# 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 4

### סעיף א'

נניח ש־$G_1, G_2$ הם PRG כך ש־$G_1=G_2$. אזי $G$ המוגדר כבשאלה אינו PRG.

יהי $\ell\left(n\right)>n$ פולינום כך ש־$\left|G_1\left(s\right)\right|=\ell\left(\left|s\right|\right)$. נראה מבחין (distinguisher) יעיל שמבדיל בין פלט של $G$ לבין פלט אקראי בסיכוי לא זניח. נגדיר את $D\left(c\right)$ להחזיר 0 אם $|c|$ אי־זוגי. אחרת, אם $|c|=2k$ אז $D$ יחזיר 1 אס"ם $c\left[0.\dots k-1\right]=c\left[k\dots 2k-1\right]$, כלומר אם $k$ הביטים הראשונים ב־$c$ זהים ל־$k$ הביטים האחרונים בו.

אם כך, לכל קלט $s$ בעל $n$ ביטים כך ש־$c=G\left(s\right)=G_1\left(s\right)||G_2\left(s\right)=G_1\left(s\right)||G_1\left(s\right)$ מתקיים ש־$\ell\left(n\right)$ הביטים הראשונים ב־$c$ זהים ל־$\ell\left(n\right)$ הביטים האחרונים, ולכן $D$ על $c$ יחזיר 1 (תמיד). לכן:

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

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

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

### סעיף ב'

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

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

עבור אינסוף ערכי $n$. לכן, לאינסוף $n$:

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

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

$$\begin{aligned}\Pr\left[D\left(H\left(U_n\right)\right)=1\right]&=\Pr\left[D\left(H\left(U_n\right)\right)=1|U_n=0^n\right]\Pr\left[U_n=0^n\right]\\&+\Pr\left[D\left(H\left(U_n\right)\right)=1|U_n\neq0^n\right]\Pr\left[U_n\neq0^n\right]\\&=\overbrace{\Pr\left[D\left(H\left(0^n\right)\right)=1\right]}^{q}\cdot2^{-n}+\Pr\left[D\left(G\left(U_n\right)\right)=1\right]\cdot\left(1-2^{-n}\right)\\&=q\cdot2^{-n}+\Pr\left[D\left(G\left(U_n\right)\right)=1\right]-\overbrace{\Pr\left[D\left(G\left(U_n\right)\right)=1\right]}^{r}\cdot2^{-n}\\&=\left(q-r\right)2^{-n}+\Pr\left[D\left(G\left(U_n\right)\right)=1\right]\overset{(*)}{>}\Pr\left[D\left(U_{2n}\right)=1\right]+\frac{1}{p\left(n\right)}\end{aligned}$$

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־$\pm1$ 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:

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

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:

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

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-$\mathrm{Func}_n$. לכן:

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

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**

**הערה 0.2** המבחין $D$ המתואר למטה מחשב את הערך $F_{1^n}(x)$. זה בעייתי כי התיאור של $F$ הוא אקספוננציאלי ב־$n$ (חייב להכיל מיפוי של כל ערך ב־$\{0,1\}^n$) ולכן חישוב זה עלול להפוך את המבחין ללא־יעיל. לא הצלחתי להימנע מכך (אינטואיטיבית, עובדה זו רק מחזקת את הקושי בהבחנה של $H$ מפונ' אקראית). בהינתן שחישוב זה יכול להתבצע ביעילות, גם המבחין $D$ ירוץ בזמן פולינומיאלי.

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

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

לאינסוף $n$. נבנה מבחין $D$ ל־$F$ הפועל כך: בהינתן $1^n$ וגישת אורקל ל־$\mathcal{O}$, $D$ יריץ את $B$ עם הפרמטר $1^n$. לכל בקשה לגישת אורקל לערך $x\in\{0,1\}^n$ מ־$B$, $D$ יחשב את $F_{1^n}(x)$ ויחזיר ל־$B$ את $\mathcal{O}(x)\oplus F_{1^n}(x)$ (זה אפשרי כי תיאור $F$ הוא פומבי; וזה בעייתי כי תיאור $F$ הוא ענק). $D$ יחזיר 1 אם"ם $B$ החזיר 1.

נשים לב שלכל $n\in\mathbb{N}$, עבור $\mathcal{O}=F_k$ עבור $k\leftarrow\{0,1\}^n$, $D$ מדמה את ריצת $B$ עם אורקל $H_k$ - לכן:

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

כמוכן אם $\mathcal{O}=f$ עבור $f\leftarrow\mathrm{Func}_{n,2n}$ 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:

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

לאינסוף $n$ בסתירה לכך ש־$F$ פסאודו רנדומית.

**סעיף 2**

$G$ אינו בהכרח PRG.

נגדיר פונ' $F'$ באופן הבא:

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

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

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

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

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

לכן, לאינסוף $n$:

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

כאשר המעבר האחרון נובע מאי־שוויון המשולש. באופן דומה לבשאלה 5, $\left|(q_n - r_n)\cdot 2^{-n}\right| - \frac{1}{p(n)}$ 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 אם"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.

# 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־$\Pr[\mathrm{IND}_{\Pi,\mathcal{A}}(n) = 1] = 1$. יהי $b \in \{0,1\}$ כך ש־$c^* = \mathrm{Enc}_k(m_b)$. $G$ 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"ם $c^* \oplus x = 1^n$.

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, $x = c \oplus m = (F_k(0^n) \oplus m) \oplus m = F_k(0^n)$ ולכן המערכת לא בטוחה נגד CPA.

עם זאת, למערכת יש הצפנות בלתי ניתנות להבחנה (IND-Secure). נניח בשלילה שלא, ויהיו $F$ PRF, יריב $\mathcal{A}$ ופולינום $p$ כך שלאינסוף $n \in \mathbb{N}$ מתקיים:

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

נבנה מבחין $D$ שבהינתן הקלט $1^n$ וגישת אורקל לפונקציה $\mathcal{O}$, 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"ם $b' = b$ 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 $f \equiv \mathcal{O}$ עבור $f \leftarrow \mathrm{Func}_n$ 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:

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

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 בכיתה, ולכן בטוחה כפי שהוכחנו.

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

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

נבנה מבחין $D$ ל־$F$ באופן הבא: בהינתן אורקל $\mathcal{O}$ וקלט $1^n$, $D$ 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"ם $B$ 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 $f \leftarrow \mathrm{Func}_n$ אז הערך $f(r)$ שקול לערך המפולג אחיד ב־$\{0,1\}^n$, וכך גם $f(r) \oplus r$. לכן:

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

עבור אינסוף $n$ בסתירה לכך ש־$F$ היא PRF.