קריפטוגרפיה 2

הרצאה 4: מתיחת גנרטורים

Textbook: Katz and Lindell. Introduction to Modern Cryptography.

מרצה: אורי שטמר

<u>תזכורת להגדרת גנרטור פסאודואקראי:</u>

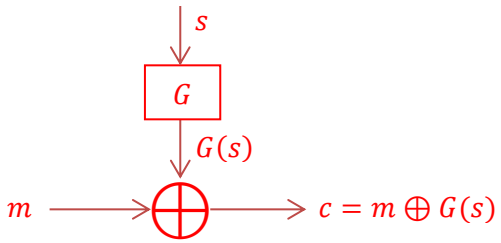
יהי $\ell(\cdot)$ פולינום ו- G אלגוריתם פולינומי (דטרמניסטי) כך שלכל n ולכל קלט $s \in \{0,1\}^n$ מתקיים $|G(s)| = \ell(n)$. נאמר ש- G הוא גנרטור (או יצרן) פסאודו אקראי אם מתקיים:

(1) <u>הרחבה:</u> לכל n מתקיים ש- $\ell(n) > n$

(2) <u>פסאודואקראיות:</u> לכל אלגוריתם (מבחין) פולינומי אקראי D קיימת פונקציה זניחה $negl$ כך שלכל n מתקיים:

$$\left| \Pr_{\substack{r \sim U_{\ell(n)} \\ D}} [D(r) = 1] - \Pr_{\substack{s \sim U_n \\ D}} [D(G(s)) = 1] \right| \leq negl(n)$$

בפעם שעברה ראינו איך אפשר להשתמש ביצרן פסאודואקראי כדי לבנות מערכת הצפנה סימטרית, כאשר בעזרת מפתח באורך n יכולנו להצפין הודעה באורך $\ell(n)$:



איך נוכל להצפין הודעות ארוכות יותר?

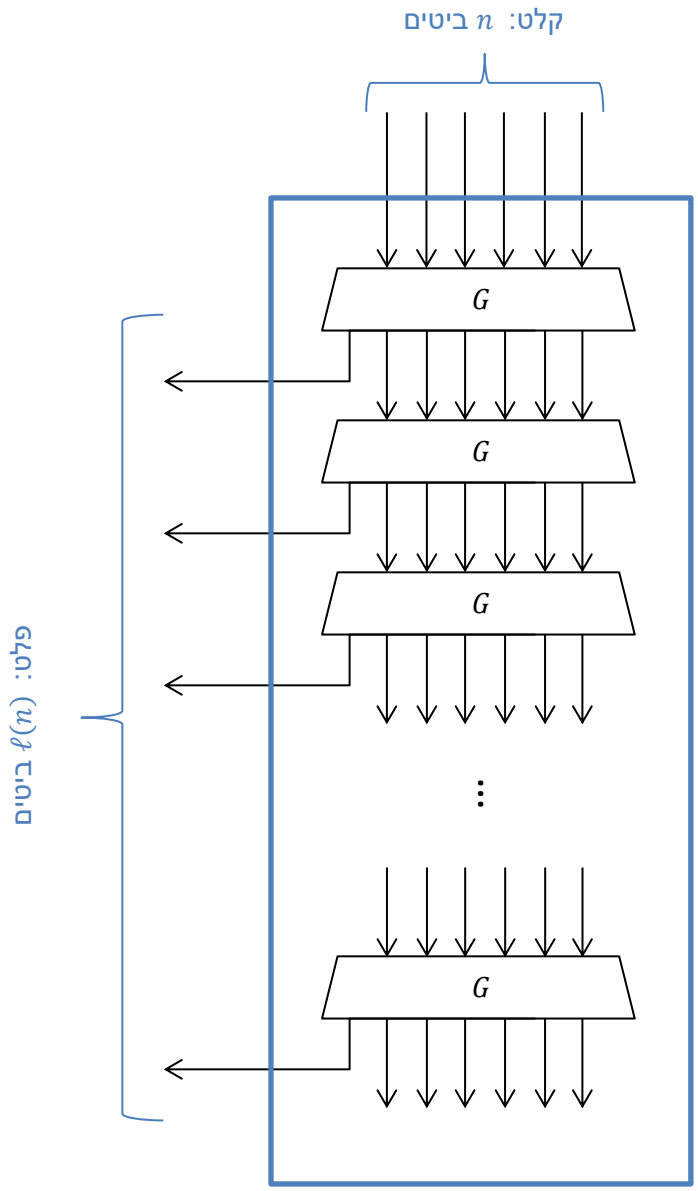
<u>משפט:</u> אם קיים גנרטור שמרחיב בביט אחד, אזי לכל פולינום $\ell(n) > n$ קיים גנרטור עם הרחבה $\ell(n)$.

<u>הוכחה:</u>

נתון גנרטור G שמרחיב בביט אחד. אנחנו רוצים להשתמש ב G כדי לבנות גנרטור עם הרחבה $\ell(n)$.

<u>הרעיון:</u> בהתחלה נרחיב מ n ביטים ל- $(n+1)$ ביטים. אחד מתוך $(n+1)$ הביטים האלה ניקח בתור הביט הראשון בפלט שלנו. על שאר הביטים נפעיל שוב את G ונקבל $(n+1)$ ביטים וכן הלאה.

בציור:



הערה: היינו יכולים לקחת לפלט את כל $(n+1)$ הביטים שמחזירה ההפעלה האחרונה של G. כאן אנחנו לא ניקח אותם לפלט כדי לפשט את הסימונים בהוכחה.

באופן פורמלי, נגדיר גנרטור G' באופן הבא:

קלט: $s \in \{0,1\}^n$
פלט: $z \in \{0,1\}^{\ell(n)}$

(1) $s_0 \leftarrow s$
(2) עבור $j = 0$ עד $\ell(n) - 1$ בצע:
   א. $(x_1, x_2, \dots, x_{n+1}) \leftarrow G(s_j)$
   ב. $z_j \leftarrow x_1$
   ג. $s_{j+1} \leftarrow (x_2, x_3, \dots, x_{n+1})$
(3) החזר את $z = (z_0, z_1, \dots, z_{\ell(n)-1})$

אנחנו רוצים להוכיח ש- G' הוא גנרטור פסאודואקראי. נוכיח זאת על ידי רדוקציה: נניח שיש יריב D' ששובר את G' בהסתברות לא זניחה ונבנה יריב D ששובר את G כדי לקבל סתירה.

מההנחה בשלילה, D' מבחין בין מחרוזת אקראית באורך $\ell(n)$ לבין מחרוזת פסאודואקראית (פלט של G') באותו האורך בהסתברות $\epsilon(n)$ לא זניחה. כלומר, D' מבחין בין ההתפלגות האחידה $U_{\ell(n)}$ לבין ההתפלגות על הפלטים של G' על קלט באורך n.

כמו שאמרנו, אנחנו רוצים להשתמש ב D' (היריב ששובר את G' מההנחה בשלילה) כדי לבנות יריב D ששובר את G. העניין הוא שבתוך G' השתמשנו/הפעלנו את G הרבה פעמים. היריב D אמור לשבור רק הפעלה אחת של G. איך נעשה כזה דבר? רעיון ההוכחה הוא רעיון שמשתמשים בו בהרבה הוכחות בקריפטוגרפיה – היברידים.

נגדיר סדרה של התפלגויות ביניים (היברידים) $H_0, H_1, \dots, H_{\ell(n)}$ שמקשרת בין ההתפלגות האחידה $U_{\ell(n)}$ לבין ההתפלגות על הפלטים של G' על קלט באורך n.

כל צעד בסדרה הזאת מתאים להפעלה נוספת של G בתוך G'.

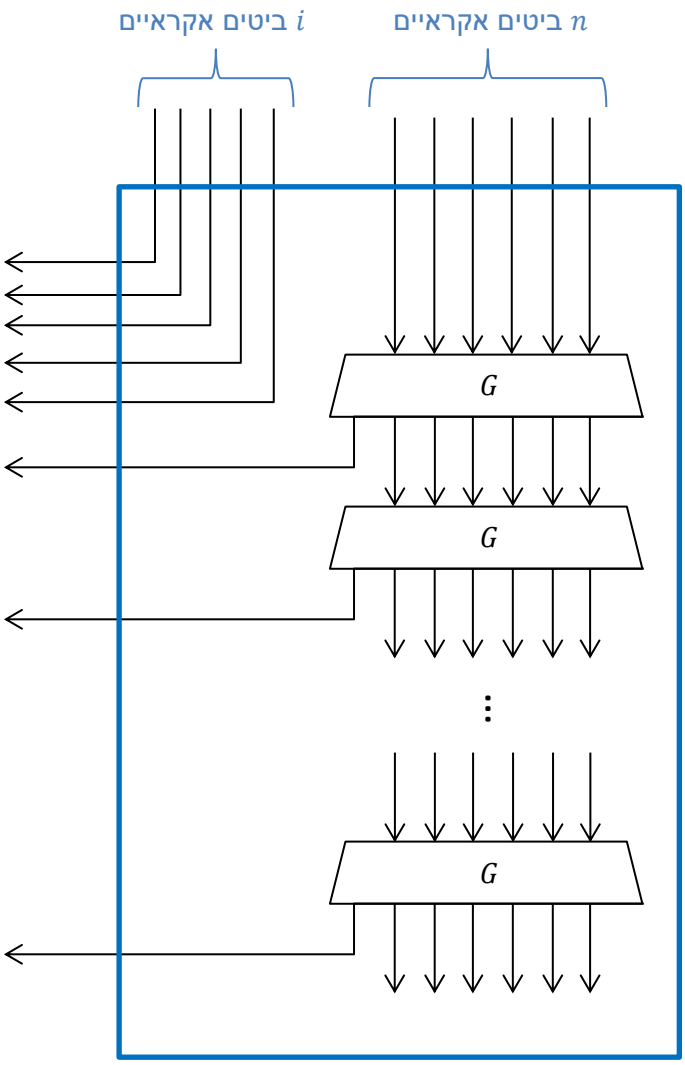
ההתפלגות H_i:

(א) הגרל $(n+i)$ ביטים באקראי $z_0, z_1, \dots, z_{n+i-1}$.

(ב) הרץ את G' משלב $j=i$ לקבלת $(\ell(n)-i)$ ביטים פסאודואקראיים $r_i, r_{i+1}, \dots, r_{\ell(n)-1}$.
כלומר:
- $s_i \leftarrow (z_i, \dots, z_{i+n-1})$
- עבור $j=i$ עד $\ell(n)-1$ בצע:
  - $(x_1, x_2, \dots, x_{n+1}) \leftarrow G(s_j)$
  - $r_j \leftarrow x_1$
  - $s_{j+1} \leftarrow (x_2, x_3, \dots, x_{n+1})$

(ג) החזר $z_0, z_1, \dots, z_{i-1}, r_i, r_{i+1}, \dots, r_{\ell(n)-1}$

H_i בציור:
מגרילים $(n+i)$ ביטים אקראיים. i מתוכם נשארים כמו שהם ואת n הביטים האחרים אנחנו מותחים כמו ב G'.



<u>אבחנה:</u>

$H_{\ell(n)}$ = מחרוזת אקראית

H_0 = פלט הגנרטור G' על קלט אקראי באורך n ביטים

<u>טענת עזר:</u> קיים i כך ש-

$$\left| \Pr_{\substack{r\sim H_i \\ D'}}[D'(r)=1] - \Pr_{\substack{r\sim H_{i-1} \\ D'}}[D'(r)=1] \right| \geq \frac{\epsilon(n)}{\ell(n)}$$

<u>הוכחת טענת העזר:</u>

$$\epsilon(n) = \left| \Pr_{\substack{r\sim U_{\ell(n)} \\ D'}}[D'(r)=1] - \Pr_{\substack{s\sim U_n \\ D'}}[D'(G'(s))=1] \right|$$

$$= \left| \Pr_{\substack{r\sim H_{\ell(n)} \\ D'}}[D'(r)=1] - \Pr_{\substack{s\sim H_0 \\ D'}}[D'(r)=1] \right|$$

$$= \left| \Pr_{\substack{r\sim H_{\ell(n)} \\ D'}}[D'(r)=1] - \Pr_{\substack{r\sim H_{\ell(n)-1} \\ D'}}[D'(r)=1] + \Pr_{\substack{r\sim H_{\ell(n)-1} \\ D'}}[D'(r)=1] - \cdots + \Pr_{\substack{s\sim H_1 \\ D'}}[D'(r)=1] + \Pr_{\substack{s\sim H_0 \\ D'}}[D'(r)=1] \right|$$

$$\leq \sum_{i=1}^{\ell(n)} \left| \Pr_{\substack{r\sim H_i \\ D'}}[D'(r)=1] - \Pr_{\substack{r\sim H_{i-1} \\ D'}}[D'(r)=1] \right|$$

כלומר, קיים i כך שההפרש הוא לפחות $\frac{\epsilon(n)}{\ell(n)}$.
כלומר, לכל n קיים i_n כך ש- D' מבחין בין ההיבריד H_{i_n} לבין ההיבריד H_{i_n+1}.
זה מסיים את הוכחת טענת העזר.

<u>נחזור להוכחת המשפט:</u>

איפה אנחנו עומדים בהוכחה? התחלנו מגנרטור פסאודואקראי G שמרחיב בביט אחד ובנינו ממנו גנרטור G' שמרחיב ב $\ell(n)$ ביטים. כדי להוכיח ש- G' הוא באמת גנרטור פסאודואקראי אנחנו רוצים להראות שאם יש מבחין D' ששובר את G' אז נוכל לבנות ממנו מבחין D ששובר את G, מה שלא יתכן, ולכן G' בטוח. אז הנחנו בשלילה שיש מבחין D' ששובר את G', ועכשיו אנחנו צריכים לבנות ממנו מבחין D עבור G. לצורך כך נשתמש במה שהוכחנו בטענת העזר: קיים i_n כך ש- D' מבחין בין ההיבריד H_{i_n} לבין ההיבריד H_{i_n+1}.

תאור המבחין D:

קלט: $r = (r_0, r_1, r_2, \dots, r_n) \in \{0,1\}^{n+1}$ (D אמור להבחין האם r אקראי או פלט של G)

(1) הגרל $i_n - 1$ ביטים אקראיים $z_0, \dots, z_{i_n-2}$

(2) $z_{i_n-1} \leftarrow r_0$

(3) הרץ את G' משלב $j = i_n$ לקבלת $(\ell(n) - i_n)$ ביטים פסאודואקראיים. כלומר:

- $s_{i_n} \leftarrow (r_1, \dots, r_n)$
- עבור $j = i_n$ עד $\ell(n) - 1$ בצע:
  - $(x_1, \dots, x_{n+1}) \leftarrow G(s_j)$
  - $y_j \leftarrow x_1$
  - $s_{j+1} \leftarrow (x_2, \dots, x_{n+1})$

(4) הפעל $D'(z_0, \dots, z_{i_n-2}, z_{i_n-1}, y_{i_n}, \dots, y_{\ell(n)-1})$ וענה כמוהו.

נבחן שני מקרים:

- אם r אקראי אזי $z_{i_n-1} = r_0$ אקראי ולכן $z_0, z_1, \dots, z_{i_n-1}$ אקראיים. בנוסף, בשלב (3) הפעלנו את G' על מחרוזת אקראית $r_1, \dots, r_n$ במשך $\ell(n) - i_n$ צעדים. לכן בשלב (4) הפעלנו את D' על פלט אקראי של H_{i_n}.

- אם $r = G(s)$ אזי $z_0, \dots, z_{i_n-2}$ אקראיים ו- $(z_{i_n-1}, y_{i_n}, \dots, y_{\ell(n)-1})$ נוצרו על ידי G', כלומר הפעלנו את D' על פלט אקראי מ- H_{i_n-1}.

לכן, על פי טענת העזרת נקבל:

$$\left|\Pr[D(r)=1] - \Pr\left[D\left(G(s)\right)=1\right]\right| = \left|\Pr_{\substack{r\sim H_i \\ D'}}[D'(r)=1] - \Pr_{\substack{r\sim H_{i-1} \\ D'}}[D'(r)=1]\right| \geq \frac{\epsilon(n)}{\ell(n)}$$

מכיוון ש- $\ell(\cdot)$ הוא פולינום, אנו יודעים שאם $\epsilon(n)$ היא לא פונקציה זניחה אזי גם $\frac{\epsilon(n)}{\ell(n)}$ היא לא פונקציה זניחה, בסתירה לכך ש- G יצרן פסאודו אקראי.

זה מסיים את הוכחת המשפט.

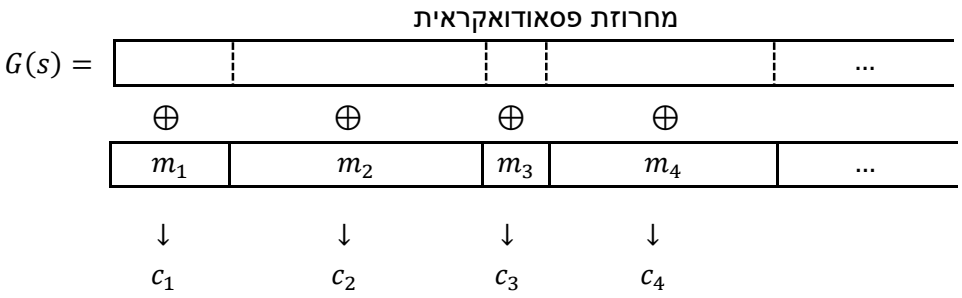
הערות לגבי המבחין D שבנינו:

- בהוכחה ראינו כי לכל n קיים i_n כך ש- D' מבחין בין H_{i_n} לבין H_{i_n-1}.
- המבחין D שבנינו הכיר את הסדרה $i_1, i_2, \dots$. איך זה יכול להיות?
- המבחין D שבנינו הוא לא-אחיד. יריב לא אחיד יכול לקבל עיצה באורך פולינומי (עיצה שונה לכל ערך של n). במקרה שלנו העיצה היא i_n.
- מה שקיבלנו זה שאם G בטוח כנגד יריבים לא-אחידים (פחות טוב – הנחה יותר חזקה) אזי G' שבנינו יהיה בטוח כנגד יריבים לא-אחידים (יותר טוב – תוצאה חזקה)
- בתרגיל הבית תראו איך אפשר להימנע מהצורך הזה לדעת את i_n.

בטיחות בהצפנות מרובות

אנחנו רוצים לבנות עכשיו מערכת הצפנה שתהייה בטוחה כנגד הצפנות מרובות. ישנן 2 גישות לכך:

גישה 1 – מודל סינכרוני:



חיסרון: צריך לתחזק "מצב" – מספר הביטים של $G(s)$ בהם כבר השתמשנו.

גישה 2:

נגדיר "יצרן פסאודואקראי משוכלל" המקבל כקלט שתי מחרוזות k, x באורך n ביטים כל אחת ומחזיר מחרוזת באורך n ביטים. נדרוש ש- $G(k,x)$ הוא פסאודואקראי גם אם x ידוע למבחין. בנוסף, נדרוש שאם הרצנו את $G(k,\cdot)$ הרבה פעמים (עם מחרוזת x שונה בכל פעם, אבל עם אותה מחרוזת k), אז גם השרשור של כל הפלטים של G שנקבל בצורה הזאת יהיה פסאודואקראי (גם אם ה-x-ים שהשתמשנו בהם ידועים ליריב).

כלומר, מתוך $G(k,\cdot)$ אנחנו יכולים לחלץ המון מחרוזות פסאודואקראיות. לכן, באופן דומה לגישה 1, נוכל להשתמש ביצרן כזה כדי לבנות מערכת הצפנה עם מצב:

$G(k,1)$	$G(k,2)$	$G(k,3)$	$G(k,4)$	...
$\oplus$	$\oplus$	$\oplus$	$\oplus$	
m_1	m_2	m_3	m_4	...
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	
c_1	c_2	c_3	c_4	

אבל בעצם, במקום לזכור את המצב (האינדקס x כך שבהפעלה הבאה אנחנו אמורים להשתמש ב $G(k,x)$), אנחנו יכולים פשוט להגריל אותו. כל עוד נצפין מספר פולינומי (ב- n) של הודעות, אז בהסתברות גבוהה לא נשתמש באותה מחרוזת x פעמיים.

כלומר, כדי להצפין הודעה m עם מפתח k, נגריל $x \in \{0,1\}^n$ ונחזיר את הצופן

$$(x, c) = (x, G(k,x) \oplus m)$$

(כלומר את x אנחנו מגלים כחלק מהצופן)

בציור:

$x_1 \sim U_n$	$x_2 \sim U_n$	$x_3 \sim U_n$	$x_4 \sim U_n$	...
$G(k,x_1)$	$G(k,x_2)$	$G(k,x_3)$	$G(k,x_4)$	...
$\oplus$	$\oplus$	$\oplus$	$\oplus$	
m_1	m_2	m_3	m_4	...
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	
(x_1, c_1)	(x_2, c_2)	(x_3, c_3)	(x_4, c_4)	

כדי לפענח צופן (x,c) בעזרת המפתח k נחשב

$$m = c \oplus G(k,x)$$

"יצרן פסאודואקראי משוכלל" כזה נקרא ***פונקציה פסאודואקראית***.
בהרצאה הבאה נגדיר את המושג הזה באופן פורמלי.