Εισαγωγή στη Θεωρία Αριθμών και στην Κρυπτογραφία 23 Ιανουαρίου 2012

Lecture 19

Ομιλητής: Άρης Παγουρτζής *Σημειώσεις: Μάρκος-Σπυρίδων Επιτρόπου*

1 Ψηφιακές Υπογραφές Επιπρόσθετης Λειτουργικότητας

1.1 Τυφλές Υπογραφές

Στόχος είναι να δημιουργηθεί η υπογραφή πάνω σε $m^* = f(m)$, που είναι το m "τυφλωμένο", έτσι ώστε να μπορούμε από $sig(m^*)$ να υπολογίσουμε $sig(m)$, δηλαδή $\exists f'$ τέτοιο ώστε $f'(sig(m^*)) = sig(m)$.

Σχήμα Chaum

- Α διαθέτει δημόσιο RSA κλειδί: (n, e_b)
- Β διαθέτει ιδιωτικό RSA κλειδί: (p, q, d_b)
- Α: $k \xleftarrow{R} \{0, \ldots, n-1\}, gcd(k, n) = 1$
- Α: $m^* = m \cdot k^{e_b} \mod n$
- $A \xrightarrow{m^*} B$
- Β: $s^* = sig(m^*) = (m^*)^{d_b} \mod n \ (= m^{d_b} \cdot k \mod n)$
- $A \xleftarrow{s^*} B$
- Α: $s = s^* \cdot k^{-1} \mod n$

Ο Bob υπέγραψε το m χωρίς ποτέ στη διαδικασία να μάθει το ίδιο το m, αλλά το m^*.

1.2 Αδιαμφισβήτητες Υπογραφές

Οι αδιαμφισβήτητες υπογραφές είναι ψηφιακές υπογραφές που για να επαληθευτούν χρειάζονται και την συνεργασία εκείνου που υπέγραψε. Ωστόσο, υπάρχει περίπτωση η υπογραφή να είναι πλαστή. Σε αυτήν την περίπτωση αυτός που κανονικά υπογράφει θα πρέπει να έχει το δικαίωμα να αποδείξει την μη γνησιότητα της υπογραφής. Έτσι λοιπόν ένα σχήμα αδιαμφισβήτητης υπογραφής αποτελείται από τα παρακάτω μέρη:

- Αλγόριθμος Υπογραφής
- Πρωτόκολλο Επαλήθευσης: άν η υπογραφή είναι πλαστή, το πρωτόκολλο αποτυγχάνει με μεγάλη πιθανότητα.
- Πρωτόκολλο Αποκύρηξης: άν η υπογραφή είναι πλαστή, το πρωτόκολλο επιτυγχάνει με μεγάλη πιθανότητα, ενώ αν δεν είναι πλαστή, αποτυγχάνει με μεγάλη πιθανότητα.

Σχήμα Chaum - Van Andwerpen (DLP-based)

- Α διαθέτει ιδιωτικό κλειδί: a

- Β διαθέτει κλειδί: (p, α, β), όπου $\beta = \alpha^a \mod p$
- Υπογραφή:
  - Α: $s = sig(m) = m^a \mod p$
  - $A \xrightarrow{(m,s)} B$
- Επαλήθευση:
  - Β: $c = s^{e_1}\beta^{e2} \mod p$, όπου $e_1, e_2 \xleftarrow{R}$
  - $A \xleftarrow{c} B$
  - Α: $d = c^{a^{-1} \mod q} \mod p$
  - $A \xrightarrow{d} B$
  - Β: $Ver(m, d) = \begin{cases} True & \text{if } d = m^{e_1}\alpha^{e_2} \mod p \\ False & \text{otherwise} \end{cases}$

Θεώρημα 1 *Άν $s \not\equiv m^a \mod p$ τότε ο Β θα αποδεχθεί την s ώς έγκυρη υπογραφή για το m με πιθανότητα $\frac{1}{q}$. (Uncoditional Security)*

Proof: Έστω ότι ο Oscar θέλει να πλαστογραφήσει την υπογραφή της Α. Τότε ο Β θα χρειαστεί να επαληθεύσει την υπογραφή ζητώντας την συνεργασία του Ο. Σύμφωνα με το πρωτόκολλο επαλήθευσης:

- $O \xrightarrow{(m,s)} B$
- $O \xleftarrow{c} B$
- $O \xrightarrow{d} B$

Ο Ο θα προσπαθήσει να βρεί d τέτοιο ώστε $d \equiv m^{e_1}\alpha^{e_2} \mod p$ χωρίς να γνωρίζει τα e_1, e_2. Ωστόσο ξέρει $c \equiv s^{e_1}\beta^{e_2} \mod p$. Έτσι λοιπόν θα επιχειρήσει να υπολογίσει τα e_1, e_2.

Θα προσπαθήσουμε να βρούμε την λύση ενός γραμμικού συστήματος, θεωρώντας ότι $m = \alpha^k, s = \alpha^\lambda, c = \alpha^i, d = a^j$.

$$(1) : \alpha^i \equiv \alpha^{\lambda e_1 + a e_2} \mod p$$
$$\xLeftrightarrow{ord(a)=q} i \equiv \lambda e_1 + a e_2 \mod q$$
$$(2) : \alpha^j \equiv \alpha^{k e_1 + e_2} \mod p$$
$$\xLeftrightarrow{ord(a)=q} j \equiv k e_1 + e_2 \mod q$$

Το σύστημα έχει μοναδική λύση θεωρώντας δύο εκ των k, λ, i, j γνωστές και για κάθε ζευγάρι e_1, e_2. Επομένως το σύστημα μπορεί να προσωμοιώσει την ψηφιακή υπογραφή. Αν κοιτάξουμε την εξίσωση (1) παρατηρούμε ότι για κάποιο στιγμιότυπο του κρυπτογραφικού συστήματος υπάρχουν q ζευγάρια (e_1, e_2) που την ικανοποιούν. Επομένως έχουμε 1/q πιθανότητα να διαλέξουμε το σωστό ζευγάρι. □

2 Συναρτήσεις Κατακερματισμού (Hash Functions)

2.1 Ορισμός

Έστω h μια συνάρτηση κατακερματισμού. Η συνάρτηση κατακερματισμού είναι μια δημόσια γνωστή συνάρτηση που χρησιμοποιείται για την μείωση του μήκους ενός μηνύματος. Αυτό μπορεί να γίνει για παράδειγμα στις ψηφιακές υπογραφές. Αν το μήνυμα είναι μεγάλο θα θέλαμε να μειώσουμε το μήκος του με κάποιο τρόπο ώστε η υπογραφή να είναι μικρή και συγχρόνως να παραμένει ασφαλής.

$$h : \Sigma^m \to \Sigma^k, m > k$$

Hash Functions για Ψηφιακή Υπογραφή

- Υπογραφή: $m \to h(m) \to sig(h(m))$
- Επαλήθευση: $m \to h(m)$, $ver(h(m), s)) =?$

Προφανώς, αφού μειώσαμε το πεδίο τιμών η h δεν είναι "1-1". Ιδανικά θα θέλαμε το αποτέλεσμα της h να κατανέμεται ομοιόμορφα στο πεδίο τιμών. Επίσης οι συγκρούσεις $h(m) = h(m')$ είναι ανεπιθύμητες γιατί προκύπτει η ίδια υπογραφή.

2.2 Επιθυμητές Ιδιότητες

1. Αντίσταση Πρώτου Ορίσματος (one-way): Δοσμένου y είναι "δύσκολο" να βρεθεί $h^{-1}(y)$, δηλαδή x τέτοιο ώστε $h(x) = y$.
2. Αντίσταση Δεύτερου Ορίσματος (weakly collision free): Δοσμένου x είναι "δύσκολο" να βρεθεί x' τέτοιο ώστε $h(x) = h(x')$.
3. Δυσκολία Εύρεσης Συγκρούσεων (strongly collision free): Είναι "δύσκολο" να βρεθούν $x, x' : h(x) = h(x')$.

Ορισμός 2 $(1), (2) \Rightarrow$ *One-way Hash Function*

Ορισμός 3 $(3) \Rightarrow$ *Collision-free Hash Function*

Πρόταση 4 $(3) \Rightarrow (1), (2)$