Εισαγωγή στη Θεωρία Αριθμών και στην Κρυπτογραφία 13 Ιανουαρίου 2012

Lecture 16

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

1 Παράδοξο των Γενεθλίων

Έστω ότι έχουμε ένα σύνολο n στοιχείων. Διαλέγουμε k τυχαίους αριθμούς από το σύνολο προσπαθώντας να βρούμε κάποια σύγκρουση μέσα στο σύνολο. Ο συνολικός αριθμος των ενδεχομένων που υπάρχουν είναι n^k, αφού κάθε τυχαίος αριθμός είναι οποιοσδήποτε από ένα σύνολο n στοιχείων. Τα ενδεχόμενα να μην βρεθεί καμία σύγκρουση είναι $n\cdot(n-1)\cdots(n-k+1) = \binom{n}{k}k!$.

$$\Pr[\text{no collision}] = \frac{\binom{n}{k}k!}{n^k} = \prod_{i=1}^{k-1}(1-\frac{1}{n}) \leq \prod_{i=1}^{k-1} e^{-\frac{i}{n}} = e^{-\sum_{i=1}^{k-1}\frac{i}{n}} = e^{-\frac{k(k-1)}{2n}}.$$

Θέλουμε να βρούμε τον αριθμό των στοιχείων k που χρειάζεται ώστε η πιθανότητα να βρεθεί μια σύγκρουση να ξεπεράσει το 1/2. Έτσι λοιπόν:

$$\Pr[\text{no collision}] \leq \frac{1}{2} \iff$$

$$e^{-\frac{k(k-1)}{2n}} \leq \frac{1}{2} \iff$$

$$k \geq 1.17\sqrt{n}$$

Αποδεικνύεται ότι άν $k \ll n$, το φράγμα είναι αυστηρό.

2 Άσκηση (RSA για Ψηφιακή Υπογραφή)

Χρησιμοποιείται το σύστημα κρυπτογράφησης RSA για ψηφιακή υπογραφή. Θυμίζουμε ότι ο χρήστης διαλέγει πρώτους αριθμούς p, q και υπολογίζει το γινόμενο $n = p \cdot q$. Το ιδιωτικό και το δημόσιο κλειδί είναι αντίστοιχα $sk = d$ και $pk = e$, τέτοια ώστε $e \cdot d \equiv 1 \bmod \phi(n)$.

- Υπογραφή: $\sigma = sign(m) = m^d \mod n$
- Επαλήθευση: $ver(m, \sigma) = (\sigma^e \equiv m \bmod n)$

Έστω τωρα ότι χρησιμοποιείται ένας διαφορετικός αλγόριθμος κρυπτογράφησης $\widetilde{sign}$ που αποτελείται από τα παρακάτω βήματα υπολογισμού:

1. $a_1 = m^d \mod p$
2. $a_2 = m^d \mod q$
3. $\left.\begin{matrix} x \equiv a_1 \mod p \\ x \equiv a_2 \mod q \end{matrix}\right\} \xrightarrow{CRT} \sigma = x$

Θεωρούμε ότι $\widetilde{sign}$ υπολογίζει λάθος το βήμα 2 και επιστρέφει $\widetilde{\sigma}$.

$$\left.\begin{matrix} x \equiv a_1 & \mod p \\ x \equiv \widetilde{a_2} & \mod q \end{matrix}\right\} \xrightarrow{CRT} \widetilde{\sigma} = x$$

Δείξτε ότι έχοντας $(m, \widetilde{\sigma}, pk)$ μπορούμε να παραγοντοποιήσουμε το n.
Solution: Γνωρίζουμε οτι:

1. $\widetilde{\sigma} = m^d \mod p \Rightarrow \widetilde{\sigma}^e \equiv m^{de} \equiv m \mod p$
2. $\widetilde{\sigma} \not\equiv m^d \mod q \Rightarrow \widetilde{\sigma}^e \not\equiv m^{de} \equiv m \mod q$

$(1) \Rightarrow \widetilde{\sigma}^e - m = \lambda \cdot p$.
Αν θεωρήσουμε ότι $gcd(\lambda, q) = 1$, τότε μπορούμε να υπολογίσουμε $p = gcd(\lambda \cdot p, p \cdot q)$. Επομένως αρκεί να αποδείξουμε οτι $gcd(\lambda, q) = 1$, που αποδεικνύεται από (2). Αυτό σημαίνει ότι μπορώ να παραγοντοποιήσω υπολογίζοντας $gcd(\widetilde{\sigma}^e - m, n)$ σε πολυωνυμικό χρόνο ως προς τα ψηφία. Ωστόσο $\widetilde{\sigma}^e - m$ υπάρχει περίπτωση να έχει μεγάλο αριθμό ψηφίων. Για να μειώσουμε τον αριθμό των ψηφίων θα υπολογίσουμε $gcd(\widetilde{\sigma}^e - m, n) = gcd(\widetilde{\sigma}^e - m \mod n, n)$. □

3 Άσκηση (DLP)

- G "ομάδα" τάξης 2^m (2^m στοιχεία)
- $G =< g >$ (g γεννήτορας της G)

Δείξτε ότι έχοντας στοιχείο $x \in G$, μπορώ να υπολογίσω λ τέτοιο ώστε $g^\lambda = x$.
Solution: λ μπορεί να γραφεί ώς εξής:

$$\lambda = b_{m-1} \cdot 2^{m-1} + \ldots + b_1 \cdot 2 + b_0$$

Επομένως:

$$\lambda \cdot 2^{m-1} = b_{m-1} \cdot 2^{2(m-1)} + \ldots + b_1 \cdot 2^m + b_0 \cdot 2^{m-1} \Leftarrow$$

$$g^{\lambda \cdot 2^{m-1}} = g^{b_{m-1} \cdot 2^{2^{(m-1)}}} \cdots g^{b_1 \cdot 2^m} \cdot g^{b_0 \cdot 2^{m-1}} = g^{b_0 \cdot 2^{m-1}}, \text{ αφού } g^{2^m} = 1_G$$

- Άν $b_0 = 0 \Rightarrow g^{b_0 \cdot 2^{m-1}} = 1_G$
- Άν $b_0 = 1 \Rightarrow g^{b_0 \cdot 2^{m-1}} \neq 1_G$

Έτσι λοιπόν υψώνοντας το x στο 2^{m-1} μας δίνει το b_0 συγκρίνοντας το αποτέλεσμα με την πολλαπλασιαστική μονάδα της ομάδας. Εφαρμόζουμε επαγωγικά και βρίσκουμε τελικά το λ. Επομένως:

- $x^{2^{m-1}} \xrightarrow{\text{μας δίνει}} b_0$
- $(\frac{x}{g})^{2^{m-2}} \xrightarrow{\text{μας δίνει}} b_1$

  ⋮
- $(\frac{x}{g^{m-1}}) \xrightarrow{\text{μας δίνει}} b_{m-1}$

□