הרצאה 8: פונקציות חד-כיווניות וביט קשה (המשך)

Textbook: Katz and Lindell. Introduction to Modern Cryptography.

מרצה: אורי שטמר

בשביל ההוכחה המלאה של המשפט של GL נצטרך עוד קצת רגע מהסתברות:

משפט (אי-שיוויון צ'בישב): יהי X משתנה מקרי עם תוחלת $\mathbb{E}[X]$ ועם שונות $Var[X] = \mathbb{E}[(X - \mathbb{E}[X])^2]$. אזי לכל $\delta > 0$ מתקיים:

$$\Pr\left[\ |X - \mathbb{E}[X]| \geq \delta\ \right] \leq \frac{Var[X]}{\delta^2}$$

הוכחה:

$$\Pr\left[\ |X - \mathbb{E}[X]| \geq \delta\ \right] = \Pr\left[\ (X - \mathbb{E}[X])^2 \geq \delta^2\ \right] \underset{\text{מרקוב}}{\leq} \frac{\mathbb{E}[(X - \mathbb{E}[X])^2]}{\delta^2} = \frac{Var[X]}{\delta^2}$$

הגדרה: משתנים מקריים $X_1, X_2, \dots, X_m$ הם בלתי תלויים בזוגות אם לכל $i \neq j$ מתקיים ש- X_i, X_j הם ב"ת.

דוגמה: נגדיר 3 מ"מ $X_1, X_2, X_3 \in \{0,1\}$ באופן הבא:

- $X_1, X_2 \in \{0,1\}$ מתפלגים אחיד ובאופן ב"ת
- $X_3 = X_1 \oplus X_2$

אזי X_1, X_2, X_3 הם ב"ת בזוגות (למרות שהשלשה X_1, X_2, X_3 אינה ב"ת...)

עובדה: אם $X_1, \dots, X_m$ הם בלתי תלויים בזוגות, אזי

$$Var\left[\sum_{i=1}^{m} X_i\right] = \sum_{i=1}^{m} Var[X_i]$$

(נובע מההגדרה של שונות בצירוף העובדה כי אם X_i, X_j בלתי תלויים אזי $\mathbb{E}[X_i \cdot X_j] = \mathbb{E}[X_i] \cdot \mathbb{E}[X_j]$)

משפט: נקבע $\epsilon > 0$ ו- $b \in \{0,1\}$. יהיו $X_1, \dots, X_m$ משתנים מקריים בינאריים ב"ת בזוגות כך שלכל i מתקיים $\Pr[X_i = b] \geq \frac{1}{2} + \epsilon$. (כלומר, לכל i ההסתברות ש- X_i מנחש את b היא קצת יותר מ- ½.)
נסמן ב- X_{maj} את החלטת הרוב מבין $X_1, \dots, X_m$. אזי

$$\Pr[X_{maj} \neq b] \leq \frac{1}{4 \cdot \epsilon^2 \cdot m}$$

(כלומר, אם m מספיק גדול אז ההסתברות שהחלטת הרוב טועה בניחוש b היא קטנה...)

הוכחה: נניח כי $b = 1$ (ההוכחה סמטרית עבור $b = 0$). נסמן $\tilde{\epsilon}$ כך ש- $\mathbb{E}\left[\frac{\sum_{i=1}^{m} X_i}{m}\right] = \frac{1}{2} + \tilde{\epsilon}$ ונשים לב ש- $\tilde{\epsilon} \geq \epsilon$ מכיוון שמתקיים:

$$\frac{1}{2} + \tilde{\epsilon} = \mathbb{E}\left[\frac{\sum_{i=1}^{m} X_i}{m}\right] = \frac{1}{m}\sum_{i=1}^{m} \mathbb{E}[X_i] = \frac{1}{m}\sum_{i=1}^{m} \Pr[X_i = 1] \underbrace{\geq}_{\text{כי } b=1} \frac{1}{2} + \epsilon$$

נחשב:

$$\Pr[X_{maj} \neq 1] = \Pr\left[\sum_{i=1}^{m} X_i \leq \frac{m}{2}\right] = \Pr\left[\frac{\sum_{i=1}^{m} X_i}{m} - \frac{1}{2} \leq 0\right] = \Pr\left[\frac{\sum_{i=1}^{m} X_i}{m} - \left(\frac{1}{2} + \tilde{\epsilon}\right) \leq -\tilde{\epsilon}\right]$$

$$\leq \Pr\left[\left|\frac{\sum_{i=1}^{m} X_i}{m} - \left(\frac{1}{2} + \tilde{\epsilon}\right)\right| \geq \tilde{\epsilon}\right] \underbrace{\leq}_{\text{צבישב}} \frac{Var\left[\frac{\sum_{i=1}^{m} X_i}{m}\right]}{\tilde{\epsilon}^2} \underbrace{=}_{\text{ב"ת בזוגות}} \frac{\frac{1}{m^2}\sum_{i=1}^{m} Var[X_i]}{\tilde{\epsilon}^2} \underbrace{\leq}_{\substack{\text{השונות של מ"מ בינארי היא תמיד} \\ \text{לכל היותר } \frac{1}{4}}} \frac{\frac{1}{m^2} \cdot \frac{m}{4}}{\tilde{\epsilon}^2}$$

$$= \frac{1}{4 \cdot \tilde{\epsilon}^2 \cdot m} \leq \frac{1}{4 \cdot \epsilon^2 \cdot m}$$

עכשיו אנחנו יכולים לחזור להוכחה ש- GL היא ביט קשה.

<u>תזכורת:</u> עבור פונקציה חד-כיוונית f הגדרנו $g(x,r) = (f(x), r)$ והגדרנו $GL(x,r) = \oplus_{i=1}^{n} x_i \cdot r_i$. צ"ל GL היא ביט קשה עבור g.

נוכיח את המשפט הבא:

<u>משפט:</u> אם קיים אלגוריתם $\mathcal{A}$ הסתברותי פולינומי ופולינום p כך שלאינסוף ערכי n מתקיים

$$\Pr_{\substack{x\in\{0,1\}^n \\ r\in\{0,1\}^n \\ \mathcal{A}}}[\mathcal{A}(f(x),r) = GL(x,r)] \geq \frac{1}{2} + p(n)$$

אזי קיים אלגוריתם $\mathcal{B}$ הסתברותי פולינומי ופולינום q כך שלאותם ערכי n מתקיים:

$$\Pr_{x,\mathcal{B}}[\mathcal{B}(f(x)) \in f^{-1}(f(x))] \geq \frac{1}{q(n)}$$

(ולכן אם f חד-כיוונית אז לא קיים $\mathcal{B}$ כזה ולכן לא קיים $\mathcal{A}$ כנ"ל ולכן GL היא ביט קשה של g)

כמו בחימום 2, אפשר להראות שיש הרבה x-ים "טובים" עבורם אם נגריל r באקראי אזי $\mathcal{A}(f(x),r)$ מצליח לנחש את $GL(x,r)$ בהסתברות טובה:

<u>למה:</u> יהי n כך ש-

$$\Pr_{\mathcal{A},x,r}[\mathcal{A}(f(x),r) = GL(x,r)] \geq \frac{1}{2} + \frac{1}{p(n)}$$

אזי קיימת $S_n \subseteq \{0,1\}^n$ שגודלה $|S_n| \geq \frac{2^n}{2 \cdot p(n)}$ כך שלכל $x \in S_n$ מתקיים:

$$\Pr_{\mathcal{A},r}[\mathcal{A}(f(x),r) = GL(x,r)] \geq \frac{1}{2} + \frac{1}{2 \cdot p(n)}$$

(ההוכחה זהה להוכחה שראינו בחימום 2)

<u>דיון:</u> מה הקושי עכשיו בהשוואה לחימום 2?
אנחנו יודעים שאם עבור r מסויים יש לנו גם את $GL(x,r)$ וגם את $GL(x, r \oplus e_i)$ אז נוכל לחשב את x_i. בחימום 2, עבור r אקראי, התקיים ש- $\mathcal{A}$ מצליח לנחש <u>כ"א</u> מ- $GL(x,r), GL(x, r \oplus e_i)$ בהסתברות $\gg$ ¾ ולכן מחסם האיחוד $\mathcal{A}$ הצליח לנחש <u>בו זמנית</u> גם את $GL(x,r)$ וגם את $GL(x, r \oplus e_i)$ בהסתברות $\gg$ ½. במקרה זה יכולנו

לחשב את x_iוהגברנו את הביטחון שלנו ע"י חזרות. העניין הוא שעכשיו $\mathcal{A}$ מנחש כ"א מהם בהסתברות $\gg \frac{1}{2}$ ולכן לא נוכל להגיד משהו מועיל על ההסתברות ש- $\mathcal{A}$ מנחש את שניהם.

הרעיון: במקום להשתמש ב- $\mathcal{A}$ כדי לנחש גם את $GL(x,r)$ וגם את $GL(x,r\oplus e_i)$ נשתמש בו רק כדי לנחש אחד מהם ואת השני "ננחש בעצמנו". ספציפית, כדי לחשב את x_i אנחנו מבצעים הרבה חזרות (עם הרבה ערכים ל- r) ומחשבים ניחוש ל- x_i:

$$\tilde{x}_i = \underbrace{GL(x,r)}_{\text{ננחש בעצמנו}} \oplus \underbrace{\mathcal{A}(f(x),r\oplus e_i)}_{\text{הניחוש של } \mathcal{A}}$$

$\left(\text{מצליח בהסתברות } \gg \frac{1}{2}\right)$

לכן, אם כל הניחושים שלנו ל- $GL(x,r)$ (על פני כל החזרות על r) הצליחו, אזי כל נסיון פוגע ב- x_i בהסתברות $\gg \frac{1}{2}$ ולכן החלטת הרוב תהייה טובה.

השאלה היא למה שהניחושים שלנו יהיו טובים. בפרט, אם כל ה-r-ים הם ב"ת ולכל r ננחש את $GL(x,r)$ באופן ב"ת אזי ההסתברות שכל הניחושים שלנו יצליחו תהייה זניחה (כי מספר החזרות הוא פולינומי...)

התשובה: במקום להגריל את ה-r-ים באופן ב"ת על פני החזרות, נגריל r-ים ב"ת בזוגות בצורה כזאת שהניחושים שלנו יצליחו (כולם ביחד) בהסתברות לא זניחה.

ספציפית, כדי לייצר m ערכים ל- r, נגריל $\ell = \lceil \log(m+1) \rceil$ מחרוזות אקראיות ב"ת $s^1, s^2, \dots, s^\ell \in \{0,1\}^n$.
עכשיו, לכל תת קבוצה לא ריקה $I \subseteq \{1,2,\dots,\ell\}$ נגדיר

$$r^I = \bigoplus_{i\in I} s^i$$

(זה מגדיר $2^\ell - 1 = 2^{\lceil \log(m+1) \rceil} - 1 \geq m$ מחרוזות r^I)

מתקיים:
(1) לכל I מתקיים ש- r^I מתפלג אחיד על $\{0,1\}^n$
(2) לכל $I \neq J$ מתקיים ש- r^I, r^J הם ב"ת (כלומר ה-r^I-ים הם ב"ת בזוגות)

הסבר ל- (2): נניח למשל שקיים אינדקס j כך ש- $j \in J$ אבל $j \notin I$. אזי s^j מתפלג אחיד ובאופן ב"ת מ- r^I. מכיוון ש- s^j משתתף ב XOR שמגדיר את r^J נקבל ש- r^J מתפלג אחיד ובאופן ב"ת מ- r^I.

אבחנה 1: בהינתן $GL(x,s^1), \dots, GL(x,s^\ell)$ ניתן לחשב את $GL(x,r^I)$ לכל $I \subseteq \{1,2,\dots,\ell\}$.

הוכחה:

$$GL(x,r^I) = GL\left(x, \bigoplus_{i\in I} s^i\right) = \bigoplus_{j=1}^{n} x_j \cdot \left(\bigoplus_{i\in I} s_j^i\right) = \bigoplus_{j=1}^{n}\left(\bigoplus_{i\in I} x_j \cdot s_j^i\right)$$

$$= \bigoplus_{i\in I}\left(\bigoplus_{j=1}^{n} x_j \cdot s_j^i\right) = \bigoplus_{i\in I} GL(x,s^i)$$

אבחנה 2: אם ננחש את $GL(x,s^1), \dots, GL(x,s^\ell)$ ע"י הגרלת ביט ב"ת לכל אחד מהם, אז כל הניחושים ביחד מצליחים בהסתברות $\frac{1}{2^\ell} \approx \frac{1}{m}$, כאשר $m = poly(n)$ הוא מספר החזרות.

בעזרת 2 האבחנות האלה נוכל לבנות אלגוריתם שמתוך $f(x)$ מחשב את x, באופן דומה למה שעשינו בחימום 2:

אלגוריתם $\mathcal{B}$ להיפוך f:

קלט: $y = f(x)$

(1) סמן $m = 2 \cdot n \cdot p^2(n)$ וסמן $\ell = \lceil \log(m+1) \rceil$

(2) הגרל בהתפלגות אחידה ובאופן ב"ת $s^1, \dots, s^\ell \in \{0,1\}^n$ ו- $\sigma^1, \dots, \sigma^\ell \in \{0,1\}$

(3) לכל תת קבוצה לא ריקה $I \subseteq \{1,2,\dots,\ell\}$ חשב $r^I = \oplus_{i \in I} s^i$ ו- $\sigma^I = \oplus_{i \in I} \sigma^I$

(4) עבור $j = 1,2,\dots,n$ בצע:

(א) לכל תת קבוצה לא ריקה $I \subseteq \{1,2,\dots,\ell\}$ חשב $x_j^I = \sigma^I \oplus \mathcal{A}(y, r^I \oplus e_j)$

(ב) קבע $z_j = \text{majority}\{x_j^I : I \subseteq \{1,2,\dots,\ell\}, I \neq \emptyset\}$

(5) החזר $z = z_1 z_2 \dots z_n$

<u>ניתוח:</u> נקבע $x \in S_n$ ונניח כי לכל $1 \leq i \leq \ell$ מתקיים $\sigma^i = GL(x, s^i)$. במקרה זה, לכל $I \subseteq \{1,2,\dots,\ell\}$ לא ריקה מתקיים $\sigma^I = GL(x, r^I)$. נקבע קואורדינטה $1 \leq j \leq n$. לכל I לא ריקה מתקיים:

$$\Pr_{r^I, \mathcal{A}}[x_j^I = x_i] \underbrace{\geq}_{\text{כי אנחנו מניחים ש } \sigma^I = GL(x, r^I)} \Pr_{r^I, \mathcal{A}}[\mathcal{A}(f(x), r^I \oplus e_j) = GL(x, r^I \oplus e_j)] \underbrace{\geq}_{\substack{x \in S_n \text{ כי} \\ r^I \oplus e_j \text{ וכי} \\ \text{מתפלג אחיד ב } \{0,1\}^n}} \frac{1}{2} + \frac{1}{2 \cdot p(n)}$$

בנוסף, המשתנים $\{x_j^I\}_{I \subseteq \{1,2,\dots,\ell\}}$ הם ב"ת בזוגות מכיוון ש- $\{r^I\}_{I \subseteq \{1,2,\dots,\ell\}}$ הם ב"ת בזוגות. לפי המשפט שראינו לגבי החלטת הרוב מבין אינדוקטורים ב"ת בזוגות, מתקיים:

$$\Pr[\underbrace{z_j}_{=\text{maj}\{x_j^I\}} \neq x_j] \leq \frac{1}{4 \cdot \left(\frac{1}{2 \cdot p(n)}\right)^2 \cdot (2^\ell - 1)} \underbrace{\leq}_{\ell \text{ הצבת}} \frac{1}{2n}$$

כלומר, כל קואו' של x אנחנו מנחשים נכון בהסתברות $\geq \left(1 - \frac{1}{2n}\right)$. לפי חסם האיחוד, אנחנו מנחשים נכון את <u>כל</u> x בהסתברות $\geq \frac{1}{2}$.

<u>בסה"כ:</u> בהסתברות לפחות $\frac{1}{2 \cdot p(n)}$ מתקיים ש- $x \in S_n$. בנוסף, באופן ב"ת, בהסתברות לפחות $1/2^\ell$ אנחנו מנחשים נכון את כל ה-σ^i-ים. כשזה קורה, אנחנו מחזירים $z = x$ בהסתברות לפחות $1/2$. לכן,

$$\Pr[\mathcal{B}(f(x)) = x] \geq \frac{1}{2 \cdot p(n)} \cdot \frac{1}{2^\ell} \cdot \frac{1}{2} \geq \frac{1}{2 \cdot p(n)} \cdot \frac{1}{5 \cdot n \cdot p^2(n)} \cdot \frac{1}{2} = \frac{1}{20 \cdot n \cdot p^3(n)}$$

אז אנחנו יודעים לייצר ביטים קשים עבור פונקציה/פרמוטציה חד-כיוונית. עכשיו אנחנו רוצים להשתמש בזה כדי לבנות גנרטור פסאודואקראי.

<u>משפט:</u> אם קיימת פרמוטציה חד-כיוונית אזי קיים גנרטור המרחיב בביט אחד.

<u>הוכחה:</u>

תהי f פרמוטציה חד-כיוונית שיש לה ביט קשה $hc: \{0,1\}^* \to \{0,1\}$

(על פי המשפט שהוכחנו לגבי קיום של ביט קשה, זה בלי הגבלת הכלליות...)
נגדיר $G(s) = \big(f(s), hc(s)\big)$.
נראה כי לכל מבחין אקראי D קיימת פונקציה זניחה $negl$ כך ש-
$$\Pr_{r\in\{0,1\}^{n+1}}[D(r)=1] - \Pr_{s\in\{0,1\}^n}\big[D\big(G(s)\big)=1\big] \le negl(n)$$
(טיעון דומה יראה שגם הכיוון השני נכון)

<u>מצד אחד:</u>

$$\Pr_{r\in\{0,1\}^{n+1}}[D(r)=1] = \Pr_{\substack{r\in\{0,1\}^n \\ r'\in\{0,1\}}}[D(r\circ r')=1] \overset{\text{כי } f \text{ פרמוטציה}}{=} \Pr_{\substack{s\in\{0,1\}^n \\ r'\in\{0,1\}}}[D(f(s)\circ r')=1]$$

$$= \frac{1}{2}\cdot \Pr_{s\in\{0,1\}^n}\big[D\big(f(s)\circ hc(s)\big)=1\big] + \frac{1}{2}\cdot \Pr_{s\in\{0,1\}^n}\big[D\big(f(s)\circ \overline{hc(s)}\big)=1\big]$$

<u>ומצד שני:</u>

$$\Pr_{s\in\{0,1\}^n}\big[D\big(G(s)\big)=1\big] = \Pr_{s\in\{0,1\}^n}\big[D\big(f(s)\circ hc(s)\big)=1\big]$$

כלומר אנחנו צריכים להוכיח כי

$$\epsilon(n) = \frac{1}{2}\Big(\Pr_{s\in\{0,1\}^n}\big[D\big(f(s)\circ \overline{hc(s)}\big)=1\big] - \Pr_{s\in\{0,1\}^n}\big[D\big(f(s)\circ hc(s)\big)=1\big]\Big) \le negl(n)$$

נראה יריב שמנחש את הביט הקשה בהסתברות $\frac{1}{2}+\epsilon(n)$ (מה שמוכיח ש- ϵ שניח...)

<u>היריב $\mathcal{A}$:</u> קלט $y=f(s)$ עבור $s\in\{0,1\}^n$ אקראי
(1) הגרל $r'\in\{0,1\}$ אקראי
(2) הרץ $D(f(s)\circ r')$. אם D מחזיר 0 החזר r' ואחרת החזר $\overline{r'}$.

נחשב:

$$\Pr_{s\in\{0,1\}^n}\big[\mathcal{A}\big(f(s)\big)=hc(s)\big] =$$

$$= \frac{1}{2}\cdot \Pr_{s\in\{0,1\}^n}\big[\mathcal{A}\big(f(s)\big)=hc(s)\big|r'=hc(s)\big] + \frac{1}{2}\cdot \Pr_{s\in\{0,1\}^n}\Big[\mathcal{A}\big(f(s)\big)=hc(s)\Big|r'=\overline{hc(s)}\Big]$$

$$= \frac{1}{2}\cdot \Pr_{s\in\{0,1\}^n}\big[D\big(f(s)\circ hc(s)\big)=0\big] + \frac{1}{2}\cdot \Pr_{s\in\{0,1\}^n}\Big[D\Big(f(s)\circ \overline{hc(s)}\Big)=1\Big]$$

$$= \frac{1}{2}\Bigg(\Big(1-\Pr_{s\in\{0,1\}^n}\big[D\big(f(s)\circ hc(s)\big)=1\big]\Big) + \Pr_{s\in\{0,1\}^n}\Big[D\Big(f(s)\circ \overline{hc(s)}\Big)=1\Big]\Bigg) = \frac{1}{2}+\epsilon(n)$$

כיוון ש- hc ביט קשה, ההסתברות ש- $\mathcal{A}$ מנחש אותו חסומה ע"י $\frac{1}{2}+negl(n)$, כלומר ϵ פונקציה זניחה כנדרש.