

מבוא לקריפטוגרפיה ואבטחת תוכנה

תרגיל 1

רן שחם - 203781000

5 באפריל 2017

הערה 0.1 לאורך התרגיל אני מסמן ב- U_n איבר מההתפלגות האחידה על $\{0, 1\}^n$. למשל:

$$\Pr[D(U_n) = 1] = \Pr_{s \leftarrow \{0, 1\}^n}[D(s) = 1]$$

שאלה 1

הערה 0.2 נשים לב שההתפלגות C על \mathcal{C} נקבעת על סמך ההתפלגות M על \mathcal{M} ו- K על \mathcal{K}

תהי Π מערכת הצפנה בטוחה מושלמת. אזי לכל התפלגות M על \mathcal{M} , לכל $m \in \mathcal{M}$ ולכל $c \in \mathcal{C}$ כך ש- $\Pr[C = c] > 0$ מתקיים:

$$\Pr[M = m|C = c] = \Pr[M = m]$$

מנוסחת בייס,

$$(*) : \Pr[M = m|C = c] \Pr[C = c] = \Pr[C = c|M = m] \Pr[M = m]$$

ולכן:

$$\Pr[M = m] \Pr[C = c] = \Pr[C = c|M = m] \Pr[M = m]$$

אם נניח ש- $\Pr[M = m] > 0$, נוכל לצמצם את $\Pr[M = m]$ ונקבל:

$$\Pr[C = c] = \Pr[C = c|M = m]$$

כנדרש.

בכיוון השני, נניח שלכל התפלגות M על \mathcal{M} , לכל $m \in \mathcal{M}$ כך ש- $\Pr[M = m] > 0$ ולכל $c \in \mathcal{C}$ מתקיים:

$$\Pr[C = c|M = m] = \Pr[C = c]$$

מהנ"ל ומ- $(*)$ מתקיים:

$$\Pr[M = m|C = c] \Pr[C = c] = \Pr[C = c] \Pr[M = m]$$

ולכן, אם $\Pr[C = c] > 0$ מתקיים $\Pr[M = m|C = c] = \Pr[M = m]$, כלומר Π היא מע' בטוחה מושלמת.

שאלה 2

בספר.

שאלה 3

תהי $\nu(n)$ פונ' זניחה ויהי p פולינום. נראה ש- $\nu(n) \cdot p(n)$ היא פונ' זניחה. יהי q פולינום כלשהו. נזכור כי מכפלת פולינומים היא פולינום, כלומר $p \cdot q$ פולינום. מכך ש- $\nu(n)$ זניחה, קיים N כך שלכל $n > N$ מתקיים:

$$\nu(n) < \frac{1}{p(n)q(n)}$$

אם כך, לכל $n > N$:

$$p(n)\nu(n) < p(n) \frac{1}{p(n)q(n)} = \frac{1}{q(n)}$$

כלומר לכל פולינום q קיים N כך שלכל $n > N$ מתקיים $p(n)\nu(n) < \frac{1}{q(n)}$, לכן לפי הגדרה $\nu(n)p(n)$ פונ' זניחה.

שאלה 4

סעיף א'

נניח ש- G_1, G_2 הם PRG כך ש- $G_1 = G_2$. אזי G המוגדר כבשאלה אינו PRG. יהי $n > \ell(n)$ פולינום כך ש- $|G_1(s)| = \ell(|s|)$. נראה מבחין (distinguisher) יעיל שמבדיל בין פלט של G לבין פלט אקראי בסיכוי לא זניח. נגדיר את $D(c)$ להחזיר 0 אם $|c|$ אי-זוגי. אחרת, אם $|c| = 2k$ אז D יחזיר 1 אם $c[0 \dots k-1] = c[k \dots 2k-1]$, כלומר אם k הביטים הראשונים ב- c זהים ל- k הביטים האחרונים בו. אם כך, לכל קלט s בעל n ביטים כך ש- $G_2(s) = G_1(s) || G_1(s)$ מתקיים $c = G(s) = G_1(s) || G_2(s) = G_1(s) || G_1(s)$ הביטים הראשונים ב- c זהים ל- $\ell(n)$ הביטים האחרונים, ולכן D על c יחזיר 1 (תמיד). לכן:

$$\left| \Pr_{s \leftarrow \{0,1\}^n} [D(G(s)) = 1] - \Pr_{r \leftarrow \{0,1\}^{2\ell(n)}} [D(r)] = 1 \right| = \left| 1 - (1/2)^{\ell(n)} \right| = 1 - (1/2)^{\ell(n)}$$

כי הסיכוי שהביט ה- i יהיה שווה לביט ה- $i + \ell(n)$ לכל $0 \leq i < \ell(n)$ הוא $1/2$, והביט ה- i ב"ת בביט ה- j לכל $0 \leq i < j < \ell(n)$ (מכיוון שההתפלגות בה נבחר r היא אחידה).

לכן, לפי הגדרה, G אינו PRG כי ברור שהפונקציה $1 - (1/2)^{\ell(n)}$ אינה זניחה (היא גדולה למשל מ- $1/n$ עבור אינסוף n).

סעיף ב'

יהי $n > \ell(n)$ כך ש- $|G_1(s)| = |G_2(s)| = \ell(n)$. נניח בשלילה שקיים מבחין יעיל D (PPT) ופולינום $p(n)$ כך ש-:

$$|\Pr[D(G(U_{2n})) = 1] - \Pr[D(U_{2\ell(n)}) = 1]| > \frac{2}{p(n)}$$

עבור אינסוף ערכי n . לכן, לאינסוף n :

$$\begin{aligned}
\frac{2}{p(n)} &< \left| \Pr_{s \leftarrow \{0,1\}^{2n}} [D(G(s)) = 1] - \Pr_{r \leftarrow \{0,1\}^{2\ell(n)}} [D(r) = 1] \right| \\
&= \left| \Pr_{s_1, s_2 \leftarrow \{0,1\}^n} [D(G(s_1||s_2)) = 1] - \Pr_{r_1, r_2 \leftarrow \{0,1\}^{\ell(n)}} [D(r_1||r_2) = 1] \right| \\
&\stackrel{1}{=} \left| \Pr_{s_1, s_2 \leftarrow \{0,1\}^n} [D(G_1(s_1)||G_2(s_2)) = 1] - \Pr_{r_1, r_2 \leftarrow \{0,1\}^{\ell(n)}} [D(r_1||r_2) = 1] \right| \\
&= \left| \Pr_{s_1 \leftarrow \{0,1\}^n} [D(G_1(s_1)||G_2(s_2)) = 1] - \Pr_{s_1 \leftarrow \{0,1\}^n, r_2 \leftarrow \{0,1\}^{\ell(n)}} [D(G_1(s_1)||r_2) = 1] \right. \\
&\quad \left. + \Pr_{s_1 \leftarrow \{0,1\}^n, r_2 \leftarrow \{0,1\}^{\ell(n)}} [D(G_1(s_1)||r_2) = 1] - \Pr_{r_1, r_2 \leftarrow \{0,1\}^{\ell(n)}} [D(r_1||r_2) = 1] \right| \\
&\stackrel{2}{\leq} \underbrace{\left| \Pr_{s_1, s_2 \leftarrow \{0,1\}^n} [D(G_1(s_1)||G_2(s_2)) = 1] - \Pr_{s_1 \leftarrow \{0,1\}^n, r_2 \leftarrow \{0,1\}^{\ell(n)}} [D(G_1(s_1)||r_2) = 1] \right|}_A \\
&\quad + \underbrace{\left| \Pr_{s_1 \leftarrow \{0,1\}^n, r_2 \leftarrow \{0,1\}^{\ell(n)}} [D(G_1(s_1)||r_2) = 1] - \Pr_{r_1, r_2 \leftarrow \{0,1\}^{\ell(n)}} [D(r_1||r_2) = 1] \right|}_B
\end{aligned}$$

כאשר:

1. לפי הגדרת G

2. אי שוויון המשולש

ולכן, מתקיים $A > \frac{2}{2p(n)} = \frac{1}{p(n)}$ או ש- $B > \frac{1}{p(n)}$ לאינסוף ערכי n .

נניח שהראשון מתקיים. נגדיר את D_2 להיות מבחין יעיל ל- G_2 באופן הבא: עבור קלט s , D_2 ידגום $s_1 \leftarrow \{0,1\}^{|s|}$ ויחזיר $D(G_1(s_1)||s)$. מכיוון ש- D מבחין יעיל גם D_2 יעיל. נשים לב שעבור אינסוף n מתקיים:

$$\begin{aligned}
&\left| \Pr_{s_2 \leftarrow \{0,1\}^n} [D_2(G_2(s_2)) = 1] - \Pr_{r_2 \leftarrow \{0,1\}^{\ell(n)}} [D_2(r_2) = 1] \right| \\
&= \left| \Pr_{s_1, s_2 \leftarrow \{0,1\}^n} [D(G_1(s_1)||G_2(s_2)) = 1] - \Pr_{s_1 \leftarrow \{0,1\}^n, r_2 \leftarrow \{0,1\}^{\ell(n)}} [D(G_1(s_1)||r_2) = 1] \right| \\
&> \frac{1}{p(n)}
\end{aligned}$$

מהנחה ש- $A > \frac{1}{p(n)}$, ובסתירה לכך ש- G_2 הוא PRG.

באופן דומה, אם $B > \frac{1}{p(n)}$ אז נבנה מבחין D_1 שעבור קלט s דוגם $s_2 \leftarrow \{0,1\}^{|s|}$ ומחזיר $D(s||G_2(s_2))$. מחישוב דומה מתקבל:

$$\left| \Pr_{s_1 \leftarrow \{0,1\}^n} [D_1(G_1(s_1)) = 1] - \Pr_{r_1 \leftarrow \{0,1\}^{\ell(n)}} [D_1(r_1) = 1] \right| > \frac{1}{p(n)}$$

עבור אינסוף n , בסתירה ל-PRG של G_1 .

לכן, לא קיים מבחין D כנ"ל ו- G הוא PRG כנדרש.

שאלה 5

למה 0.3 לכל פונ' זניחה $\nu : \mathbb{N} \rightarrow \mathbb{R}$ ולכל פולינום $p : \mathbb{N} \rightarrow \mathbb{R}_+$, הפונקציה המוגדרת על ידי $q(n) = \frac{1}{p(n)} + \nu(n)$ אינה זניחה

הוכחה: ν זניחה, לכן קיים $N \in \mathbb{N}$ כך שלכל $n > N$ מתקיים:

$$\begin{aligned} |\nu(n)| \leq \frac{1}{2p(n)} &\iff -\frac{1}{2p(n)} \leq \nu(n) \leq \frac{1}{2p(n)} \\ &\iff \frac{1}{2p(n)} \leq \nu(n) + \frac{1}{p(n)} \leq \frac{3}{2p(n)} \end{aligned}$$

ו- $2p(n)$ הוא פולינום, לכן לכל $n > N$ מתקיים ש- $\frac{1}{2p(n)} q(n) \geq q$ ולכן q אינה זניחה.

נגדיר את H כך:

$$H(s) = \begin{cases} G(s), & s \neq 0^n \\ 0^{2n}, & s = 0^n \end{cases}$$

ונטען ש- H הוא PRG. נניח בשלילה שלא, כלומר שקיים מבחין D כך ש-:

$$|\Pr[D(H(U_n)) = 1] - \Pr[D(U_{2n}) = 1]| > \frac{1}{p(n)}$$

עבור אינסוף n ופולינום $p(n)$ כלשהו. מכאן ש- $\frac{1}{p(n)} \Pr[D(U_{2n}) = 1] > \Pr[D(H(U_n)) = 1] - \Pr[D(U_{2n}) = 1]$ (*): עבור אינסוף n . לכן:

$$\begin{aligned} \Pr[D(H(U_n)) = 1] &= \Pr[D(H(U_n)) = 1 | U_n = 0^n] \Pr[U_n = 0^n] \\ &\quad + \Pr[D(H(U_n)) = 1 | U_n \neq 0^n] \Pr[U_n \neq 0^n] \\ &= \overbrace{\Pr[D(H(0^n)) = 1]}^q \cdot 2^{-n} + \Pr[D(G(U_n)) = 1] \cdot (1 - 2^{-n}) \\ &= q \cdot 2^{-n} + \Pr[D(G(U_n)) = 1] - \overbrace{\Pr[D(G(U_n)) = 1]}^r \cdot 2^{-n} \\ &= (q - r) 2^{-n} + \Pr[D(G(U_n)) = 1] \stackrel{(*)}{>} \Pr[D(U_{2n}) = 1] + \frac{1}{p(n)} \end{aligned}$$

נעביר אגפים ונקבל:

$$\begin{aligned} |\Pr[D(G(U_n)) = 1] - \Pr[D(U_{2n}) = 1]| &\geq \Pr[D(G(U_n)) = 1] - \Pr[D(U_{2n}) = 1] \\ &> (r - q) 2^{-n} + \frac{1}{p(n)} \end{aligned}$$

כאשר הא"ש הראשון נובע מתכונות הערך המוחלט והא"ש השני נובע מהחישוב לעיל.

נשים לב ש- $(r - q) 2^{-n} \pm 1$ חסומה ב- 2^{-n} זניחה ולכן לפי lemma 0.3 גם $(r - q) 2^{-n} + \frac{1}{p(n)}$ לא זניחה. מכאן ש- D מבחין בסיכוי לא זניח קלטים מ- G , בסתירה לכך ש- G PRG.

שאלה 6

נשים לב ש- G מקיים את תכונת ההרחבה (כלומר, מחזיר פלט עם יותר ביטים מאשר בקלט), כי גם אם הפלט של F הוא באורך ביט אחד, G מוגדר על ידי שרשור של $n + 1$ כאלה, עבור קלט באורך n ביטים. נניח שהפלט של F הוא באורך ביט אחד (לשם פשטות. שאר הניתוח לא משתנה מהותית עבור כל ערך אחר).

נניח בשלילה ש- D מבחין יעיל ל- G (כלומר G אינו PRG), כלומר מתקיים:

$$\left| \Pr_{s \leftarrow \{0,1\}^n} [D(G(s)) = 1] - \Pr_{r \leftarrow \{0,1\}^{n+1}} [D(r) = 1] \right| > \frac{1}{p(n)}$$

עבור פולינום p כלשהו, לאינסוף n . נבנה מבחין יעיל ל- F . בהינתן קלט 1^n וגישת אורקל לפונקציית \mathcal{O} , המבחין יחשב את:

$$x = \mathcal{O}(1) \parallel \mathcal{O}(2) \parallel \dots \parallel \mathcal{O}(n+1)$$

לאחר מכן, יחשב את $D(x)$ ויענה כמוהו. נשים לב:

1. $D^{\mathcal{O}(\cdot)}$ יעיל כי D יעיל וכי יש מספר לינארי ב- n של קריאות לאורקל

2. אם $\mathcal{O} \equiv F_s$ אז $x = G(s)$ לכל s , לפי הגדרה

3. אם $\mathcal{O} \equiv f$ כאשר $f \leftarrow \text{Func}_1$ (כאשר $f : \{0, 1\}^* \rightarrow \{0, 1\}$) אז x שקול לערך הנבחר מהתפלגות אחידה על מחרוזות באורך $n+1$ ביטים - כי כל ביט בו נבחר באקראי

לכן:

$$\left| \Pr_{s \leftarrow \{0,1\}^n} [D^{F_s(\cdot)}(1^n) = 1] - \Pr_{f \leftarrow \text{Func}_1} [D^{f(\cdot)}(1^n) = 1] \right| = 1$$

$$= \left| \Pr_{s \leftarrow \{0,1\}^n} [D(G(s)) = 1] - \Pr_{r \leftarrow \{0,1\}^{n+1}} [D(r) = 1] \right| > \frac{1}{p(n)}$$

עבור אינסוף n , לפי הנחת השלילה. זו סתירה לכך ש- F היא PRF, ולכן D כנ"ל לא קיים - כלומר G הוא PRG כרצוי.

שאלה 7

בשני הסעיפים נניח כמובן ש- F היא PRF כמתואר בשאלה.

סעיף 1

PRF לא P . מבחין יעיל D יפעל באופן הבא: עבור הקלט 1^n וגישת אורקל לפונ' \mathcal{O} , D יחשב את $x = \mathcal{O}(1^n)$. אם $x = 0^n$ יחזיר 1, אחרת יחזיר 0. ברור ש- D רץ בזמן פולינומי ב- n . נשים לב שאם $\mathcal{O} \equiv P_k$ אז $P_k(1^n) = F_k(1^n) \oplus F_k(1^n) = 0^n$ ולכן D יחזיר 1 בהסתברות 1 לכל $k \in \{0, 1\}^n$. אם $\mathcal{O} \equiv f$ כאשר $f \leftarrow \text{Func}_n$ אז $f(1^n) = 0^n$ יקרה בהסתברות 2^{-n} ולכן ההסתברות ש- D יחזיר 1 היא 2^{-n} . אם כך:

$$\left| \Pr_{k \leftarrow \{0,1\}^n} [D^{P_k(\cdot)}(1^n) = 1] - \Pr_{f \leftarrow \text{Func}_n} [D^{f(\cdot)}(1^n) = 1] \right|$$

$$= |1 - 2^{-n}| = 1 - 2^{-n} > \frac{1}{n}$$

עבור אינסוף n , לכן P אינה PRF.

סעיף 2

H אכן PRF. נניח בשלילה שלא. יהי B מבחין יעיל ל- H , כלומר קיים פולינום p כך ש:

$$\left| \Pr_{k \leftarrow \{0,1\}^n} [B^{H_k(\cdot)}(1^n) = 1] - \Pr_{f \leftarrow \text{Func}_n} [B^{f(\cdot)}(1^n) = 1] \right| > \frac{1}{p(n)}$$

עבור אינסוף ערכי n . נבנה מבחין יעיל D ל- F . בהינתן גישת אורקל ל- \mathcal{O} , D יריץ את B עם גישת אורקל ל- $\mathcal{O} \oplus 1^n$. כלומר, כאשר B יבקש את הפלט עבור הערך x , D יחשב את $y = \mathcal{O}(x) \oplus 1^n$ על ידי גישת האורקל שלו ויחזיר ל- B את y . D יחזיר פלט זהה לשל B . D יעיל כי B יעיל ולכן מבצע מס' פולינומיאלי של קריאות לאורקל, שכל אחת מהן מתבצעת בזמן פולינומיאלי (גישת אורקל ופעולת XOR). כמוכן, אם $\mathcal{O} \equiv F_k$ אז $y = F_k(x) \oplus 1^n = H_k(x)$ לכל $x, k \in \{0, 1\}^n$, כלומר B הרץ ב- D מקבל גישת אורקל ל- H_k . אם $\mathcal{O} \equiv f$ אז ה-XOR עם 1^n אינו משנה את ההסתברות לערך y מסויים על פני אחר, עבור x כלשהו, כלומר B מקבל גישת אורקל לפונ' שנבחרת בהתפלגות אחידה מ- Func_n . לכן:

$$\left| \Pr_{k \leftarrow \{0,1\}^n} [D^{F_k(\cdot)}(1^n) = 1] - \Pr_{f \leftarrow \text{Func}_n} [D^{f(\cdot)}(1^n) = 1] \right|$$

$$= \left| \Pr_{k \leftarrow \{0,1\}^n} [B^{H_k(\cdot)}(1^n) = 1] - \Pr_{f \leftarrow \text{Func}_n} [B^{f \oplus 1^n(\cdot)}(1^n) = 1] \right|$$

$$= \left| \Pr_{k \leftarrow \{0,1\}^n} [B^{H_k(\cdot)}(1^n) = 1] - \Pr_{f \leftarrow \text{Func}_n} [B^{f(\cdot)}(1^n) = 1] \right| > \frac{1}{p(n)}$$

לאינסוף n , לפי ההנחה - ובסתירה לכך ש- F היא PRF. לכן H היא PRF כנדרש.

שאלה 8

בשני הסעיפים נניח ש- F היא כבתיאור השאלה.

סעיף 1

H היא PRF. אחרת, יהיו B מבחין ל- H ו- p פולינום כך ש:

$$\left| \Pr_{k \leftarrow \{0,1\}^n} [B^{H_k(\cdot)}(1^n) = 1] - \Pr_{f \leftarrow \text{Func}_{n,2n}} [B^{f(\cdot)}(1^n) = 1] \right| > \frac{1}{p(n)}$$

לאינסוף n . נבנה מבחין D ל- F הפועל כך: בהינתן 1^n וגישת אורקל ל- \mathcal{O} , יריץ את B עם הפרמטר 1^n . לכל בקשה של B לגישת אורקל לערך $D, x \in \{0,1\}^n$ יחשב¹ את $F_{1^n}(x)$ ויחזיר ל- B את $\mathcal{O}(x) \oplus F_{1^n}(x)$. D יחזיר 1 אם B החזיר 1. D פועל בזמן פולינומיאלי בקלט כי B מבצע מס' פולינומיאלי ב- n של קריאות לאורקל, כאשר כל אחת מהן "מטופלת" בזמן פולינומיאלי - כי D מבצע חישוב של F עם מפתח וקלט ידועים ומבצע XOR (והרכבת פולינומים היא פולינום). נשים לב שלכל $n \in \mathbb{N}$, עבור $\mathcal{O} = F_k$ ועבור $k \in \{0,1\}^n$ מדמה את ריצת B עם אורקל H_k - לכן:

$$\Pr_{k \leftarrow \{0,1\}^n} [D^{F_k(\cdot)}(1^n) = 1] = \Pr_{k \leftarrow \{0,1\}^n} [B^{H_k(\cdot)}(1^n) = 1]$$

כמוכן אם $\mathcal{O} = f \leftarrow \text{Func}_{n,2n}$ עבור $f \leftarrow \text{Func}_{n,2n}$ אז הערך $f(x) \oplus F_{1^n}(x)$ הוא ערך המפולג באופן אחיד ב- $\{0,1\}^{2n}$ ובלתי תלוי ב- $f(x') \oplus F_{1^n}(x')$ עבור $x' \neq x \in \{0,1\}^n$. לכן:

$$\begin{aligned} & \left| \Pr_{k \leftarrow \{0,1\}^n} [D^{F_k(\cdot)}(1^n) = 1] - \Pr_{f \leftarrow \text{Func}_{n,2n}} [D^{f(\cdot)}(1^n) = 1] \right| \\ &= \left| \Pr_{k \leftarrow \{0,1\}^n} [B^{H_k(\cdot)}(1^n) = 1] - \Pr_{f \leftarrow \text{Func}_{n,2n}} [B^{f(\cdot)}(1^n) = 1] \right| > \frac{1}{p(n)} \end{aligned}$$

לאינסוף n בסתירה לכך ש- F פסאודו רנדומית.

סעיף 2

G אינו בהכרח PRG.

נגדיר פונ' F' באופן הבא:

$$F'_k(x) = \begin{cases} F_k(x), & k \neq 0^n \\ 0^{2n}, & k = 0^n \end{cases}$$

לכל $k, x \in \{0,1\}^n$. נטען ש- F' היא PRF. אחרת, נניח ש- B מבחין יעיל ל- F' המקיים:

$$\left| \Pr_{k \leftarrow \{0,1\}^n} [B^{F'_k(\cdot)}(1^n) = 1] - \Pr_{f \leftarrow \text{Func}_{n,2n}} [B^{f(\cdot)}(1^n) = 1] \right| > \frac{1}{p(n)}$$

עבור p פולינום ואינסוף ערכי $n \in \mathbb{N}$. לכל $n \in \mathbb{N}$ מתקיים:

$$\begin{aligned} \Pr_{k \leftarrow \{0,1\}^n} [B^{F'_k(\cdot)}(1^n) = 1] &= \Pr [B^{F'_k(\cdot)}(1^n) = 1 \mid k \neq 0^n] \Pr [k \neq 0^n] \\ &\quad + \Pr [B^{F'_k(\cdot)}(1^n) = 1 \mid k = 0^n] \Pr [k = 0^n] \\ &= \Pr [B^{F_k(\cdot)}(1^n) = 1] \cdot (1 - 2^{-n}) + q_n \cdot 2^{-n} \\ &= \Pr [B^{F_k(\cdot)}(1^n) = 1] + 2^{-n} \cdot (q_n - r_n) \end{aligned}$$

לכן, לאינסוף n :

$$\begin{aligned} \frac{1}{p(n)} &< \left| \Pr_{k \leftarrow \{0,1\}^n} [B^{F'_k(\cdot)}(1^n) = 1] - \Pr_{f \leftarrow \text{Func}_{n,2n}} [B^{f(\cdot)}(1^n) = 1] \right| \\ &= \left| \Pr [B^{F_k(\cdot)}(1^n) = 1] + 2^{-n} \cdot (q_n - r_n) - \Pr_{f \leftarrow \text{Func}_{n,2n}} [B^{f(\cdot)}(1^n) = 1] \right| \\ &\leq \left| \Pr [B^{F_k(\cdot)}(1^n) = 1] - \Pr_{f \leftarrow \text{Func}_{n,2n}} [B^{f(\cdot)}(1^n) = 1] \right| + |(q_n - r_n) \cdot 2^{-n}| \end{aligned}$$

¹אם אפשרי כי תיאור F הוא פומבי; אנחנו מניחים ש- F ניתנת לחישוב יעיל. כלומר, בהינתן קלט $k, x \in \{0,1\}^n$, אפשר לחשב את $F_k(x)$ בזמן פולינומיאלי ב- n , לכל $n \in \mathbb{N}$.

כאשר המעבר האחרון נובע מאי־שוויון המשולש. באופן דומה לבשאלה 5, $\left| \frac{1}{p(n)} - |(q_n - r_n) \cdot 2^{-n}| \right|$, אינה פונ' זניחה מ-lemma 0.3, וזו סתירה לכך ש- F היא PRF, כי בחישוב הנ"ל אפשר לראות ש- B מבחין יעיל עבורה. לכן F' היא PRF. נטען עתה ש- G המוגדר על ידי $G(s) = F'_{0^n}(s)$ אינו PRG. נבנה מבחין D ל- G : בהינתן קלט $s \in \{0,1\}^{2n}$, D יחזיר 1 אם $s = 0^{2n}$. נשים לב ש- D יחזיר 1 על $G(s)$ לכל $s \in \{0,1\}^n$, כלומר $\Pr[D(G(U_n)) = 1] = 1$. כמוכן עבור ערך $r \leftarrow \{0,1\}^{2n}$, D יחזיר 1 בהסתברות בה $r = 0^{2n}$ שהיא 2^{-2n} . לכן:

$$\begin{aligned} & \left| \Pr_{s \leftarrow \{0,1\}^n} [D(G(s)) = 1] - \Pr_{r \leftarrow \{0,1\}^{2n}} [D(r) = 1] \right| \\ &= \left| 1 - \Pr_{r \leftarrow \{0,1\}^{2n}} [r = 0^{2n}] \right| \\ &= |1 - 2^{-2n}| = 1 - 2^{-2n} > \frac{1}{n} \end{aligned}$$

עבור אינסוף n , כלומר G אינה PRG.

שאלה 9

סעיף 1

המערכת לא בטוחה (לא IND ובפרט לא CPA). נבנה יריב \mathcal{A} המזהה הצפנות בהסתברות 1. בהינתן הפרמטר $n \in \mathbb{N}$, היריב יפלוט שתי הודעות $m_0 = 0^n, m_1 = 1^n$ ויקבל הצפנה $c^* = (r^*, s^*)$ - כאשר r^* הוא n הביטים הראשונים ב- c^* ו- s^* הוא יתר המחרוזת. \mathcal{A} יחשב את $m^* = G(r^*) \oplus s^*$ ויחזיר:

$$b' = \begin{cases} 0, & m^* = 0^n \\ 1, & m^* = 1^n \end{cases}$$

נטען ש- $\Pr[\text{IND}_{\Pi, \mathcal{A}}(n) = 1] = 1$. יהי $b \in \{0,1\}$ כך ש- $c^* = \text{Enc}_k(m_b)$. G ידועה וניתנת לחישוב בזמן יעיל, r^* ידוע ולכן החישוב:

$$m^* = G(r^*) \oplus s^* = G(r^*) \oplus (G(r^*) \oplus m_b) = m_b$$

מתבצע באופן יעיל. מכאן $b' = b$ כנדרש.

סעיף 2

המערכת אינה CPA-בטוחה. נגדיר יריב \mathcal{A} הפועל באופן הבא: מבקש הצפנה להודעה $m \neq 0^n, 1^n$ כלשהי ומקבל צופן c . אח"כ יחשב את $x = c \oplus m$. לבסוף יפלוט $m_0 = 0^n, m_1 = 1^n$ ויקבל צופן c^* - אז \mathcal{A} יחזיר 1 אם $c^* \oplus x = 1^n$. נטען ש- $x = F_k(0^n)$ ונסיים - כי אז:

$$x \oplus c^* = F_k(0^n) \oplus (m_b \oplus F_k(0^n)) = m_b$$

אכן, $x = c \oplus m = (F_k(0^n) \oplus m) \oplus m = F_k(0^n)$. CPA. נניח בשלילה שלא, ויהיו F PRF, יריב \mathcal{A} ופולינום p כך שלאינסוף $n \in \mathbb{N}$ מתקיים:

$$\Pr[\text{IND}_{\Pi, \mathcal{A}}(n) = 1] > \frac{1}{2} + \frac{1}{p(n)}$$

נבנה מבחין D שבהינתן הקלט 1^n וגישת אורקל לפונקציית \mathcal{O} , מריץ את \mathcal{A} ומקבל זוג הודעות m_0, m_1 דוגם $b \leftarrow \{0,1\}$ ומחזיר ל- \mathcal{A} את $c^* = \mathcal{O}(0^n) \oplus m_b$. לבסוף D עונה 1 אם $b' = b$ כאשר b' הוא הפלט של \mathcal{A} . ראשית, קל לראות ש- D רץ בזמן פולינומיאלי כי \mathcal{A} הוא PPT לפי הנחה (וגישת אורקל ו-XOR מתבצעות באופן יעיל). נשים לב שכאשר $\mathcal{O} \equiv f$ עבור $f \leftarrow \text{Func}_n$ אז $f(0^n)$ שקול לערך המפולג אחיד מ- $\{0,1\}^n$, כלומר הסיכוי של \mathcal{A} לענות נכונה בניסוי IND הוא $\frac{1}{2}$. אם $\mathcal{O} \equiv F_k$ אז \mathcal{A} מקבל בדיוק את ההצפנות של המערכת, כלומר D מדמה את הניסוי בו \mathcal{A} מצליח לפי הנחה. לכן:

$$\begin{aligned} & \left| \Pr_{k \leftarrow \{0,1\}^n} [D^{F_k(\cdot)}(1^n) = 1] - \Pr_{f \leftarrow \text{Func}_n} [D^{f(\cdot)}(1^n) = 1] \right| \\ &= \left| \Pr[\text{IND}_{\Pi, \mathcal{A}}(n) = 1] - \frac{1}{2} \right| > \left| \frac{1}{2} + \frac{1}{p(n)} - \frac{1}{2} \right| = \frac{1}{p(n)} \end{aligned}$$

לאינסוף n , בסתירה לכך ש- F היא PRF. לכן המערכת בעלת הצפנות בלתי ניתנות להבחנה.

סעיף 3

המערכת בטוחה בפני CPA ולכן גם בעלת הצפנות בלתי ניתנות להבחנה.

ראינו בכיתה שהמערכת המחזירה $(r, F_k(r) \oplus m)$ עבור PRF F , $r, k \leftarrow \{0, 1\}^n$ והודעה m היא בטוחה בפני CPA. אם נראה שהפונקצייה H המוגדרת על ידי: $H_k(r) = r \oplus F_k(r)$ היא PRF נקבל שהמערכת המתוארת בסעיף היא בדיוק המתוארת בכיתה², ולכן בטוחה כפי שהוכחנו.

נניח בשלילה ש- H אינה PRF. יהי B מבחין ל- H ו- p פולינום כך ש:

$$\left| \Pr_{k \leftarrow \{0,1\}^n} [B^{H_k(\cdot)}(1^n) = 1] - \Pr_{f \leftarrow \text{Func}_n} [B^{f(\cdot)}(1^n) = 1] \right| > \frac{1}{p(n)}$$

נבנה מבחין D ל- F באופן הבא: בהינתן אורקל \mathcal{O} וקלט 1^n , יריץ את B . לכל בקשת אורקל של B לערך $r \in \{0, 1\}^n$, D יחזיר לו $\mathcal{O}(r) \oplus r$. לבסוף D יענה 1 אם B ענה 1.

נשים לב שאם $\mathcal{O} = F_k$ אז $\mathcal{O}(r) \oplus r = H_k(r)$, כלומר D מדמה את ריצת המבחין B עם אורקל H_k . כמוכן אם $\mathcal{O} = f$ כאשר $f \leftarrow \text{Func}_n$ אז הערך $f(r)$ שקול לערך המפולג אחיד ב- $\{0, 1\}^n$, וכך גם $f(r) \oplus r$. לכן:

$$\begin{aligned} & \left| \Pr_{k \leftarrow \{0,1\}^n} [D^{F_k(\cdot)}(1^n) = 1] - \Pr_{f \leftarrow \text{Func}_n} [D^{f(\cdot)}(1^n) = 1] \right| \\ &= \left| \Pr_{k \leftarrow \{0,1\}^n} [B^{H_k(\cdot)}(1^n) = 1] - \Pr_{f \leftarrow \text{Func}_n} [B^{f(\cdot)}(1^n) = 1] \right| > \frac{1}{p(n)} \end{aligned}$$

עבור אינסוף n בסתירה לכך ש- F היא PRF.

²כי: $(r, H_k(r) \oplus m) = (r, (F_k(r) \oplus r) \oplus m) = (r, r \oplus F_k(r) \oplus m)$