Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών

Σημειώσεις Διαλέξεων

Στοιχεία Θεωρίας Αριθμών

&

Εφαρμογές στην Κρυπτογραφία

Επιμέλεια σημειώσεων:
Δημητρέλλος Παναγιώτης

Διδάσκοντες:
Στάθης Ζάχος
Άρης Παγουρτζής

21 Δεκεμβρίου 2012

1 Fail-Stop Υπογραφές

1.1 van Heyst-Pederson sign scheme

'Εστω δύο πρώτοι αριθμοί p, q τέτοιοι ώστε $p = 2q + 1$.
Θεωρούμε ότι υπάρχει μια τρίτη έμπιστη αρχή,*(TTP)* η οποία επιλέγει $\alpha_0 \in \mathbb{Z}_q^*$ που είναι απολύτως κρυφό.
'Ετσι η έμπιστη αρχή στέλνει στο παίκτη A(υπογράφων) τα εξής:

- $\alpha \in \mathbb{Z}_q^*$,όπου το α είναι ένας γεννήτορας της ομάδας.
- Τον αριθμό $\beta = \alpha^{\alpha_0} \underline{\text{mod}} p$
- Τους πρώτους αριθμούς p, q

'Ετσι ο A επιλέγει τη τετράδα $S_A = (a_1, a_2, b_1, b_2) \in \mathbb{Z}_q$,το οποίο είναι το μυστικό κλειδί του A (secret key).'Επειτα υπολογίζει τα:

$$c_1 = \alpha^{a_1} \cdot \beta^{a_2} \underline{\text{mod}} p$$
$$c_2 = \alpha^{b_1} \cdot \beta^{b_2} \underline{\text{mod}} p$$

'Ετσι το σύνολο $(c_1, c_2, \alpha, \beta, p, q)$ είναι το δημόσιο κλειδί του παίκτη A ,και έτσι το σύστημα "στήθηκε".

1.2 Υπογραφές

Η υπογραφή του παίκτη A έχει ως εξής:

$$s = sig_{SA}(m) = (s_1, s_2), \text{όπου}$$
$$s_1 = (a_1 + m \cdot b_1) \underline{\text{mod}} q$$
$$s_2 = (a_2 + m \cdot b_2) \underline{\text{mod}} q$$

1.3 Επαλήθευση

Η συνθήκη επαλήθευσης της υπογραφής είναι:

$$ver_{pA}(m, (s_1, s_2)) = True \iff c_1 \cdot c_2^m \equiv \alpha^{s_1} \cdot \beta^{s_2} (\text{mod} p)$$

το οποίο προκύπτει σχετικά εύκολα μετά από απλές πράξεις.

1.4 Βασικές ιδιότητες

1. Τονίζεται πως η πιθανότητα εύρεσης από τον B ενός $m' \neq m$ τέτοιου ώστε:

$$sig_{SA}(m') = sig_{SA}(m)$$

είναι αμελητέα,όπως και επίσης η εύρεση ενός επιπλέον SA' τέτοιου ώστε:

$$sig_{SA'}(m') = sig_{SA}(m)$$

2. Αν ο παίκτης B βάσει των (m, s) βρει (m', s') τέτοια ώστε $ver_{pA}(m', s') = True$ τότε ο A μπορεί να αποδείξει τη πλαστογράφηση(π.χ. στην έμπιστη αρχή).

Ισχύει ότι πλήθος τετράδων (a_1, a_2, b_1, b_2) δίνουν τα ίδια c_1, c_2.Αυτό είναι ευνο'ι'κό για τον A καθώς:

$$c_1 \equiv \alpha^{a_1+\alpha_0 a_2} (\text{mod} p)\ c_2 \equiv \alpha^{b_1+\alpha_0 b_2} (\text{mod} p)$$

και για να βρούμε άλλα c_1, c_2 έχουμε ότι:
$a_1 + \alpha_0 a_2 \equiv a_1' + \alpha_0 a_2' (\text{mod} q) \Rightarrow a_1' \equiv a_1 + \alpha_0(a_2 - a_2') (\text{mod} q)$
'Αρα για κάθε a_2' παίρνουμε ένα a_1' το οποίο είναι αποδεκτό,άρα έχουμε q δεκτά ζεύγη,και ομοίως εργαζόμαστε για τα b_1, b_2.
Λήμμα 1:Υπάρχουν $q \cdot q = q^2$ τετράδες (a_1, a_2, b_1, b_2) στο $\mathbb{Z}_q^4$ που δίνουν τα ίδια c_1, c_2 (public key).
'Αρα ο "επιτιθέμενος" έχει πιθανότητα $\frac{1}{q^2}$ να βρει το σωστό ιδιωτικό κλειδί.
Λήμμα 2: q από τις q^2 "ισοδύναμες" τετράδες δίνουν την ίδια υπογραφή με την έγκυρη,άρα για τυχαία (και ίσως ασυνάρτητα) (m', s') ο B δύναται να "κάνει" τον A να υπογράψει (ενώ αυτό δεν έγινε) τα (m', s') με πιθανότητα $\frac{1}{q}$, η οποία δεν είναι αμελητέα,και προκύπτει από τη διερεύνηση συστήματος με ορίζουσα det$= 0$ το οποίο έχει q λύσεις τάξης (rank) $= 3$ και διάστασης 1.

1.5 Απόδειξη της πλαστογράφησης

'Εστω ότι ο B υπολογίζει κάποια (m', s') τέτοια ώστε:

$$ver_{pA}(m', s') = True \Rightarrow c_1 \cdot c_2 \equiv \alpha^{s_1'} \cdot \beta^{s_2'} (\text{mod} p) \textbf{ (I)}$$

Ο παίκτης A υπολογίζει την έγκυρη υπογραφή του για το m':
$s_1 = a_1 + m'b_1 \underline{\text{mod}} q$
$s_2 = a_2 + m'b_2 \underline{\text{mod}} q$
και βάσει των λημμάτων έχουμε ότι: $Pr[s = s'] \leq \frac{1}{q}$
, και έστω πως είναι διαφορετικές.Τότε ισχύει:
$c_1 \cdot c_2^{m'} \equiv \alpha^{s_1} \cdot \beta^{s_2} (\text{mod} p)$ **(II)**
και από τις σχέσεις **(I),(II)**$\Rightarrow \alpha^{(s_1' - s_1)} \equiv \beta^{(s_2 - s_2')} (\text{mod} p) \Rightarrow$
$\Rightarrow s_1' - s_1 \equiv \alpha_0 \cdot (s_2 - s_2') (\text{mod} q) \Rightarrow \alpha_0 \equiv (s_2 - s_2')^{-1} \cdot (s_1' - s_1) (\text{mod} q)$

Βιβλιογραφία

Zac12 : Σημειώσεις Ζάχου, ΕΜΠ, 2012.

Sti06 : D. Stinson: Cryptography: Theory and Practice, 3rd edition, CRC Press, 2005.