

# מבוא לקריפטוגרפיה ואבטחת תוכנה

## תרגיל 1

רן שחם - 203781000

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

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

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

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

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:

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

מההנחה 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-PRGיות של  $G_1$ .

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

## שאלה 5

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- $\Pr[D(H(U_n)) = 1] > \Pr[D(U_{2n}) = 1] + \frac{1}{p(n)}$  (\*): 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 מהחיסוב לעיל.

נטען ש- $(r - q) 2^{-n} + \frac{1}{p(n)}$  אינה זניחה ובכך נקבל ש- $D$  מבחין יעיל ל- $G$  בסתירה לכך ש- $G$  PRG. מכיוון ש- $(r - q) 2^{-n}$  זניחה (כי  $r - q$  חסומה ב- $\pm 1$  ו- $2^{-n}$  זניחה), קיים  $n_0$  כך שלכל  $n > n_0$  מתקיים:

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

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:

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

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.  $D^{(\cdot)}$  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  $\text{Func}_1 = \{g : \{0, 1\}^* \rightarrow \{0, 1\}\}$ ) אז  $x$  שקול לערך הנבחר מהתפלגות אחידה על מחרוזות באורך  $n+1$  ביטים - כי כל ביט בו נבחר באקראי

לכן:

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

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

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:

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

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:

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

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 זה 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  $\mathcal{O}(x) \oplus 1^n = F_k(x) \oplus 1^n = H_k(x)$  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- $\text{Func}_n$ . לכן:

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

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

## סעיף 2

**הערה 0.3** יש בעיה עם יעילות המבחין שיתואר בהמשך, שכן התיאור של  $F$  הוא בגודל אקספוננציאלי, ולכן ללא גישת אורקל לא יוכל לחשב את  $F_{0^n}(s)$  באופן יעיל.

$G$  הוא PRG. בשלילה שלא, כלומר קיים פולינום  $p$  ומבחין יעיל  $B$  כך ש:

$$\left| \Pr_{s \leftarrow \{0,1\}^n} [B(G(s)) = 1] - \Pr_{r \leftarrow \{0,1\}^{2n}} [B(r) = 1] \right| > \frac{1}{p(n)}$$

עבור אינסוף ערכי  $n$ .

$G$  אינו PRG. נבנה מבחין  $D$  הפועל כך: בהינתן קלט  $s$  באורך  $n$  ביטים,  $D$  יחשב את  $F_{0^n}(s)$