מבוא לקריפטוגרפיה ואבטחת תוכנה
תרגיל 1

רן שחם - 203781000

4 באפריל 2017

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

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

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 בצורה מושלמת. אזי לכל התפלגות M על $\mathcal{M}$, לכל $m\in\mathcal{M}$ ולכל $c\in\mathcal{C}$ כך ש־$\Pr\left[C=c\right]>0$ מתקיים:

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

מנוסחת בייס,

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

ולכן:

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

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

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

כנדרש.

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

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

מהנ"ל ומ־$(*)$ מתקיים:

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

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

שאלה 2

בספר.

שאלה 3

תהי $\nu(n)$ פונ' זניחה ויהי p פולינום. נראה ש־$p(n)\cdot\nu(n)$ 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 $p(n)\,\nu(n)$ 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 $\ell(n)>n$ 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 אס"ם $c[0.\dots k-1]=c[k\dots 2k-1]$, כלומר אם k הביטים הראשונים ב־c זהים ל־k הביטים האחרונים בו.

אם כך, לכל קלט s בעל n ביטים כך ש־$c=G(s)=G_1(s)\,||G_2(s)=G_1(s)\,||G_1(s)$ מתקיים ש־$\ell(n)$ 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 $0\le i<\ell(n)$ הוא $1/2$, והביט ה־i ב"ת בביט ה־j לכל $0\le i<j<\ell(n)$ (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 $\ell(n)>n$ כך ש־$|G_1(s)|=|G_2(s)|=\ell(n)$. נניח בשלילה שקיים מבחין יעיל D (PPT) ופולינום $p(n)$ כך ש־:

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

עבור אינסוף ערכי n. לכן, לאינסוף n:

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

כאשר:

1. לפי הגדרת G
2. אי שוויון המשולש

ולכן, מתקיים $\frac{1}{p(n)} = \frac{2}{2p(n)} < A$ או ש־$\frac{1}{p(n)} < B$ 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 $D\left(G_1\left(s_1\right)||s\right)$. מכיוון ש־$D$ מבחין יעיל גם D_2 יעיל. נשים לב שעבור אינסוף n מתקיים:

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

מההנחה ש־$\frac{1}{p(n)} < A$, ובסתירה לכך ש־G_2 הוא PRG.

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

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

עבור אינסוף n, בסתירה ל־PRGיות של G_1.
לכן, לא קיים מבחין D כנ"ל ו־G הוא PRG כנדרש.

שאלה 5

נגדיר את H כך:

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

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

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

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

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

נעביר אגפים ונקבל:

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

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

נטען ש־ $\left(r-q\right)2^{-n}+\frac{1}{p(n)}$ אינה זניחה ובכך נקבל ש־D מבחין יעיל ל־G בסתירה לכך ש־G PRG.

מכיוון ש־$\left(r-q\right)2^{-n}$ זניחה (כי $r-q$ חסומה ב־± 1 ו־2^{-n} זניחה), קיים n_0 כך שלכל $n>n_0$ מתקיים:

$$\begin{aligned}&\left|\left(r-q\right)2^{-n}\right|<\frac{1}{2p\left(n\right)}\\\iff&-\left|\left(r-q\right)2^{-n}\right|>-\frac{1}{2p\left(n\right)}\\\iff&\frac{1}{p\left(n\right)}-\left|\left(r-q\right)2^{-n}\right|>\frac{1}{2p\left(n\right)}\\\implies&\frac{1}{p\left(n\right)}+\left(r-q\right)2^{-n}\geq\frac{1}{p\left(n\right)}-\left|\left(r-q\right)2^{-n}\right|>\frac{1}{2p\left(n\right)}\end{aligned}$$

כלומר הפונ' אינה זניחה כנדרש.

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:

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

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

$$x=\mathcal{O}\left(1\right)||\mathcal{O}\left(2\right)||\cdots||\mathcal{O}\left(n+1\right)$$

לאחר מכן, יחשב את $D\left(x\right)$ 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 $x=G\left(s\right)$ לכל s, לפי הגדרה

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

לכן:

$$\left|\Pr_{s \leftarrow \{0,1\}^n}\left[D^{F_s(\cdot)}\left(1^n\right) = 1\right] - \Pr_{f \leftarrow \mathrm{Func}_1}\left[D^{f(\cdot)}\left(1^n\right)\right] = 1\right|$$
$$= \left|\Pr_{s \leftarrow \{0,1\}^n}\left[D\left(G\left(s\right)\right) = 1\right] - \Pr_{r \leftarrow \{0,1\}^{n+1}}\left[D\left(r\right) = 1\right]\right| > \frac{1}{p\left(n\right)}$$

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

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

$$\left|\Pr_{k \leftarrow \{0,1\}^n}\left[D^{P_k(\cdot)}\left(1^n\right) = 1\right] - \Pr_{f \leftarrow \mathrm{Func}_n}\left[D^{f(\cdot)}\left(1^n\right) = 1\right]\right|$$
$$= \left|1 - 2^{-n}\right| = 1 - 2^{-n} > \frac{1}{n}$$

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:

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

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 $y = \mathcal{O}\left(x\right) \oplus 1^n$ 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 $y = F_k\left(x\right) \oplus 1^n = H_k\left(x\right)$ 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:

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

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

נגדיר:

$$F'_k(x) = \begin{cases} F_k(x), & k \neq 1^n \\ 0^{2n}, & k = 1^n \end{cases}$$

לכל $x \in \{0,1\}^n$. נטען ש־F' היא PRF. יהי D מבחין יעיל ל־F' ונגדיר:

$$\nu(n) = \left| \Pr_{k \leftarrow \{0,1\}^n} \left[D^{F'_k(\cdot)}(1^n) = 1 \right] - \Pr_{f \leftarrow \mathrm{Func}_{n,2n}} \left[D^{f(\cdot)}(1^n) = 1 \right] \right|$$

כעת יהי B מבחין יעיל ל־F.

כלומר F' היא PRF כנדרש.

נטען ש־$H_k(x) = F'_k(x) \oplus F'_{1^n}(x)$ לכל $x, k \in \{0,1\}^n$ אינה PRF. נשים לב ש־$F'_{1^n}(x) = 0^{2n}$ לכל $x \in \{0,1\}^n$, לכן: $H_k(x) = F'_k(x) \oplus 1^{2n}$ וראינו בשאלה 7 סעיף 2 ש־H כזאת (כמעט) אינה PRF.

נבנה מבחין D כך: בהינתן קלט 1^n וגישת אורקל $\mathcal{O}$,

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:

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

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

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

לכן, לאינסוף n:

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

כאשר המעבר האחרון נובע מאי־שוויון המשולש. באופן דומה לבשאלה 5, $\frac{1}{p(n)} - \left|(q_n - r_n) \cdot 2^{-n}\right|$ אינה פונ' זניחה, 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 אס"ם $s = 0^{2n}$. 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:

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

עבור אינסוף n, כלומר G אינה PRG.