מבוא לקריפטוגרפיה - תרגיל בית 2

נא להגיש עד ה 2.02.2017 דרך המודל. ההגשה היא ביחידים. התייעצות מותרת, אך חובה לרשום את הפתרונות לבד.

נושאים: מערכות הצפנה עם בטיחות חישובית ,יצרנים פסוודו אקראיים וחיות אחרות

סימונים: בהינתן מחרוזת x, נסמן ב $x[i,j]$ את תת המחרוזת

$x_i, x_{i+1}, \ldots, x_j$

כולל.

1. (יצרנים פסוודו אקראיים) יהי $G : \{0,1\}^* \to \{0,1\}^*$ יצרן פסוודו אקראי (PRG) עם פרמטר הרחבה (פולינום) $\ell(n) > n$. הוכח או הפרך.

   א. הפונקציה $G' : \{0,1\}^* \to \{0,1\}^*$ המוגדרת באופן הבא:

$$G'(x) : 1.\ \text{Run } G(x),\ \text{obtaining } y = y_1, y_2, \ldots, y_{\ell(|x|)}.$$

$$2.\ \text{Output } y_1, \ldots, y_{n+1}.$$

   . היא גם PRG.

   ב. הפונקציה $G_2 : \{0,1\}^* \to \{0,1\}^*$ המוגדרת ע"י
   $G_2(x_1, \ldots, x_n) = x_1, \ldots, x_n, x_1 \oplus x_2 \ldots \oplus x_n$

   היא PRG.

   ג. הפונקציה $G_3 : \{0,1\}^* \to \{0,1\}^*$ השווה ל G על כל קלט, פרט לקלטים מהצורה $0^n = 000\ldots000$. כל קלט מהצורה $x = 0^n$ מתמפה ל $G_3(x) = 0^{\ell(n)}$.

   היא PRG.

   ד. הפונקציה $G_4 : \{0,1\}^* \to \{0,1\}^*$ המוגדרת כ
   $G_4(x) = G(0^{\lceil |x|/2 \rceil}, x[\lceil |x|/2 \rceil + 1, n])$

   היא PRG.

2. (טיעוני היברידים) בשאלה זו נראה את בטיחות הבניה שלנו של PRG ללא הגבלת G' אורך מ PRG רגיל. נזכיר כי הבניה הוגדרה כך. בהנתן PRG G עם $\ell(n) = n + 1$

$$
\begin{aligned}
G'(x, 1^l): \ & 1.\text{Let } x_0 = x \\
& 2.\text{For } i := 1 \text{ to } l \\
& \quad 2.1 \qquad\qquad \text{Let } x_i = G(x_{i-1})[1, n] \\
& \quad 2.2 \qquad\qquad \text{Let } b_i = G(x_{i-1})[n+1] \\
& 3.\text{Output } b_1, b_2, \ldots, b_l
\end{aligned}
$$

א. נשתמש בטיעון היברידים לצורך ההוכחה. הגדירו התפלגויות היברידיות $D_0, D_1, \ldots, D_l$ כך ש $D_0 = G'(U_n, l), D_l = U_l$. סדרת ההתפלגויות שתבחרו צריכה להיות כזו שתהיה שימושית לצורך ההוכחה בסעיף הבא.

ב. נניח בשלילה כי הבניה אינה מייצרת PRG ללא הגבלת אורך. אזי קיים פולינום $l(n)$ כך ש $G'_{l(n)}$ אינו PRG. מותר לכם להניח ללא הוכחה שמבחין זה הוא דטרמיניסטי. השתמשו בהתפלגויות שבניתם בסעיף הקודם, ובמבחין עבור $G'_{l(n)}$ עם יתרון לא זניח על מנת לבנות מבחין פולינומי עם יתרון לא זניח עבור G (וזו סתירה). שימו לב שהמבחין המתקבל הוא בעצם מבחין יעיל עם עצה חסומה פולינומית.

ג. בונוס: אחד הגורמים לכך שהמבחין שמתקבל בהוכחה בשלילה בסעיף הקודם זקוק לעצה הוא הצורך לנחש אינדקס i מתאים של זוג התפלגויות עוקבות מבין אלה בסעיף 1. הראו כיצד אפשר למצוא את i ביעילות ללא צורך בניחוש (במסגרת המבחין).

3. (מערכת הצפנה מפונקציות פסוודו אקראיות) השלימו את הוכחת הנכונות של הבניה של מערכת הצפנה עם בטיחות CPA המבוססת משפחת פונקציות פסוודו-אקראיות עם אורך קבוע שראינו בהרצאה (זו שבה $E(k, m; r) = (r, F(k, r) \oplus m)$.