

Ψηφιακές Υπογραφές

Παναγιώτης Γροντάς

ΕΜΠ

Κρυπτογραφία

2025 - 2026



Με βάση παλιότερες διαφάνειες Άρη Παγουρτζή

Περιεχόμενα

- Ορισμός - Μοντελοποίηση
- Ψηφιακές Υπογραφές RSA
 - Επιθέσεις - Παραλλαγές
 - Το μοντέλο του τυχαίου μαντείου
- Ψηφιακές Υπογραφές DLP
 - Επιθέσεις - Παραλλαγές
- Το πρόβλημα της αυθεντικότητας κλειδιών
- Προχωρημένα Σχήματα

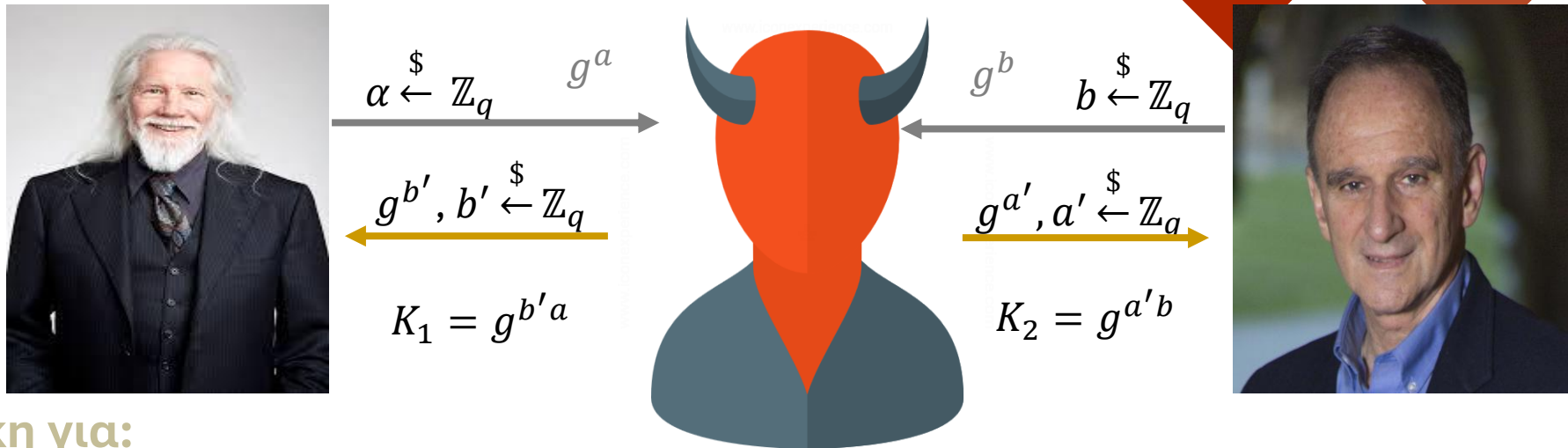




Ορισμός - Μοντελοποίηση

Motivation

- Ανταλλαγή κλειδιού Diffie-Hellman με ενεργούς αντιπάλους
 - MiTM attacks



- **Ανάγκη για:**
 - **Ακεραιότητα:** Το μήνυμα είναι ακριβώς αυτό που έστειλε ο αποστολέας.
 - **Αυθεντικότητα:** Το μήνυμα στάλθηκε από αυτόν που φαίνεται ότι στάλθηκε
- **MACs:** Μειονεκτήματα συμμετρικής κρυπτογραφίας

Ψηφιακές Υπογραφές

- Ασύμμετρα MACs
- Αποστολέας S (υπογράφων)
- Παραλήπτης V (επαληθεύων)
- Ο αποστολέας S
 - Εκτελεί αλγόριθμο $KGen$ και παράγει ζεύγος κλειδιών (vk, sk)
 - Το κλειδί υπογραφής sk παραμένει **ιδιωτικό**.
 - Το κλειδί επαλήθευσης vk **δημοσιοποιείται**
- Υπογραφή:
 - Μετασχηματισμός μηνύματος με τη βοήθεια του κλειδιού
 - Η υπογραφή εξαρτάται από το μήνυμα
 - Αλγόριθμος $Sign(sk, m) \rightarrow \sigma$
- Επαλήθευση:
 - Αλγόριθμος $Vf(pk, m, \sigma) \rightarrow 0/1$
 - Χρειάζεται και το μήνυμα
- Μετάδοση:
 - Οποιαδήποτε αλλοίωση θα γίνει αντιληπτή, γιατί θα χαλάσει την αντιστοιχία μηνύματος υπογραφής

Πλεονεκτήματα

- Εύκολη διανομή κλειδιού
- Δημόσια επαληθευσσιμότητα
 - Δεν επαληθεύει μόνο ο V
 - Οποιοσδήποτε αποκτήσει το δημόσιο κλειδί του S
- Μη αποκήρυξη (non – repudation)
 - Κανείς δεν μπορεί να αρνηθεί την υπογραφή του
 - Τα κλειδιά sk, vk συνδέονται μαθηματικά
- Αυθεντικοποίηση
 - Με την υπόθεση της κατοχής του ιδιωτικού κλειδιού

- 
- Προηγμένες Λειτουργίες
 - Ιδιωτικότητα
 - Τυφλές υπογραφές
 - Ανωνυμία
 - Ομαδικές υπογραφές, υπογραφές δακτυλίου
 - Ελεγχόμενη επαληθευσσιμότητα
 - Καθορισμένος επαληθευτής

Μειονεκτήματα

- **Αυθεντικότητα κλειδιού**
 - Πώς είμαστε σίγουροι ότι το δημόσιο κλειδί αντιστοιχεί όντως στην ταυτότητα του S (που φαίνεται στον δημόσιο κατάλογο)
 - Πώς είμαστε σίγουροι ότι το ιδιωτικό κλειδί ήταν όντως στην κατοχή του S κατά τη δημιουργία της υπογραφής
- **Οι ψηφιακές υπογραφές λύνουν τα προβλήματα**
 - Ανταλλαγής κλειδιού
 - Αυθεντικότητας μηνύματος
 - Ακεραιότητας μηνύματος
- **Οι ψηφιακές υπογραφές δημιουργούν το πρόβλημα**
 - Αυθεντικότητας κλειδιού
- **Μαθηματικές και μη λύσεις**

Ορισμός

- **Σχήμα υπογραφής:** Μια τριάδα αλγορίθμων
 - $KGen(1^\lambda) \rightarrow (vk, sk)$
 - $Sign(sk, m) \rightarrow \sigma, \mathbf{m} \in \{0, 1\}^*$
 - $Vf(vk, m, \sigma) \rightarrow \textcolor{red}{0}/\textcolor{green}{1}$
- **Έγκυρη υπογραφή**
 - $Vf(vk, m, \sigma) = 1$
- **Ορθότητα**
 - $Vf(vk, m, Sign(sk, m)) = 1, \forall (vk, sk) \leftarrow KGen(1^\lambda)$

Πλαστογράφηση

Πλαστογραφηση (Forgery)

Ο $\mathcal{A}$ παράγει μια έγκυρη υπογραφή για κάποιο μήνυμα **χωρίς τη συμμετοχή του S** – δηλ. του κατόχου του ιδιωτικού κλειδιού που αντιστοιχεί στο δημόσιο που την επαληθεύει

- **Καθολική (universal)**
 - Ο $\mathcal{A}$ παράγει μια έγκυρη υπογραφή για **οποιοδήποτε** μήνυμα
 - Ισοδυναμεί με την κατοχή του ιδιωτικού κλειδιού του S
- **Επιλεκτική (selective)**
 - Ο $\mathcal{A}$ παράγει μια έγκυρη υπογραφή για ένα **συγκεκριμένο μήνυμα της επιλογής του**
 - Το μήνυμα επιλέγεται **ΠPIN** την επίθεση
 - **Πρακτικά: Το μήνυμα πρέπει να έχει κάποιες προδιαγραφές. Π.χ.**
 - **Να έχει νόημα σε κάποιο πρωτόκολλο**
 - **Να έχει συγκεκριμένες ιδιότητες**
- **Υπαρξιακή (existential)**
 - Ο $\mathcal{A}$ παράγει μια έγκυρη υπογραφή για ένα **συγκεκριμένο μήνυμα της επιλογής του**
 - Το μήνυμα επιλέγεται **ελεύθερα**
 - **Πρακτικά:**
 - μπορεί να αποτελείται και από τυχαία bits.
 - π.χ. έξοδος hash

Αντίπαλοι

- **Παθητικός (passive)**
 - Γνωρίζει μόνο το κλειδί επαλήθευσης και ζεύγη (μηνυμάτων, έγκυρων υπογραφών)
- **Ενεργός (active)**
 - Μπορεί να αποκτήσει **έγκυρες** υπογραφές σε μηνύματα της επιλογής του (chosen message attack)
- **Ενεργός με προσαρμοστικότητα (adaptive active)**
 - Μπορεί να αποκτήσει **έγκυρες** υπογραφές σε μηνύματα της επιλογής του που εξαρτώνται από προηγούμενες **έγκυρες** υπογραφές

Ασφάλεια Ψηφιακών Υπογραφών



Ασφάλεια ως προς

- τον δυνατότερο αντίπαλο (adaptive adversary)
- ευνοϊκότερη επίθεση (chosen message attack)
- ευκολότερη συνθήκη νίκης (existential unforgeability)

EUF-CMA

Ένα σχήμα υπογραφής είναι **ασφαλές** αν δεν επιτρέπει σε κανέναν **ενεργό** αντίπαλο με **προσαρμοστικότητα** να επιτύχει **υπαρξιακή** πλαστογράφιση σε επίθεση **επιλεγμένων** μηνυμάτων

Ασφάλεια Ψηφιακών Υπογραφών

Το παιχνίδι πλαστογράφησης Forge-Game για EUF-CMA

- $(vk, sk) \leftarrow KGen(1^\lambda)$
- $Q = \{(m_i, \sigma_i)\}_{i=1}^{poly(\lambda)} \leftarrow \mathcal{A}^{Sign}(vk)$
- $(m^*, \sigma^*) \leftarrow \mathcal{A}(vk, Q)$
- If $Vf(vk, m^*, \sigma^*) = 1$ and $m^* \notin Q$ then return 1
- Else return 0

Ένα πρωτόκολλο υπογραφών $\Pi = (KGen, Sign, Vf)$ παρέχει ασφάλεια EUF-CMA αν $\forall PPT \mathcal{A}$:

$$\Pr[Forge - Game_{\mathcal{A}, \Pi}(1^\lambda) = 1] \leq negl(\lambda)$$

Ο αντίπαλος απλά δεν πρέπει να έχει δει το συγκεκριμένο ζεύγος μηνύματος υπογραφής
Μπορεί να φτιάξει νέα πλαστογράφιση για m^*
π.χ μέσω malleability

m^* είναι **νέο** μήνυμα (για το οποίο δεν έχει ζητηθεί **καμία** υπογραφή).

Παραλλαγή strong EUF-CMA (SUF-CMA):

Παιχνίδιο: όμοιο με **EUF-CMA**

Νέα συνθήκη νίκης $\mathcal{A}$

$$Vf(vk, m^*, \sigma^*) = 1 \text{ and } (m^*, \sigma^*) \notin Q$$

SUF-CMA security $\Rightarrow$ EUF-CMA security



Υπογραφές RSA

Υπογραφές RSA

- Δημιουργία Κλειδιών:
 - $KGen(1^\lambda) \rightarrow (sk, vk) = (d, (e, n))$
 - $n = p \cdot q$
 - $\gcd(e, \varphi(n)) = 1$
 - $d = e^{-1} \bmod \varphi(n)$
- Υπογραφή – ‘Αποκρυπτογράφηση’ RSA
 - $Sign(d, m) \rightarrow m^d \bmod n$
- Επαλήθευση – ‘Κρυπτογράφηση’ RSA
 - $Vf((e, n), m, \sigma) \rightarrow \sigma^e = m \bmod n$

Ορθότητα: $\sigma^e = (m^d)^e = m^{ed} = m \bmod n$ λόγω Θ. Euler

Καθόλου Ασφάλεια!

Επίθεση χωρίς μήνυμα

- Είσοδος $\mathcal{A}$: $vk = (e, n)$
- $Q = \emptyset$ - δεν υποβάλλεται κανένα μήνυμα για υπογραφή
- Ο $\mathcal{A}$ επιλέγει κάποιο $\sigma^* \xleftarrow{\$} \mathbb{Z}_n^*$
- Εφαρμόζει το κλειδί επαλήθευσης και υπολογίζει $\sigma^{*e} \rightarrow m^* \in \mathbb{Z}_n^*$
- Το σ^* είναι πλαστογράφιση για το (κάποιο) m^*
 - αφού ικανοποιεί τη σχέση επαλήθευσης
 - Το m^* δεν έχει ρωτηθεί στο Q
- Ο $\mathcal{A}$ ' κερδίζει πάντα $\Pr[\text{Forge} - \text{Game}_{\mathcal{A}, \text{RSA}}(1^\lambda) = 1] = 1$
Έχει νόημα η επίθεση; **Ναι**, μπορεί m^* να παράγεται από κάποια δυαδική κωδικοποίηση. Με επαναλήψεις, μπορούν να βρεθούν m^* όπου κάποια bits μπορεί να αντιστοιχούν σε έγκυρα τμήματα μηνυμάτων

Chosen message attack - malleability

- Είσοδος $\mathcal{A}$: $vk = (e, n)$
- Στόχος: Υπογραφή για συγκεκριμένο $m^* \in \mathbb{Z}_n^*$
- Ο $\mathcal{A}$ επιλέγει $m_1 \xleftarrow{\$} \mathbb{Z}_n^*$ (Ισχύει $m_1^{-1} \in \mathbb{Z}_n^*$)
- Ρωτάει το μαντείο υπογραφής για υπογραφές στα $m_1, m_2 = m^*/m_1$
- $Q = \{(m_1, \sigma_1), (m_2, \sigma_2)\}$
- Υπολογισμός $\sigma^* = \sigma_1 \cdot \sigma_2 = m_1^d \cdot m_2^d = (m_1 \cdot m^*/m_1)^d = m^{*d}$
- Το ζεύγος (m^*, σ^*) αποτελεί έγκυρη υπογραφή και $(m^*, \sigma^*) \notin Q$
- Ο $\mathcal{A}$ κερδίζει πάντα $\Pr[\text{Forge} - \text{Game}_{\mathcal{A}, \text{RSA}}(1^\lambda) = 1] = 1$

Chosen message attack - blinding

- Είσοδος $\mathcal{A}$: $vk = (e, n)$
- Στόχος: Υπογραφή για κάποιο $m^* \in \mathbb{Z}_n^*$
- Ο $\mathcal{A}$ επιλέγει $r \leftarrow \mathbb{Z}_n^*$
- Ρωτάει το μαντείο υπογραφής για υπογραφή στο $m = m^* r^e$ και λαμβάνει την υπογραφή $\sigma = (m^* r^e)^d = m^{*d} r$
- $Q = \{(m, \sigma)\}$
- Υπολογισμός $\sigma^* \leftarrow \sigma^d \cdot r^{-1} = m^{*d} \pmod{n}$
- Το ζεύγος (m^*, σ^*) αποτελεί έγκυρη υπογραφή και $(m^*, \sigma^*) \notin Q$
- Ο $\mathcal{A}$ κερδίζει πάντα $\Pr[\text{Forge} - \text{Game}_{\mathcal{A}, \text{RSA}}(1^\lambda) = 1] = 1$

Υπογραφές RSA – FDH (Full Domain Hash)

- Δημιουργία Κλειδιών:
 - $KGen(1^\lambda) \rightarrow (sk, vk) = (\textcolor{red}{d}, (e, n))$
 - $n = p \cdot q$
 - $\gcd(e, \varphi(n)) = 1$
 - $\textcolor{red}{d} = e^{-1} \bmod \varphi(n)$
 - Επιλογή $H: \{0,1\}^* \rightarrow \mathbb{Z}_n^*$ με δυσκολία εύρεσης συγκρούσεων
 - Πρακτικά: $FDH(m) = H(m||0)|| H(m||1)|| \dots$
- Υπογραφή – Αποκρυπτογράφηση RSA
 - $Sign(\textcolor{red}{d}, m) \rightarrow \textcolor{green}{H}(\textcolor{red}{m})^d \bmod n$
- Επαλήθευση – Κρυπτογράφηση RSA
 - $Vf((e, n), m, \sigma) \rightarrow \sigma^e = \textcolor{green}{H}(\textcolor{red}{m}) \bmod n$

Πλεονέκτημα:

Υπογραφή
συμβολοσειρών και όχι
μόνο στοιχείων $\mathbb{Z}_n^*$

Ορθότητα: $\sigma^e = (\textcolor{green}{H}(\textcolor{red}{m})^{\textcolor{red}{d}})^e = \textcolor{green}{H}(\textcolor{red}{m})^{e\textcolor{red}{d}} = \textcolor{green}{H}(\textcolor{red}{m}) \bmod n$ λόγω Θ. Euler

Υπογραφές RSA – FDH (Full Domain Hash)

- **No message attack**

- Είσοδος $\mathcal{A}$: $vk = (e, n)$
- $Q = \emptyset$ δεν υποβάλλεται κανένα μήνυμα για υπογραφή
- Ο $\mathcal{A}$ επιλέγει $\sigma^* \leftarrow_{\$} \mathbb{Z}_n^*$
- Εφαρμόζει το κλειδί επαλήθευσης και υπολογίζει $\sigma^{*e} \rightarrow H(m)^* \in \mathbb{Z}_n^*$
- Για να παράξει το m^* , θα πρέπει να μπορεί να αντιστρέψει την H .

- **Chosen message attack**

- Είσοδος $\mathcal{A}$: $vk = (e, n)$
- Στόχος: Υπογραφή για κάποιο $m^* \in \mathbb{Z}_n^*$
- Ο $\mathcal{A}$ επιλέγει $m_1 \leftarrow \$ \mathbb{Z}_n^*$ (Ισχύει $m_1^{-1} \in \mathbb{Z}_n^*$)
- Ρωτάει το μαντείο υπογραφής για υπογραφές στα $m_1, m_2 = m^*/m_1$
- $Q = \{(m_1, \sigma_1), (m_2, \sigma_2)\}$
- Υπολογισμός $\sigma^* = \sigma_1 \cdot \sigma_2 = H(m_1)^d H(m_2)^d$

Απόδειξη Ασφάλειας RSA-FDH

- Αρκούν οι ιδιότητες των συναρτήσεων σύνοψης?
 - **Pre-image resistance**
 - **Second Pre-image resistance**
 - **Collision Resistance**
- **ΌΧΙ**
 - Χρειάζεται κάτι ισχυρότερο
 - Μπορεί να ταυτίζονται τμήματα δύο hash π.χ.
 - Χρειάζεται η H να συμπεριφέρεται ως τυχαία συνάρτηση.
 - Απόδειξη στο **μοντέλο του τυχαίου μαντείου** (M. Bellare, P. Rogaway – 1993)

Mihir Bellare and Phillip Rogaway. 1993. Random oracles are practical: a paradigm for designing efficient protocols. In Proceedings of the 1st ACM conference on Computer and communications security (CCS '93). Association for Computing Machinery, New York, NY, USA, 62–73. <https://doi.org/10.1145/168588.168596>

Το μοντέλο του τυχαίου μαντείου

Μοντελοποίηση τυχαίας συνάρτησης: Πώς θα φτιάχναμε μια πραγματικά τυχαία συνάρτηση:



Input (n bits)	Output ($l(n)$ bits)
0000...0000000	Συμβολοσειρά με πιθανότητα εμφάνισης $1/l(n)$
0000...0000001	Συμβολοσειρά με πιθανότητα εμφάνισης $1/l(n)$
0000...0000010	Συμβολοσειρά με πιθανότητα εμφάνισης $1/l(n)$
0000...0000011	Συμβολοσειρά με πιθανότητα εμφάνισης $1/l(n)$
.....	
1111111...1111	Συμβολοσειρά με πιθανότητα εμφάνισης $1/l(n)$

Το μοντέλο του τυχαίου μαντείου

- Όμως είναι πρακτικά αδύνατο να κατασκευαστεί αποδοτικά
 - $H: \{0,1\}^n \rightarrow \{0,1\}^{l(n)}$ με $\Pr[H(x) = h] = \frac{1}{2^{l(n)}}$
 - Θα θέλαμε 2^n ανεξάρτητες αποτιμήσεις
 - Εκθετική αποθήκευση και αποτίμηση
 - Επίσης συνήθως $H: \{0,1\}^* \rightarrow \{0,1\}^{l(n)}$
- Τυχαίο μαντείο: αφαίρεση τυχαίας συνάρτησης

Το μοντέλο του τυχαίου μαντείου

- Τυχαίο μαντείο: αφαίρεση τυχαίας συνάρτησης
 - Μαύρο κουτί - απαντάει σε ερωτήσεις
 - (Τέλεια) Ασφάλεια στο κανάλι επικοινωνίας (μοντελοποίηση τοπικής αποτίμησης)
 - Είναι συνάρτηση (ίδια είσοδος - ίδια έξοδος σε κάθε κλήση)
 - Είναι συνάρτηση σύνοψης (υπάρχουν συγκρούσεις – αλλά είναι δύσκολο να βρεθούν)
- Δυναμική κατασκευή - Lazy Evaluation
 - Εσωτερικός πίνακας - αρχικά άδειος
 - Για κάθε ερώτηση: έλεγχος αν έχει ήδη απαντηθεί
 - Αν ναι, τότε ανάκτηση της απάντησης
 - Αν όχι, απάντηση με τυχαία τιμή και αποθήκευση για μελλοντική αναφορά

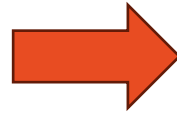
Αποδείξεις στο μοντέλο τυχαίου μαντείου

- Ο $\mathcal{A}$ νομίζει ότι αλληλεπιδρά με το τυχαίο μαντείο
- Στην πραγματικότητα το προσομοιώνει η αναγωγή
- Μπορούμε να μάθουμε τις ερωτήσεις του $\mathcal{A}$
- Μπορούμε να προγραμματίσουμε τις απαντήσεις ώστε να εκμεταλλευτούμε την ύπαρξη του αντιπάλου (programmability)
- Οι απαντήσεις δεν πρέπει να διαχωρίζονται από ομοιόμορφα επιλεγμένες τιμές.
- Στο πραγματικό πρωτόκολλο το τυχαίο μαντείο αντικαθίσταται από μία πραγματική συνάρτηση (πχ. SHA256)

Απόδειξη Ασφάλειας RSA-FDH

ΘΕΩΡΗΜΑ

Αν το πρόβλημα **RSA** είναι **δύσκολο**, τότε οι υπογραφές **RSA-FDH** παρέχουν **ασφάλεια** έναντι υπαρξιακής πλαστογράφησης με επιλεγμένα μηνύματα (**EUFCMA**) στο μοντέλο του τυχαίου μαντείου.



ΘΕΩΡΗΜΑ

Αν υπάρχει αντίπαλος F ο οποίος παράγει πλαστογράφηση στο RSA-FDH με πιθανότητα τουλάχιστον p_F μετά από q_H ερωτήματα στο τυχαίο μαντείο, τότε μπορούμε να κατασκευάσουμε αντίπαλο R ο οποίος λύνει το πρόβλημα RSA με πιθανότητα $p_R \geq \frac{p_F}{q_H}$.

Απόδειξη Ασφάλειας RSA-FDH

Επίθεση χωρίς μήνυμα

- Ο F μπορεί να κατασκευάσει πλαστογράφηση
- Θα κατασκευάσουμε αντίπαλο R που με χρήση του F και του RO θα λύσει το πρόβλημα RSA.
 - Είσοδος R : $(e, n), y \in \mathbb{Z}_n^*$
 - Έξοδος R : $y^{e^{-1}}$, **χωρίς γνώση του d**
- Υπόθεση: Για την πλαστογράφηση (m^*, σ^*) έχει ερωτηθεί προηγουμένως το RO για το m^*
- Συνέπεια: Αν σ^* είναι έγκυρη υπογραφή τότε: $\sigma^{*e} = H(m^*)$
- Άρα: $\sigma^* = H(m^*)^{e^{-1}}$
- **Ο R πρέπει να μαντέψει πότε ο F θα ρωτήσει το m^* στο RO .**

Απόδειξη Ασφάλειας RSA-FDH

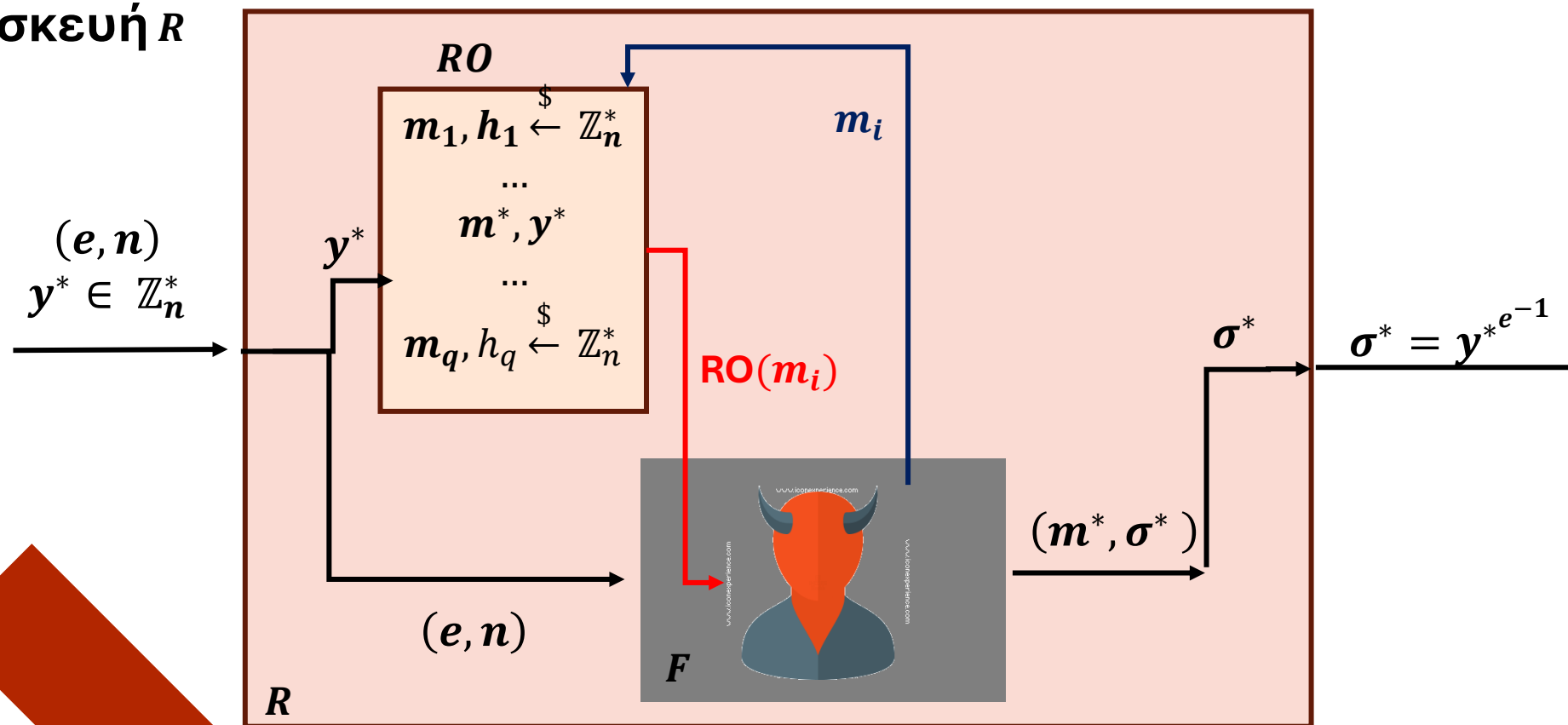
Επίθεση χωρίς μήνυμα

- Ο R απαντάει τις ερωτήσεις για το m_i με $h_i \xleftarrow{\$} \mathbb{Z}_n^*$ για $i \in [q_H]$
- Δηλαδή $RO(m_i) = h_i$
- Ο R μαντεύει ότι η πλαστογράφιση θα γίνει στο ερώτημα j
- Δηλαδή $m^* = m_j$
- Πιθανότητα να έχει μαντέψει σωστά $1/q_H$
- Τότε απαντάει με y^*
- Δηλαδή $RO(m_j) = y^*$
- Αν ο F κάνει πλαστογράφιση στο ερώτημα j τότε σ^* έγκυρη υπογραφή
- Δηλαδή $\sigma^* = RO(m_j)^{e^{-1}} = y^{*e^{-1}}$
- Πιθανότητα πλαστογράφισης $\geq p_F$
- Πιθανότητα πλαστογράφισης στο j ερώτημα $\geq p_F/q_H$

Απόδειξη Ασφάλειας RSA-FDH Επίθεση χωρίς μήνυμα

$$\sigma^{*e} = H(m^*) \Rightarrow$$
$$\sigma^* = H(m^*)^d = H(m^*)^{e^{-1}}$$

Κατασκευή R



Απόδειξη Ασφάλειας RSA-FDH

Επίθεση χωρίς μήνυμα

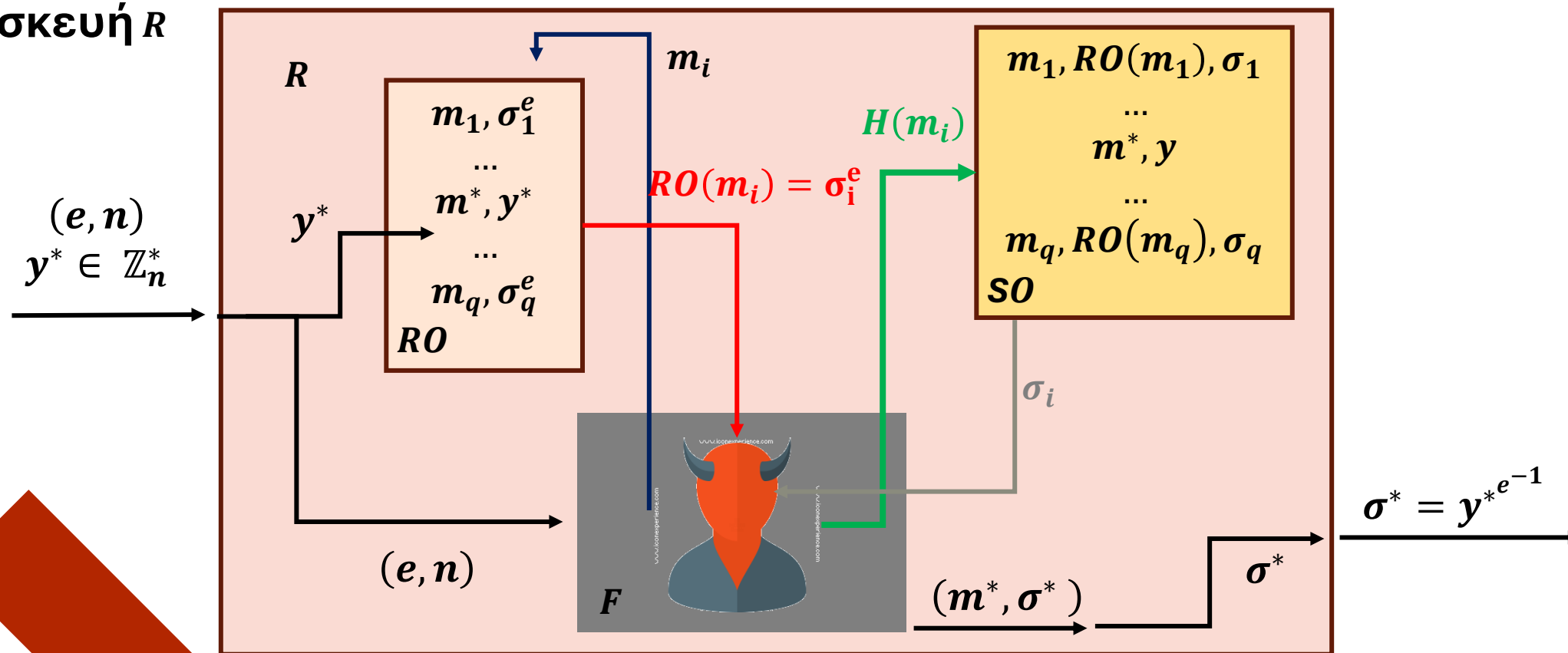
- **Ασυμπτωτικά** έχουμε:
 - $q_H \in \text{poly}(\lambda)$ γιατί ο F είναι PPT.
 - Αν το πρόβλημα RSA είναι δύσκολο:
 - $p_R \in \text{negl}(\lambda)$
 - Άρα:
 - $p_F \leq p_R \cdot q_H \in \text{negl}(\lambda)$
- **Πρακτικά** υπάρχει απώλεια ασφάλειας q_H :
 - Π.χ. αν $p_R = 2^{-60}$ και $q_H = 2^{50}$ τότε $p_F \leq 2^{-10}$

Απόδειξη Ασφάλειας RSA-FDH Επίθεση επιλεγμένου μηνύματος (CMA)

$$\sigma^{*e} = H(m^*) \Rightarrow$$

$$\sigma^* = H(m^*)^d = H(m^*)^{e-1}$$

Κατασκευή R



Απόδειξη Ασφάλειας RSA-FDH

Επίθεση επιλεγμένου μηνύματος (CMA)

- Ο F ζητάει συνόψεις **ΚΑΙ υπογραφές** από τον R
- Ο R **δεν μπορεί να υπογράψει** εφόσον δεν γνωρίζει το $sk = d$
- Θα εκμεταλλευτεί ότι μπορεί να προσομοιώσει το RO
- Ερώτηση για $RO(m)$
 - Επιλογή $\sigma \in \mathbb{Z}_n^*$ και επιστροφή σ^e
 - Αποθήκευση τριάδας: (m, σ, σ^e)
- Ερώτηση για $Sign(m)$
 - Ανάκτηση σ από την τριάδα (m, σ, σ^e)
- Τετριμμένα:
 - $\sigma^e = (\sigma^e) = RO(m)$
- Άρα σ είναι **έγκυρη** υπογραφή!

Κριτική μοντέλου τυχαίου μαντείου

ΜΕΙΟΝΕΚΤΗΜΑΤΑ

- Άχρηστη' απόδειξη: Καμία πραγματική συνάρτηση H δεν είναι random oracle
- Programmability: Η περιγραφή της H είναι σταθερή στην πραγματικότητα
- Ύπαρξη 'θεωρητικών' σχημάτων τα οποία αποδεικνύονται ασφαλή, αλλά οποιαδήποτε κατασκευή τους είναι μη ασφαλής

ΠΛΕΟΝΕΚΤΗΜΑΤΑ

- Η απόδειξη εστιάζει στο πρωτόκολλο και όχι στο H
- Απόδειξη με χρήση τυχαίου μαντείου είναι καλύτερη από απουσία απόδειξης
- Η μόνη αδυναμία: η συνάρτηση σύνοψης
- Δεν υπάρχουν (μέχρι τώρα) πραγματικές επιθέσεις που να έχουν εκμεταλλευτεί το τυχαίο μαντείο



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
- $x \xleftarrow{\$} \{2, \dots, p-2\}$
- $Y \leftarrow g^x \bmod p$

- 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
 - $k \xleftarrow{\$} \mathbb{Z}_{p-1}^* \quad (gcd(k, p-1) = 1)$
 - $r \leftarrow g^k \bmod p$
 - $s \leftarrow (m - xr)k^{-1} \bmod (p-1)$
 - 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
- **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 Τυχειότητας

- Έστω δύο υπογραφές σ_1, σ_2 με το ίδιο k
- $\sigma_1 = (r, s_1) = (g^k, (m_1 - xr)k^{-1} \bmod (p - 1))$
- $\sigma_2 = (r, s_2) = (g^k, (m_2 - xr)k^{-1} \bmod (p - 1))$
- Υπολογισμός: $s_1 - s_2 = (m_1 - m_2)k^{-1} \Rightarrow (s_1 - s_2)k = m_1 - m_2 \bmod (p - 1)$
- 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 Τυχειότητας

- 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: $s'k = m' \pmod{p'}$ και $k = m's'^{-1} \pmod{p'}$ αφού $\gcd(s', p') = 1$
- d λύσεις: $k = m'(s')^{-1} - 1 + ip' \pmod{p - 1}$ με $i \in \{0, \dots, d - 1\}$
- Δοκιμάζουμε ποια από αυτές επαληθεύει την $r = g^k \pmod{p}$

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:
 - $r = g^i Y^j \pmod{p}$ για $i, j \in \{0, \dots, p-2\}$, $\gcd(\{j, i\}, p-1) = 1$
 - $s = -r \cdot j^{-1} \pmod{p-1}$
 - $m = s \cdot i \pmod{p-1}$
 - 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: $g \in \mathbb{G}$, $\text{ord}(\mathbb{G}) = q$, $vk \in \mathbb{G}$

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

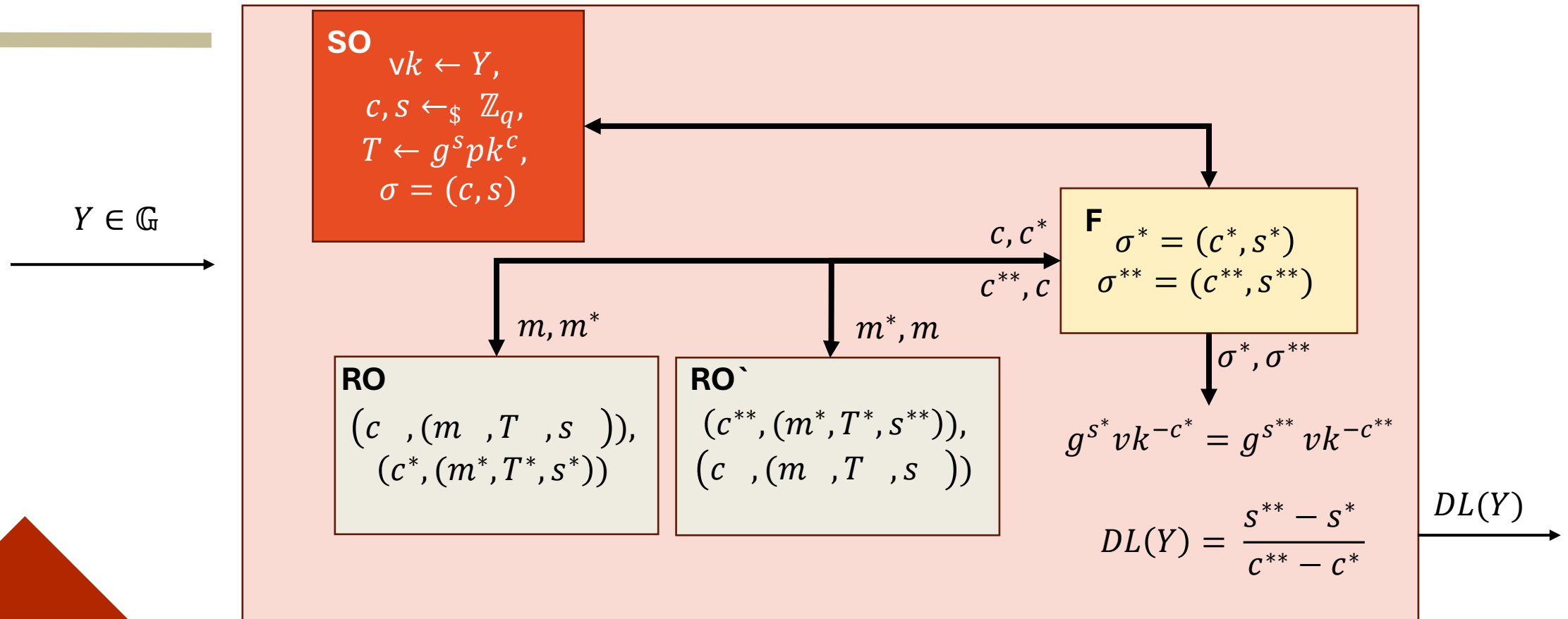
Τα βήματα του P

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

Απόδειξη Ασφάλειας (Γενικά)

- Βασίζεται στην ειδική ορθότητα του Σ -πρωτοκόλλου του Schnorr
 - Ίδιο commitment, διαφορετικά challenges, responses
 - Εύρεση witness - διακριτού λογαρίθμου vk (ιδιωτικό κλειδί)
- Chosen – message attack:
 - Προσομοίωση SO με χρήση simulator του Σ -πρωτοκόλλου
 - $T \leftarrow g^s pk^c$
- Random Oracle: Είσοδος (g, vk, 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^* με **διαφορετικό random oracle**
- **Oracle Replay Attack:** Στο ερώτημα (g, vk, 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)



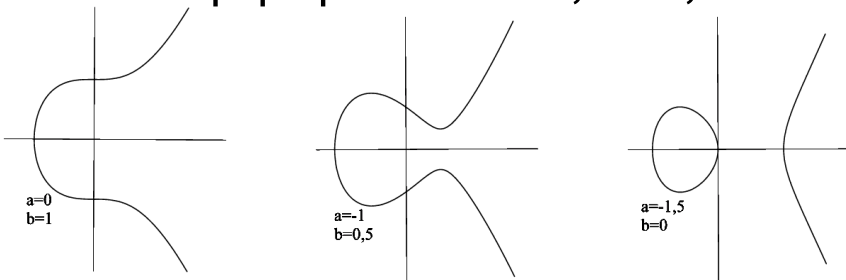
Υπογραφές ECDSA

- Προέλευση: DSA (NIST 1991)

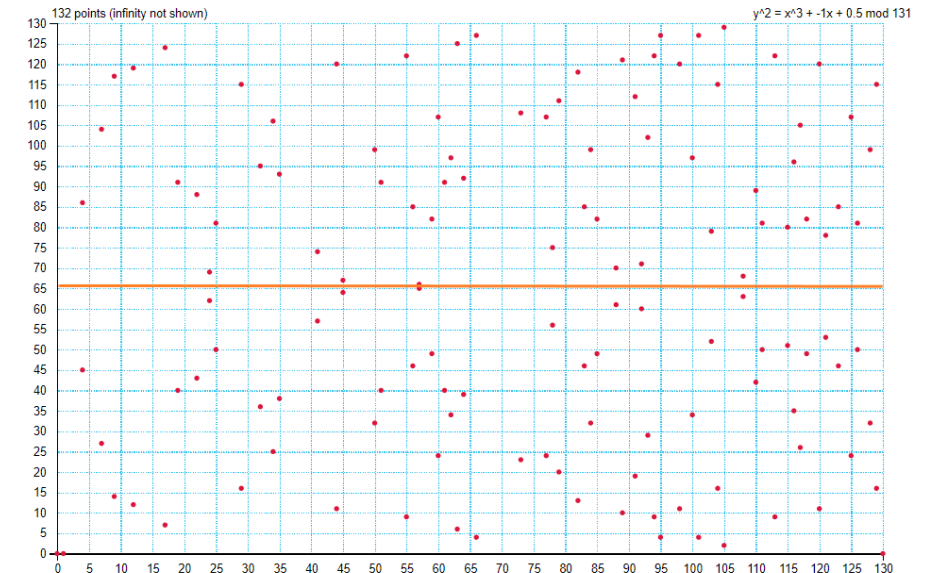
- Στόχος: Παράκαμψη πατέντας Schnorr
- Παραλλαγή του ElGamal, λειτουργία σε υποομάδα τάξης 2^{160}

- 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 $k \xleftarrow{\$} \{1, \dots, q - 1\}$
- Υπολογισμός του σημείου $P = kG = (x_P, y_P)$
- Υπολογισμός του $r = x_P \bmod q$
- Αν $r = 0 \bmod q$ τότε επανάληψη με καινούριο k
- $s \leftarrow (h + xr)k^{-1} \bmod q$
- Αν $s = 0 \bmod q$ 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 $x \in \{1, \dots, q - 1\}$
- Δημόσιο κλειδί: Το σημείο $Y = xG \in \mathcal{E}$

Υπογραφές ECDSA

- Επαλήθευση

- $h \leftarrow H(m)$
- $u_1 \leftarrow s^{-1}h \bmod q$
- $u_2 \leftarrow s^{-1}r \bmod q$
- $P' \leftarrow u_1G + u_2Y$
- Έγκυρη αν $r = x'_P \bmod q$

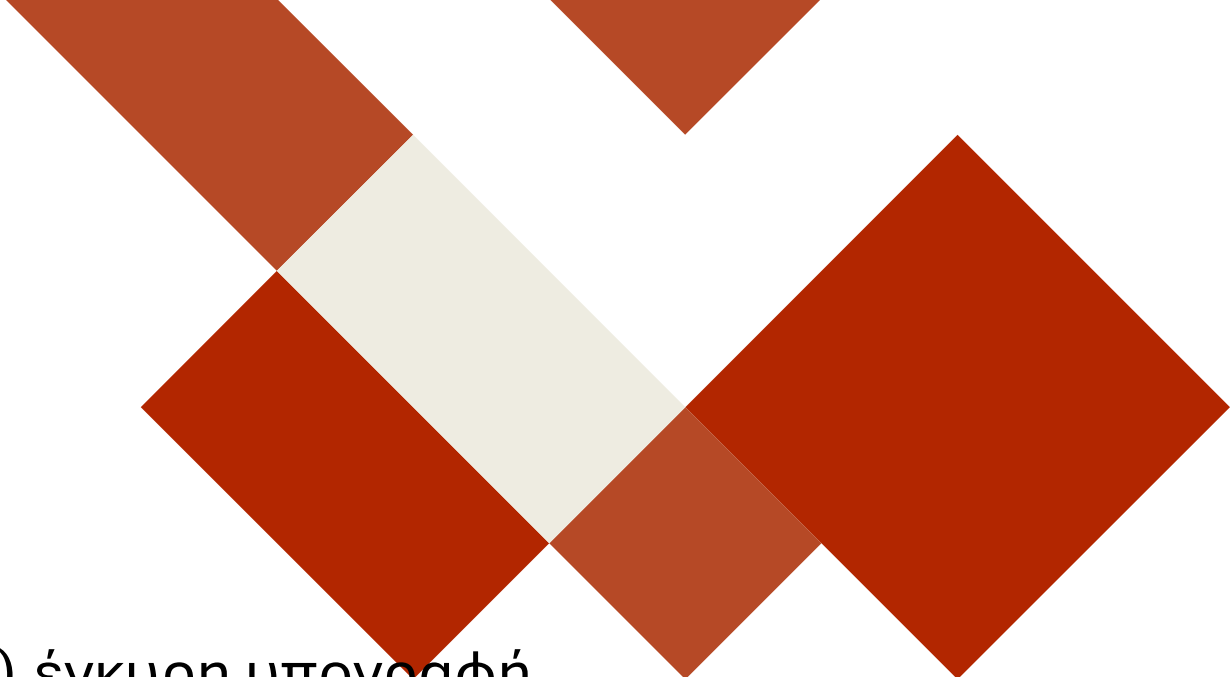
Ορθότητα:

$$u_1G + u_2Y = s^{-1}(h + xr)G = s^{-1}ksG = kG = P$$

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
 - $P = u_1G + u_2Y \Rightarrow Y = (P - u_1G) \cdot u_2^{-1} = r^{-1}(H(m) \cdot G - sP)$
 - Δηλαδή: Το δημόσιο κλειδί μπορεί να εκφραστεί ως συνάρτηση του $(r, s), m$
 - 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 k ανά υπογραφή**
 - Αλλιώς: Ανάκτηση ιδιωτικού κλειδιού
- **Δύο υπογραφές $(r_1, s_1)(r_2, s_2)$ με κοινό k**
 - $r_1 = r_2 = x_{kG}$
 - $s_1 - s_2 = k^{-1}(h_1 - h_2) \bmod q$
 - $k = (h_1 - h_2)(s_1 - s_2)^{-1} \bmod q$
 - $x = (ks_1 - h_1)r^{-1} \bmod q$
- **Sony Playstation 3 Hack (2011)**

```
int getRandomNumber()
{
    return 4; // chosen by fair dice roll.
              // guaranteed to be random.
}
```

[xkcd: Random Number](#)

Υπογραφές edDSA

- Daniel J. Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang (2012)
- Υπογραφές Schnorr σε ελλειπτικές καμπύλες Edwards (μετά τη λήξη της πατέντας)
- Ντετερμινιστική τυχαιότητα κατά την υπογραφή
- Γεννήτρια τυχαιότητας μόνο κατά τη δημιουργία κλειδιών



edDSA – Δημιουργία κλειδιών

- Δημόσια διαθέσιμες παράμετροι

- $(q = 2^{255} - 19, \mathcal{E} = -x^2 + y^2 = 1 - \frac{121655}{121666}x^2y^2, G)$

- Επιλογή κλειδιών

- $k \xleftarrow{\$} \{0,1\}^{256}$
 - $h = H(k)$ με H : SHA – 512
 - Κλειδί υπογραφής: $x \leftarrow h[0..255]$
 - Κλειδί τυχαιότητας: $r \leftarrow h[256..511]$
 - Δημόσιο κλειδί $Y = xG$
 - Ιδιωτικό κλειδί $sk = (x, r)$



edDSA – Υπογραφή & Επαλήθευση

- **Ντετερμινιστική τυχαιότητα**

- $r_m \leftarrow H(\textcolor{red}{r} || m)$

- **Υπογραφή Schnorr**

- $R_m \leftarrow r_m G$
 - $c \leftarrow H(vk, R_m, m)$
 - $s \leftarrow r_m + cx \text{ mod } q$
 - $\sigma = (R_m, s)$

- **Ίδιο μήνυμα – ίδια υπογραφή**

- **Επαλήθευση**

- $c' \leftarrow H(vk, R_m, m)$
 - Έλεγχος αν $sG = R_m + c'vk$



BLS Signatures

- **Δημιουργία Κλειδιών**

- Επιλογή $\mathbb{G}$, $\mathbb{G}_T$ τάξης q με δύσκολο CDH
- ώστε να υπάρχει συμμετρικό pairing $e: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$
- Επιλογή hash function $H: \{0,1\}^* \rightarrow \mathbb{G}$
- $sk \leftarrow_{\$} \mathbb{Z}_q$
- $vk \leftarrow g^{sk}$

- **Υπογραφή**

- $Sign(sk, m): \sigma \leftarrow H(m)^{sk}$

- **Επαλήθευση**

- Έλεγχος αν:
 $Vf(vk, m, \sigma) \rightarrow e(vk, H(m)) = e(g, \sigma)$

Ορθότητα

$$\begin{aligned} e(vk, H(m)) &= e(g^{sk}, H(m)) = e(g, H(m))^{sk} = \\ e(g, H(m)^{sk}) &= e(g, \sigma) \end{aligned}$$

Ασφάλεια

Ανάγεται στο CDH στην $\mathbb{G}$



Αυθεντικότητα Κλειδιών

Πρακτική χρήση ψηφιακών υπογραφών

- Διαφορά Συμμετρικών- Ασύμμετρων Κρυπτοσυστημάτων
 - Συμμετρικά: Δύσκολη διανομή, Εύκολη Αυθεντικότητα (λόγω φυσικών υποθέσεων)
 - Ασύμμετρα: Εύκολη διανομή, Δύσκολη Αυθεντικότητα
- Αντιστοιχία (?) Ταυτότητας Χρήστη- Δημοσίου, Ιδιωτικού Κλειδιού (binding)
- Ενεργός αντίπαλος- Πλαστοπροσωπία- αλλαγή κλειδιών
- Απαραίτητη η διασφάλιση για χρήση σε ευρεία κλίμακα
- Δεν υπάρχει λύση που να δουλεύει θεωρητικά και πρακτικά
- Στην πράξη: μετάθεση του προβλήματος με μείωση της έκτασης (αρκεί 1 αυθεντικό κλειδί)

Αρχές πιστοποίησης

- Έμπιστες Τρίτες Οντότητες- (Πάροχοι Υπηρεσιών Πιστοποίησης)
- Πιστοποίηση Αντιστοιχίας Ταυτότητας Κλειδιών
 - Εγγυάται ότι το δημόσιο κλειδί όντως αντιστοιχεί στον χρήστη
 - **Πώς;** Υπογράφοντας ‘ψηφιακά’ το ζεύγος (ID, PK_{ID}) •
 - **Πλεονέκτημα:** Μείωση κλειδιών που πρέπει να αποκτήσουμε με έμπιστο τρόπο
 - Μόνο το κλειδί της CA
 - Για τα υπόλοιπα ‘εγγυάται’ το πιστοποιητικό
- **Μειονέκτημα:** Ποιος εγγυάται την σχέση κλειδιών-ταυτότητας για την CA;
 - **Η ίδια!** (υπογράφει η ίδια μία δήλωση για τον εαυτό της) ή
 - Μια άλλη - **ανώτερη** - αρχή πιστοποίησης

Υποδομή Δημοσίου Κλειδιού (PKI)

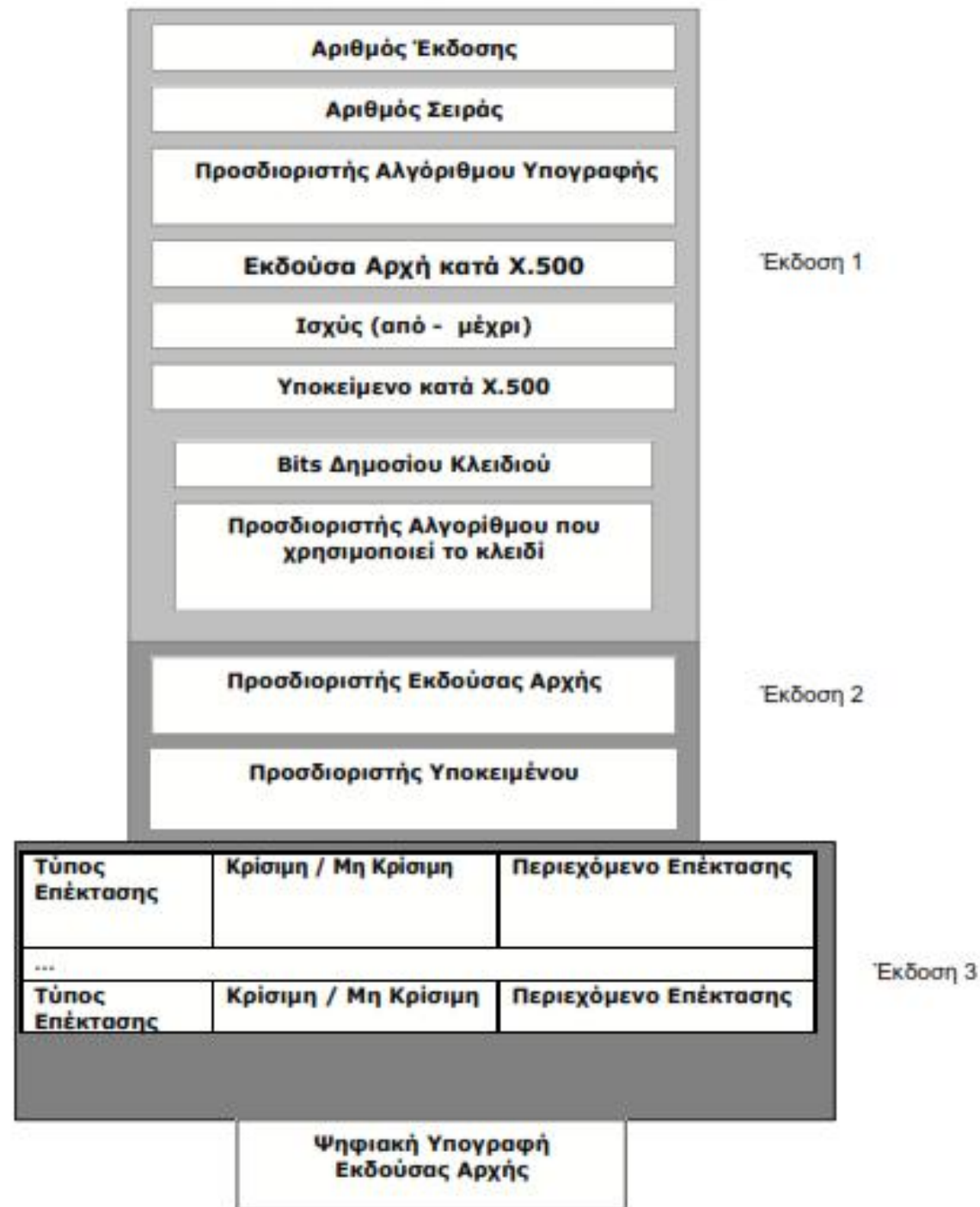
- Loren Kohnfelder, MIT BSc thesis, 1978
- Ιεραρχική οργάνωση δομών πιστοποίησης και των σχετικών υπηρεσιών
 - Ευρεία προτυποποίηση (ITU X.500, RFC 6818)
 - Ενδιάμεσες Αρχές: Υπογραφή από ανώτερη αρχή
 - Ριζικές (Root) Αρχές: Υπογράφουν μόνες τους
 - Συνήθως 3-4 επίπεδα
 - Ψηφιακό Πιστοποιητικό
 - Υπογραφή στο ζεύγος (ID, PK_{ID}) μαζί με άλλα στοιχεία

Ψηφιακά Πιστοποιητικά

Απόκτηση

- Προεγκατάσταση στο ΛΣ
- Προεγκατάσταση στον browser
- Απόκτηση από δημόσιο κατάλογο (web site)
- Απόκτηση από νομική οντότητα

Supply Chain attacks



Αρχές Πιστοποίησης – Άλλες υπηρεσίες

- Ανάκληση πιστοποιητικών
 - Απώλεια κλειδιού υπογραφής
 - Αλλαγή Στοιχείων Υποκειμένου
 - Ενημέρωση Χρηστών με 2 τρόπους
 - Certificate Revocation Lists (CRL):
 - ‘Μαύρη’ λίστα από SN για πιστοποιητικά που δεν ισχύουν
 - Υπογεγραμμένη από την CA
 - Ανάκτηση σε τακτά χρονικά διαστήματα
 - OCSP (Online Certificate Status Protocol)
 - Ερώτηση στην CA για ισχύ πιστοποιητικού
 - Η CA συμμετέχει σε κάθε συναλλαγή
- Διάδοση Πιστοποιητικών σε αποθετήρια
- Εγγραφή-Επαλήθευση Ταυτότητας Χρηστών
- Δημιουργία κρυπτογραφικών κλειδιών (αυστηρές προδιαγραφές ασφάλειας)
- Χρονοσήμανση- Αρχειοθέτηση

Web of Trust (PGP)

Ομότιμη έκδοση και επαλήθευση ταυτότητας (web of trust)

- Κάθε χρήστης είναι CA
- Υπογράφει αντιστοιχίες ταυτότητας, κλειδιού που γνωρίζει
- Λήψη πιστοποιητικών μόνο από γνωστούς χρήστες
- Ο κάθε χρήστης 'εγγυάται' για τους γνωστούς του



Identity – Based Crypto



Signatures: Shamir (1984)

Encryption: Boneh-Franklin (2001)

- Οποιοδήποτε όνομα κάποιου χρήστη πχ. email είναι η ταυτότητα
- Δεν χρειάζεται διανομή κλειδιού
- Χρειάζεται κεντρική TTP
- Παράγει τα ιδιωτικά κλειδιά από την ταυτότητα

Identity Based Signatures

- TTP έχει κλειδί RSA $((e, n), d)$
- Δημιουργία ιδιωτικού κλειδιού από ταυτότητα χρήστη id
- Υπογραφή σύνοψης της ταυτότητας $k = H(id)^d \bmod n$
- Ασφαλής Διανομή στον κάτοχο
- Υπογραφή από χρήστη id
 - Επιλογή τυχαίου r
 - Υπολογισμός $t = r^e \bmod n$
- $s = k \cdot r^{H(m,t)} \bmod n$
- Η υπογραφή είναι (t, s)
- Επαλήθευση υπογραφής με την ταυτότητα:
- Έλεγχος αν: $H(id)t^{H(m,t)} = s^e$
- Ορθότητα:
 - $s^e = k^e r^{eH(m,t)} = H(id)t^{H(m,t)}$



Ψηφιακές Υπογραφές με ιδιωτικότητα

Τυφλές Υπογραφές
Υπογραφές Δακτυλίου

Motivation

- Ψηφιακές Υπογραφές:

- Ακεραιότητα
- Αυθεντικότητα
- Μη Αποκήρυξη
- Δημόσια επαληθευσιμότητα
- Χωρίς ιδιωτικότητα όμως...

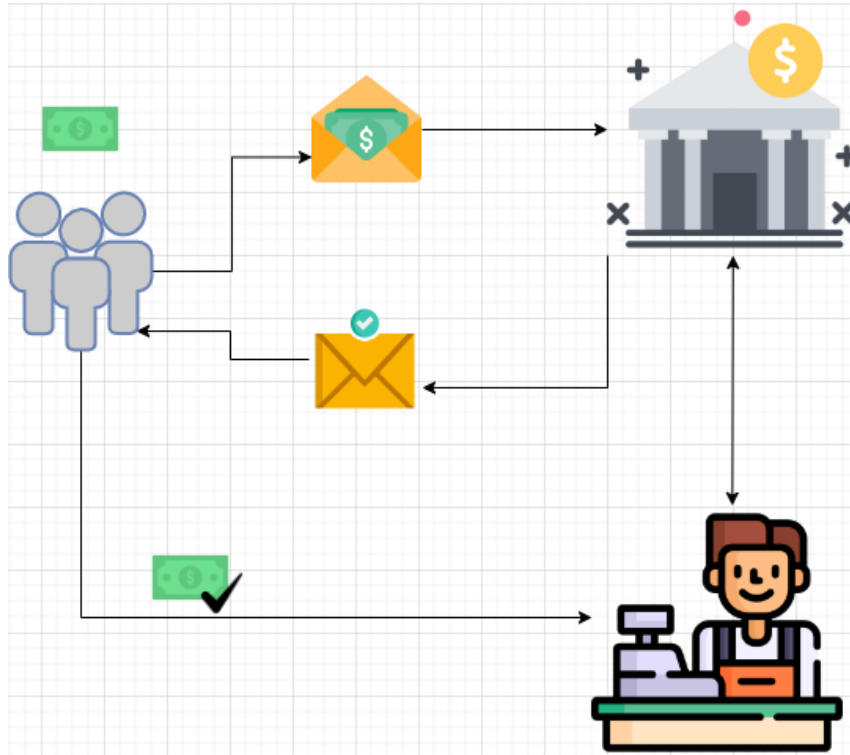


- Ο υπογράφων
 - βλέπει το μήνυμά που υπογράφει και
 - μπορεί να συσχετίσει την υπογραφή με το αίτημα δημιουργίας της
- Το δημόσιο κλειδί επαλήθευσης προδίδει τον signer.
- Τα παραπάνω δεν είναι επιθυμητά σε πολλές εφαρμογές
 - Ηλεκτρονικό χρήμα
 - Ηλεκτρονικές ψηφοφορίες
 - Whistleblowing

Υπογραφές για ηλεκτρονικό χρήμα

- Νόμισμα $c \stackrel{\$}{\leftarrow} \{0,1\}^*$
- 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:** $Vf(m, \mathbf{Sign}\langle S(sk), U(m), vk \rangle, vk) = 1$ για $(sk, vk, prms) \leftarrow KGen(1^\lambda)$

Τυφλές υπογραφές RSA

- **Δημιουργία Κλειδιών:**
 - Όπως στο RSA. Τελικά: $(sk, vk) = (d, (e, n))$
- **Υπογραφή:**
 - $Blind(m, vk) \rightarrow H(m) \cdot r^e \bmod n, r \leftarrow Z_n^*$
 - $Sign(m', sk) \rightarrow m'^d \bmod n \rightarrow (H(m)^d r) \bmod n$
 - $UnBlind(\sigma', vk) \rightarrow \sigma' r^{-1} \bmod n \rightarrow H(m)^d \bmod n$
- **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
 - $\Pr[BGame_A(1^\lambda) = 1] = \frac{1}{2}$
- Computational Blindness
 - $\Pr[BGame_A(1^\lambda) = 1] \leq \frac{1}{2} + \text{negl}(\lambda)$

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 $\emptyset$

Μοντέλο Ασφάλειας Τυφλών Υπογραφών

- **Unforgeability**

- Δεν έχει νόημα το μοντέλο των κλασικών υπογραφών (EUF-CMA).
 - Ο S δημιουργήσε (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 πλαστογράφιση

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 $Vf(pk, m_i, \sigma_i) = 1 \forall i \in [l + 1]$ 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

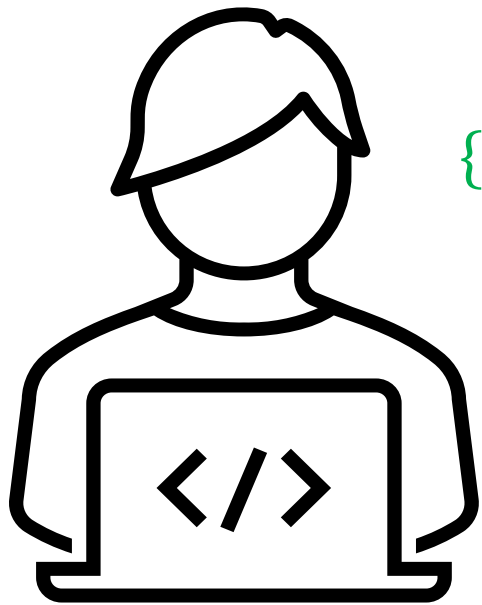
- **Κατασκευή από OR-proofs**

- 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

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



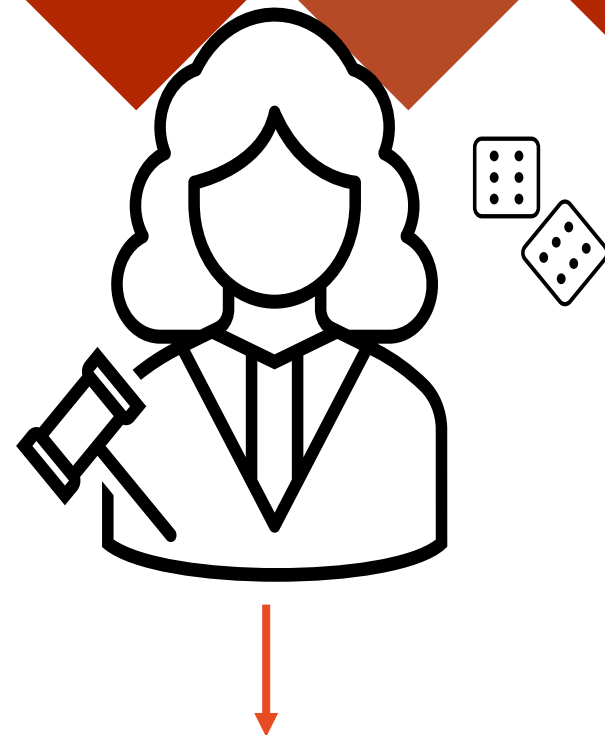
$$T_k = g^{t_k},$$
$$\{T_i = g^{t_i} Y_i^{-c_i}, t_i, c_i \xleftarrow{\$} \mathbb{Z}_q\}, i \in [n]/\{k\}$$

$$c \leftarrow H(R, \mathbf{m}, \{T_i\}_{i=1}^n)$$

$$c_k \leftarrow c - \sum_i c_i \bmod q$$

$$s_k \leftarrow (t_k + c_k x_k) \bmod q$$

$$s_i \leftarrow t_i, i \in [n]/\{k\}$$



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