תרגול מס' 2 במבוא לקריפטוגרפיה מודרנית

24 אוקטובר

אי־הבחנה בין התפלגויות (Indistinguishability) ופסאודו־אקראיות (Pseudo-Randomness)

- מוטיבציה: רוצים לייצר "הרבה אקראיות ממעט אקראיות" (ציור).
- דוג': ראיתם שאפשר להצפין בעזרת OTP, אבל עם מפתח באורך ההודעות (בתרגיל: הכרחי אם רוצים בטיחות מושלמת). האם אפשר לחקות את OTP אם מסתפקים בבטיחות נגד יריבים חסומים?
- באיזה מובן "לחקות"? היינו רוצים מערכת הצפנה 'OTP שמשתמת במפתח קצר, אבל כך שלא ניתן להבחין האם הצפנה מסויימת נוצרה ע"י OTP או ע"י 'OTP.

הגדרה 0.1 נאמר ששתי התפלגויות D_0, D_1 על $\{0,1\}^n$ הנן ϵ־לא־ניתנות־להבחנה (ϵ-indistinguishable) עבור מבחין A בעל פלט של ביט אחד $b \in \{0,1\}$ אם

$$|\Pr_{d_0 \leftarrow D_0}[A(d_0) = 1] - \Pr_{d_1 \leftarrow D_1}[A(d_1) = 1]| \leq \epsilon$$

(לכל $n \in N$ מספיק גדול).

1. אם D_0, D_1 ϵ־לא־ניתנות־להבחנה לכל A לא חסום, אז נאמר שהן לא ניתנות להבחנה סטטיסטית (מושלמת אם $\epsilon = 0$). נסמן $D_0 \approx_{s,\epsilon} D_1$.
2. אם D_0, D_1 ϵ־לא־ניתנות־להבחנה לכל A פולינומי, אז נאמר שהן לא ניתנות להבחנה חישובית (בד"כ דורשים כי ϵ פונ' זניחה של n). נסמן $D_0 \approx_{c,\epsilon} D_1$.

טענה 0.2 D_0, D_1 $\epsilon-$לא ניתנות להבחנה סטטיסטית (חישובית בהתאמה) אמ"מ

$$\left| \Pr_{\substack{b \leftarrow \{0,1\} \\ d_b \leftarrow D_b}} [A(d_b) = b] - \frac{1}{2} \right| \leq \frac{\epsilon}{2}$$

לכל A לא חסום (פולינומי בהתאמה).

- פירוש: כל אסטרטגיית הבחנה אינה טובה מ"ניחוש אקראי".

הגדרה 0.3 Pseudo-Random Generator: פונ' $G : \{0,1\}^n \to \{0,1\}^{n+s}$ היא $\epsilon - \mathrm{PRG}$ אם:

$$G(U_n) \approx_{c,\epsilon} U_{\{n+s\}}$$

כלומר "הפלט של G אינו ניתן להבחנה חישוביות מפלט אקראי באמת". נקרא ל־s ה־Strech.

טענה 0.4 מבחין לא חסום תמיד יכול להבחין בפער של לפחות $1 - 2^{-s}$.

- האם קיימים PRGs ?

משפט 0.5 PRGs קיימים אמ"מ OWFs קיימות.

- כיוון קל: כל PRG הוא OWF בעצמו (טענה חזקה יותר).

דוג' ל־PRG מבעיית דיפי־הלמן

- תהי G חבורה ציקלית מסדר q (ראשוני) עם יוצר g.
- בעיית Diffie-Hellman ב־G:

1. <u>בעיית חיפוש (Computational־DH)</u>

   (א) קלט: g^x, g^y, עבור $(x, y) \leftarrow Z_q$.

   (ב) אתגר, מצא את g^{xy}.

2. <u>בעיית ההבחנה (Decisional־DH)</u>

(א) נגדיר שתי התפלגויות:

$$D_0 = \{g^x, g^y, g^{xy} : (x,y) \leftarrow Z_q \times Z_q\}$$

$$D_1 = \{g^x, g^y, g^z : (x,y,z) \leftarrow Z_q \times Z_q \times Z_q\}$$

(ב) קלט: $b \leftarrow \{0,1\}$ עבור $d_b \leftarrow D_b$

(ג) אתגר, נחש את b.

- <u>אבחנה</u>: מ־DDH נובע PRG:

$$PRG : Z_q \times Z_q \to G \times G \times G$$

כל איבר ב־Z_q או ב־ G ניתן לייצוג ע"י $\log q$ביטים ו־PRG מותח $2\log q$ ביטים ל־$3\log q$ביטים.

טענה 0.6 (מנוסחת באופן לא פורמלי) "DDH קשה" גורר "CDH קשה" גורר "DL" קשה.

הוכחה: נראה חלק מהטענה. נראה כי אם A מצליח באתגר ה־CDH בהסתברות ϵאז ניתן לבנות ממנו A' שמצליח באתגר ה־CDH בהסתברות $\frac{1}{2} + \frac{\epsilon - 1/q}{2}$. (מילה על רדוקציה)

בהנתן קלט g^x, g^y, g^w צריך לנחש האם $w = xy$ (נדגם מ־D_0) או נבחר באקראי באופן בלתי תלוי מ־Z_q (נדגם מ־D_1).

A' מריץ את A על g^x, g^y מקבל תוצאה $g^{w'}$ובודק האם $g^{w'} = g^w$. אם כן, הוא מסיק כי כנראה $w = ab$ומוציא 0. אחרת הוא מסיק כי כנראה wנדגם באקראי ומוציא 1.

ננתח את הס' ההצלחה שלו:

$$\Pr_{b \leftarrow \{0,1\}}[A'(d_b) = b] =$$

$$\Pr[b=0]\Pr[A'(g^x,g^y,g^{xy}) = 0 | b=0] + \Pr[b=1]\Pr[A'(g^x,g^y,g^z) = 1 | b=1] =$$

$$\frac{1}{2}\Pr[A'(g^x,g^y) = g^{xy}] + \frac{1}{2}\Pr[A'(g^x,g^y) \neq g^z] =$$

$$\frac{\epsilon}{2} + \frac{1 - 1/q}{2}$$

■

דוג' לחבורות בהן הבעיות נחשבות קשות

- דיברנו על בעיית הלוגריתם הדיסקרטי ב־ Z_p^*.
- גם CDH נחשבת קשה ב־ Z_p^*.
- האם DDH קשה ב־Z_p^*?נראה בהמשך שלא.
- במקום מסתכלים על תת חבורה מתאימה. למשל עבור $p = 2q + 1$ מסתכלים על תת חבורה מסדר q (זוהי חבורה השאריות הריבועיות, נתקבל בה בהמשך).