1 Ψηφιακές Υπογραφές

Η ψηφιακή υπογραφή είναι μια βασική κρυπτογραφική έννοια, τεχνολογικά ισοδύναμη με την χειρόγραφη υπογραφή. Σε πολλές Εφαρμογές, οι ψηφιακές υπογραφές χρησιμοποιούνται ως δομικά συστατικά για μεγαλύτερα κρυπτογραφικά πρωτόκολλα και συστήματα.

Σε ένα σχήμα υπογραφής, κάθε μέρος έχει ένα μοναδικό κλειδί υπογραφής sk που μοναδικά υπογράφει το μήνυμα . Κάθε μεριά δημοσιεύει το αντίστοιχο δημόσιο κλειδί επαλήθευσης pk. Μόνο κάποιος με την γνώση του sk μπορεί να υπογράψει ένα μήνυμα, αλλά όλες οι μεριές έχουν πρόσβαση στο pk και μπορούν να επαληθέψουν μιαν υπογραφή. Τέτοια σχήματα είναι χρήσιμα γιατί αποφεύγουν πως κάποιος μέσω του κλειδιού επαλήθευσης να μπορεί να υπολογίσει το κλειδί υπογραφής με μη αμελητέα πιθανότητα. Επιπλέον είναι ανέφικτο για κάποιον αντίπαλο να παράγει ένα έγκυρο ζευγάρι μήνυμα-υπογραφή ως προς κάποιο κλειδί επαλήθευσης.

Definition 1.0.1. Ένα ***σχήμα ψηφιακής υπογραφής (digital signature scheme)*** είναι μια τριάδα αλγορίθμων (Gen,Sign,Verify)[1] τέτοια ώστε

- Ο αλγόριθμος παραγωγής κλειδιού Gen: Πάρε ως είσοδο μια παράμετρο ασφαλείας 1^λ και επέστρεψε το ζευγάρι (pk, sk). Θα ονομάζουμε το κλειδί pk ως δημόσιο ή επαλήθευσης και το κλειδί sk ως κρυφό ή υπογραφής
- Ο αλγόριθμος υπογραφής Sign: Πάρε ως είσοδο την κρυπτογραφική παράμετρο 1^λ, το κλειδί υπογραφής sk και ένα μήνυμα M και παρήγαγε την ψηφιακή υπογραφή σ του M.
- Ο αλγόριθμος επαλήθευσης Verify: Πάρε ως είσοδο το κλειδί επαλήθευσης vk, μια ψηφιακή υπογραφή σ και ένα μήνυμα m. Επέστρεψε `True`$= 1$ ή `False`=0 δείχνοντας αν η υπογραφή είναι έγκυρη ή όχι.

Ο κύριος στόχος των ψηφιακών υπογραφών είναι ***μη δυνατότητα πλαστογράφησης (unforgeability)***, ή διαφορετικά πως ένας PPT αντίπαλος δεν μπορεί να κατασκευάσει ένα έγκυρο ζευγάρι μηνύματος-υπογραφής. Η δυνατότερη επίθεση ενάντια σε ψηφιακές υπογραφές ονομάζετε ***επίθεση επιλεγμένης μεθόδου (chosen method attack)***. Σε μια τέτοια επίθεση, ο αντίπαλος έχει απεριόριστη πρόσβαση σε ένα μαντείο υπογραφών που υπογράφει μηνύματα που διαλέγει ο αντίπαλος.

Definition 1.0.2. Ένα σχήμα ψηφιακών υπογραφών (Gen,Sign,Verify) χαρακτηρίζεται από ***μη δυνατότητα πλαστογράφησης ενάντια σε επιθέσεις επιλεγμένου μηνύματος (unforgeability against chosen message attacks)*** (UF-CMA) αν για κάθε PPT αντίπαλο $\mathcal{A}$ που χρησιμοποιεί το μαντείο υπογραφών $\mathsf{Sign}(sk, \cdot)$ ℓ φορές, η πιθανότητα να παράξει ο $\mathcal{A}$ $\ell + 1$ διαφορετικά έγκυρα ζευγάρια μηνύματος υπογραφής είναι αμελητέα. Όταν τα μηνύματα είναι διακριτά, θα λέμε πως υπάρχει ***ισχυρή μη δυνατότητα πλαστογράφησης (strong unforgeability)***. Όταν τα ζευγάρια μηνύματος-υπογραφής είναι διακριτά, θα λέμε πως υπάρχει ***απλή μη δυνατότητα πλαστογράφησης (regular unforgeability)***.

1.1 Η συνάρτηση RSA : Η ύψωση στην e-οστή δύναμη στο $\mathbb{Z}_n^*$

Το κρυπτοσύστημα RSA αναπτύχθηκε το 1977 στο MIT από τους Ron Rivest, Adi Shamer, and Leonard Adleman. Ήταν το πρώτο σχήμα κρυπτογράφησης δημοσίου κλειδιού που μπορούσε να κρυπτογραφήσει και να υπογράψει μηνύματα. Όπως και με το πρωτόκολλο ανταλλαγής κλειδιού Diffie-Hellman, το σύστημα έδινε τη δυνατότητα σε δύο μεριές να επικοινωνήσουν σε ένα δημόσιο κανάλι.

Υποθέστε πως η Αλίκη αποφασίζει να στείλει στον αγαπητό της φίλο Βασίλη ένα μήνυμα. Για να εξασφαλιστεί μια ιδιωτική συνομιλία σε ένα μη ασφαλές κανάλι, ο Βασίλης διαλέγει και δημοσιεύει τους ακεραίους n και e. Η Αλίκη γράφει το μήνυμα x και υπολογίζει το

$$E(x) = x^e \bmod n,$$

[1] Ο Gen και ο Sign είναι PPT αλγόριθμοι, ο Verify είναι ντετερμινιστικός πολυωνυμικού χρόνου αλγόριθμος.

που είναι γνωστό ως η ***ύψωση στην e-οστη δύναμη (e-th Power map*** του x. Τότε στέλνει το $y = E(x)$ στον Βασίλη, ο οποίος για να δει το μήνυμα, πρέπει να υπολογίσει την e-οστη ρίζα του y. Πιστεύεται πως αυτό είναι δύσκολο, όπως συζητήθηκε και στην ενότητα **??**. Αν ο Βασίλης διαλέξει τα n και e με ανάλογα, υπάρχει και μια εναλλακτική μέθοδος. Βλέπουμε πως ο Βασίλης μπορεί να εφαρμόσει την ύψωση στην d-οστη δύναμη του y για να πάρει το x,

$$D(y) = y^d = x^{ed} \equiv x^{1+\varphi(n)k} \equiv x \bmod n$$

όπου το $k \in \mathbb{Z}_n$ και η συνάρτηση Euler $\varphi(n)$ ορίζεται ως εξής:

Definition 1.1.1. Για κάθε $n \in \mathbb{N}$, η ***συνάρτηση Euler (Euler function)*** $\varphi(n)$ υπολογίζει τον αριθμό των ακεραίων στο $\mathbb{Z}_n$ που είναι σχετικά πρώτοι με το n:

$$\varphi(n) = \#\left\{k \in \mathbb{Z}_n : \ \gcd(k, n) = 1\right\}.$$

Αντίστοιχα, το $\varphi(n)$ είναι ο αριθμός των αντιστρέψιμος στοιχείων στο $\mathbb{Z}_n$:

$$\varphi(n) = \#\left\{k \in \mathbb{Z}_n : k\ell = 1 \text{ for some } \ell \in \mathbb{Z}_n\right\}.$$

Για να υπολογίσουμε την συνάρτηση Euler μελετάμε τις εξής περιπτώσεις

$$\varphi(n) = \begin{cases} p^e - p^{e-1}, & n = p^e \text{ for prime } p \\ \displaystyle\prod_{i=1}^{j} \varphi(p_i^{e_i}), & n = p_1^{e_1} \cdots p_j^{e_j} \text{ for distinct primes } p_i. \end{cases}$$

Αν $n = p^e$, είναι εύκολο να μετρήσουμε τους αριθμούς υπόλοιπο n τους οποίους το p δεν διαιρεί. Μπορούμε να επεκτείνουμε το φ σε ένα σύνθετο ακέραιο $n = p_1^{e_1} \cdots p_j^{e_j}$ χρησιμοποιώντας το γεγονός ότι το φ είναι πολλαπλασιαστικό σε σχετικά πρώτους ακέραιους: $\varphi(mn) = \varphi(m)\varphi(n)$ όταν $\gcd(m, n) = 1$. Αυτό μπορεί να δειχθεί αποδεικνύοντας ότι

$$\mathbb{Z}_{mn}^* \cong \mathbb{Z}_m^* \times \mathbb{Z}_n^*$$

χρησιμοποιώντας το Κινέζικο θεώρημα υπολοίπων.

Ενδιαφερόμαστε στην ειδική περίπτωση όπου n είναι το γινόμενο δύο μεγάλων πρώτων p και q. Η πολλαπλασιαστική ομάδα $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : \ \gcd(a, n) = 1\}$ αποτελείτε από $\varphi(n) = (p-1)(q-1)$ στοιχεία. Για να είναι το παραπάνω πρωτόκολλο αποτελεσματικό (δηλαδή μόνο ο Βασίλης να γνωρίζει το d) επιλέγουμε το e να είναι ένας πρώτος τέτοιος ώστε $1 \leq e \leq \varphi(n)$ και $\gcd(e, \varphi(n)) = 1$. Τότε η ύψωση στην e-οστη δύναμη

$$E \colon \mathbb{Z}_n^* \longrightarrow \mathbb{Z}_n^*,$$

που ορίζεται από το $x \mapsto x^e \bmod n$ είναι αντιστρέψιμη. Συγκεκριμένα, όταν $ed \equiv 1 \bmod \varphi(n)$, η ύψωση στην d-οστή δύναμη D αντιστρέφει την E. Αν ο Βασίλης διαλέξει τα e και $\varphi(n)$ προσεκτικά, μπορεί εύκολα να βρει το d χρησιμοποιώντας τον αλγόριθμο του Ευκλείδη.

Είναι ξεκάθαρα πως η δύναμη αυτής της τεχνικής βασίζεται στην επιλογή του Βασίλη για το n. Αν τα p και q είναι προφανή τότε κάθε ενδιαφερόμενη μεριά θα μπορούσε να υπολογίσει το $\varphi(n)$ και στη συνέχεια το d. Αντίστοιχα, δεδομένου του n και του $\varphi(n)$ μπορεί κανείς να υπολογίσει το d. Αυτό συνεπάγεται πως το να βρει κανείς e-οστές ρίζες στο $\mathbb{Z}_n^*$ εξασφαλίζεται από την παραγοντοποίηση του n. Επειδή το πρόβλημα της παραγωντοποίησης πιστεύεται πως είναι δύσκολο, η συνάρτηση RSA φαίνεται πως είναι δύσκολο να αντιστραφεί σε πολυωνυμικό χρόνο και συνεπώς αποτελεί συνάρτηση μιας κατεύθυνσης. Η ***υπόθεση RSA (RSA assumption)*** θεωρεί πως είναι δύσκολο να αντιστρέψει κανείς την συνάρτηση RSA.

1.2 Ψηφιακές υπογραφές RSA

Μετά την εισαγωγή του, η ασφάλεια του σχήματος υπογραφής RSA εξετάστηκε στο Κατακερματισμό πλήρους πεδίου ορισμού και αποδείχθηκε ασφαλές κάτω από το μοντέλο τυχαίου μαντείου βασιζόμενοι στην υπόθεση RSA.

Γενικά μια ***συνάρτηση κατακερματισμού (hash function)*** είναι μια αντιστοίχηση που παίρνει ως είσοδο ένα μήνυμα αυθαίρετου μήκους και επιστρέφει ένα στοιχείο φραγμένου μεγέθους.

Μια ιδανική συνάρτηση κατακερματισμού θα πρέπει να είναι εύκολα υπολογίσιμη, μη αντιστρέψιμη και να συμπεριφέρεται σαν ένεση υπό την έννοια ότι είναι σχεδόν απίθανο δύο μηνύματα, ανεξαρτήτως πόσο όμοια είναι, να αντιστοιχίζονται στην ίδια συμβολοσειρά. Σε αυτήν την ενότητα, θα θεωρήσουμε πως η συνάρτηση κατακερματισμού μας H είναι ιδανική με εύρος

$$H\colon \{0,1\}^* \longrightarrow \mathbb{Z}_n^*,$$

όπου $\{0,1\}^* = \bigcup_{k=0}^{\infty} \{0,1\}^k$.

Στο σχήμα υπογραφών RSA,

- Τον γεννήτορα κλειδιού Gen: Πρώτα διάλεξε δύο τυχαίους πρώτους αριθμούς p και q τέτοιους ώστε $|p| = |q| = \lambda$. Υπολόγισε τα $n = pq$ και $\varphi(n) = (p-1)(q-1)$. Δεύτερον, διάλεξε έναν τυχαίο πρώτο $e < \varphi(n)$ τέτοιο ώστε $\gcd(e, \varphi(n)) = 1$ και υπολόγισε το $d \equiv e^{-1} \bmod \varphi(n)$. Το κλειδί επαλήθευσης είναι το (n, e) και το κλειδί υπογραφής το d. Μια συνάρτηση κατακερματισμού πλήρους πεδίου ορισμού H είναι προσβάσιμη σε όλες τις μεριές.

- Ένα κλειδί υπογραφής Sign: Δεδομένου του d και ενός μηνύματος M, επέστρεψε την ψηφιακή υπογραφή $\sigma = H(M)^d \bmod n$.

- Ένας αλγόριθμος επαλήθευσης Verify: Δεδομένων (n, e) και (M, σ), επαλήθευσε ότι $\sigma^e = H(M) \bmod n$. Αν η ισότητα ισχύει το αποτέλεσμα είναι `True`; διαφορετικά το αποτέλεσμα είναι `False`.

Θα ονομάζουμε ως σύγκρουση όταν δύο μηνύματα έχουν την ίδια υπογραφή υπό μια συνάρτηση κατακερματισμού. Αυτές οι περιπτώσεις προκαλούν πλαστογραφήσεις. Για παράδειγμα, αν το (M, σ) είναι ένα έγκυρο ζευγάρι μηνύματος-υπογραφής και το m' είναι ένα μήνυμα τέτοιο ώστε $H(M) = H(M')$, τότε το (M', σ) είναι επίσης ένα έγκυρο ζευγάρι μηνύματος-υπογραφής. Για να ισχύει η υπόθεση RSA, το H πρέπει να ικανοποιεί μια μορφη ανοχής σε συγκρούσεις. Αυτό αποδεικνύεται στο λεγόμενο μοντέλο τυχαίου μαντείου.

Ένα ***τυχαίο μαντείο (random oracle)*** είναι μια συνάρτηση που παράγει μια φαινομενικά τυχαία έξοδο για κάθε ερώτημα που λαμβάνει. Θα πρέπει να είναι συνεπής με τις απαντήσεις της: αν ένα ερώτημα επαναληφθεί θα πρέπει το μαντείο να επιστρέψει την ίδια απάντηση. Η απώλεια κάποιας συγκεκριμένης δομής του τυχαίων μαντείων τα καθιστά χρήσιμα σε κρυπτογραφικές εφαρμογές όταν για να σκεφτούμε αφαιρετικά για μια συνάρτηση κατακερματισμού. Αν ένα σχήμα είναι ασφαλές θεωρώντας πως ο αντίπαλος βλέπει κάποια συνάρτηση σαν τυχαίο μαντείο, λέμε πως είναι ασφαλές στο ***Μοντέλο Τυχαίου Μαντείου (Random Oracle Model)***.

Η εικόνα 3 παρουσιάζει πως μια συνάρτηση κατακερματισμού H μοντελοποιείται ως τυχαίο μαντείο.

• Δεδομένου $M \notin History$, διάλεξε $t \xleftarrow{r} \mathbb{Z}_n^*$ και εισήγαγε (M, t) στο $History$. Επέστρεψε t. • Δεδομένου M τέτοιου ώστε $(M, t) \in History$ για κάποιο t, επέστρεψε t.

Σχήμα 1: Ένα τυχαίο μαντείο, όπου το $History$ αναπαριστά το σύνολο όλων των ζευγαριών (*εισόδου,εξόδου*) που εξυπηρέτησε το μαντείο.

Θα δείξουμε πως το σχήμα υπογραφής RSA είναι ασφαλές στο Μοντέλου Τυχαίου Μαντείου υπό την υπόθεση RSA.

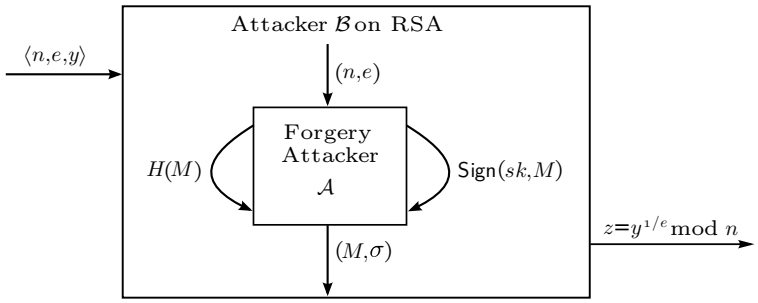
Theorem 1.2.1. *Στο Μοντέλο Τυχαίου Μαντείου, κάθε PPT αλγόριθμος πλαστογράφησης που επιτίθεται στο σχήμα ψηφιακών υπογραφών RSA και βρίσκει μια πλαστογραφημένη υπογραφή με πιθανότητα α μπορεί να μεταμορφωθεί σε έναν αλγόριθμο που βρίσκει e-οστές ρίζες με πιθανότητα τουλάχιστον*

$$\frac{1}{q_H} \cdot (\alpha - \frac{1}{2^\lambda}),$$

όπου λ είναι η παράμετρος ασφαλείας και q_H είναι αριθμός επερωτήσεων που γίνονται στο τυχαίο μαντείο H.

Απόδειξη. Έστω $\mathcal{A}$ να είναι ένας αντίπαλος που βρίσκει μια πλαστογραφημένη υπογραφή με πιθανότηταα. Θα κατασκευάσουμε έναν αλγόριθμο $\mathcal{B}$ που λύνει το πρόβλημα RSA.

Έστω πως δίνεται στον $\mathcal{B}$ η είσοδος $\langle n, e, y\rangle$, όπου τα n και e δίνονται από τον αλγόριθμο γέννεσης κλειδιού του RSA Gen και το y διαλέγεται τυχαία από το $\mathbb{Z}_n^*$. Ο στόχος του $\mathcal{B}$ είναι να βρει ένα $z \in \mathbb{Z}_n^*$ τέτοιο ώστε $z = y^{1/e} \bmod n$. Για να το πετύχει αυτό, ο $\mathcal{B}$ διαμορφώνει το κλειδί επαλήθευσης (n, e) και το δίνει στον $\mathcal{A}$. Ο $\mathcal{A}$ θα κάνει ερωτήσεις στο τυχαίο μαντείο καθώς επίσης και στο μαντείο υπογραφής. Και στις δύο περιπτώσεις ο $\mathcal{B}$ θα πρέπει να απαντήσει. Υποθέτουμε πως ο $\mathcal{B}$ ξέρει το q_H. Αυτό δεν είναι πρόβλημα φού ο $\mathcal{A}$ φράσσεται από πολυωνυμικό χρόνο εκτέλεσης και το q_H είναι σίγουρα μικρότερο από τον αριθμό των βημάτων εκτέλεσης του $\mathcal{A}$. Η εικόνα 2 παρουσιάζει πως λειτουργεί ο $\mathcal{B}$ έχοντας πρόσβαση στον $\mathcal{A}$.



Σχήμα 2: Ο αντίπαλος $\mathcal{B}$ πρέπει να εξομοιώσει τα H και Sign για να χρησιμοποιήσει το $\mathcal{A}$.

Πρώτα υποθέτουμε πως ο $\mathcal{A}$ δεν χρησιμοποιεί τον αλγόριθμο υπογραφής Sign, συνεπώς ο $\mathcal{A}$ παράγει το (M, σ) αφού κάνει q_H ερωτήματα στο τυχαίο μαντείο H. Ο $\mathcal{B}$ απαντάει αυτά τα ερωτήματα εξομοιώνοντας το H όπως φαίνεται στην Εικόνα 3. Εξ υποθέσεως, το σ είναι μια έγκυρη υπογραφή για το M με πιθανότητα α. Υποθέτουμε πως είναι έγκυρη, συνεπώς ισχύει πως $\sigma = H(M)^d \bmod n$. Αν $H(M) = y$, τότε $\sigma = H(M)^d = y^d \bmod n$ και το σ είναι μια e-οστή ρίζα του y (αφού $d \equiv e^{-1} \bmod \varphi(n)$).

Παρατηρείστε πως το παραπάνω είναι εξαιρετικά απίθανο, αφού η πιθανότητα πως $H(M) = y$ είναι πολυ μικρή. Αυτό ισχύει επειδή δεν υπάρχει σχέση μεταξύ της εξομοίωσης του τυχαίου μοντέλου από τον $\mathcal{B}$ και την τιμή y. Για να πάρουμε αυτό το αποτέλεσμα με μια λογική τυχαιότητα, ο $\mathcal{B}$ αποκλίνει από την Εικόνα 3 όταν απαντά τα ερωτήματα στο τυχαίο μαντείο. Ο $\mathcal{B}$ διαλέγει έναν τυχαίο αριθμό j στο $\{1, \ldots, q_H\}$ και δοκιμάζει να απαντήσει το j-οστό ερώτημα στο τυχαίο μαντείο με y: $H(M) = y$. Συγκεκριμένα το τυχαίο μαντείο τροποποιείται παραμετροποιώντας το με τα j, y και λειτουργεί ως εξής:

Κράτα έναν μετρητή για τα ερωτήματα.
- Δεδομένου ενός $M \notin History$: αν είναι το j-οστό ερώτημα, θέσε $t = y$, αλλιώς διάλεξε $t \xleftarrow{r} \mathbb{Z}_n^*$. Εισήγαγε το (M, t) στο $History$. Επέστρεψε t.
- Δεδομένου ενός M τέτοιου ώστε $(M, t) \in History$ για κάποιο t, επέστρεψε t.

Σχήμα 3: Μια τροποποιημένη εξομοίωση του τυχαίου μοντέλου που χρησιμοποιείται από τον αλγόριθμο $\mathcal{B}$ για να "βάλει" μια πρόκληση y στις απαντήσεις του μαντείου.

Στη συνέχεια θα συμβολίζουμε το πλαστογραφημένο μήνυμα εξόδου του αντίπαλου με M, και τα ερωτήματα στο μαντείο υπογραφών $M_1, \ldots, M_{q_S}$. Όπως συζητήθηκε πάνω θα θεωρήσουμε αρχικά πως $q_S = 0$, i.e., δεν γίνονται ερωτήσεις στο μαντείο υπογραφών.

Θεωρείστε το γεγονός E, πως $m \in History$ και το γεγονός $\neg E$ ως το συμπληρωματικό του E. Επιπλέον έστω S να είναι το γεγονός ότι ο αντίπαλος $\mathcal{A}$ επιτυχώς παράγει μια πλαστογραφημένη υπογραφή (δηλαδή ο αλγόριθμος επαλήθευσης με είσοδο M, σ επιστρέφει 1). Βασιζόμενοι στο θεώρημα, γνωρίζουμε πως $\mathsf{Prob}[S] = \alpha$. Από την άλλη παρατηρείστε ότι $\mathsf{Prob}[S|\neg E] \leq 1/\varphi(n) \leq 2^{-\lambda}$. Σε αυτή την περίπτωση αφού βρισκόμαστε στην χώρο υποσυνθήκης του $\neg E$ ο αντίπαλος δεν έχει ρωτήσει M στο H και συνεπώς η τιμή $H(M)$ δεν είναι απροσδιόριστη μέχρι και την εμπλοκή του αλγόριθμου επαλήθευσης. Αφού ο αντίπαλος έχει ήδη παράξει το σ, η πιθανότητα να ισχύει πως $H(M)^e = \sigma$ in $\mathbb{Z}_n^*$ είναι $1/\varphi(n) \leq 2^{-\lambda}$.

Τώρα στον χώρο πιθανοτήτων υπό συνθήκη του E, υπάρχει μια πιθανότητα $1/q_H$ πως το τυχαίο μαντείο θα απαντήσει σωστά το ερώτημα στο οποίο θα ερωτηθεί το . Θα ονομάζουμε αυτό το γεγονός G. Αν το G συμβεί, συνεπάγεται ότι $H(M) = y$, δηλαδή το y θα είχε εισαχθεί στη σωστή θέση. Σε τέτοια περίπτωση ο $\mathcal{B}$ θα έβρισκε επιτυχώς την e-οστή ρίζα του y. Θα ονομάζουμε αυτό το γεγονός V. Στη συνέχεια δίνουμε ένα κάτω φράγμα για την πιθανότητα του V.

Πρώτων έχουμε ότι $\mathsf{Prob}[S|\neg E] \leq 2^{-\lambda}$, γιαυτό

$$\mathsf{Prob}[S \wedge \neg E] = \mathsf{Prob}[S \mid \neg E] \cdot \mathsf{Prob}[\neg E] \leq 2^{-\lambda}.$$

Βασιζόμενοι σε αυτό παίρνουμε το κάτω φράγμα

$$\mathsf{Prob}[S \wedge E] \geq \alpha - 2^{-\lambda}.$$

Στη συνέχεια διαχωρίζουμε την πιθανότητα σύμφωνα με το E και υπολογίζουμε την πιθανότητα του V ως εξής:

$$\mathsf{Prob}[V] = \mathsf{Prob}[V|E] \cdot \mathsf{Prob}[E] + \mathsf{Prob}[V \wedge \neg E] \geq \mathsf{Prob}[S \wedge G|E] \cdot \mathsf{Prob}[E].$$

Λόγω της ανεξαρτησίας των γεγονότων S, G στον χώρο πιθανοτήτων υπό συνθήκη του E, έχουμε πως

$$\mathsf{Prob}[V] \geq \mathsf{Prob}[S|E] \cdot \mathsf{Prob}[G|E] \cdot \mathsf{Prob}[E] = \mathsf{Prob}[S \wedge E] \cdot \mathsf{Prob}[G|E] = \frac{\alpha - 2^{-\lambda}}{q_H}.$$

Αυτό ολοκληρώνει το θεώρημα μας για την περίπτωση $q_S = 0$. Στη συνέχεια θεωρούμε την γενική περίπτωση όπου το q_S είναι πολυωνυμικό στο λ.

Επιπρόσθετα στα ερωτήματα τυχαίου μαντείου, ο $\mathcal{A}$ ρωτάει τον $\mathcal{B}$ να υπογράψει το μήνυμα M_i'. Ο $\mathcal{B}$ θα πρέπει να απαντήσει με έναν τρόπο έτσι ώστε να είναι συνεπής με τα ερωτήματα στο τυχαίο μαντείο: Αν ο $\mathcal{B}$ επιστρέψει σ_i, θα ισχύει ότι $\sigma_i = H(M_i)^d \bmod n$ και έτσι $\sigma_i^e = H(M_i) \bmod n$. Αυτό συνεπάγεται πως το (M_i, σ_i^e) είναι στο $History$. Θα το επιτύχουμε αυτό τροποποιώντας ξανά την εξομοίωση του H από τον $\mathcal{B}$ όπως φαίνεται στην Εικόνα **??**.

Κράτα έναν μετρητή για τα ερωτήματα.
- Δεδομένου ενός $M \notin History$: Αν είναι το j-οστό ερώτημα, θέσε $t = y$, $\rho = \diamond$, διαφορετικά διάλεξε $\rho \xleftarrow{r} \mathbb{Z}_n^*$ και θέσε $t = \rho^e \bmod n$.
  Εισήγαγε το (M, t, ρ) στο $History$. Επέστρεψε t.
- Δεδομένου ενός M τέτοιου ώστε $(M, t, \rho) \in History$ για κάποιο t, επέστρεψε t.

Σχήμα 4: Μια δεύτερη τροποποίηση της εξομοίωσης του τυχαίου μαντείου από τον $\mathcal{B}$ για να βάλει το y στις απαντήσεις του μαντείου διατηρώντας το συνεπές σύμφωνα με την αλγόριθμο επαλήθευσης της ύψωσης στην e-οστή δύναμη.

Τώρα όταν θα ερωτηθεί να υπογράψει το M_i, ο $\mathcal{B}$ μπορεί πρώτα να ρωτήσει το τυχαίο μαντείο του για το M_i και μετά να συμβουλευτεί τις εγγραφές του $History$ για το (M_i, t_i, ρ_i). Εκτός από την περίπτωση $\rho_i = \diamond$ μπορεί να απαντήσει την ερώτηση με ρ_i. Παρατηρείστε πως η εξομοίωση είναι τέλεια όσο $\rho_i \neq \diamond$,

αφού $\rho_i^e = t_i \bmod n$, δηλαδή το ρ_i είναι η e-οστή ρίζα του $t_i = H(M_i)$ in $\mathbb{Z}_n^*$. Για τον σκοπό μας όμως δεν μας ενδιαφέρει η περίπτωση που $\rho_i = \diamond$ αφού σημαίνει πως ο $\mathcal{B}$ μάντεψε λάθος για την θέση του M (εξαιτίας την προϋπόθεσης για μια επιτυχής πλαστογράφηση πως ο $\mathcal{A}$ προσπαθεί να πλαστογραφήσει ένα μήνυμα που δεν ρώτησε το μαντείο υπογραφών) και συνεπώς η εξομοίωση δεν θα είναι επιτυχής.

Τελειώνουμε την απόδειξη εξασφαλίζοντας πως ο αντίπαλος $\mathcal{A}$ δεν μπορεί να καταλάβει κάποια διαφορά στις απαντήσεις του τυχαίου μαντείου όπως ορίστηκε στην Εικόνα **??**. Όντως παρατηρούμε πως οι τιμές που επιστρέφει ο αντίπαλος είναι της μορφής $\rho^e \bmod n$, σε αντίθεση με τιμές t επιλεγμένες ομοιόμορφα από το $\mathbb{Z}_n^*$. Αυτό όμως δεν θέτει κάποιο πρόβλημα αφού η συνάρτηση RSA είναι αμφιμονοσήμαντη στο $\mathbb{Z}_n^*$ και συνεπώς , $\rho^e \bmod n$ είναι μια τυχαία μεταβλητή που κατανέμεται ομοιόμορφα στο $\mathbb{Z}_n^*$ υπό την υπόθεση πως το ρ είναι ομοιόμορφα κατανεμημένο. ■

Notes by S. Pehlivanoglu, J. Todd, & H.S. Zhou