Ψηφιακές Υπογραφές

Παναγιώτης Γροντάς
ΕΜΠ

Κρυπτογραφία

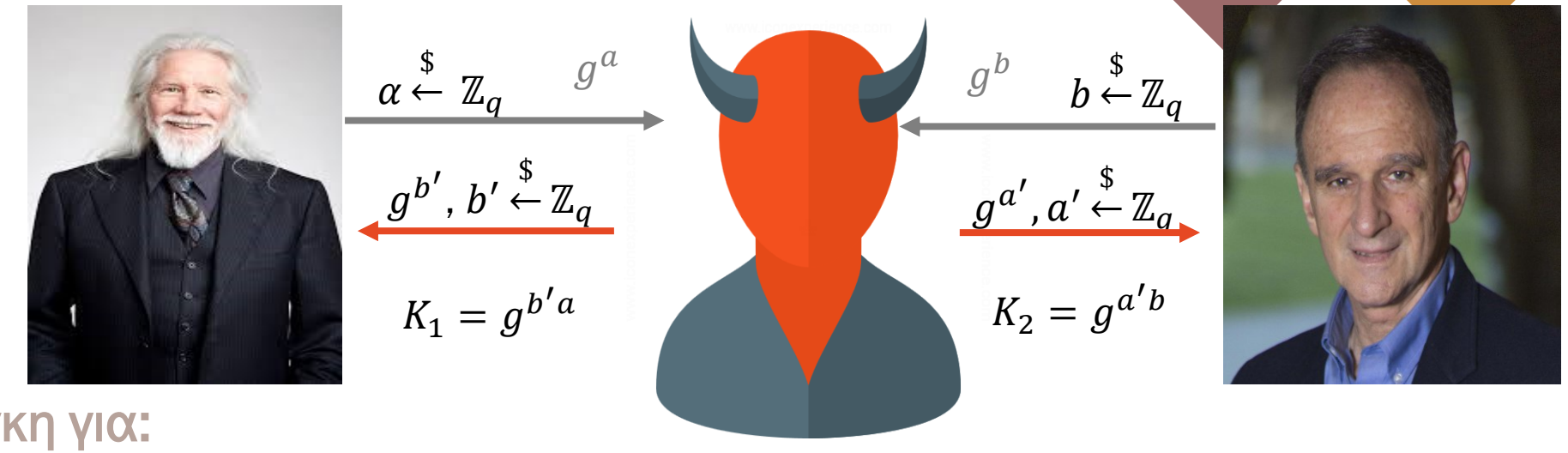
2024 - 2025

Περιεχόμενα

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 επαληθευσιμότητα
  - 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 επαληθευσιμότητα
  - 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
  - $KGen(1^{\lambda}) \rightarrow (vk, sk)$
  - $Sign(sk, m) \rightarrow \sigma, \ \mathbf{m} \in \{\mathbf{0}, \mathbf{1}\}^*$
  - $Vf(pk, m, \sigma) \rightarrow 0/1$
- Έγκυρη υπογραφή
  - $Vf(pk, m, \sigma) = 1$
- Ορθότητα
  - $Vf\big(pk, m, Sign(sk, m)\big) = 1, \ \ \forall (vk, sk) \leftarrow KGen(1^{\lambda})$

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 ΠΡΙΝ 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 πλαστογράφηση 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 $\boldsymbol{Vf(pk, m^*, \sigma^*) = 1}$ and $\boldsymbol{m^* \notin Q}$ then return 1
- Else return 0

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

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

Ο αντίπαλος απλά δεν πρέπει να έχει δει το συγκεκριμένο ζεύγος μηνύματος υπογραφής
Μπορεί να φτιάξει νέα πλαστογράφηση για $\boldsymbol{m}^*$
π.χ μέσω malleability

$\boldsymbol{m}^*$ είναι νέο μήνυμα
Δεν πρέπει να έχει ζητηθεί υπογραφή καθόλου γι' αυτό

Παραλλαγή *strong* EUF-CMA (SUF-CMA):
Ορισμός: όμοιος με **EUF-CMA**
Συνθήκη νίκης $\mathcal{A}$

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

SUF-CMA security ⇒ EUF-CMA security

Υπογραφές RSA

Υπογραφές RSA

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

Ορθότητα: $\sigma^e = (m^d)^e = m^{ed} = m \pmod{n}$ 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 $\sigma^* \xleftarrow{\$} \mathbb{Z}_n^*$
- Εφαρμόζει το κλειδί επαλήθευσης και υπολογίζει ${\sigma^*}^e \rightarrow m^* \in \mathbb{Z}_n^*$
- Το σ^* είναι πλαστογράφηση για το m^*
  - αφού ικανοποιεί τη σχέση επαλήθευσης
  - Το m^* δεν έχει ρωτηθεί στο Q
- Ο $\mathcal{A}$ ΄ κερδίζει πάντα $\Pr\left[Forge - Game_{\mathcal{A},\mathrm{RSA}}\left(1^\lambda\right) = 1\right] = 1$

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 κάποιο $m^* \in \mathbb{Z}_n^*$
- 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 $\sigma^* = \sigma_1 \cdot \sigma_2 = m_1^d \cdot m_2^d = \left(m_1 \cdot {}^{m^*}/_{m_1}\right)^d = m^{*d}$
- Το ζεύγος (m^*, σ^*) αποτελεί έγκυρη υπογραφή και $(m^*, \sigma^*) \notin Q$
- Ο $\mathcal{A}$ ΄ κερδίζει πάντα $\Pr\left[Forge - Game_{\mathcal{A},\mathrm{RSA}}\left(1^\lambda\right) = 1\right] = 1$

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 $\sigma^* = \sigma^d \cdot r^{-1} = m^{*d}$
- Το ζεύγος (m^*, σ^*) αποτελεί έγκυρη υπογραφή και $(m^*, \sigma^*) \notin Q$
- Ο $\mathcal{A}$ κερδίζει πάντα $\Pr\left[Forge - Game_{\mathcal{A},\mathrm{RSA}}(1^\lambda) = 1\right] = 1$

Υπογραφές RSA – FDH (Full Domain Hash)

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

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

Ορθότητα: $\sigma^e = \big(\boldsymbol{H(m)}^d\big)^e = \boldsymbol{H(m)}^{ed} = \boldsymbol{H(m)} (\text{mod n})$ 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)
0000000…00000000	Συμβολοσειρά με πιθανότητα εμφάνισης $1/l(n)$
0000000…00000001	Συμβολοσειρά με πιθανότητα εμφάνισης $1/l(n)$
0000000…00000010	Συμβολοσειρά με πιθανότητα εμφάνισης $1/l(n)$
0000000…00000011	Συμβολοσειρά με πιθανότητα εμφάνισης $1/l(n)$
…..	…..
1111111…11111111	Συμβολοσειρά με πιθανότητα εμφάνισης $1/l(n)$

https://crypto.stackexchange.com/questions/879/what-is-the-random-oracle-model-and-why-is-it-controversial/880

https://blog.cryptographyengineering.com/2011/10/08/what-is-random-oracle-model-and-why-2/

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

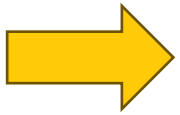
- Τυχαίο μαντείο: αφαίρεση τυχαίας συνάρτησης
  - Μαύρο κουτί - απαντάει σε ερωτήσεις
  - (Τέλεια) Ασφάλεια στο κανάλι επικοινωνίας (μοντελοποίηση τοπικής αποτίμησης)
  - Είναι συνάρτηση (ίδια είσοδος - ίδια έξοδος σε κάθε κλήση)
  - Είναι συνάρτηση σύνοψης (υπάρχουν συγκρούσεις – αλλά είναι δύσκολο 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 ομοιόμορφά 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 (EUF-CMA) 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: $\boldsymbol{\sigma^{*e} = H(m^*)}$
- Άρα: $\boldsymbol{\sigma^* = H(m^*)^{e^{-1}}}$
- Ο R πρέπει να μαντέψει πότε ο F θα ρωτήσει το m^* στο RO.

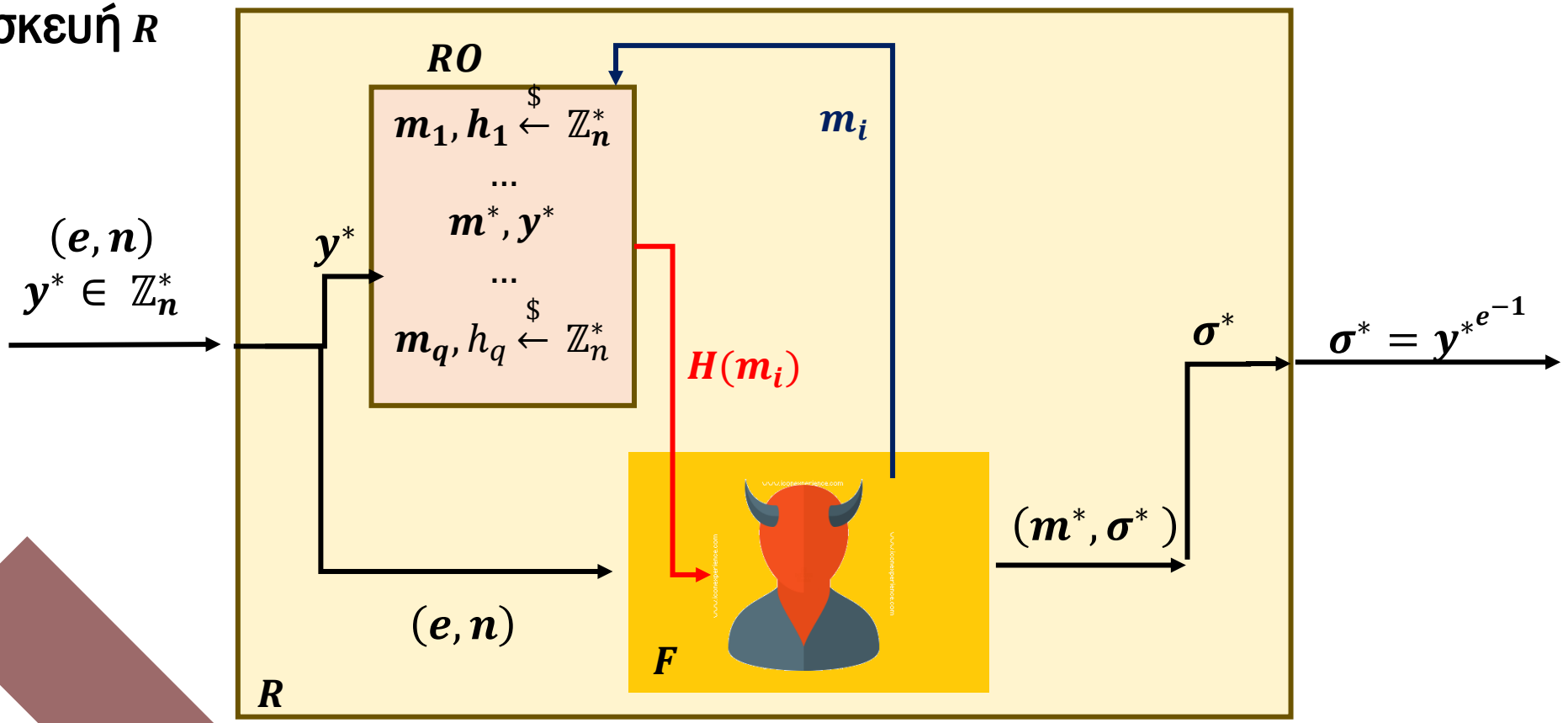
Απόδειξη Ασφάλειας RSA-FDH
Επίθεση χωρίς μήνυμα

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



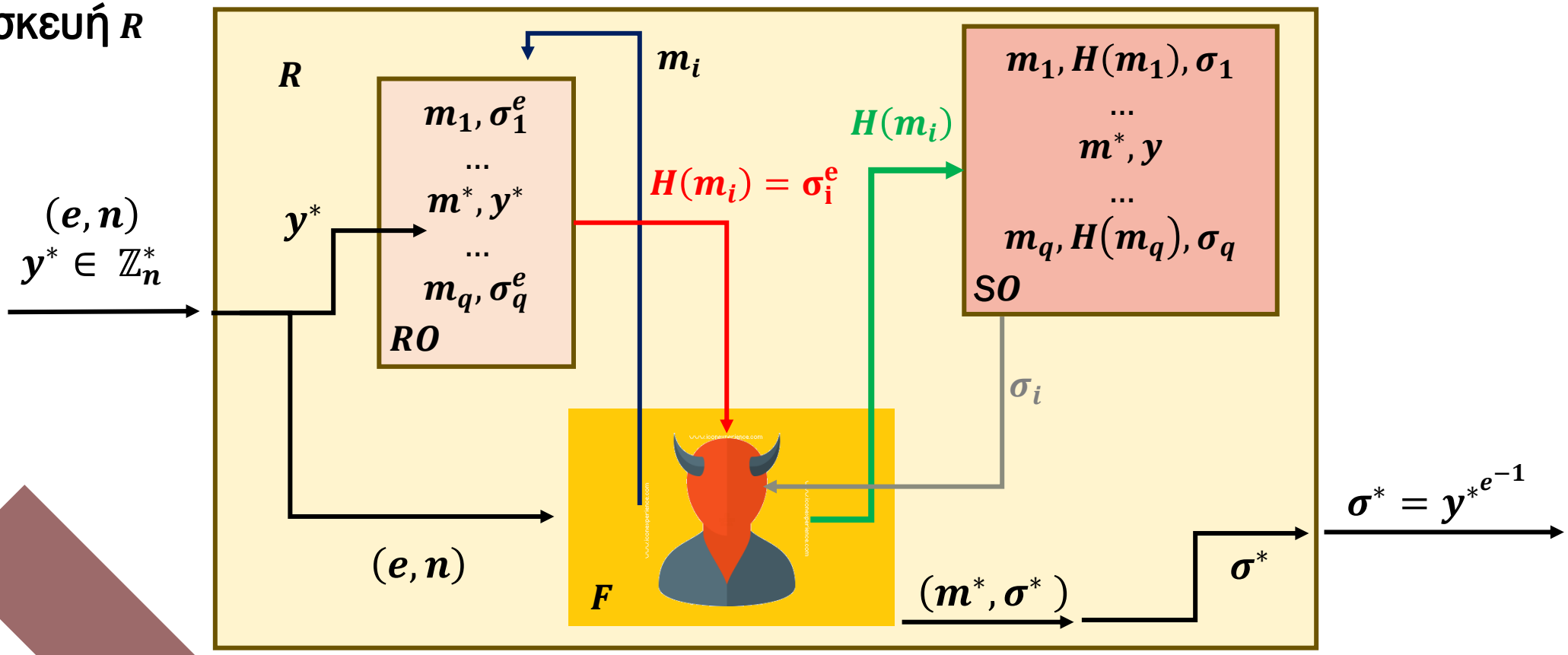
Απόδειξη Ασφάλειας RSA-FDH
Επίθεση χωρίς μήνυμα

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

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

Απόδειξη Ασφάλειας RSA-FDH
Επίθεση επιλεγμένου μηνύματος (CMA)

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 $H(m)$
  - 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:
  - $\sigma^e = (\sigma^e) = H(m)$
- 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 πραγματικές επιθέσεις που να έχουν εκμεταλλευτεί την απόδειξη μέσω τυχαίου μαντείου