $t_1, t_2 \leftarrow\$ \mathbb{Z}_q$; $T \leftarrow g_1^{t_1} g_2^{t_2}$; Στέλνει T.
- $\mathcal{V}$: $c \leftarrow\$ \mathbb{Z}_q$; Στέλνει c.
- $\mathcal{P}$: $s_1 = t_1 + x_1 c$; $s_2 = t_2 + x_2 c$;
  Στέλνει s_1, s_2.
- $\mathcal{P}$: Αποδέχεται αν $g_1^{s_1} g_2^{s_2} = TY^c$.

Παρατήρηση

Το πρωτόκολλο είναι witness indistinguishable

Διαφορετικά μυστικά κλειδιά μπορεί να αντιστοιχούν στο ίδιο δημόσιο

Αποδείξεις με διαφορετικά κλειδιά είναι μη διακρίσιμες.

Τυφλές υπογραφές Okamoto Schnorr

Σε αντιστοιχία με τις τυφλές υπογραφές Schnorr θα πρέπει να κρύψουμε τα s_1, s_2, c

Θα χρειαστούν τρεις τιμές τύφλωσης u_1, u_2, d

KGen(1^λ)

- Επιλέγεται ομάδα $\mathbb{G}$ τάξης πρώτου q με δύσκολο DLP.
- Επιλέγονται $g_1, g_2 \leftarrow\$ \mathbb{G}$.
- Επιλέγονται $x_1, x_2 \leftarrow\$ \mathbb{Z}_q$
- $Y := g_1^{x_1} g_2^{x_2}$
- Έξοδος
    - prms $= (\mathbb{G}, q, g_1, g_2)$
    - sk $= (x_1, x_2)$
    - vk $= Y$

Τυφλές υπογραφές Okamoto Schnorr

Signer (x_1, x_2) | User (m)

$t_1, t_2 \leftarrow\$ \mathbb{Z}_q$, $T = g_1^{t_1} g_2^{t_2}$

$\xrightarrow{T}$

$u_1, u_2, d \leftarrow\$ \mathbb{Z}_q$

$T' \leftarrow T g_1^{u_1} g_2^{u_2} Y^d$

$c' \leftarrow \mathsf{H}(T', Y, m)$

$c \leftarrow c' + d$

$\xleftarrow{c}$

$s_1 = t_1 + cx_1$

$s_2 = t_2 + cx_2$

$\xrightarrow{s_1, s_2}$

$\sigma_1 = s_1 + u_1$

$\sigma_2 = s_2 + u_2$

$\sigma = (T', \sigma_1, \sigma_2)$

Επαλήθευση: $g_1^{\sigma_1} g_2^{\sigma_2} = T' Y^{c'}$ με $c' = \mathsf{H}(T', Y, m)$

Blindness: Με τρόπο ανάλογο ως προς τυφλές υπογραφές Schnorr (άσκηση)

Unforgeability [?]

Αν το πρόβλημα DLP είναι δύσκολο στην $\mathbb{G}$ τότε οι τυφλές υπογραφές παρέχουν **strong** one-more unforgeability

Βασίζεται στο forking lemma

Απόδειξη (sketch)

Έστω $\mathcal{B}$ που κερδίζει στο παίγνιο One-More Forgery, δηλαδή με με l (παράλληλες) συνόδους μπορεί να παράξει $l+1$ υπογραφές.

Θα κατασκευαστεί $\mathcal{A}$ που μπορεί να λύσει το DLP στην $\mathbb{G}$

Είσοδος $\mathcal{A}$: $\mathbb{G}, g, g_1, g_2$

Επιλέγει sk $= (x_1, x_2) \leftarrow\$ \mathbb{Z}_q^2$ και θέτει pk $= Y = g_1^{x_1} g_2^{x_2}$

Με το sk μπορεί να συμμετέχει σε πρωτόκολλα Sign με τον $\mathcal{B}$ και να δημιουργεί έγκυρες υπογραφές

Oracle replay Ο $\mathcal{A}$ διαλέγει δύο τυχαία μαντεία H, H' τα οποία δίνουν ίδιες απαντήσεις μέχρι την j ερώτηση:

$$\mathsf{H} = \{c_1, c_2, \cdots, c_j, \cdots, c_Q\}$$
$$\mathsf{H}' = \{c_1, c_2, \cdots, c'_j, \cdots, c'_Q\}$$

Αν ο $\mathcal{B}$ παράξει δύο έγκυρες υπογραφές $(T', c_j, \sigma_1, \sigma_2)$ και $(T', c'_j, \sigma'_1, \sigma'_2)$ στην ερώτηση j τότε από την εξίσωση επαλήθευσης:

$$T' = g_1^{\sigma_1} g_2^{\sigma_2} Y^{-c_j}$$
$$T' = g_1^{\sigma'_1} g_2^{\sigma'_2} Y^{-c'_j}$$

Ανάλυση ασφάλειας iii

Κατά συνέπεια:

$$
\begin{aligned}
g_1^{\sigma_1'} g_2^{\sigma_2'} Y^{-c_j'} = g_1^{\sigma_1} g_2^{\sigma_2} Y^{-c_j} \Rightarrow \\
Y^{c_j - c_j'} = g_1^{\sigma_1' - \sigma_1} g_2^{\sigma_2' - sig_2} \Rightarrow \\
Y = g_1^{(\sigma_1' - \sigma_1)(c_j - c_j')^{-1}} g_2^{(\sigma_2' - \sigma_2)(c_j - c_j')^{-1}}
\end{aligned}
$$

Όμως $Y = g_1^{x_1} g_2^{x_2}$ για x_1, x_2 γνωστά στον $\mathcal{A}$.

Ανάλυση $\mathcal{B}$ [**?**]:

Για ασφάλεια πρέπει $\frac{Q^l}{q} \ll 1$. Άρα $l < \lambda$

και ασυμπτωτικά $l = \mathcal{O}(polylog(\lambda))$

[**?**] **Δεν** δίνεται εγγύηση ασφάλειας απέναντι σε αντιπάλους που μπορούν να κάνουν πολυωνυμικό αριθμό συνόδων Sign

Unforgeability II i

ROS$_l$ - Random inhomogenities in an Overdetermined Solvable system of linear equations

ROS$_l$ problem - [?]

Δίνεται ένα random oracle $\mathsf{H} : \mathbb{Z}_q^l \to \mathbb{Z}_q$.

Για συντελεστές $a_{k,l}$ να βρεθεί ένα **επιλύσιμο** σύστημα $l+1$ εξισώσεων με αγνώστους $c_1, \cdots, c_l \in \mathbb{Z}_q$ ώστε:

$$\left\{a_{k,1}c_1 + \cdots + a_{k,l}c_l = \mathsf{H}(a_{k,1}, \cdots, a_{k,l})\right\}_{k=1}^{l+1}$$

Δίνεται ένα σύνολο από $n \gg l$ γραμμικές εξισώσεις **mod**q με l αγνώστους και τυχαίους σταθερούς όρους.

Ζητείται ένα επιλύσιμο συστημα με $l+1$ από αυτές τις εξισώσεις.

Το 2021 βρέθηκε πολυωνυμικός αλγόριθμος. [?]

- Ο $\mathcal{A}$ (forger) ανοίγει l παράλληλα sessions λαμβάνοντας l commitments από τον $\mathcal{S}$:

$$\{T_j = g^{t_j}\}_{j\in[l]}$$

- Ο $\mathcal{A}$ επιλέγει $n \gg l$ και μηνύματα $m_1, \cdots, m_n$
- Ο $\mathcal{A}$ επιλέγει $n \times l$ συντελεστές $\{a_{k,j}\}_{k\in[n],j\in[l]} \in \mathbb{Z}_q$
- Υπολογίζει

$$\{F_k = T_1^{a_{k,1}} \cdots T_l^{a_{k,l}} \text{και } \mathsf{H}(F_k, Y, m_k)\}_{k\in[n]}$$

- Σχηματίζει το σύστημα με αγνώστους $c_1, \cdots, c_l$.

$$\{a_{k,1}c_1 + \cdots + a_{k,l}c_l = \mathsf{H}(F_k, Y, m_k)\}_{k\in[l+1]}$$

- Λύνει το πρόβλημα $\textsf{ROS}_l$ και στέλνει τις λύσεις $c_1, \cdots, c_l$ ως challenges στα αντίστοιχα sessions με τον $\mathcal{S}$

Μια παράλληλη επίθεση χρησιμοποιώντας το ROS ii

- Ο $\mathcal{S}$ απαντάει με τα l responses

$$\{s_j = t_j + c_j x\}_{j \in [l]}$$

- Ο $\mathcal{S}$ φτιάχνει **για κάθε λυμένη εξίσωση** τις υπογραφές $\{(F_k^*, c_k^*, s_k^*)\}_{k \in [l+1]}$ με:

$$F_k^* = T_1^{a_{k,1}} \cdots T_l^{a_{k,l}}$$

$$s_k^* = \sum_{j=1}^{l} a_{k,j} s_j$$

$$c_k^* = \sum_{j=1}^{l} a_{k,j} c_j$$

Μια παράλληλη επίθεση χρησιμοποιώντας το ROS iii

- **Κάθε** υπογραφή (F_k^*, c_k^*, s_k^*) $k \in [l+1]$ είναι έγκυρη γιατί:

$$\begin{aligned} g^{s_k^*} &= g^{\sum_{j=1}^{l} a_{k,j} s_j} = g^{\sum_{j=1}^{l} a_{k,j}(t_j + c_j x)} \\ &= g^{\sum_{j=1}^{l} a_{k,j} t_j + \sum_{j=1}^{l} a_{k,j} c_j x} \\ &= \prod_{j=1}^{l} T_j^{a_{k,j}} \cdot Y^{\sum_{j=1}^{l} c_j a_{k,j}} = \\ &= F_k^* Y^{c_k^*} \end{aligned}$$

και

$$c_k^* = \sum_{j=1}^{l} a_{k,j} c_j = \mathsf{H}(F_k^*, Y, m_k)$$

Συμπέρασμα: Με l signing sessions ο $\mathcal{A}$ έφτιαξε $l+1$ έγκυρες υπογραφές!!!

Παρατηρήσεις:

- Γιατί αυτή η επίθεση αφορά **μόνο** τις τυφλές υπογραφές Schnorr (και όχι τις απλές - στην interactive μορφή τους)?
- Η επίθεση παρακάμπτει το πρόβλημα του διακριτού λογαρίθμου. Εξαρτάται μόνο από την τάξη της ομάδας.
- Εφαρμόζεται και στο σχήμα υπογραφών Okamoto - Schnorr (άσκηση).
- Για $l < \log_2 q = \lambda$ υποεκθετικός αλγόριθμος (Wagner)
- Πρόσφατα [**?**] ασφάλεια τυφλών υπογραφών Schnorr βασίζεται σε δυσκολία του OMDL + ROS στο AGM.
- Επίσης πρόσφατα: [**?**]: Το ROS έχει πολυωνυμικό αλγόριθμο για $l \geq \log_2 q = \lambda$.

Μια παράλληλη επίθεση χρησιμοποιώντας το ROS v

- Πρακτικά για $\lambda = 256$:
  - Για $l = 16$ η πλαστογράφηση γίνεται σε χρόνο $\mathcal{O}(2^{55})$
  - Για $l = 256$ η πλαστογράφηση γίνεται σε δευτερόλεπτα με υπολογιστές κοινής χρήσης.
- **Συμπέρασμα** Μη πρακτική χρήση όλων των σχημάτων τυφλών υπογραφών εκτός από το RSA, BLS.
- Διάφορες προσπάθειες επίλυσης - Ενεργό Πεδίο Έρευνας! [**?**, **?**, **?**, **?**]

Sign

Signer(x, Y)		User(m, Y)
$t_1, t_0 \leftarrow\!\!\$\ \mathbb{Z}_q$		
$T_1 \leftarrow g^{t_1}, T_0 \leftarrow g^{t_0}$		
	$\xrightarrow{T_1,\, T_0}$	
		Blind
		$\alpha_1, \beta_1, \alpha_0, \beta_0 \leftarrow\!\!\$\ \mathbb{Z}_q$
		$T_1' \leftarrow T_1 g^{\alpha_1} Y^{\beta_1},\ T_0' \leftarrow T_0 g^{\alpha_0} Y^{\beta_0}$
		$c_1' = \mathsf{H}(T_1', Y, m),\ c_0' = \mathsf{H}(T_0', Y, m)$
		$c_1 \leftarrow c_1' + \beta_1,\ c_0 \leftarrow c_0' + \beta_0$
	$\xleftarrow{c_1,\, c_0}$	
$\mathbf{b} \leftarrow\!\!\$\ \{\mathbf{0}, \mathbf{1}\}$		
$s = t_b + c_b x$		
	$\xrightarrow{b,\, s}$	
		Unblind
		$s' = s + \alpha_b$
		$\sigma = (T_b', s')$

Παρατηρήσεις:

- Η υπογραφή παραμένει ίδια.
- Στην επίθεση ROS ο $\mathcal{A}$ λύνει το σύστημα **πριν** μάθει το response
- Κατά συνέπεια έχοντας λάβει l **ζεύγη** commitments πρέπει να μαντέψει ποια από αυτά θα οδηγήσουν σε υπογραφές και δεν θα γίνουν abort.
- 2^l πιθανοί συνδυασμοί

Βιβλιογραφία i

- Foteini Baldimtsi and Anna Lysyanskaya, *On the security of one-witness blind signature schemes*, ASIACRYPT, 2013.
- Fabrice Benhamouda, Tancrède Lepoint, Julian Loss, Michele Orrù, and Mariana Raykova, *On the (in)security of ros*, EUROCRYPT 2021, 2021.
- M. Bellare, C. Namprempre, D. Pointcheval, and M. Semanko, *The one-more-rsa-inversion problems and the security of chaum's blind signature scheme*, Cryptology ePrint Archive, Paper 2001/002, 2001, https://eprint.iacr.org/2001/002.
- Paulo L. Barreto and Gustavo H. M. Zanon, *Blind signatures from zero-knowledge arguments*, Cryptology ePrint Archive, Paper 2023/067.

Βιβλιογραφία ii

- Rutchathon Chairattana-Apirom, Lucjan Hanzlik, Julian Loss, Anna Lysyanskaya, and Benedikt Wagner, *Pi-cut-choo and friends: Compact blind signatures via parallel instance cut-and-choose and more*, CRYPTO 2022, 2022.
- David Chaum, *Blind signatures for untraceable payments*, CRYPTO 83.
- Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta, *A practical secret voting scheme for large scale elections*, AUSCRYPT '92 (Jennifer Seberry and Yuliang Zheng, eds.), 1993.
- Georg Fuchsbauer, Antoine Plouviez, and Yannick Seurin, *Blind schnorr signatures and signed elgamal encryption in the algebraic group model*, EUROCRYPT 2020, 2020.
- Lucjan Hanzlik, Julian Loss, and Benedikt Wagner, *Rai-choo! evolving blind signatures to the next level*, EUROCRYPT 2023.

Βιβλιογραφία iii

- Julia Kastner, Julian Loss, and Omar Renawi, *Concurrent security of anonymous credentials light, revisited*, Cryptology ePrint Archive, Paper 2023/707.
- Tatsuaki Okamoto, *Provably secure and practical identification schemes and corresponding signature schemes*, CRYPTO' 92, 1993.
- David Pointcheval and Jacques Stern, *Security arguments for digital signatures and blind signatures*, J. Cryptol. **13** (2000), no. 3, 361–396.
- Claus Peter Schnorr, *Security of blind discrete log signatures against interactive attacks*, Information and Communications Security, 2001.