Υπογραφές
με βάση τον Διακριτό Λογάριθμο

Υπογραφές ElGamal

- Δημιουργία Κλειδιών:
  - $KGen(1^{\lambda}) \rightarrow (sk, vk) = \langle x, (Y, g, p) \rangle$
  - Επιλογή πρώτου p μήκους λ bits
  - $\mathbb{G} = \mathbb{Z}_p^*$ με γεννήτορα g
  - $x \xleftarrow{\$} \{2, \cdots . p-2\}$
  - $Y \leftarrow g^x \bmod p$

- Επαλήθευση
  - $Vf(Y, m, \sigma) \rightarrow Y^r r^s = g^m \pmod p$

- Υπογραφή
  - $Sign(x, m) \rightarrow \sigma = (r, s)$
    - Επιλογή εφήμερου κλειδιού
      - $k \xleftarrow{\$} \mathbb{Z}_{p-1}^* \ (\gcd(\mathrm{k}, \mathrm{p}-1) = 1)$
    - $r \leftarrow g^k \bmod p$
    - $s \leftarrow (m - xr)k^{-1} \bmod (p-1)$
    - Επανάληψη μέχρις ότου $s \neq 0 \bmod (p-1)$
    - Η υπογραφή είναι $\sigma = (r, s)$ με μέγεθος 2λ bits

Ορθότητα: $Y^r r^s = Y^r g^{k(m-xr)k^{-1}} = Y^r g^m Y^{-r} = g^m \pmod p$

Παρατηρήσεις

- Πιθανοτικό σχήμα υπογραφής
  - πολλές έγκυρες υπογραφές για το ίδιο μήνυμα m (διαφορετικά k)
  - Η συνάρτηση επαλήθευσης δέχεται οποιαδήποτε από αυτές ως έγκυρη
- Χειρισμός Τυχαιότητας
  - Το r δεν εξαρτάται από το μήνυμα
  - Το τυχαία επιλεγμένο k πρέπει να κρατείται κρυφό
  - Αλλιώς:
    - ανάκτηση x από $s = (m - xr)k^{-1} \pmod{(p-1)}$
- Η επανάληψη του ίδιου k σε διαφορετικές υπογραφές καθιστά εφικτό τον υπολογισμό του

Επαναχρησιμοποίηση Τυχαιότητας

- Έστω δύο υπογραφές $\boldsymbol{\sigma_1, \sigma_2}$ με το ίδιο $\boldsymbol{k}$
- $\sigma_1 = (r, s_1) = (g^k, (m_1 - xr)k^{-1}\ mod\ (p-1))$
- $\sigma_2 = (r, s_2) = (g^k, (m_2 - xr)k^{-1}\ mod\ (p-1))$
- Υπολογισμός: $s_1 - s_2 = (m_1 - m_2)k^{-1} \Rightarrow (s_1 - s_2)k = m_1 - m_2\ (mod\ (p-1))$
- Αν $\gcd((s_1 - s_2\ ), (p-1))\ =\ 1$ τότε $k = (m_1 - m_2)\ (s_1 - s_2)^{-1}$
- Αλλιώς εύρεση με δοκιμές από τις $\gcd((s_1 - s_2\ ), (p-1))$ λύσεις ελέγχοντας αν $g^k = r$.

Επαναχρησιμοποίηση Τυχαιότητας

- Αναλυτικά:
- Έστω $d = gcd(s_1 - s_2, p - 1)$
- $d|(p - 1)$ και $d|(s_1 - s_2)$. Άρα $d|(m_1 - m_2)$
- Θέτουμε $m' = \frac{m_1 - m_2}{d}$, $s' = \frac{s_1 - s_2}{d}$, $p' = p - 1$
- Άρα: $s'k = m' \ (mod\ p')$ και $k = m's'^{-1} \ (mod\ p')$ αφού $\gcd(s', p') = 1$
- d λύσεις: $k = m'(s') - 1 + ip' \ (\mathrm{mod}\ p - 1)$ με $i \in \{0, \cdots, d - 1\}$
- Δοκιμάζουμε ποια από αυτές επαληθεύει την $r = g^k \ (mod\ p)$

Επιθέσεις πλαστογράφησης

- No-message attack
  - Επιλογή r, s
    - Εύρεση m: $Y^r \cdot r^s = g^m$ – Επίλυση DLOG
- Chosen message attack
  - Επιλογή m, r
    - Εύρεση s: $r^s = g^m Y^{-r}$ - Επίλυση DLOG
  - Επιλογή m, s
    - Εύρεση r: $Y^r \cdot r^s = g^m$ - Δύσκολο πρόβλημα – Άγνωστη η σχέση του με DLOG
  - Επιλογή m, r, s ταυτόχρονα:
    - $r = g^i Y^j \pmod{\text{p}}$ για $i, j \in \{0, \dots, p-2\},\ \gcd(\{j, i\}, p-1) = 1$
    - $s = -r \cdot j^{-1} \pmod{\text{p} - 1}$
    - $m = s \cdot i \pmod{\text{p} - 1}$
    - Έγκυρη υπογραφή: $Y^r \cdot r^s = Y^r (g^{is} Y^{js}) = Y^r (g^m Y^{-r}) = g^m$
    - Υπαρξιακή πλαστογράφηση – Επίλυση με συνάρτηση σύνοψης.

Εύρεση έγκυρης υπογραφής (m, σ).

$$Y^r \cdot r^s = g^m$$

Υπογραφές Schnorr

Αποδείξεις μηδενικής γνώσης **του ιδιωτικού κλειδιού** υπογραφής που λαμβάνουν υπ' όψιν και το μήνυμα

Δημόσια Είσοδος: $g \in \mathbb{G},\ ord(\mathbb{G}) = q, pk \in \mathbb{G}$

Ιδιωτική Είσοδος: $sk \in \mathbb{Z}_q : Y = g^{sk}$

Τα βήματα του P

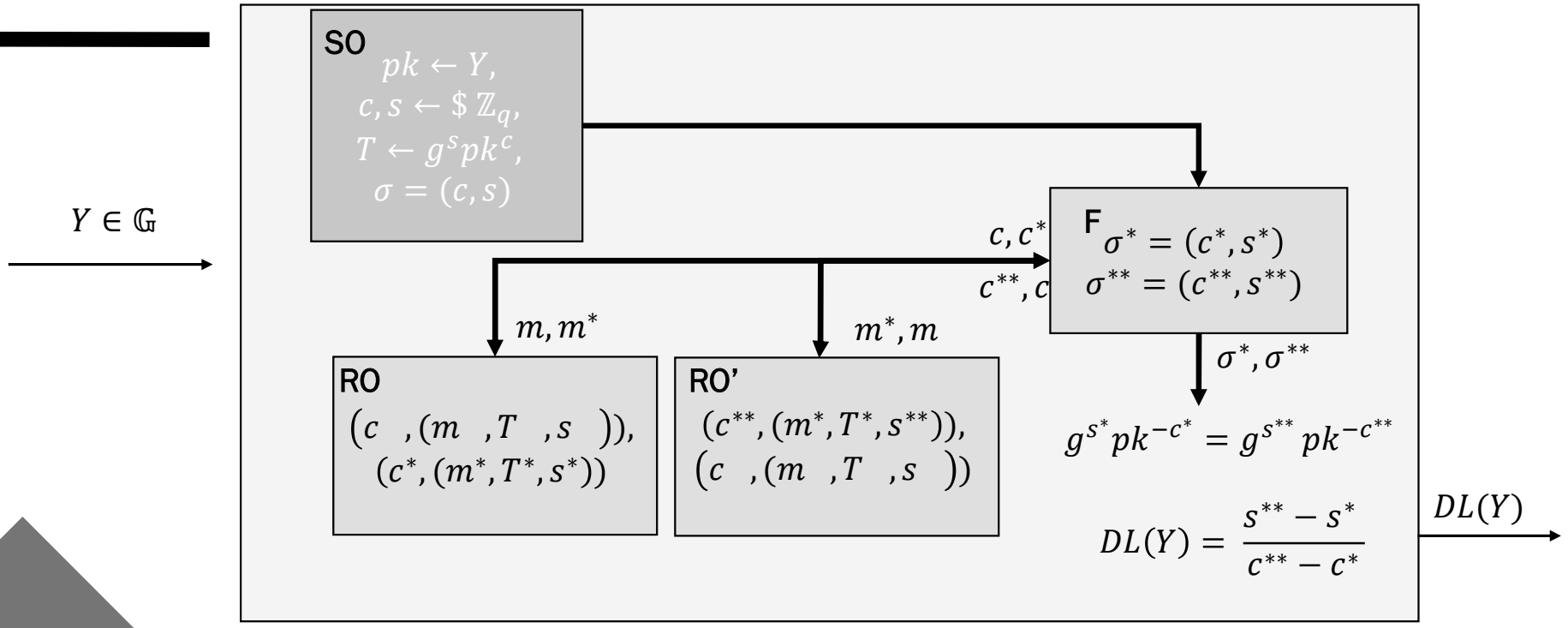
1. Επιλογή $t \leftarrow \$\ \mathbb{Z}_q$ και υπολογισμός $T = g^t$
2. Υπολογισμός $\boldsymbol{c \leftarrow H(g, pk, T, m)}$
3. Υπολογισμός $s \leftarrow t + c \cdot sk$
4. Η υπογραφή είναι: $\sigma = (c, s)$
5. Επαλήθευση (**από οποιονδήποτε**) αν και μόνο αν
$$c = H(g, pk, g^s pk^{-c}, m)$$

Pointcheval, D., Stern, J. (1996). Security Proofs for Signature Schemes. In: Maurer, U. (eds) Advances in Cryptology — EUROCRYPT '96. EUROCRYPT 1996. Lecture Notes in Computer Science, vol 1070. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-68339-9_33

Απόδειξη Ασφάλειας (Γενικά)

- Βασίζεται στην ειδική ορθότητα του Σ-πρωτοκόλλου του Schnorr
  - Ίδιο commitment, διαφορετικά challenges, responses
  - Εύρεση witness - διακριτού λογαρίθμου pk (ιδιωτικό κλειδί)
- Chosen – message attack:
  - Προσομοίωση SO με χρήση simulator του Σ-πρωτοκόλλου
  - $T \leftarrow g^s pk^c$
- Random Oracle: Είσοδος (g, pk, T, m) Απάντηση με $c \leftarrow \$\ \mathbb{Z}_q$
- Η αναγωγή μαντεύει σε ποιο ερώτημα (g, pk, T^*, m^*) αντιστοιχεί η πλαστογράφηση και απαντάει με c^*
- Μετά την πλαστογράφηση (T^*, s^*), η αναγωγή κάνει rewind τον F πριν την ερώτηση που απαντήθηκε με c^*
- **Oracle Replay Attack:** Στο ερώτημα (g, pk, T^*, m^*) θα δοθεί απάντηση $c^{**} \neq c^*$
- **Forking Lemma:** Με μη αμελητέα πιθανότητα θα ξαναδοθεί πλαστογράφηση (T^*, s^{**})
- Επίλυση διακριτού λογαρίθμου

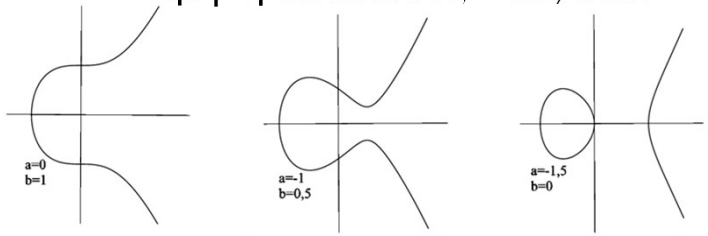
Απόδειξη Ασφάλειας (Γενικά)

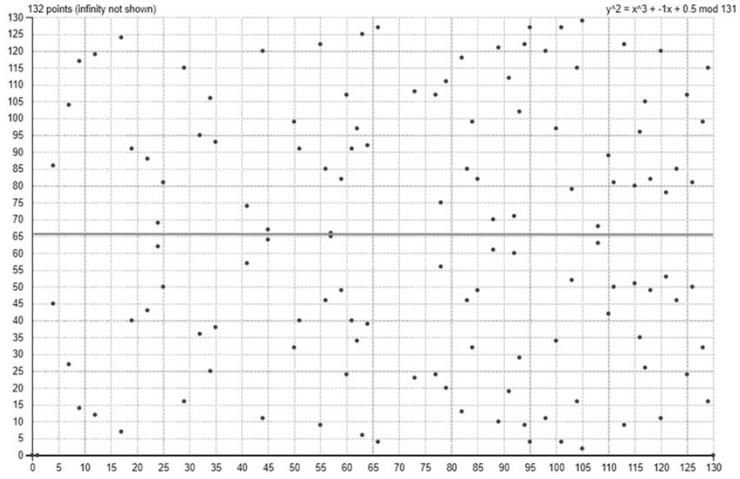


Pointcheval, D., Stern, J. (1996). Security Proofs for Signature Schemes. In: Maurer, U. (eds) Advances in Cryptology — EUROCRYPT '96. EUROCRYPT 1996. Lecture Notes in Computer Science, vol 1070. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-68339-9_33

Υπογραφές ECDSA

- Προέλευση: DSA (NIST 1991)
  - Στόχος: Παράκαμψη πατέντας Schnorr
  - Παραλλαγή του ElGamal, λειτουργία σε υποομάδα τάξης 2^{160}
- ECDSA
  - Υλοποίηση με ελλειπτικές καμπύλες
  - Χρήση σε Bitcoin, SSL, SSH





- Δεν υπάρχει απόδειξη ασφάλειας!

Υπογραφές ECDSA

Υπογραφή $Sign(x, m) \rightarrow \sigma = (r, s)$

- Υπολογισμός σύνοψης του μηνύματος $h = H(m)$ και προσαρμογή της στο $[0, \dots, q-1]$
- Επιλογή εφήμερου κλειδιού $k \xleftarrow{\$} \{1, \cdots, q-1\}$
- Υπολογισμός του σημείου $P = kG = (x_P, y_P)$
- Υπολογισμός του $r = x_P \ mod \ q$
- Αν $r = 0 \ (mod \ q)$ τότε επανάληψη με καινούριο k
- $s \leftarrow (h + xr)k^{-1} \bmod q$
- Αν $s = 0 \ (mod \ q)$ τότε επανάληψη με καινούριο k
- Η υπογραφή είναι $\sigma = (r, s)$

Δημιουργία Κλειδιών:

- Δημόσια Διαθέσιμες Παράμετροι: $(p, a, b, \#\mathcal{E}, q, G)$
- Δουλεύουμε σε υποομάδα τάξης q στην καμπύλη
- $y^2 = x^3 + ax + b, \ \ a, b \in \mathbb{F}_p$ με σημείο βάσης το G
- Ιδιωτικό κλειδί: Ένας τυχαίος ακέραιος $x \in \{1, \cdots, q-1\}$
- Δημόσιο κλειδί: Το σημείο $Y = xG \in \mathcal{E}$

Υπογραφές ECDSA

- Επαλήθευση
  - $h \leftarrow H(m)$
  - $u_1 \leftarrow s^{-1}h \; mod \; q$
  - $u_2 \leftarrow s^{-1}r \; mod \; q$
  - $P' \leftarrow u_1 G + u_2 Y$
  - Έγκυρη αν $r = x'_P \; (mod \; q)$

Ορθότητα:

$$u_1 G + u_2 Y = s^{-1}(h + xr)G = s^{-1}ksG = kG = P$$

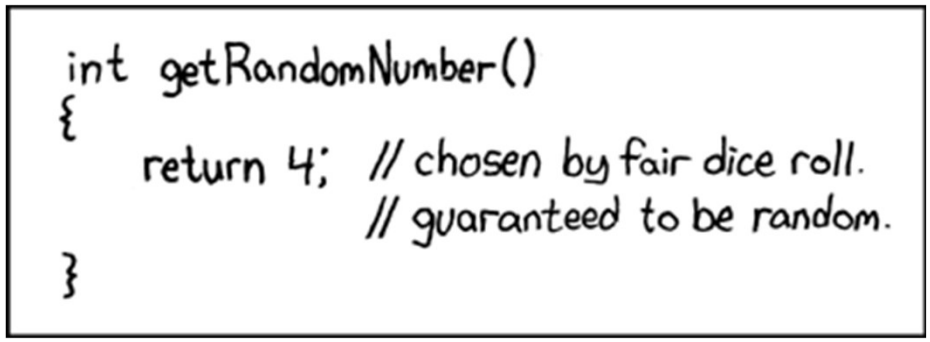
Υπολογισμός του σημείου P με δύο διαφορετικούς τρόπους

ECDSA Malleability

- Όχι SUF – CMA
- Αν (r, s) έγκυρη υπογραφή τότε και $(r, -s)$ έγκυρη υπογραφή
  - Θα υπολογίζεται το σημείο $P'' = -P$
  - Το σημείο αυτό ανήκει στην καμπύλη λόγω συμμετρίας
- Επίσης
  - $P = u_1 G + u_2 Y \Rightarrow Y = (P - u_1 G) \cdot u_2^{-1} = r^{-1}(H(m) \cdot G \ - sP)$
  - Δηλαδή: Το δημόσιο κλειδί μπορεί να εκφραστεί ως συνάρτηση του (r, s)
  - Αν βρω μια έγκυρη υπογραφή, μπορώ να αλλάξω $(r, s), m$ ώστε να βρω μια έγκυρη υπογραφή για διαφορετικό κλειδί

ECDSA Nonce reuse

- Επιλογή διαφορετικού κλειδιού $\boldsymbol{k}$ ανά υπογραφή
  - Αλλιώς: Ανάκτηση ιδιωτικού κλειδιού
- Δύο υπογραφές $(r_1, s_1)(r_2, s_2)$ με κοινό k
  - $r_1 = r_2 = x_{kG}$
  - $s_1 - s_2 = k^{-1}(h_1 - h_2)\ mod\ q$
  - $k = (h_1 - h_2)(s_1 - s_2)^{-1}\ mod\ q$
  - $x = (ks_1 - h_1)r^{-1} mod\ q$
- Sony Playstation 3 Hack (2011)



xkcd: Random Number

Ψηφιακές Υπογραφές με ιδιωτικότητα

Τυφλές Υπογραφές

Υπογραφές Δακτυλίου

Motivation

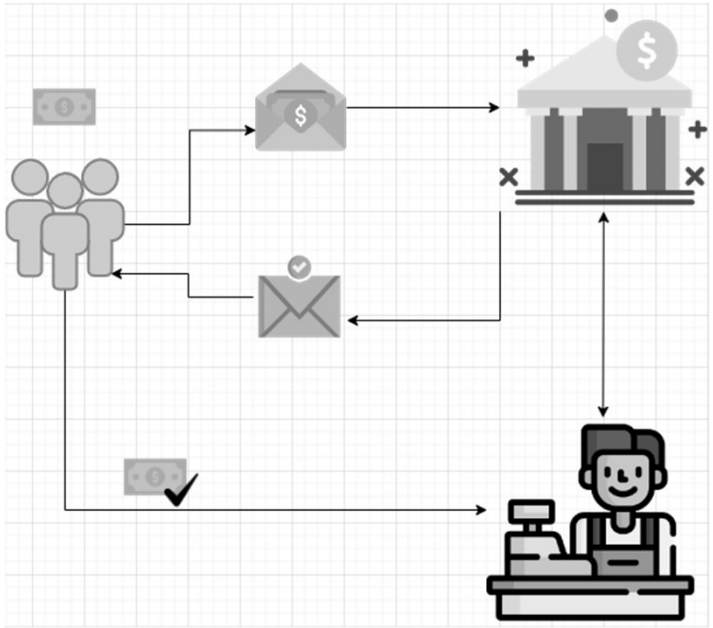
- Ψηφιακές Υπογραφές:
  - Ακεραιότητα
  - Αυθεντικότητα
  - Μη Αποκήρυξη
  - Δημόσια επαληθευσιμότητα
  - Χωρίς ιδιωτικότητα όμως…

- Ο υπογράφων
  - βλέπει το μήνυμά που υπογράφει και
  - μπορεί να συσχετίσει την υπογραφή με το αίτημα δημιουργίας της
- Το δημόσιο κλειδί επαλήθευσης προδίδει τον signer.
- Τα παραπάνω δεν είναι επιθυμητά σε πολλές εφαρμογές
  - Ηλεκτρονικό χρήμα
  - Ηλεκτρονικές ψηφοφορίες
  - Whistleblowing

Υπογραφές για ηλεκτρονικό χρήμα

- Νόμισμα $c \xleftarrow{\$} \{0,1\}^*$
- Ο Αγοραστής ζητάει από την Τράπεζα υπογραφή σε ένα νόμισμα c.
  - Αποφυγή double, overspending
  - Συγκεκριμένη αξία ανά υπογραφή
- 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

Τυφλές Υπογραφές



- Φάκελος με καρμπόν
- Το νόμισμα μπαίνει σε φάκελο
- Η τράπεζα υπογράφει τον φάκελο
  - Αφού ελέγξει επαρκές υπόλοιπο
- Η υπογραφή μεταφέρεται στο νόμισμα
- Το νόμισμα βγαίνει από τον φάκελο
  - Με την υπογραφή
- Ξοδεύεται (αν δεν έχει ξοδευτεί ήδη)
  - Επαλήθευση υπογραφής
- Η τράπεζα δεν μπορεί να συσχετίσει νόμισμα με φάκελο

Τυφλές Υπογραφές

Σχήμα τυφλών υπογραφών:

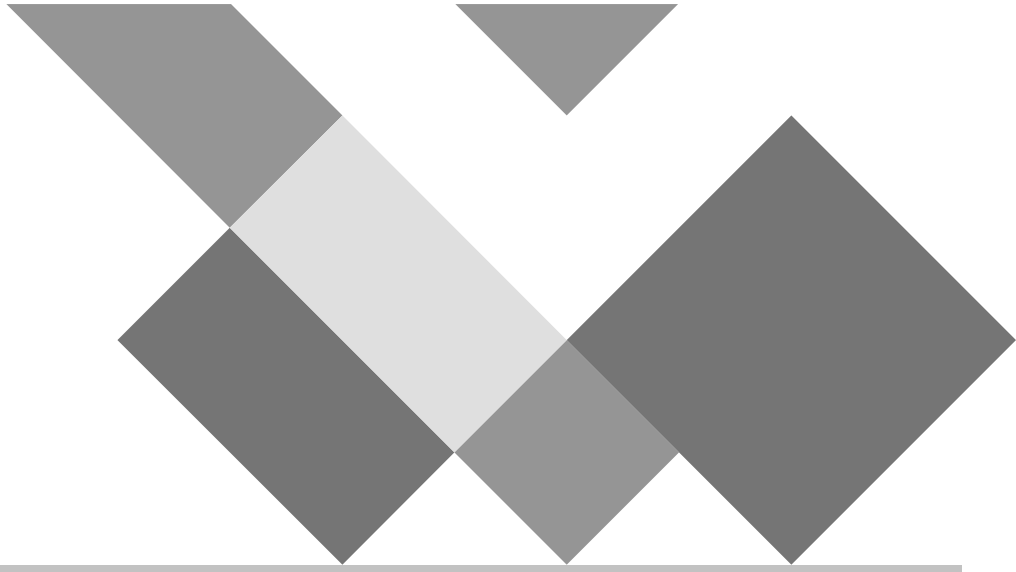
- τριάδα $\Pi = (KGen, Sign, Vf)$
- $(sk, vk) \leftarrow KGen(1^{\lambda})$
  - Δημιουργία κλειδιών και κρυπτογραφικών παραμέτρων
- $\sigma \leftarrow \mathbf{Sign}\langle S(sk), U(m), vk\rangle$
  - Το Sign είναι **πρωτόκολλο** και όχι αλγόριθμος. Συνήθως:
    - $m' \leftarrow Blind(m, vk)$ εκτελείται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

Τυφλές υπογραφές RSA

- Δημιουργία Κλειδιών:
  - Όπως στο RSA. Τελικά: $(sk, vk) = (d, (e, n))$
- Υπογραφή:
  - $Blind(m, vk) \rightarrow H(m) \cdot r^e \bmod n, r \leftarrow Z_n^*$
  - $Sign(m', sk) \rightarrow m'^d \bmod n \rightarrow \left(H(m)^d r\right) \bmod n$
  - $UnBlind(\sigma', vk) \rightarrow \sigma' r^{-1} \bmod n \rightarrow H(m)^d \bmod n$
- Επαλήθευση:
  - Η τελική υπογραφή είναι κανονική υπογραφή RSA

Μοντέλο Ασφάλειας Τυφλών Υπογραφών

- Τυφλότητα
  - Ο υπογράφων δεν μαθαίνει τίποτα για το μήνυμα
  - Ο αντίπαλος είναι ο υπογράφων
  - Πιο τυπικά:
    - Με δεδομένο ένα μήνυμα και μια υπογραφή ο αντίπαλος δεν πρέπει να μάθει από ποιο signing session προέκυψε.
  - Perfect Blindness
    - $\Pr\left[BGame_A\left(1^\lambda\right) = 1\right] = \frac{1}{2}$
  - Computational Blindness
    - $\Pr\left[BGame_A\left(1^\lambda\right) = 1\right] \leq \frac{1}{2} + negl(\lambda)$



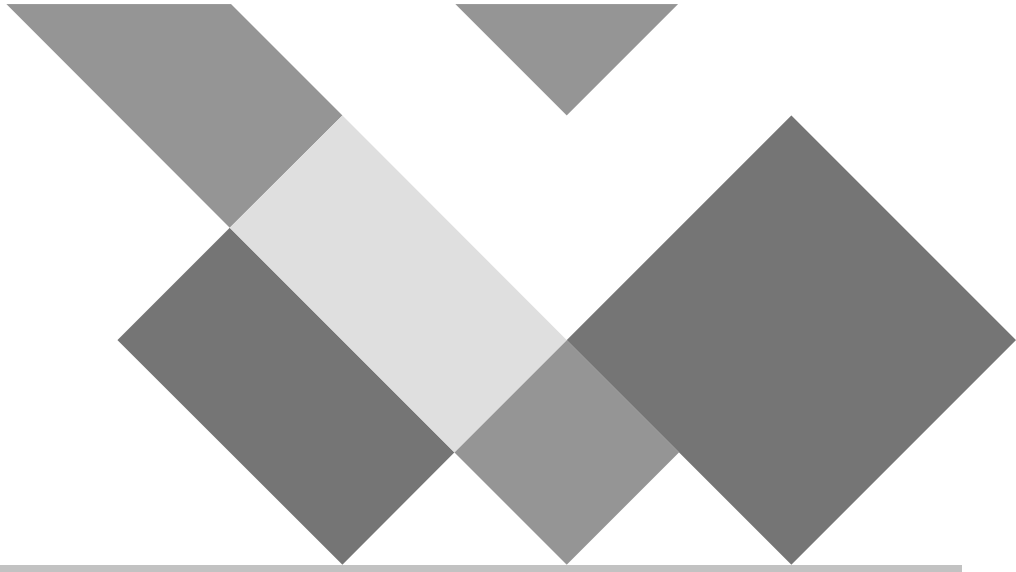
BG (Blindness Game)

- $(vk, sk) \leftarrow KGen(1^\lambda)$
- $Send\ sk\ to\ A$
- $m_0, m_1 \leftarrow A(vk, sk)$
- $b \xleftarrow{\$} \{0,1\}$
- $\sigma_b \leftarrow \mathbf{Sign}\langle A(sk), U(m_b), vk\rangle$
- $\sigma_{1-b} \leftarrow \mathbf{Sign}\langle A(sk), U(m_{1-b}), vk\rangle$
- If $Vf(pk, m_b, \sigma_b) = 1$ and $Vf(pk, m_{1-b}, \sigma_{1-b}) = 1$ then
  - $b \leftarrow A(\sigma_b, \sigma_{1-b})$
  - return $b = b'$
- Else
  - return 0

Μοντέλο Ασφάλειας Τυφλών Υπογραφών

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

Μοντέλο Ασφάλειας Τυφλών Υπογραφών



- Unforgeability με βάση τη χρήση
  - Στο ηλεκτρονικό χρήμα δεν θέλουμε να μπορούν να δημιουργηθούν περισσότερα χρήματα από όσα υπέγραψε η τράπεζα
  - Αντίπαλος ο χρήστης!
  - Έχοντας λάβει l υπογραφές από τον signer, ο χρήστης δεν μπορεί να παρουσιάσει $l + 1$ έγκυρες
  - One-more unforgeability

OMUF (One-More Unforgeability Game)

- $(vk, sk) \leftarrow KGen(1^{\lambda})$
- $(m_i, \sigma_i) \leftarrow \mathbf{Sign}\langle S(sk), A(m_j), vk\rangle$ με $i \in [l+1]$ και $j \in [k]$
- `If` $\boldsymbol{Vf(pk, m_i, \sigma_i) = 1\ \forall i \in [l+1]}$ and $m_i's$ **are distinct** and $k \leq l$ `then`
  - `return 1`
- `Else`
  - `return 0`

l: Το μέγιστο πλήθος των sessions $\langle S, A\rangle$.
Μπορούν να είναι σειριακά ή **παράλληλα!**

Ομαδικές Υπογραφές

- Η υπογραφή προέρχεται από μια ομάδα, όπου υπάρχει αρχηγός
- Διατηρείται ανωνυμία, ως προς το ποιο μέλος υπέγραψε
- Τα μέλη ορίζονται εξ’ αρχής από τον αρχηγό
- Δυναμική ομάδα: Μπορούν να ανακληθούν (revocation) ή να προστεθούν καινούρια
- Ο αρχηγός μπορεί να αποκαλύψει ποιος υπέγραψε (traceability)

Υπογραφές δακτυλίου

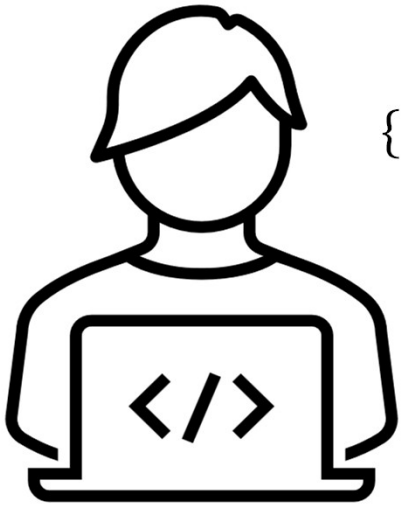
- Η Alice είναι μέλος του υπουργικού συμβουλίου και θέλει να αποκαλύψει ένα σκάνδαλο στον δημοσιογράφο Bob
- Ο Bob θέλει να πειστεί ότι η αποκάλυψη έρχεται από κάποιο μέλος του υπουργικού συμβουλίου Η Alice δεν μπορεί να υπογράψει κάποιο μήνυμα, γιατί θα αποκαλυφθεί από την επαλήθευση
- Δημιουργία δακτυλίου με (όλα τα) δημόσια κλειδιά των υπουργών
- Υπογραφή προέρχεται από το δακτύλιο έγκυρη, αλλά χωρίς να είναι δυνατόν να αποκαλυφθεί ποιο μέλος του υπέγραψε
- Ad-hoc επιλογή δακτυλίου

Υπογραφές δακτυλίου

- Κατασκευή από OR-proofs
  - Σ-πρωτόκολλα ότι ο υπογράφων γνωρίζει το ιδιωτικό κλειδί για ένα από τα n δημόσια κλειδιά των μελών του δακτυλίου
    - Για όσα δεν το γνωρίζει χρήση του Simulator
  - Χρόνος δημιουργίας $O(n)$
  - Μέγεθος υπογραφής $O(n)$
  - Χρόνος επαλήθευσης $O(n)$
  - Πολλές προσπάθειες μείωσης

Υπογραφές δακτυλίου

$$R = \{Y_1. Y_2, \dots, Y_n\}$$



$$T_\kappa = g^{t_\kappa},$$

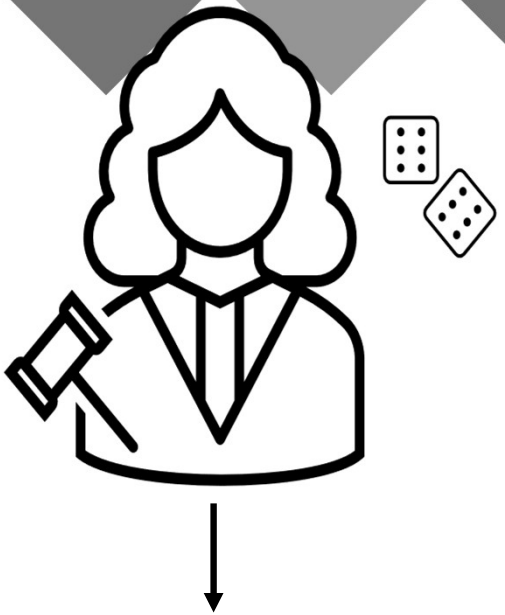
$$\{ T_i = g^{c_i} Y_i^{-t_i}, t_i, c_i \xleftarrow{\$} \mathbb{Z}_q \}, i \in [n]/\{k\}$$

$$tc \leftarrow H(R, \boldsymbol{m}, \{T_i\}_{i=1}^{n})t$$

$$tc_k \leftarrow c - \sum_i c_i \bmod qt$$

$$ts_k \leftarrow (t_k + c_k x_k) \bmod q \; t$$

$$ts_i \leftarrow t_i, i \in [n]/\{k\} \; t$$



$$\forall i \in [n] \; g^{s_i} =_? T_i Y_i^{c_i} \quad \text{και} \; c = \sum_i c_i \bmod q$$