פתרון תרגיל מספר 2 ־ מבוא לקריפטוגרפיה ואבטחת תוכנה

שם: מיכאל גרינבאום, **ת.ז:** 211747639

18 במאי 2022

1. **צ"ל:** $G(s)=F_s(1)||F_s(2)||\ldots||F_s(n+1)$ היא PRG

הוכחה:
תחילה נשים לב כי אנחנו רצים $n+1=|s|+1$ פעמים ומפעילים את F_s שפועל זמן פולינומי, ואיחוד של מספרים בינאריים גם הוא פולינומי, ולכן נקבל שזמן הריצה של G הוא פולינומי ב־ s.
עתה נשים לב כי G מגדיל את הקלט כי הוא ממפה קלט באורך $|s|=n$ לפלט באורך $n+1>n=|s|$.
נשאר להראות כי לכל מבחין D שהוא רץ בזמן פולינומי וקיימת פונקציה זניחה $v(\cdot)$ כך ש־

$$\left|\underset{s\leftarrow\{0,1\}^n}{\mathbb{P}}\left(D\left(G\left(s\right)\right)=1\right)-\underset{r\leftarrow\{0,1\}^{n+1}}{\mathbb{P}}\left(D\left(r\right)=1\right)\right|\leq v\left(n\right)$$

נניח בשלילה שקיים יריב $\mathcal{A}$ שהוא רץ בזמן פולינומי וקיים פולינום $p(n)$ כך ש־

$$\left|\underset{s\leftarrow\{0,1\}^n}{\mathbb{P}}\left(\mathcal{A}\left(G\left(s\right)\right)=1\right)-\underset{r\leftarrow\{0,1\}^{n+1}}{\mathbb{P}}\left(\mathcal{A}\left(r\right)=1\right)\right|>\frac{1}{p\left(n\right)}$$

עבור אינסוף ערכים של $n\in\mathbb{N}$,
נגדיר D ל־ F עם גישה לאורקל $\mathcal{O}$ באופן הבא:

(א) לכל $1\leq i\leq n+1$ נריץ את $\mathcal{O}$ על i ונשמור את התוצאה ב־ s_i
(ב) נריץ את $s_1||s_2||\ldots||s_{n+1}$ על $\mathcal{A}$ ונחזיר את הפלט של $\mathcal{A}$

תחילה נשים לב שאם $\mathcal{O}=F_k$, נקבל כי $s_1||s_2||\ldots||s_{n+1}=F_k(1)||F_k(2)||\ldots||F_k(n+1)=G(k)$,
וגם נשים לב שאם $\mathcal{O}=f\leftarrow Func_{n\to n}$, נקבל כי $s_1||s_2||\ldots||s_{n+1}=f(1)||f(2)||\ldots||f(n+1)$ זאת התפלגות באופן אחיד ובלתי תלוי על כל המרחב $\{0,1\}^{n+1}$ (אין תלות בין הערכים) ולכן $s_1||s_2||\ldots||s_{n+1}\sim\{0,1\}^{n+1}$
נשים לב כי D רץ בזמן פולינומי כי הוא מפעיל את F_s מספר פולינומי של פעמים ואז מפעיל את $\mathcal{A}$ שרץ בזמן פולינומי.
עתה נשים לב כי

$$\begin{aligned}
&\left|\underset{k\leftarrow\{0,1\}^n}{\mathbb{P}}\left(D^{F_k(\cdot)}\left(1^n\right)=1\right)-\underset{f\leftarrow Func_{n\to n+1}}{\mathbb{P}}\left(D^{f(\cdot)}\left(1^n\right)=1\right)\right|\\
=&\left|\underset{k\leftarrow\{0,1\}^n}{\mathbb{P}}\left(\mathcal{A}\left(G\left(s_1||s_2||\ldots||s_{n+1}\right)\right)=1\right)-\underset{f\leftarrow Func_{n\to n+1}}{\mathbb{P}}\left(\mathcal{A}\left(f\left(1\right)||f\left(2\right)||\ldots||f\left(n+1\right)\right)=1\right)\right|\\
=&\left|\underset{k\leftarrow\{0,1\}^n}{\mathbb{P}}\left(\mathcal{A}\left(G\left(k\right)\right)=1\right)-\underset{f\leftarrow Func_{n\to n+1}}{\mathbb{P}}\left(\mathcal{A}\left(f\left(1\right)||f\left(2\right)||\ldots||f\left(n+1\right)\right)=1\right)\right|\\
=&\left|\underset{k\leftarrow\{0,1\}^n}{\mathbb{P}}\left(\mathcal{A}\left(G\left(k\right)\right)=1\right)-\underset{r\leftarrow\{0,1\}^{n+1}}{\mathbb{P}}\left(\mathcal{A}\left(r\right)=1\right)\right|\\
=&\left|\underset{s\leftarrow\{0,1\}^n}{\mathbb{P}}\left(\mathcal{A}\left(G\left(s\right)\right)=1\right)-\underset{r\leftarrow\{0,1\}^{n+1}}{\mathbb{P}}\left(\mathcal{A}\left(r\right)=1\right)\right|>\frac{1}{p\left(n\right)}
\end{aligned}$$

עבור אינסוף ערכים של $n\in\mathbb{N}$, כלומר קיבלנו סתירה לכך ש־ F היא PRF,
לכן G הוא PPT שמגדיל את אורך הקלט ולכל אלגוריתם PPT שנסמנו $\mathcal{A}$ קיימת פונקציה זניחה $\nu(\cdot)$ כך ש

$$\left|\Pr_{s\leftarrow\{0,1\}^n}\left[\mathcal{A}\left(G\left(s\right)\right)=1\right]-\Pr_{r\leftarrow\{0,1\}^{2n}}\left[\mathcal{A}\left(r\right)=1\right]\right|\leq\nu\left(n\right)$$

לכל $n\in\mathbb{N}$,
כלומר G הוא PRG מההגדרה

מ.ש.ל.☺

2. **פתרון:**

(א) **צ"ל:** $H_k\left(x\right)=F_k\left(x\right)\oplus F_{1^n}\left(x\right)$ הוא PRF

הוכחה:
תחילה נשים לב כי H_k היא PPT בגלל שהיא משתמשת ב־ F שהיא PPT ורק עושה קסור עליהם (בזמן לינארי).
עתה נניח בשלילה שקיים יריב $\mathcal{A}$ שהוא PPT ופולינום $p\left(\cdot\right)$ כך שמתקיים

$$\left|\mathbb{P}_{k\leftarrow\{0,1\}^n}\left(\mathcal{A}^{H_k(\cdot)}\left(1^n\right)=1\right)-\mathbb{P}_{f\leftarrow Func_{n\to2n}}\left(\mathcal{A}^{f(\cdot)}\left(1^n\right)=1\right)\right|>\frac{1}{p\left(n\right)}$$

עבור אינסוף ערכים של $n\in\mathbb{N}$,
נגדיר יריב ל־ F שנסמנו D עם אורקל $\mathcal{O}$ באופן הבא:

i. נקבל את פרמטר הבטיחות 1^n
ii. נריץ את $\mathcal{A}$ עם 1^n ולכל בקשה שלו x לאורקל נחזיר את $\mathcal{O}\left(x\right)\oplus F_{1^n}\left(x\right)$, ($F_{1^n}$ ידוע מראש ולכן ניתן לחישוב)
iii. נחזיר את התוצאה של $\mathcal{A}$

נשים לב שאם $\mathcal{O}=F_k$, אז מה ש־ $\mathcal{A}$ יקבל עבור $\mathcal{O}\left(x\right)\oplus F_{1^n}\left(x\right)=F_k\left(x\right)\oplus F_{1^n}\left(x\right)=H_k\left(x\right)$, ולכן ריצה זאת מסמלצת את $\mathcal{A}$ עם אורקל H_k במקרה זה.
נשים לב שאם $\mathcal{O}=f\leftarrow Func_{n\to2n}$, אז מה ש־ $\mathcal{A}$ יקבל עבור $\mathcal{O}\left(x\right)\oplus F_{1^n}\left(x\right)=f\left(x\right)\oplus F_{1^n}\left(x\right)$, נשים לב שזה פונקציה רנדומלית כי רק קיסרנו עם קבוע ולכן ריצה זאת מסמלצת את $\mathcal{A}$ עם אורקל $f\leftarrow Func_{n\to2n}$ במקרה זה
נשים לב כי D הוא PPT כי רוב הרצתו זאת הרצת $\mathcal{A}$ ו F_{1^n} מספר פולינומי של פעמים וגם

$$\begin{aligned}&\left|\mathbb{P}_{k\leftarrow\{0,1\}^n}\left(D^{F_k(\cdot)}\left(1^n\right)=1\right)-\mathbb{P}_{f\leftarrow Func_{n\to2n}}\left(D^{f(\cdot)}\left(1^n\right)=1\right)\right|\\=&\left|\mathbb{P}_{k\leftarrow\{0,1\}^n}\left(\mathcal{A}^{F_k(\cdot)\oplus F_{1^n}(\cdot)}\left(1^n\right)=1\right)-\mathbb{P}_{f\leftarrow Func_{n\to2n}}\left(\mathcal{A}^{f(\cdot)\oplus F_{1^n}(\cdot)}\left(1^n\right)=1\right)\right|\\=&\left|\mathbb{P}_{k\leftarrow\{0,1\}^n}\left(\mathcal{A}^{H_k(\cdot)}\left(1^n\right)=1\right)-\mathbb{P}_{f\leftarrow Func_{n\to2n}}\left(\mathcal{A}^{f(\cdot)\oplus F_{1^n}(\cdot)}\left(1^n\right)=1\right)\right|\\=&\left|\mathbb{P}_{k\leftarrow\{0,1\}^n}\left(\mathcal{A}^{H_k(\cdot)}\left(1^n\right)=1\right)-\mathbb{P}_{f\leftarrow Func_{n\to2n}}\left(\mathcal{A}^{f(\cdot)}\left(1^n\right)=1\right)\right|>\frac{1}{p\left(n\right)}\end{aligned}$$

עבור אינסוף ערכים של $n\in\mathbb{N}$, כלומר קיבלנו סתירה לכך ש־ F הוא PRF,
כלומר H הוא PPT וגם ולכל אלגוריתם PPT שנסמנו $\mathcal{A}$ קיימת פונקציה זניחה $\nu\left(\cdot\right)$ כך ש

$$\left|\mathbb{P}_{k\leftarrow\{0,1\}^n}\left(\mathcal{A}^{H_k(\cdot)}\left(1^n\right)=1\right)-\mathbb{P}_{f\leftarrow Func_{n\to2n}}\left(\mathcal{A}^{f(\cdot)}\left(1^n\right)=1\right)\right|\leq\nu\left(n\right)$$

לכל $n\in\mathbb{N}$,
כלומר H הוא PRF מההגדרה

מ.ש.ל.א.☺

(ב) **צ"ל:** $G(s)=F_{0^n}(s)$ הוא לא בהכרח PRG

הוכחה:

תחילה נגדיר $H_k(x)=F_k(x)\oplus F_{0^n}(x)$,

נשים לב שמהסעיף הקודם ניתן להסיק ש־ H היא PRF (רק החלפנו את 1^n ב־ 0^n אבל כל ההוכחה זהה עד כדי שינוי הפונקציה המחושבת באורקל)

נניח בשלילה ש־ $G(s)=F_{0^n}(s)$ היא PRG לכל F שהינה PRF,

לכן מהנימוק מלעיל H הינה PRF, לכן נקבל כי $G'(s)=H_{0^n}(s)$ הוא PRG.

נשים לב כי

$$G'(s)=H_{0^n}(s)=F_{0^n}(x)\oplus F_{0^n}(x)=0^{2n}$$

כלומר G' היא הפונקציה הקבועה 0^{2n}, ולא PRG (על ידי יריב שמחזיר 1 אם הקלט הוא 0^{2n})

כלומר קיבלנו סתירה להנחה שלנו, ולכן מתקיים ש$G(s)=F_{0^n}(s)$ הוא לא בהכרח PRG

מ.ש.ל.ב.☺

3. **פתרון:**

(א) **צ"ל:** Π היא לא $IND-SECURE$ וגם לא $CPA-SECURE$

הוכחה:

נגדיר יריב $\mathcal{A}$ שהוא PPT שמנצח בניסוי IND בהסתברות 1 באופן הבא:

i. נקבל פרמטר בטיחות 1^n

ii. נשלח את ההודעות $m_0=0^n$ ו־ $m_1=1^n$ למצפין

iii. נקבל את ההודעה המוצפנת $c=(r,t)$, נחשב $m=t\oplus G(r)$

iv. נחזיר 1 אם"ם $m=m_1$

תחילה נשים לב כי $\mathcal{A}$ הוא PPT כי הוא רק עושה קסור והפעלה יחידה של אלגוריתם הצפנה וקריאה ל־ Enc שהם PPT.

נסמן את ההצפנה של הודעה m_0 ב־ (r_0,t_0) ושל ההודעה m_1 ב־ (r_1,t_1),

נשים לב כי $t_0=G(r_0)\oplus m_0$, וגם $t_1=G(r_1)\oplus m_1$, אזי

$$\begin{aligned}\mathbb{P}(\mathcal{A}(Enc(K,m_0))=0)&=\mathbb{P}(G(r_0)\oplus t_0\neq m_1)=\mathbb{P}(G(r_0)\oplus(G(r_0)\oplus m_0)\neq m_1)\\&=\mathbb{P}(m_0\neq m_1)=1\end{aligned}$$

ובאופן דומה נשים לב כי

$$\begin{aligned}\mathbb{P}(\mathcal{A}(Enc(K,m_1))=1)&=\mathbb{P}(G(r_1)\oplus t_1=m_1)=\mathbb{P}(G(r_1)\oplus(G(r_1)\oplus m_1)=m_1)\\&=\mathbb{P}(m_1=m_1)=1\end{aligned}$$

לכן

$$\begin{aligned}\mathbb{P}[IND_{\Pi,\mathcal{A}}(n)=1]=&\Pr_{b\leftarrow\{0,1\}}[\mathcal{A}(Enc(K,m_b))=b]\\=&\frac{1}{2}\cdot[\mathbb{P}(\mathcal{A}(Enc(K,m_0))=0)+\mathbb{P}(\mathcal{A}(Enc(K,m_1))=1)]\\=&\frac{1}{2}\cdot[1+1]=\frac{1}{2}\cdot 2=1\end{aligned}$$

כלומר קיבלנו כי יש יריב $\mathcal{A}$ שהוא PPT וקיים פולינום $p(n)=2$ כך שמתקיים

$$\mathbb{P}[IND_{\Pi,\mathcal{A}}(n)=1]\geq\frac{1}{2}+\frac{1}{p(n)}$$

לכל $n\in\mathbb{N}$,

כלומר Π היא לא $IND-SECURE$.

נניח בשלילה ש־ Π היא $CPA-SECURE$, לכן מהמשפט שהוכחנו בהרצאה נקבל כי Π היא $IND-SECURE$ בסתירה למה שהוכחנו מלעיל.

לכן Π היא לא $IND-SECURE$ וגם לא $CPA-SECURE$

מ.ש.ל.א.☺

(ב) **צ"ל:** Π היא $IND-SECURE$ אבל לא $CPA-SECURE$

הוכחה:

תחילה נשים לב כי Π היא בעלת הצפנה דטרמינסטית ולכן היא לא $CPA-SECURE$ לפי הטענה שנאמרה בהרצאה.
עתה נוכיח ש־ Π היא כן $IND-SECURE$,
כלומר נניח בשלילה ש־ Π היא לא $IND-SECURE$, כלומר קיים אלגוריתם $\mathcal{A}$ שהוא PPT ופולינום $p(\cdot)$ שמקיימים

$$\mathbb{P}\left[IND_{\Pi,\mathcal{A}}(n)=1\right]\geq\frac{1}{2}+\frac{1}{p(n)}$$

עבור אינסוף ערכים של $n\in\mathbb{N}$,
נגדיר מבחין D עם אורקל $\mathcal{O}$ באופן הבא:

i. נקבל פרמטר בטיחות 1^n
ii. נריץ את היריב $\mathcal{A}$ עם 1^n ונקבל ממנו הודעות m_0,m_1
iii. נבחר $b\leftarrow\{0,1\}$ ונחזיר ל־ $\mathcal{A}$ את $\mathcal{O}(0^n)\oplus m_b$
iv. נסמן את התוצאה של $\mathcal{A}$ ב־ b'
v. ונחזיר 1 אם"ם $b=b'$

נשים לב ש־ D הוא PPT כי הוא רוב ריצתו היא גישה לאורקול והפעלת $\mathcal{A}$ מספר פולינומי של פעמים (והם גם PPT בעצמם)
נשים לב שאם $\mathcal{O}=F_k$ אז $\mathcal{A}$ מקבל חזרה את $\mathcal{O}(0^n)\oplus m_b=F_k(0^n)\oplus m_b=Enc(m_b)$, כלומר מסמלצים ל־ $\mathcal{A}$ את הניסוי $IND_{\Pi,A}(n)$, ולכן

$$\mathbb{P}\left[IND_{\Pi,\mathcal{A}}(n)=1\right]=\underset{k\leftarrow\{0,1\}^n}{\mathbb{P}}\left(D^{F_k(\cdot)}(1^n)=1\right)$$

נשים לב שאם $\mathcal{O}=f\leftarrow Func_{n\to n}$, אז $\mathcal{O}(0^n)=f(0^n)$ מתפלג באופן אחיד ובלתי תלוי ולכן גם $\mathcal{O}(0^n)\oplus m_b=f(0^n)\oplus m_b$ מתפלג באופן אחיד ובלתי תלוי בשום דבר אחר, ולכן הוא בלתי תלוי ב־ $\mathcal{A}$ ולכן

$$\underset{f\leftarrow Func_{n\to n}}{\mathbb{P}}\left(D^{f(\cdot)}(1^n)=1\right)=\frac{1}{2}$$

לכן נקבל כי

$$\begin{aligned}&\left|\underset{k\leftarrow\{0,1\}^n}{\mathbb{P}}\left(D^{F_k(\cdot)}(1^n)=1\right)-\underset{f\leftarrow Func_{n\to n}}{\mathbb{P}}\left(D^{f(\cdot)}(1^n)=1\right)\right|\\&=\left|\mathbb{P}\left[IND_{\Pi,\mathcal{A}}(n)=1\right]-\frac{1}{2}\right|=\mathbb{P}\left[IND_{\Pi,\mathcal{A}}(n)=1\right]-\frac{1}{2}\\&\geq\frac{1}{2}+\frac{1}{p(n)}-\frac{1}{2}=\frac{1}{p(n)}\end{aligned}$$

כלומר הראנו שקיים מבחין D שהוא PPT ופולינום $p(n)$ כך ש־

$$\left|\underset{k\leftarrow\{0,1\}^n}{\mathbb{P}}\left(D^{F_k(\cdot)}(1^n)=1\right)-\underset{f\leftarrow Func_{n\to n}}{\mathbb{P}}\left(D^{f(\cdot)}(1^n)=1\right)\right|\geq\frac{1}{p(n)}$$

עבור אינסוף ערכים של $n\in\mathbb{N}$, בסתירה לכך ש־ F_k הוא PRF,
כלומר נקבל כי ההנחה שהנחנו לא נכונה, כלומר לכל יריב $\mathcal{A}$ שהוא PPT קיימת פונקציה זניחה $\nu(\cdot)$ כך ש

$$\mathbb{P}\left[IND_{\Pi,\mathcal{A}}(n)=1\right]<\frac{1}{2}+\nu(n)$$

לכל $n\in\mathbb{N}$,
כלומר Π היא $IND-SECURE$ ומהנימוק שניתן בהתחלה היא לא $CPA-SECURE$,
כלומר Π היא $IND-SECURE$ אבל לא $CPA-SECURE$

מ.ש.ל.ב.☺

(ג) **צ"ל:** Π היא $IND-SECURE$ וגם $CPA-SECURE$

הוכחה:

תחילה נוכיח טענת עזר שלכל פונקצית F שהיא PRF מתקיים כי $H_k(x)=x\oplus F_k(x)$ היא גם PRF.

תחילה נשים לב ש־ H היא PPT בגלל ש־ F היא PPT,

עתה נניח בשלילה ש־ H היא לא PRF, כלומר כלומר קיים מבחין $\mathcal{A}$ שהוא PPT ופולינום $p(\cdot)$ שמקיימים

$$\left|\underset{k\leftarrow\{0,1\}^n}{\mathbb{P}}\left(\mathcal{A}^{H_k(\cdot)}(1^n)=1\right)-\underset{h\leftarrow Func_{n\to n}}{\mathbb{P}}\left(\mathcal{A}^{h(\cdot)}(1^n)=1\right)\right|>\frac{1}{p(n)}$$

עבור אינסוף ערכים של $n\in\mathbb{N}$,

נגדיר יריב D עם גישה לאורקל $\mathcal{O}$ באופן הבא:

i. נקבל פרמטר בטיחות 1^n
ii. נריץ את היריב $\mathcal{A}$ עם 1^n, ולכל בקשה שלו לאורקל נחזיר את x את $\mathcal{O}(x)\oplus x$
iii. נחזיר את התוצאה של $\mathcal{A}$

נשים לב ש־ D הוא PPT כי הוא רץ מריץ את $\mathcal{A}$ ו־ $\mathcal{O}$ שהינם PPT מספר פולינומי של פעמים.

עתה נשים לב שאם $\mathcal{O}=F_k$ אז $\mathcal{O}(x)\oplus x=F_k(x)\oplus x=H_k(x)$, ולכן אנחנו מסמלצים ריצה של $\mathcal{A}$ עם אוקרל H_k, ולכן

$$\underset{k\leftarrow\{0,1\}^n}{\mathbb{P}}\left(\mathcal{A}^{H_k(\cdot)}(1^n)=1\right)=\underset{k\leftarrow\{0,1\}^n}{\mathbb{P}}\left(D^{F_k(\cdot)}(1^n)=1\right)$$

ואם $\mathcal{O}=f\leftarrow Func_{n\to n}$, נשים לב כי $\mathcal{O}(x)=f(x)$ מתפלג באופן אחיד ובלתי תלוי ב־ x ובערכים האחרים ולכן $\mathcal{O}(x)\oplus x=f(x)\oplus x$ מתפלג באופן אחיד ובלתי תלוי בקלט ובפלטים האחרים ולכן

$$\underset{f\leftarrow Func_{n\to n}}{\mathbb{P}}\left(D^{f(\cdot)}(1^n)=1\right)=\underset{h\leftarrow Func_{n\to n}}{\mathbb{P}}\left(\mathcal{A}^{h(\cdot)}(1^n)=1\right)$$

ולכן

$$\begin{aligned}&\left|\underset{k\leftarrow\{0,1\}^n}{\mathbb{P}}\left(D^{F_k(\cdot)}(1^n)=1\right)-\underset{f\leftarrow Func_{n\to n}}{\mathbb{P}}\left(D^{f(\cdot)}(1^n)=1\right)\right|\\=&\left|\underset{k\leftarrow\{0,1\}^n}{\mathbb{P}}\left(\mathcal{A}^{H_k(\cdot)}(1^n)=1\right)-\underset{h\leftarrow Func_{n\to n}}{\mathbb{P}}\left(\mathcal{A}^{h(\cdot)}(1^n)=1\right)\right|>\frac{1}{p(n)}\end{aligned}$$

עבור אינסוף ערכים של $n\in\mathbb{N}$, בסתירה לכך ש־ F_k הוא PRF,

כלומר H_k היא PPT וגם לכל יריב $\mathcal{A}$ שהוא PPT קיימת פונקציה זניחה $\nu(\cdot)$ כך ש

$$\left|\underset{k\leftarrow\{0,1\}^n}{\mathbb{P}}\left(\mathcal{A}^{H_k(\cdot)}(1^n)=1\right)-\underset{h\leftarrow Func_{n\to n}}{\mathbb{P}}\left(\mathcal{A}^{h(\cdot)}(1^n)=1\right)\right|\le\nu(n)$$

לכל $n\in\mathbb{N}$,

כלומר H_k היא PRF מההגדרה,

לפי מה שראינו בהרצאה ההצפנה $(r,H_k(r)\oplus m)=(r,r\oplus F_k(r)\oplus m)$ היא $CPA-SECURE$, וזאת בדיוק ההצפנה של Π ולכן Π היא $CPA-SECURE$,

ולפי מה שהוכח בהרצאה, אם Π היא $CPA-SECURE$ אז היא $IND-SECURE$, ולכן Π היא $IND-SECURE$,

כלומר Π היא $IND-SECURE$ וגם $CPA-SECURE$

מ.ש.ל.ג.☺

4. **צ"ל:** H_k היא לא PRF

הוכחה:

נגדיר אלגוריתם $\mathcal{A}$ עם אורקול $\mathcal{O}$ באופן הבא:

(א) נקבל פרמטר בטיחות 1^n

(ב) נשמור את $s_1=\mathcal{O}\left(0^n0^n\right), s_2=\mathcal{O}\left(0^n1^n\right), s_3=\mathcal{O}\left(1^n0^n\right), s_4=\mathcal{O}\left(1^n1^n\right)$

(ג) נחשב את $s_1\oplus s_2\oplus s_3\oplus s_4=s$

(ד) נחזיר 1 אם"ם $s=0$

נשים לב ש־ $\mathcal{A}$ הוא PPT כי רק ניגשנו ל־ $\mathcal{O}$ 4 פעמים וקיסרנו אותם.
עתה נשים לב כי אם $\mathcal{O}=H_k$ אזי מתקיים

$$\begin{aligned}s&=s_1\oplus s_2\oplus s_3\oplus s_4=H_k\left(0^n0^n\right)\oplus H_k\left(0^n1^n\right)\oplus H_k\left(1^n0^n\right)\oplus H_k\left(1^n1^n\right)\\&=\left(F_{k_L}\left(0^n\right)\oplus F_{k_R}\left(0^n\right)\right)\oplus\left(F_{k_L}\left(0^n\right)\oplus F_{k_R}\left(1^n\right)\right)\oplus\left(F_{k_L}\left(1^n\right)\oplus F_{k_R}\left(0^n\right)\right)\oplus\left(F_{k_L}\left(1^n\right)\oplus F_{k_R}\left(1^n\right)\right)\\&=\left(F_{k_L}\left(0^n\right)\oplus F_{k_L}\left(0^n\right)\right)\oplus\left(F_{k_R}\left(1^n\right)\oplus F_{k_R}\left(1^n\right)\right)\oplus\left(F_{k_R}\left(0^n\right)\oplus F_{k_R}\left(0^n\right)\right)\oplus\left(F_{k_L}\left(1^n\right)\oplus F_{k_L}\left(1^n\right)\right)\\&=0^n\oplus0^n\oplus0^n\oplus0^n=0^n\end{aligned}$$

כלומר תמיד ננצח בניסוי ולכן

$$\mathop{\mathbb{P}}_{k\leftarrow\{0,1\}^n}\left(\mathcal{A}^{H_k(\cdot)}\left(1^n\right)=1\right)=1$$

וגם עבור $\mathcal{O}=f\leftarrow Func_{n\to n}$, נשים לב כי s_1,s_2,s_3,s_4 מתפלגים באופן אחיד ובלתי תלוי אחד בשני ולכן $s=s_1\oplus s_2\oplus s_3\oplus s_4$ מתפלג באופן אחד ולכן

$$\mathop{\mathbb{P}}_{h\leftarrow Func_{n\to n}}\left(\mathcal{A}^{h(\cdot)}\left(1^n\right)=1\right)=\mathop{\mathbb{P}}_{s\leftarrow\{0,1\}^n}\left(s=0\right)=\frac{1}{2^n}$$

ולכן

$$\left|\mathop{\mathbb{P}}_{k\leftarrow\{0,1\}^n}\left(\mathcal{A}^{H_k(\cdot)}\left(1^n\right)=1\right)=1-\mathop{\mathbb{P}}_{h\leftarrow Func_{n\to n}}\left(\mathcal{A}^{h(\cdot)}\left(1^n\right)=1\right)\right|=\left|1-\frac{1}{2^n}\right|=1-\frac{1}{2^n}\geq\frac{1}{2}$$

כלומר הראנו שקיים יריב $\mathcal{A}$ ופולינום $p\left(n\right)=2$ כך ש

$$\left|\mathop{\mathbb{P}}_{k\leftarrow\{0,1\}^n}\left(\mathcal{A}^{H_k(\cdot)}\left(1^n\right)=1\right)=1-\mathop{\mathbb{P}}_{h\leftarrow Func_{n\to n}}\left(\mathcal{A}^{h(\cdot)}\left(1^n\right)=1\right)\right|\geq\frac{1}{p\left(n\right)}$$

לכל $n\in\mathbb{N}$,
ולכן הראנו ש־ H לא PRF (אחרת הטענה שהוכחנו מלעיל הייתה לא נכונה)

מ.ש.ל.☺

5. **צ"ל:** $x_L||x_R||F_{k_L}\left(x_L\right)\oplus F_{k_R}\left(x_R\right)$ בלתי ניתנת לאבחנה מההתפלגות האחידה
הוכחה:
נסמן את ההתפלגות $x_L||x_R||F_{k_L}\left(x_L\right)\oplus F_{k_R}\left(x_R\right)=X$,
נניח בשלילה ש־ X ניתנת לאבחנה מההתפלגות האחידה אז קיים יריב $\mathcal{A}$ שהוא PPT ופולינום $p\left(\cdot\right)$ כך ש־

$$\left|\mathbb{P}_{x\leftarrow X_n}\left(\mathcal{A}\left(1^n,x\right)=1\right)-\mathbb{P}_{y\leftarrow\{0,1\}^{3n}}\left(\mathcal{A}\left(1^n,y\right)=1\right)\right|\geq\frac{1}{p\left(n\right)}$$

עבור אינסוף ערכים של $n\in\mathbb{N}$,
נגדיר מבחין D עם גישה לאורקל $\mathcal{O}$ באופן הבא:

(א) נקבל פרמטר בטיחות 1^n

(ב) נגריל $x_L,x_R,k_R\leftarrow\{0,1\}^n$

(ג) נחשב $s=x_L||x_R||\mathcal{O}\left(x_L\right)\oplus F_{k_R}\left(x_R\right)$

(ד) נחזיר את התוצאה של $\mathcal{A}\left(1^n,s\right)$

תחילה נשים לב ש־ D הוא PPT כי הוא ניגש רק ל־ $F_k, \mathcal{A}, \mathcal{O}$ מספר פולינומי של פעמים והם PPT.
עתה נשים לב שאם $\mathcal{O} = F_{k_L}$ אז מתקיים

$$s = x_L || x_R || \mathcal{O}\left(x_L\right) \oplus F_{k_R}\left(x_R\right) = x_L || x_R || F_{k_L}\left(x_L\right) \oplus F_{k_R}\left(x_R\right) \sim X$$

ולכן אנחנו מריצים את $\mathcal{A}$ על ההתפלגות של X_n ולכן

$$\mathbb{P}_{k_L \leftarrow \{0,1\}^n}\left(D^{F_{k_L}(\cdot)}\left(1^n\right) = 1\right) = \mathbb{P}_{x \leftarrow X_n}\left(\mathcal{A}\left(1^n, x\right) = 1\right)$$

וגם נשים שלב שאם $\mathcal{O} = f \leftarrow Func_{n \to n}$, נשים לב כי

$$s = x_L || x_R || \mathcal{O}\left(x_L\right) \oplus F_{k_R}\left(x_R\right) = x_L || x_R || f\left(x_L\right) \oplus F_{k_R}\left(x_R\right)$$

נשים לב כי $x_L, x_R, f\left(x_L\right)$ מתפלגים באופן אחיד ובלתי תלוי ולכן s מתפלג באופן אחיד ולכן

$$\mathbb{P}_{f \leftarrow Func_{n \to n}}\left(D^{f(\cdot)}\left(1^n\right) = 1\right) = \mathbb{P}_{y \leftarrow \{0,1\}^{3n}}\left(\mathcal{A}\left(1^n, y\right) = 1\right)$$

עתה נקבל כי

$$\begin{aligned} &\left|\mathbb{P}_{k_L \leftarrow \{0,1\}^n}\left(D^{F_{k_L}(\cdot)}\left(1^n\right) = 1\right) - \mathbb{P}_{f \leftarrow Func_{n \to n}}\left(D^{f(\cdot)}\left(1^n\right) = 1\right)\right| \\ = &\left|\mathbb{P}_{x \leftarrow X}\left(\mathcal{A}\left(1^n, x\right) = 1\right) - \mathbb{P}_{y \leftarrow \{0,1\}^{3n}}\left(\mathcal{A}\left(1^n, y\right) = 1\right)\right| \geq \frac{1}{p\left(n\right)} \end{aligned}$$

עבור אינסוף ערכים של $n \in \mathbb{N}$, בסתירה לכך ש־ F_k הוא PRF,
כלומר קיבלנו כי לכל יריב $\mathcal{A}$ שהוא PPT קיימת פונקציה זניחה $\nu\left(\cdot\right)$ כך ש־

$$\left|\mathbb{P}_{x \leftarrow X}\left(\mathcal{A}\left(1^n, x\right) = 1\right) - \mathbb{P}_{y \leftarrow \{0,1\}^{3n}}\left(\mathcal{A}\left(1^n, y\right) = 1\right)\right| \leq \nu\left(n\right)$$

לכל $n \in \mathbb{N}$,
לכן מההגדרה $x_L || x_R || F_{k_L}\left(x_L\right) \oplus F_{k_R}\left(x_R\right)$ בלתי ניתנת לאבחנה מההתפלגות האחידה

מ.ש.ל.☺