Α31 ΚΡΥΠΤΟΓΡΑΦΙΑ
Φυλλάδιο ασκήσεων #2

Θεόδουλος Γαρεφαλάκης

4 Μαρτίου 2022

1. Έστω $G : \{0,1\}^\ell \to \{0,1\}^n$ μία ασφαλής PRG.

   (α΄) Δείξτε ότι η $G' : \{0,1\}^{2\ell} \to \{0,1\}^n$ με $G'(s1, s2) = G(s_1) \oplus G(s_2)$ είναι ασφαλής.

   (β΄) Δείξτε ότι η $G'' : \{0,1\}^\ell \to \{0,1\}^{2n}$ με $G''(s) = (G(s), G(s))$ δεν είναι ασφαλής.

2. (α΄) Έστω μία PRG, $G : \mathcal{S} \to \mathcal{R}$, όπου $|\mathcal{R}| \geq 2|\mathcal{S}|$, για την οποία υπάρχει αποτελεσματικός αλγόριθμος ο οποίος αποφασίζει εάν ένα δοσμένο $r \in \mathcal{R}$ ανήκει στην εικόνα της G. Αποδείξτε ότι η G δεν είναι ασφαλής.

   (β΄) Έστω η γραμμική απεικόνιση $L : \mathbb{F}_2^n \to \mathbb{F}_2^m$, με $m > n$. Δείξτε ότι η L δεν είναι ασφαλής PRG.

   (γ΄) Κατασκευάστε ένα αντίπαλο στο παιχνίδι του ορισμού ασφαλείας της PRG, $G : \mathcal{S} \to \mathcal{R}$, ο οποίος κάνει $O(|\mathcal{S}|)$ βήματα και έχει μη αμελητέο πλεονέκτημα. Συμπεράνετε ότι για να είναι ασφαλής η G, πρέπει το $|\mathcal{S}|$ να είναι υπερ-πολυωνυμικό.

3. Έστω $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ μία ασφαλής PRF.

   (α΄) Δείξτε ότι η $F_1(k, x) = (F(k, x), F(k, x \oplus 1^n))$ δεν είναι ασφαλής.

   (β΄) Δείξτε ότι η $F_2(k, (x, y)) = (F(k, x), F(k, y))$ δεν είναι ασφαλής.

   (γ΄) Δείξτε ότι η $F_3(k, x) = F(k, x) \oplus x$ είναι ασφαλής.

4. Η Αλίκη επικοινωνεί με το Βασίλη χρησιμοποιώντας ένα σύστημα κρυπτογράφησης τύπου Feistel. Ειδικότερα, κάθε block έχει μήκος 128 bits, ο αλγόριθμος έχει 3 γύρους και το κοινό, κρυφό κλειδί της Αλίκης και του Βασίλη είναι το (k_1, k_2, k_3), όπου $k_i \in \mathbb{F}_2^{64}$, $i = 1, 2, 3$ είναι το κλειδί του i γύρου. Το αρχικό (καθαρό) μήνυμα χωρίζεται σε δύο μέρη των 64 bits έκαστο (το αριστερό και το δεξιό) L_0 και R_0. Στη συνέχεια ο αλγόριθμος κρυπτογράφησης υπολογίζει τα

   $$\begin{aligned} L_i &= R_{i-1} \\ R_i &= L_{i-1} + F(k_i, R_{i-1}), \end{aligned}$$

   για $i = 1, 2, 3$. Η απεικόνιση $F : \mathbb{F}_2^{64} \times \mathbb{F}_2^{64} \longrightarrow \mathbb{F}_2^{64}$ είναι η $F(k, R) = R + k$. (Στους παραπάνω ορισμούς, η πράξη «+» είναι πρόσθεση στο $\mathbb{F}_2^{64}$.) Το κρυπτογραφημένο μήνυμα είναι το (L_3, R_3). Η Αλίκη, για να σας επιδείξει τον αλγόριθμο της, δέχεται να κρυπτογραφήσει ένα τυχαίο μήνυμα, ας πούμε το (L'_0, R'_0). Δείξτε πώς μπορείτε, με δεδομένο το (L_3, R_3) και το ζεύγάρι καθαρού μηνύματος (L'_0, R'_0) και κρυπτογραφήματος (L'_3, R'_3), να υπολογίσετε το καθαρό μήνυμα (L_0, R_0).

   Αφού καταφέρατε να παραβιάσετε την ασφάλεια του συστήματος τους, η Αλίκη και ο Βασίλης αποφασίζουν να το βελτιώσουν με τον εξής τρόπο: επιλέγουν μία απεικόνιση $\sigma : \mathbb{F}_2^{64} \longrightarrow \mathbb{F}_2^{64}$ και τροποποιούν την απεικόνιση F, να είναι $F(k, R) = \sigma(R) + k$. Η απεικόνιση σ είναι γνωστή σε όλους (δεν είναι μέρος του κλειδιού). Για ευκολία, επιλέγουν τη σ να είναι $\mathbb{F}_2$-γραμμική απεικόνιση. Είναι το κρυπτοσύστημα τους τώρα ασφαλέστερο; Θα ήταν ασφαλέστερο εάν είχε περισσότερους γύρους;

   Υπόδειξη: εκφράστε τα L_0, R_0 συναρτήσει των L_3, R_3 των κλειδιών k_1, k_2, k_3 και της σ. Υπολογίστε τις διαφορές $L_0 - L'_0$ και $R_0 - R'_0$. Τι παρατηρείτε;