מבוא לקריפטוגרפיה וסיבוכיות חישובית

תרגיל מס' 1

מיכאל הנשאר,
313584401

שאלה 1: הוכחה:

$\Rightarrow$: יהי $\Pi = (KeyGen, Enc, Dec)$ שמקיים שלמות מושלמת, צ"ל שלכל התפלגות M על מרחב ההודעות $\mathcal{M}$, לכל הודעה $m \in \mathcal{M}$ עם הסתברות חיובית $Pr[M=m] > 0$, ולכל הצפנה $c \in \mathcal{C}$ שמקיים כי: $Pr[C=c] = Pr[C=c \mid M=m]$.

יהי, מכך התפלגות על מרחב ההודעות M, ועבור הודעה m עם הסתברות חיובית $m \in \mathcal{M}$, $Pr[M=m] > 0$, ועבור הצפנה $c \in C$.

נמלץ למקרים?

(*) נאמר כי $\Pr[C=c] > 0$ עבור M:

כאשר m הוא אורך ההודעה הגדול ביותר עבור M ($m \geq k$)

Π הינה הצפנה מושלמית, אזי,

מתקיים, שמתקיים:

(**) $\Pr[M=m \mid C=c] = \Pr[M=m]$.

שקול:

$$\Pr[C=c \mid M=m] = \frac{\Pr[C=c] \cdot \Pr[M=m \mid C=c]}{\Pr[M=m]}$$

↓ לפי תנאי בייס

$$= \frac{\Pr[C=c] \cdot \Pr[M=m]}{\Pr[M=m]} = \Pr[C=c]$$

↓ לפי (**)

נשים לב.

(*) נאמר כי $\Pr[C=c] = 0$ עבור M:

אזי:

$$\Pr[C=c \mid M=m] = \frac{\Pr[C=c \wedge M=m]}{\Pr[M=m]} \leq$$

↓ מהגדרת ההסתברות המותנית

עמ' 2

$$\leq \frac{Pr[C=c]}{Pr[M=m]} = \frac{0}{Pr[M=m]} = 0$$

כי ההצרנה
$M=m \wedge C=c$
אינה
אפשרית

מכאן שמתקיים השוויון הנדרש:

$$Pr[C=c \mid M=m] = Pr[C=c] \quad (=0)$$

$\Pi = (KeyGen, Enc, Dec)$ נניח $\Rightarrow$

שלכל התפלגות M על קבוצת ההודעות $\mathcal{M}$,
לכל הודעה $m \in \mathcal{M}$ שעבורה $Pr[M=m] > 0$, ולכל הצפנה $c \in C$ שעבורה:
$Pr[C=c \mid M=m] = Pr[C=c]$, מתקיים כי Π הינה סודית מושלמת:

אזי, ניקח התפלגות M על מרחב ההודעות $\mathcal{M}$,
ניקח הודעה $m \in \mathcal{M}$ וניקח הצפנה
$c \in C$ כלשהי המקיימת כמובן $\Pr[C=c] > 0$.

ונשאל, מהן ההסתברויות:

(*) עבור $\Pr[M=m] > 0$ עבור M
(כלומר מרחב ההודעות שלקח על פחות אז m),
(**) אז מתקיים כי: $\Pr[C=c] = \Pr[C=c \mid M=m]$.

לפי בייס:

$$\Pr[M=m \mid C=c] = \frac{\Pr[M=m] \cdot \Pr[C=c \mid M=m]}{\Pr[C=c]}$$

לפי תכונת הכפל

$$= \frac{\Pr[M=m] \cdot \Pr[C=c]}{\Pr[C=c]} = \Pr[M=m]$$

לפי (**)

כלומר.

(*) ולכן עבור M ; $\Pr[M=m] = 0$

כלומר:

$$Pr[M=m \mid C=c] = \frac{Pr[M=m \wedge C=c]}{Pr[C=c]} \leq$$

מהגדרת ההסתברות המותנית

$$\leq \frac{Pr[M=m]}{Pr[C=c]} = \frac{0}{Pr[C=c]} = 0$$

שווה ל-0

שמאל

$m=M$ שבו הוא מוגרל

$c=C \wedge m=M$

לכן: שתי המילים הללו בלתי

$$Pr[M=m \mid C=c] = Pr[M=m] \quad (=0)$$

זה מה שרצינו.

שאלה 2: נראה כי ההגדרה של **פסודו-אקראיות** אינה שקולה לזו שראינו בכיתה (distinguishers). שנזכיר שלפי ההגדרה שראינו בכיתה, פונקציה G היא **פסודו-אקראית** אם לכל D (אלגוריתם שמקבל קלט באורך $l(n)$ ומחזיר ביט) מתקיים כי:

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

לכל $n \in \mathbb{N}$:

נראה ש- brute force attack:

שמקיים האלגוריתם D הבא, ושעבור כל n ניתן לחשב אותו ביעילות: עבור קלט w, האלגוריתם D פולט 1 אם ורק אם קיים $s \in \{0,1\}^n$ כך ש: $G(s) = w$.

מכיוון שיש לכל היותר 2^n מחרוזות $s \in \{0,1\}^n$ שעבורן $G(s) = w$, אז לכל היותר 2^n מחרוזות $w \in \{0,1\}^{l(n)}$ יגרמו ל- D להחזיר 1.

(חישוב של $G(s)$ לכל $s \in \{0,1\}^n$.
(הכוונה, שהאלגוריתם G ניתן לחישוב ביעילות פולינומית).
לכן, אם w הוא פלט האפשרי של G,
אז D מחזיר 1 בהסתברות 1.

אחרת, אם w נבחר באופן אחיד
מ- $\{0,1\}^{l(n)}$, אז ההסתברות שקיים s
כך ש: $w = G(s)$ היא לכל היותר
$\frac{2^n}{2^{l(n)}}$ (כי בתקרה הזו על G הוא סותג
חח"ע). ומאחר והתרחבה עליה, נדרש שמתקיים
לפחות, $l(n) > n$ ולכן
לכל $n \in \mathbb{N}$ מתקיים: $l(n) \geq n+1$, ומתקיים: $\frac{2^n}{2^{l(n)}} \leq \frac{1}{2^{n+1-n}} = \frac{1}{2}$
(הוספנו הסתברות)

לכן D פולינומי ש- w נבחר באופן
אחיד מ- $\{0,1\}^{l(n)}$ ההסתברות לכל היותר $\frac{1}{2}$.

לכן: לכל $n \in \mathbb{N}$ מתקיים:

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

סתירה.

שאלה 3: תהי f פונקציה ששאלון אלגוריתמי
ל-בוליאנית הפונקציה: $G: \{0,1\}^* \to \{0,1\}$;
מוגדרת באופן הבא:

$$G(s) = F_s(1) \| F_s(2) \| \cdots \| F_s(1+n)$$

כאשר $n = |s|$. הוכח כי G הינו יצרן פסאודו-אקראי;

נסמן ע"י k את מספר הביטים שהפונקציה F פולטת
ע"י k.

נניח בשלילה ש-G אינו יצרן פסאודו-אקראי,
ונראה כי הדבר גורר כי F אינה פונקציה
פסאודו-אקראית, בסתירה לאמור.

לשם כך נשים לב כי G אכן מגדיל את
אורך הקלט (בגודה מאקסיום השלישית שלנו
יצרן פסאודו-אקראי), שהרי קלט באורך n ביטים
נשלח ל-G, שפולטת פלט באורך $(1+n)k$
ביטים. מאידך, נשים לב כי G מקיימת
תכונה נוספת, הנקראת לפעמים תכונת ההמשכיות
הצעדית, הטוענת כי עבור כל קלט s באורך n, שאין חשוב כמה ביטים

קיבלנו שפונקציה F, ואנחנו פונקציה פסאודו
ובקבועה F שמתחת טענה שמשמר בטחון פסאודו
מ- n.

מכאן שאנחנו בשלב כי G איננו
יכול ל"ג (בקבוצה פסאודו אקראי), נובע שקיים
וללגוריתם D_1 שמתן ביטחון פסאודו, וכן
קיים פולינום $p(n)$, כך שמתקיים אומנם עבור
$n \in \mathbb{N}$ שמספיק:

$$\left| \Pr_{s \in \{0,1\}^n}[D_1(G(s))=1] - \Pr_{r \in \{0,1\}^{k(n)+n}}[D_1(r)=1] \right| > \frac{1}{p(n)}$$

ולכן, שמתן D_2, הוא לגוריתם הפסאודו בדיקה;
D_2 שמקבל קלט 1^n ומן בשלב מתחיל לפונקציה
$x_i = O(i)$, ניקח את המפתח $key \in \{0,1\}^n$, $f \leftarrow Func_{n,k}$ $O = F_{key}(\cdot) \vee f(\cdot)$
ולכל $1 \le i \le 1$, $N \leftarrow O$,

[redacted]

נפעיל את $D_1(x_1 \| x_2 \| \cdots \| x_{poly})$.

כלומר, נוכל לסכם:

שאלה 4: תהא f פונקציה סמויה-אקראית, כך שלכל $k \in \{0,1\}^n$ ולכל $n \in \mathbb{N}$ מתקיים: $f_k : \{0,1\}^n \to \{0,1\}^n$.

---

1) תהא: $H_k(x) = f_k(x) \oplus f_{1^n}(x)$ עבור $n \in \mathbb{N}$ כלשהו, $k \in \{0,1\}^n$ כלשהו, $x \in \{0,1\}^n$.

נוכיח כי H היא הצפנה פונקציה סמויה-אקראית.

נניח בשלילה כי H איננה פונקציה סמויה-אקראית. לכן קיים אלגוריתם סביר D_1 וקיים פולינום $p(n)$ כך שמתקיים אינסוף אבר. n עבורם:

$$\left| \Pr_{k \in \{0,1\}^n} \left[D_1^{H_k(\cdot)}(1^n) = 1 \right] - \Pr_{\tilde{f} \in Func_{n,n}} \left[D_1^{\tilde{f}(\cdot)}(1^n) = 1 \right] \right| > \frac{1}{p(n)} \quad (**)$$

כעת, נבנה אלגוריתם הסביר D_2 הבאה לו כקלט פונקציה O, ומספר טבעי 1^n כקלט, ומנסה את האלגוריתם

D_1 על 1^n.

ובהינתן שאלת $X \in \{0,1\}^n$, עבור $N=0$ אזי $O(X)$, לכן מתקיים אזי $f_{1^n}(X)$, ולפיכך D_1-ל אזי מתקיים $O(X) \oplus f_{1^n}(X)$.

כש-D_1 יפסוק שמדובר אכן בפלט.

D_2-ל נאמן כיצד פולינומית, שאכן D_1-ל בלתי-נשלל:

כאשר שלוש אפשרויות:

א. אזי D_2 שקבל קלט $f(\cdot)$-ל שמקבלת $Func_{n,2n}$, וכל עבור $X \in \{0,1\}^n$ שמחזיר D_1-ל כאשר $f(x) \oplus f_{1^n}(X)$, ומכאן שהסתברות שאלגוריתם מחזיר 1 שווה לפחות $\frac{1}{2}$ לפחות D_1-ל.

לעומת זאת, D_2 יכול להשתמש בD_1-ל כתת-שגרה על קלט שרירותי $\tilde{f}(\cdot)$-ל שמקבלת $Func_{n,2n}$, לפיכך:

$$\Pr_{f \leftarrow Func_{n,n}}\left[D^{f(\cdot)}(1^n)=1\right] = \Pr_{h \leftarrow Func_{n,2n}}\left[D_1^{h(\cdot)}(1^n)=1\right]$$

(*) נגדיר D_2 שמקבל גישה לאורקל $f_k(\cdot)$ עבור $k \in \{0,1\}^n$ כלשהו, ועל $x \in \{0,1\}^n$ כלשהו מחשב את D_1 שלנו:

$$f_k(x) \oplus f_{1^n}(x) = H_k(x)$$

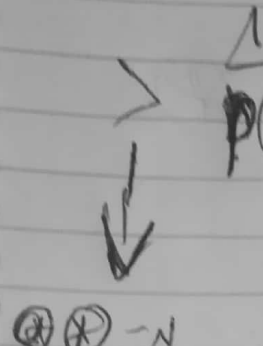
לכן, מהגדרה קל לראות שבאופן שקול $H_k(\cdot)$ ניגש לאורקל D_1 עבור $k \in \{0,1\}^n$ שרירותי:

$$\Pr_{k \leftarrow \{0,1\}^n}\left[D_2^{f_k(\cdot)}(1^n)=1\right] = \Pr_{k \in \{0,1\}^n}\left[D_1^{H_k(\cdot)}(1^n)=1\right]$$

לכן, עבור אורקל כזה מתקיים:

$$\left|\Pr_{k \in \{0,1\}^n}\left[D_2^{f_k(\cdot)}(1^n)=1\right] - \Pr_{f \leftarrow Func_{n,2n}}\left[D^{f(\cdot)}(1^n)=1\right]\right| =$$

$$= \left| \Pr_{k \in \{0,1\}^n}\left[D_1^{H_k(\cdot)}(1^n) = 1 \right] - \Pr_{h \in Func_{n,2n}}\left[D_1^{h(\cdot)}(1^n) = 1 \right] \right| >$$



נשאיר לתרגול את f פונקציה כמוגדרת מקודם

שאלה 4: 2) נתון $G(s) = f_{0^n}(s)$ עבור כל $n \in \mathbb{N}$ ו- $s \in \{0,1\}^n$.

עלינו לבדוק האם הפונקציה G יוצרת הצרנה בהינתן כמות – מקרית?

הגדרה: נתון H פונקציה כמוגדרת מקודם עבור כל $n \in \mathbb{N}$ נגדיר $H_k : \{0,1\}^n \to \{0,1\}^{2n}$ ע"י $H_k(x) = f_k(x) \oplus f_{0^n}(x)$, כאשר f מעיל הרחבה

לכל n נסמן ב-X_n את מספר הבנים של הפרט ה-n בדור הנוכחי.

נניח, מעתה והלאה, כי הוא פונקציה שמקבלת אקראי (התפלגות) בדומה למספר הבנים של כל פרט בדור הראשון, X_0 בהתאמה (כלומר, X_1, וכך הלאה לכל השאר).

נסמן לצורך, שהוא לה $G(s) = f_{X_0}(s)$ כאשר s הוא פרמטר קבוע $0 \leq s \leq 1$ (הוא הפונקציה היוצרת של X_0 כאשר s הוא פרמטר ולא משתנה), ונניח כי G הוא פונקציה אנליטית בקטע $[0,1]$ שמקיימת $G(1) = 1$.

נגדיר $f_{X_n}(s) = P_{X_n}(s) \oplus P_{X_n}(s) = G(s)$, כאשר $P_{X_n}(s) = 0$

שאלה 5: 1.) הצפנה של הודעה $m \in \{0,1\}^{n+1}$, קלאסית על $\{0,1\}^n \to r$, ומחזיר על הצופן: $(r, G(r) \oplus m)$: $g =$

מראים כי בכלל לא משקיע הצפנה מכיוון שהיא בלתי שמישה, ובפרט אינה בלתי ניתנת לפענוח כלשהו CPA, נוכיח כאשר נגדיר: שלכל לכל יריב שפועל בזמן פולינומיאלי, ושלקבוע: A, שמתקיים $\Pr[IND_{\Pi,A}(n)=1] = 1$, לכל $n \in \mathbb{N}$.

עתה נגדיר יריב A הבא: שלוקח פרמטר בטיחות 1^n, ומחזיר את ההודעות $m_0 = 0^n$, $m_1 = 1^n$, ולאחר קבלת הצפנה $c = (r, g)$.

מתקיים: אם $G(r) \oplus g = 0^n$

אז $G(r) = g = G(r) \oplus m$

עמ' 11

שאלה 2) הוכיחו שלכל $m \in \{0,1\}^n$ הפונקציה $f_k(0^n) \oplus m$:

נוכיח כי הסכמה הנ"ל מקיימת הגדרה שלמה שמשמעה שלכל יריב A מתקיים $Adv^{CPA}_{\Pi,A}(n) \leq negl(n)$.

שאלה 5: 2) נניח בשלילה שקיים PPT A, וקיים פולינום $p(n)$, כך שמתקיים $\Pr[IND^{CPA}_{\Pi,A}(n)=1] = 1$

שמתקיים לכל n שמספיק גדול. A שמקבל 1^n כקלט, מריץ $k \leftarrow KeyGen(1^n)$

ומקבל m_0, m_1 כקלט. A בוחר c באופן אחיד, ומחזיר $Enc_k(0^n) = 0^n \oplus f_k(0^n) = f_k(0^n)$

ומחזיר m_b כך ש: $m_b = Enc_k(0^n) \oplus c = f_k(0^n) \oplus f_k(0^n) \oplus m_b$

לכן $b=0$, ולכן $m_b = m_1$ ומחזיר 1. לכן $\Pr[IND^{CPA}_{\Pi,A}(n)=1]=1$,

אבל, מכאן, מהגדרה, Π לא CPA בטוח.

$C = \mathcal{O}(O^n) \oplus m_6$.

A יהיה מקרי b' , ולהגדיר $\mathcal{D}$

יהיה 1 אחרת $b' = b$. נשלח שאילתות:

אם $f = O$, כאשר f נבחרה להיות

תמיד $Func_{n,n}$, אז קיים

שמקבל $O(O^n)$

אחוז ניכר מהפלטים שווים ל A בקלט.

לפיכך מתקיים

$$\forall n \in \mathbb{N} : \Pr_{f \leftarrow Func_{n,n}}[\mathcal{D}^{f(\cdot)}(1^n) = 1] = \frac{1}{2}$$

שמן הקלט הוא $b \in \{0,1\}$ המקורי, בהסתברות אחידה.

אם $f = f_k$ אז $\mathcal{D}$ מקיים בדיוק

עבור A זה הניסוי $IND_{\Pi,A}(n)$, ולכן מתקיים:

$$\forall n \in \mathbb{N} : \Pr_{k \leftarrow \{0,1\}^n}[\mathcal{D}^{F_k(\cdot)}(1^n) = 1] = \Pr[IND_{\Pi,A}(n) = 1] >$$

$$> \frac{1}{2} + \frac{1}{p(n)}$$

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

$$= \left| \Pr\left[IND_{\Pi,A}(n)=1\right] - \frac{1}{2} \right| > \frac{1}{p(n)}$$

שאלה 3: נגדיר הצפנה של בלוק יחיד $m \in \{0,1\}^n$, באופן הבא: $k \leftarrow \{0,1\}^n$ נבחר $r \leftarrow \{0,1\}^n$ ונגדיר:

$$(r, r \oplus f_k(r) \oplus m)$$

נוכיח כי מתקיים גם הגדרה בעלת CPA, (מתאימה הגדרה IND.

נניח בשלילה כי מתקיים גרעה CPA הגדרה, קיים לכן קיים אלגוריתם A שמנצח בהגדרה הזו בהסתברות גדולה מ $\frac{1}{2} + \frac{1}{p(n)}$ כך שעבור אינסוף ערכי $n \in \mathbb{N}$ מתקיים:

$$\Pr\left[IND^{CPA}_{\Pi,A}(n)=1\right] > \frac{1}{2} + \frac{1}{p(n)}$$

אזי נוכל לבנות אלגוריתם D עם גישה
לאורקל O ובזמן ריצה פולי' יוכל להבחין
בין F, פונקציה פסאודו-אקראית, לפונקציה
אקראית אמיתית, באופן הבא נעשה:

נגריל באופן אחיד $b \in \{0,1\}$.

[redacted]

נגריל באופן אחיד $r \in \{0,1\}^n$ ונשאל את $O(r)$.

נתן ל-A את הערך $c = (r, r \oplus O(r) \oplus m_b)$.

יהי b' ערך ההחזרה של A.

אזי D יחזיר 1 אם"מ $b = b'$, אחרת 0.

נחלק למקרים:

(*) אם $O = f_k$: נקבל כי $c = (r, r \oplus F_k(r) \oplus m_b)$,

ולכן:

$$Pr[D^{F_k(\cdot)}(1^n) = 1] = Pr[IND^{CPA}_{\Omega,A}(n) = 1] \geq \frac{1}{2} + \frac{1}{p(n)}$$

(*) אם $O = f$: אזי ההסתברות ש-A מנחש נכון, ולכן: $Pr[D^{f(\cdot)}(1^n) = 1] = \frac{1}{2}$

ולכן:

סימון: מספר אינסופי של ערכי $n \in \mathbb{N}$ מקיימים:

$$\left|\Pr\left[D^{f_k(\cdot)}(1^n)=1\right]-\Pr\left[D^{f(\cdot)}(1^n)=1\right]\right| > \frac{1}{2}+\frac{1}{p(n)}-\frac{1}{2}=\frac{1}{p(n)}$$

משמעות לפונקציה f פסאודו-אקראית

הגדרה 3: 1.) פונקציה $l: \mathbb{N} \to \mathbb{N}$ נקראת פשוטה אם l חסומה על ידי פולינום ו $\forall n \in \mathbb{N}$. תהא f פונקציה יעילה חישובית כלשהי, ויהי $(KeyGen, f)$ כזוג: $KeyGen: \{0,1\}^n \to \{0,1\}^{l(n)}$

ו $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^{l(n)}$.

f פסאודו-אקראית, אם לכל מבחן D יעיל שמקבל כקלט 1^n כאשר $n \in \mathbb{N}$, קיים $N \in \mathbb{N}$ כך שלכל $n > N$ קיימת פונקציה זניחה $V(\cdot)$ שמקיימת:

$$\left|\Pr_{k \leftarrow KeyGen(1^n)}\left[D^{f_k(\cdot)}(1^n)=1\right]-\Pr_{f \leftarrow Func_{n \to l(n)}}\left[D^{f(\cdot)}(1^n)=1\right]\right| \leq V(n)$$

$k \leftarrow KeyGen(1^n)$

שאלה 6: 2) נתבונן ב- $(KeyGen', F')$

המוגדרת

על ידי $KeyGen'$, המשתמש קלט 1^n,

ומפלט $k \leftarrow KeyGen(1^n)$ ומפלט f_k,

כאשר: $KeyGen': \{0,1\}^n \to \{0,1\}^{l(n)}$.

עבור F', המשתמש הנקלט $m \in \{0,1\}^n$

ראשונה, ואז משתמש $KeyGen'(1^n) \to k$,

ומפלט את $f_k(m)$. וזהו: $f_k: \{0,1\}^n \to \{0,1\}^{l(n)}$.

נותר להוכיח כי f הינה פונקציה פסאודו-

אקראית, בהנחה כי קיימת פונקציה

פסאודו-אקראית. לפי שאלה קודמת

כיצד $KeyGen'$ ו- F' פונקציה

פסאודו-אקראית, נובע כי קיימת

בין f לבין פונקציה $f \leftarrow Func_{n,l(n)}$

שבוחרת אקראי, ולכן קיים לה מרחק

בין $KeyGen'$ לבין פונקציה שבוחרת אקראי

את $Func_{n,l(n)}$, לפי $KeyGen'$ מ"ג-ו- אפשרי

אחיד פולינומי.

שאלה 7: הוכח או הפרך: אם קיים PRF
$(KeyGen, F)$ אז קיים PRF $(KeyGen', F')$
שעמיד ל-leftmost-bit leakage resilient
(בהקשר של LBLR) m (כאשר m פולינום בפרמטר
הביטחון n). $KeyGen'$ מוגדר כך: $KeyGen'(1^n)$ מגריל
$k \leftarrow \{0,1\}^{n+1}$, ומגדיר $f_k: \{0,1\}^n \to \{0,1\}^n$,
שהוא פונקציה f_k מהקבוצה $\{0,1\}^n$ לקבוצה $\{0,1\}^n$.
אז, עבור $x \in \{0,1\}^n$ נגדיר:

$$f'_k(x) = k_1 \| f_m(x)$$

כאשר: $k = k_1 \| k_2 \| \cdots \| k_{n+1}$, $m = k_2 \| \cdots \| k_{n+1}$

נניח בשלילה כי f' אינה PRP. אזי
קיים אלגוריתם D ופולינום $p(n)$ כך
שעבור אינסוף $n \in \mathbb{N}$ מתקיים:

$$\left| \Pr_{k \leftarrow KeyGen(1^n)} \left[D^{f'_k(\cdot)}(1^n, k_1) = 1 \right] - \Pr_{\substack{k \leftarrow KeyGen'(1^n) \\ f \leftarrow Func_{n,n}}} \left[D^{f(\cdot)}(1^n, k_1) = 1 \right] \right| > \frac{1}{p(n)}$$

כלומר, נבנה אלגוריתם A שישבור את
הפסאודו-אקראיות של F:

נבנה מבחין D עבור F' באופן הבא: D מקבל 1^n ו-$k_1 \in \{0,1\}^n$, ומחשב $b = D(1^n, k_1)$. D מריץ את A ומחזיר את התשובה; על שאילתה x, D עונה $O(x)\|b$. D מחזיר 1 אם A מחזיר $O(x)\|b$ עבור כל $x \notin \{0,1\}^n$, ו-0 אחרת.

אם A מחזיר 1 נחזיר 1, ואם A מחזיר 0 נחזיר 0.

ניתוח ההסתברויות:

- אם $O = F_k$ כאשר $k \leftarrow \{0,1\}^n$, אז A מקבלת O ש-f' מחזיר, כלומר:

$$\Pr_{k \leftarrow \{0,1\}^n}\left[D^{f'_k(\cdot)}(1^n, k_1) = 1\right] = \Pr_{k \leftarrow \{0,1\}^m}\left[A^{F_k(\cdot)}(1^m) = 1\right] \quad (*)$$

שכן $b = D(1^n, k_1)$ בהגדרת $(*)$.

$$A(b\|O(x)) = A(k_1\|f_m(x)) = D(x)$$

בהגדרת $(*)$.

- אם $O = f$ אז: $(f \leftarrow Func_{n,n}$ כלומר$)$

$b \| O(x) = b \| f(x) \leftarrow \{0,1\}^n$

כלומר: $Pr\left[A^{f(\cdot)}(1^n, k_1) = 1\right]$,
$k \leftarrow KeyGen'(1^n)$
$f \leftarrow Func_{n,n}$

שים b שווה 0 או 1 בהסתברות $\frac{1}{2}$ לכל f !
A מקבלת f שנבחרה מהקבוצה $Func_{n,n}$ ו-
נגדיר D כך:

$$Pr\left[D^{f(\cdot)}(1^n, k_1) = 1\right] = Pr\left[A^{f(\cdot)}(1^n) = 1\right]$$
$k \leftarrow KeyGen'(1^n)$ $\quad$ $k \leftarrow KeyGen'(1^n)$
$f \leftarrow Func_{n,n}$ $\quad$ $f \leftarrow Func_{n,n}$

לכן כפי שהגדרנו D:

$$\left| \Pr\left[A^{f_k(\cdot)}(1^n)=1\right] - \Pr\left[A^{f(\cdot)}(1^n)=1\right] \right| =$$

$k \leftarrow KeyGen(1^n)$ $\quad$ $k \leftarrow KeyGen'(1^n)$, $f \leftarrow Func_{n,n}$

$$= \left| \Pr\left[D^{f'_k(\cdot)}(1^n, k_1)=1\right] - \Pr\left[D^{f(\cdot)}(1^n, k_1)=1\right] \right| > \frac{1}{p(n)}$$

$k \leftarrow KeyGen'(1^n)$ $\quad$ $k \leftarrow KeyGen'(1^n)$, $f \leftarrow Func_{n,n}$

שאלה 7: (2) נניח ש-$(KeyGen, f)$ היא פונקציה חד-כיוונית. פונקציה חד-כיוונית – הגדרה:

נגדיר פונקציה PRF חדשה:

$$(KeyGen', F') \text{ כך ש-} KeyGen' = KeyGen$$

deftmost-bit leakage resilient (LBLR : הגדרה)

$$KeyGen(1^n) = \begin{cases} 0 \,\|\, KeyGen(1^n) & \text{הגרלה: } \frac{1}{2} \text{ הסתברות} \\ 1 \,\|\, KeyGen(1^n) & \frac{1}{2} \text{ הסתברות} \end{cases}$$

27 (עמ')

לכל $s \in \{0,1\}^n$:

$$f'_{k_1 \| k_2 \| \cdots \| k_N}(s) = k_1 \| f_{k_2 \| \cdots \| k_N}(s)$$

כאשר $k_1 \| k_2 \| \cdots \| k_N = k' \leftarrow KeyGen'$.

נניח כי $(KeyGen', F')$ הוא PRF.

יהי D' יעקב בעל יתרון משמעותי בהבחנה בין f' לבין $f'_{k'}$ כאשר $f'(\cdot)$ היא פונקציה אקראית. כלומר, קיים פולינום $p(n)$ כך שעבור מספיק גדול n מתקיים:

$$\left| Pr\left[D'^{f'_{k'}(\cdot)}(1^n) = 1\right] - Pr\left[D'^{f'(\cdot)}(1^n) = 1\right] \right| > \frac{1}{p(n)}.$$

נבנה, בעזרת D', יעקב D בעל יתרון משמעותי בהבחנה בין $f_k(\cdot)$ לבין $f(\cdot)$ כאשר f היא פונקציה אקראית. D פועל באופן הבא:

- עבור $k_1 \leftarrow \{0,1\}^n$
- הרץ את D' על s, ומענה על שאילתה x של D' יהיה $k_1 \| O(s)$.

. PRF הוא $(KeyGen', F')$ יהי

נגדיר $(KeyGen', F')$ באופן הבא: $KeyGen'$ זהה ל-$KeyGen$ של (LBLR), אלא שבמקום לבחור k באורך n, נבחר k באורך 1. $F'_k(x)$ מוגדרת להיות $f(x)$ כאשר f היא פונקציה אקראית מתוך $Func_{n,n}$, ו-$F'_k(x)$ מוגדרת להיות k כאשר x הוא 0^n (כלומר המחרוזת בת n אפסים).

טענה:

$$\left| \Pr_{k \leftarrow KeyGen'}\left[D^{F'_k(\cdot)}(1^n, k_1) = 1\right] - \Pr_{f \leftarrow Func_{n,n}}\left[D^{f(\cdot)}(1^n, k_1) = 1\right] \right| =$$

$$= \left|1 - \frac{1}{2}\right| = \frac{1}{2}$$

לכן ישנה פונקציה יעילה, למשל D^0 שמשתמשת ב-F' כדי להבחין בין F' לבין פונקציה אקראית מאותו סוג. לכן $(KeyGen', F')$ לא יכולה להיות PRF, שכן היא לא עומדת בהגדרה של (LBLR).

עמ' 30