# Key (pre)distribution schemes & DES

Κρυπτογραφία και Πολυπλοκότητα (ΣΕΜΦΕ, ΜΠΛΑ)
Υπολογιστική Θεωρία Αριθμών και Κρυπτογραφία (ΣΗΜΜΥ)

Σημειώσεις Παρασκευής, 18 Ιανουαρίου 2013 (v2)

Μια έμπιστη αρχή $T$ θέλει να μοιράσει πληροφορίες σε $n$ παίκτες, ώστε κάθε ζεύγος $(P_i, P_j)$ να έχει ή να μπορεί να υπολογίσει ένα μοναδικό κοινό κλειδί $K_{ij}$ (πχ, για χρήση σε συμμετρική κρυπτογράφηση). Χωρίς μια έμπιστη αρχή, θα έπρεπε να σταλούν συνολικά $n(n-1)$ μηνύματα.

## 1 Bloom's key predistribution scheme

Με το σχήμα αυτό

- Επιτυγχάνεται μείωση του πλήθους των μηνυμάτων από την $T$ στους $P_i$ με εγγύηση $k$-ασφάλειας (λιγότεροι από $k$ παίκτες δεν μπορούν να "σπάσουν" το σύστημα).
- Η διαδικασία απαιτεί αποστολή $n \cdot k$ μηνυμάτων συνολικά.

### Περιγραφή του σχήματος

Setup του συστήματος

i. Η αρχή $T$ επιλέγει μυστικό συμμετρικό πίνακα $D_{k\times k}$, με στοιχεία τυχαία επιλεγμένα από το $\mathbb{Z}_p$, $p$ πρώτος.

ii. Δημιουργούνται (βλ. παρακάτω) και δημοσιεύονται τα δημόσια κλειδιά όλων των παικτών. Είναι διανύσματα $k$ θέσεων, $I_1, I_2, \ldots I_n \in \mathbb{Z}_p^k$.

iii. Υπολογίζεται και στέλνεται σε κάθε παίκτη $i$ το ιδιωτικό του κλειδί, $s_i = D \cdot I_i$.

Υπολογισμός των κοινών κλειδιών

iv. Κάθε παίκτης υπολογίζει τα συμμετρικά κλειδιά που θα έχει με τους υπόλοιπους παίκτες ως εξής:

$$K_{ij} = s_i^\top \cdot I_j$$

(και αντίστοιχα ο παίκτης $j$ υπολογίζει το κλειδί $_{ji}$)

Πράγματι $K_{ij} = (D \cdot I_i)^\top I_j$ και αφού το $K_{ij}$ είναι $1 \times 1$ πίνακας, έχουμε $K_{ij} = K_{ij}^\top \Rightarrow K_{ij} = I_j^\top D \cdot I_i = (I_j \cdot D)^\top I_i = (D \cdot I_j) I_i = K_{ji}$.

Παραγωγή δημοσίων κλειδιών

Για κάθε παίκτη $i \in \{1, \ldots, n\}$,

$$I_i = (D_{k\times k} \cdot G_{k\times k})e_i$$

$e_i$ είναι το διάνυσμα που έχει παντού 0 εκτός από την $i$-οστή θέση όπου είναι 1. Δηλαδή, σε κάθε παίτκη $i$, το δημόσιο κλειδί του είναι η στήλη $i$ του πίνακα $D \cdot G$. Ο $G$ είναι ένας $(k, n)$ MDS (Maximum Distance Seperator) linear code generator. Δηλαδή, για κάθε λέξη $m = (m_1, \ldots, m_k)$ με $m_i \in \mathbb{Z}_p$, το $m \cdot G$ δίνει την αντίστοιχη κωδική λέξη του $m$. Επιπλέον, ο κώδικας που παράγει ο πίνακας $G$ έχει απόσταση Hamming $d = n - k + 1$, που είναι η μέγιστη απόσταση που μπορεί να έχει ένας γραμμικός $[n, k, d]$ κώδικας.

### Ασφάλεια του σχήματος

Για τον πίνακα $G$ ισχύει $rank(G) = k$. Με την δημοσιοποίηση του ιδιωτικού κλειδιού $s_i$ του παίκτη $i$, γνωστοποιούνται $k$ ισοτιμίες για τον υπολογισμό του πίνακα $D$. Το πλήθος των αγνώστων όμως είναι $k^2$. Επομένως, για το "σπάσιμο" του συστήματος απαιτείται συνεργασία $k$ παικτών.

## 2 $(t, w)$ threshold scheme

Σκοπός είναι να μοιραστεί από μια έμπιστη αρχή $T$ ένα μυστικό σε $w$ παίκτες, μ' έναν τρόπο τέτοιο που λιγότεροι από $t$ παίκτες δεν θα μπορούν να ανακαλύψουν το μυστικό. Ένα απλό και διαδεδομένο σχήμα είναι αυτό του Shamir.

### Shamir's key distribution scheme

1. Η αρχή $T$ επιλέγει τυχαία συντελεστές $a_i \in_R \mathbb{Z}_p^*$, με $p$ πρώτο, για $i \in \{1, \ldots, t-1\}$ και επιλέγει επίσης $a_0 = k$ (μυστική πληροφορία). Έτσι δημιουργεί το πολυώνυμο

$$a(x) = \sum_{i=0}^{t-1} a_i x^i = k + \sum_{i=1}^{t-1} a_i x^i$$

2. Για κάθε παίκτη $j$, η αρχή επιλέγει $x_j \in \mathbb{Z}_p^*$, με $x_i \neq x_j$ για $i \neq j$, και του στέλνει το $y_j = a(x_j)$.

Μοιράζεται δηλαδή σε κάθε παίκτη ένα μέρος του συνόλου τιμών του πολυωνύμου πάνω στο $\mathbb{Z}_p$, εκτός από την τιμή $y_0$.

#### Ασφάλεια του σχήματος Shamir

Με παρεμβολή Lagrange έχουμε

$$a(x) = \sum_{i=1}^{t-1} y_i \left( \prod_{\substack{1\leq j\leq i \\ i\neq j}} \frac{x - x_j}{x_i - x_j} \right)$$

Επομένως,

$$k = a(0) = \sum_{i=1}^{t-1} y_i \left( \prod_{\substack{1\leq j\leq i \\ i\neq j}} \frac{x_j}{x_j - x_i} \right)$$

Το πρόβλημα μπορεί να εκφραστεί ως ένα σύστημα ισοτιμιών, όπως παρακάτω:

$$\begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{t-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{t-1} & x_{t-1}^2 & \cdots & x_{t-1}^{t-1} \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix} \begin{bmatrix} k \\ \vdots \\ \\ 0 \end{bmatrix} = \begin{bmatrix} y_1 \\ \vdots \\ y_{t-1} \\ y_0 \end{bmatrix}$$

Ο αριστερός πίνακας είναι ο πίνακας Vandermonde του συστήματος ισοτιμιών. Το σύστημα έχει την ιδιότητα ότι όποια τιμή κι αν υποθέσουμε για το $y_0$, θα υπάρχει πάντα λύση ως προς τον άγνωστο $k$. Έτσι, το σχήμα είναι unconditionally secure. Επιπλέον ιδιότητες του σχήματος:

- Είναι εύκολα επεκτάσιμο, ώστε να "χωρέσει" επιπλέον παίκτες.
- Δίνει τη δυνατότητα "βάρους" στους παίκτες (ανάλογα με το πλήθος των $y_i$ που θα τους στείλει η αρχή).
- $|y_i| = |k|$, το μήκος του "μεριδίου" κάθε παίκτη είναι ίσο με το μήκος του μυστικού κλειδιού. Τέτοια σχήματα ονομάζονται ideal schemes.
- Αν χρησιμοποιείται ένα $(w, w)$-threshold scheme, τότε $y_1, \ldots, y_{w-1} \in_R \mathbb{Z}_p$ και $y_w = k - \sum_{i=0}^{w-1} y_i$

# DES

## Δίκτυα Feistel

Ορίζονται βάσει συνάρτησης $F_k : \Sigma^l \to \Sigma^r$, όπου $k$ το κλειδί και $\Sigma = \{0, 1\}$ η αλφάβητος. Στο DES είναι $l = r = 32$ και $|k| = 48$.

Το plaintext $x$ χωρίζεται σε δύο ίσου μήκους blocks $L_0$ (το αριστερό) και $R_0$ (το δεξί). Με "$\|$" συμβολίζεται η πράξη της παράθεσης, δηλαδή $x = L_0 \| R_0$.

Σε κάθε γύρο $i$ χρησιμοποιείται το κλειδί $k_i$ και υπολογίζεται ένα string ως εξής:

$$L_i = R_{i-1}$$
$$R_i = F_{k_i}(R_{i-1}) \oplus L_{i-1}$$

Το DES "τρέχει" 16 τέτοιους γύρους. Εκφράζοντας τις παραπάνω σχέσεις έτσι, ώστε να φανεί το "χτήσιμο" του προηγούμενου γύρου από τον επόμενό του, λαμβάνουμε την διαδικασία αποκρυπτογράφησης:

$$R_{i-1} = L_i$$
$$L_{i-1} = R_i \oplus F_{k_i}(R_{i-1}) = R_i \oplus F_{k_i}(L_i)$$

Έτσι, η αποκρυπτογράφηση είναι σε μεγάλο βαθμό ίδια με την κρυπτογράφηση. Η διαφορά βρίσκεται στη σειρά με την οποία χρησιμοποιούνται τα κλειδιά $k_i$.