Α31 ΚΡΥΠΤΟΓΡΑΦΙΑ
Φυλλάδιο ασκήσεων #1

Θεόδουλος Γαρεφαλάκης

13 Φεβρουαρίου 2022

1. (γενίκευση του one-time-pad)

   - Έστω πεπεραμένη ομάδα $(G, \cdot)$ (υπάρχει αποτελεσματικός αλγόριθμος για την πράξη της G) και $\mathcal{K} = \mathcal{M} = \mathcal{C} = G$. Ορίζουμε το κρυπτοσύστημα $\mathcal{E} = (E, D)$, ως εξής:

     $$E(k, m) = k \cdot m \text{ και } D(k, c) = k^{-1} \cdot c.$$

     Αποδείξτε ότι το κρυπτοσύστημα $\mathcal{E}$ έχει τέλεια ασφάλεια.

   - Όπως δείξατε στο προηγούμενο ερώτημα, το κρυπτοσύστημα $\mathcal{E} = (E, D)$ πάνω από την ομάδα $(\mathbb{Z}_p^*, \cdot)$ όπου p είναι πρώτος έχει τέλεια ασφάλεια. Θεωρήστε τώρα το κρυπτοσύστημα $\mathcal{E}' = (E', D')$ με $\mathcal{K} = \{1, \ldots, p-1\}, \mathcal{M} = \{0, 1, \ldots, p-1\}, \mathcal{C} = \{0, 1, \ldots, p-1\}$ και

     $$E'(k, m) = k \cdot m \mod p, \;\; D'(k, m) = k^{-1} \cdot c \mod p.$$

     Αποδείξτε ότι το $\mathcal{E}'$ δεν είναι σημασιολογικά ασφαλές.
     Υπόδειξη: κατασκευάστε ένα αποτελεσματικό αντίπαλο, ο οποίος έχει μη τετριμμένο πλεονέκτημα στο παιχνίδι του ορισμού.

2. (Boneh-Shoup, 2.3) Έστω $\mathcal{E} = (E, D)$ ένα κρυπτοσύστημα πάνω από τα $(\mathcal{K}, \mathcal{M}, \mathcal{C})$, με $\mathcal{K} = \mathcal{M}$, το οποίο έχει τέλεια ασφάλεια. Ορίζουμε το κρυπτοσύστημα $\mathcal{E}'$ πάνω από τα $(\mathcal{K}^2, \mathcal{M}, \mathcal{C}^2)$ ως εξής: $E'((k_1, k_2), m) = (E(k_1, k_2), E(k_2, m))$. Δείξτε ότι το $\mathcal{E}'$ έχει τέλεια ασφάλεια.

3. (Boneh-Shoup, 2.10) Έστω $\mathcal{E} = (E, D)$ ένα σημασιολογικά ασφαλές κρυπτοσύστημα πάνω από τα $(\mathcal{K}, \mathcal{M}, \mathcal{C})$, με $\mathcal{M} = \mathcal{C} = \{0, 1\}^L$. Εξετάστε ποιοί από τους παρακάτω αλγορίθμους κρυπτογράφησης είναι σημασιολογικά ασφαλείς:

   (α′) $E_1(k, m) = 0 \| E(k, m)$

   (β′) $E_2(k, m) = E(k, m) \| \text{parity}(m)$

   (γ′) $E_3(k, m) = \text{reverse}(E(k, m))$

   (δ′) $E_4(k, m) = E(k, \text{reverse}(m))$

4. (Boneh-Shoup, 2.13) θεωρήστε τα παρακάτω πειράματα:

   - Πείραμα 0: Ο παίκτης με πιθανότητα $1/2$ απαντά ΚΟΡΩΝΑ και με πιθανότητα $1/2$ απαντά ΓΡΑΜΜΑΤΑ.
   - Πείραμα 1: Ο παίκτης απαντά ΓΡΑΜΜΑΤΑ.

   Στόχος του αντιπάλου, $\mathcal{A}$, είναι να διακρίνει τα δύο πειράματα: απαντά 0 ή 1. Για $b = 0, 1$, ορίζουμε W_b το ενδεχόμενο ο αντίπαλος να απαντήσει 1 στο πείραμα b. Σκοπός του αντιπάλου είναι να μεγιστοποιήσει το πλεονέκτημα του $\text{Adv}[\mathcal{A}] = |\Pr(W_0) - \Pr(W_1)|$.

   (α′) Υπολογίστε το πλεονέκτημα για καθένα από τους παρακάτω αντιπάλους:

      i. $\mathcal{A}_1$: απαντά πάντα 1.
      ii. $\mathcal{A}_2$: αναντά 1 με πιθανότητα $1/2$ και 0 με πιθανότητα $1/2$.
      iii. $\mathcal{A}_3$: απαντά 1 αν λάβει ΚΟΡΩΝΑ και 0 διαφορετικά.
      iv. $\mathcal{A}_4$: απαντά 0 αν λάβει ΚΟΡΩΝΑ και 1 διαφορετικά.

   (β′) Βρείτε το μέγιστο δυνατό πλεονέκτημα που μπορεί να έχει ένας αντίπαλος στο παιχνίδι αυτό.