

## הרצאה 12: הצפנה במפתח פומבי

Textbook: Katz and Lindell. Introduction to Modern Cryptography.

מרצה: אורי שטמר

תזכורת: מערכת הצפנה במפתח פומבי מורכבת מ-3 אלגוריתמים פולינומיים:

<b>Gen</b>	אלגוריתם אקראי לייצור מפתחות קלט: פרמטר בטיחות $1^n$ פלט: זוג מפתחות $pk, sk$
<b>Enc</b>	אלגוריתם אקראי להצפנה קלט: הודעה $m$ ומפתח פומבי $pk$ פלט: צופן $c$
<b>Dec</b>	אלגוריתם פענוח (בדרך כלל דטרמיניסטי) קלט: צופן $c$ ומפתח פרטי $sk$ פלט: הודעה $m$

**משחק הבחנה עבור מערכת הצפנה במפתח פומבי  $\Pi = (Gen, Enc, Dec)$  ועבור יריב  $\mathcal{A}$** 

1.  $(pk, sk) \leftarrow Gen(1^n)$
2. היריב  $\mathcal{A}$  מופעל על  $pk$  ובוחר זוג מסרים  $m_0, m_1$  כך ש-  $|m_0| = |m_1|$ . היריב שולח את ההודעות למצפין.
3. המצפין בוחר ביט  $b \in \{0,1\}$  באקראי, מחשב  $c \leftarrow Enc(m_b, k)$  ושולח את  $c$  ליריב.
4. היריב (צריך לנחש את  $b$ ) מחזיר ניחוש  $\hat{b}$ . היריב מנצח אם  $\hat{b} = b$ .

**הגדרה:** למערכת הצפנה במפתח פומבי  $\Pi$  יש הצפנות בלתי מובחנות מפני מאזין (EAV-בטוחה) אם לכל יריב פולינומי אקראי  $\mathcal{A}$  קיימת פונקציה זניחה  $negl$  כך שלכל  $n$  מתקיים

$$\Pr[\mathcal{A} \text{ מנצח}] \leq \frac{1}{2} + negl(n)$$

מהם ההבדלים מהגדרת EAV-בטיחות עבור מערכת הצפנה במפתח סימטרי?

1. היריב  $\mathcal{A}$  מקבל את המפתח הפומבי  $pk$
2. היריב  $\mathcal{A}$  יכול לבחור את ההודעות  $m_0, m_1$  על סמך המפתח הפומבי

מכיוון שהיריב מקבל את המפתח הפומבי  $pk$ , לאורך כל המשחק הוא יכול להצפין הודעות כרצונו. לכן, במקרה של מערכת הצפנה במפתח פומבי אין הבדל בין EAV-בטיחות לבין CPA-בטיחות (זה לא היה נכון עבור מערכת הצפנה במפתח סימטרי)

**אבחנה:** אם מערכת הצפנה במפתח פומבי  $\Pi$  היא EAV-בטוחה אז היא CPA-בטוחה.

ראינו איך לבנות מערכת הצפנה במפתח סימטרי מתוך פרמוטציה חד-כיוונית. כדי לבנות מערכת הצפנה במפתח פומבי, נתחיל מפרימיטיב חזק יותר:

**הגדרה:** פרמוטציה חד-כיוונית עם trapdoor מורכבת משלושה אלגוריתמים פולינומיים  $(Gen, f, Inv)$  כך ש:

$$(k, k_{inv}) \leftarrow Gen(1^n) \quad (1)$$

$$f_k(\cdot) = f(k, \cdot) \text{ היא פרמוטציה מ } \{0,1\}^n \text{ ל- } \{0,1\}^n \quad (2)$$

$$Inv(k_{inv}, y) = x \text{ אזי } y \leftarrow f(k, x) \text{ וגם } (k, k_{inv}) \leftarrow Gen(1^n) \text{ אם } x \in \{0,1\}^n \text{ מתקיים:} \quad (3)$$

$$\text{לכל יריב פולינומי אקראי } \mathcal{A} \text{ קיימת פונקציה זניחה } \text{negl} \text{ כך ש} \quad (4)$$

$$\Pr_{x,k}[\mathcal{A}(1^n, k, f_k(x)) = x] \leq \text{negl}(n)$$

כאשר האקראיות היא מעל  $(k, k_{inv})$  המיוצרים על פי אלגוריתם  $Gen$ , מעל הגרלת  $x \in \{0,1\}^n$  בהתפלגות אחידה, ומעל האקראיות של  $\mathcal{A}$ .

דרישה (4) אומרת שבלי  $k_{inv}$  קשה להפוך את  $f_k$ , אבל דרישה (3) אומרת שביהנתן  $k_{inv}$  קל להפוך את  $f_k$ .

**דוגמה: בנייה של פרמוטציה חד-כיוונית עם trapdoor מתוך הנחת RSA**

•  $Gen(1^n)$

1. הגרל  $p, q$  שני ראשוניים בני  $n$  ביטים והגדר  $N = p \cdot q$

2. חשב  $\phi(N) = (p-1)(q-1)$

3. הגרל  $e$  זר ל-  $\phi(N)$ , כלומר  $\gcd(e, \phi(N)) = 1$

4. חשב  $d = e^{-1} \bmod \phi(N)$

5. החזר  $k = (N, e), k_{inv} = (N, e, d)$

•  $f_k(x) = x^e \bmod N$

•  $Inv(k_{inv}, y) = y^d \bmod N$

המשפט הבא מתקבל בצורה דומה למה שעשינו בהרצאות 7-8:

**משפט:** לכל פרמוטציה חד-כיוונית עם trapdoor קיימת פרמוטציה חד-כיוונית עם trapdoor שיש לה ביט קשה.

ספציפית, אם  $\Pi = (Gen, f, Inv)$  היא פרמוטציה חד-כיוונית עם trapdoor, אז נגדיר  $\tilde{\Pi} = (\tilde{Gen}, \tilde{f}, \tilde{Inv})$  כאשר:

$$\tilde{Gen} = Gen \quad (1)$$

$$\tilde{f}_k(x, r) = (f_k(x), r) \quad (2)$$

$$\tilde{Inv}(k_{inv}, (y, r)) = (Inv(k_{inv}, y), r) \quad (3)$$

ועבור  $\tilde{\Pi}$  נגדיר ביט קשה באופן הבא:

$$hc(x, r) = \bigoplus_i x_i \cdot r_i$$

הערה: נשים לב שכאן הגדרת הפונקציה  $hc$  לא תלויה במפתח  $k$ . באופן כללי יתכן שנרצה לאפשר להגדרת הביט הקשה להיות תלויה במפתח  $k$  ולכן נסמן  $hc_k$ . לשם פשטות, אנחנו נניח בהרצאה זו שהגדרת הפונקציה  $hc$  לא תלויה במפתח  $k$ .

עכשיו נראה איך ניתן לבנות מערכת הצפנה במפתח פומבי מתוך פרמוטציה חד-כיוונית עם trapdoor. תחילה נבנה מערכת הצפנה שיודעת להצפין הודעה של ביט אחד.

תהי  $\hat{\Pi} = (\widehat{Gen}, f, Inv)$  פרמוטציה חד-כיוונית עם trapdoor שיש לה ביט קשה  $hc$ . נתבונן במערכת ההצפנה במפתח פומבי הבאה.

$Gen$	קלט: $1^n$ 1. הרץ את $\widehat{Gen}(1^n)$ וקבל $(k, k_{inv})$ . 2. החזר מפתח פומבי $pk = k$ ומפתח פרטי $sk = k_{inv}$ .
$Enc$	קלט: מפתח פומבי $k$ והודעה $m \in \{0,1\}$ 1. הגרל $x \in \{0,1\}^n$ בהתפלגות אחידה כך ש- $hc(x) = m$ 2. החזר את הצופן $c = f_k(x)$
$Dec$	קלט: מפתח פרטי $k_{inv}$ וצופן $c \in \{0,1\}^n$ 1. חשב $x = Inv(k_{inv}, c)$ 2. החזר את ההודעה $m = hc(x)$

**משפט:** אם  $\hat{\Pi} = (\widehat{Gen}, f, Inv)$  היא פרמוטציה חד-כיוונית עם trapdoor שיש לה ביט קשה  $hc$ , אז מערכת ההצפנה הנ"ל היא CPA-בטוחה.

### הוכחה:

נסמן את מערכת ההצפנה הנ"ל ב  $\Pi = (Gen, Enc, Dec)$ . לפי האבחנה מלמעלה, מספיק להראות ש-  $\Pi$  היא EAV-בטוחה. תחילה נשים לב ש  $hc$  חייבת להיות מאוזנת במובן הבא:

$$\delta_0(n) = \Pr_x[hc(x) = 0]$$

$$\delta_1(n) = \Pr_x[hc(x) = 1]$$

אזי קיימת פונקציה זניחה  $negl$  כך ש-

$$\delta_0(n), \delta_1(n) \geq \frac{1}{2} - negl(n)$$

אחרת, תוקף ל-  $hc$  יכול פשוט להחזיר את הביט השכיח יותר ולקבל סתירה לכך ש-  $hc$  היא ביט קשה.

עכשיו יהי  $\mathcal{A}$  יריב פולינומי אקראי למערכת ההצפנה  $\Pi$ . בל הגבלת הכלליות נוכל להניח שההודעות שהיריב  $\mathcal{A}$  בוחר במהלך משחק ההבחנה הן  $m_0 = 0$ ,  $m_1 = 1$ . מתקיים:

$$\Pr \left[ \begin{array}{c} \mathcal{A} \text{ מנצח} \\ \text{במשחק ההבחנה} \end{array} \right] = \frac{1}{2} \cdot \Pr \left[ \begin{array}{c} \mathcal{A} \text{ מנצח} \\ \text{במשחק ההבחנה} \mid b = 0 \end{array} \right] + \frac{1}{2} \cdot \Pr \left[ \begin{array}{c} \mathcal{A} \text{ מנצח} \\ \text{במשחק ההבחנה} \mid b = 1 \end{array} \right]$$

$$= \frac{1}{2} \cdot \Pr[\mathcal{A}(pk, f_k(x)) = 0 \mid hc(x) = 0] + \frac{1}{2} \cdot \Pr[\mathcal{A}(pk, f_k(x)) = 1 \mid hc(x) = 1]$$

אבל אז

$$\begin{aligned}
& \Pr[\mathcal{A}(k, f_k(x)) = hc(x)] = \\
& = \delta_0(n) \cdot \Pr[\mathcal{A}(k, f_k(x)) = 0 | hc(x) = 0] + \delta_0(n) \cdot \Pr[\mathcal{A}(k, f_k(x)) = 0 | hc(x) = 0] \\
& \geq \left(\frac{1}{2} - \text{negl}(n)\right) \cdot \Pr[\mathcal{A}(k, f_k(x)) = 0 | hc(x) = 0] \\
& \quad + \left(\frac{1}{2} - \text{negl}(n)\right) \cdot \Pr[\mathcal{A}(k, f_k(x)) = 0 | hc(x) = 0] \\
& \geq \frac{1}{2} \cdot \Pr[\mathcal{A}(k, f_k(x)) = 0 | hc(x) = 0] + \frac{1}{2} \cdot \Pr[\mathcal{A}(k, f_k(x)) = 0 | hc(x) = 0] - 2 \cdot \text{negl}(n) \\
& = \Pr \left[ \begin{array}{c} \mathcal{A} \text{ מנצח} \\ \text{במשחק ההבחנה} \end{array} \right] - 2 \cdot \text{negl}(n)
\end{aligned}$$

בנוסף, מכיוון ש-  $hc$  היא ביט קשה עבור  $\tilde{\Pi}$ , קיימת פונקציה זניחה  $\widehat{\text{negl}}$  כך ש-

$$\frac{1}{2} + \widehat{\text{negl}}(n) \geq \Pr[\mathcal{A}(k, f_k(x)) = hc(x)]$$

ולכן

$$\Pr \left[ \begin{array}{c} \mathcal{A} \text{ מנצח} \\ \text{במשחק ההבחנה} \end{array} \right] \leq \frac{1}{2} + \widehat{\text{negl}}(n) + 2 \cdot \text{negl}(n)$$

מ.ש.ל.

**שאלה:** איך וכל להצפין הודעות ארוכות יותר?

**תשובה 1:** ניתן להצפין כל ביט בניפרד על ידי מערכת ההצפנה הנ"ל (הוכחת בטיחות – תרגיל). החיסרון עם הפתרון הזה הוא שאם נצפין הודעה באורך  $\ell$  ביטים אז נקבל צופן באורך  $\ell \cdot n$  ביטים.

**תשובה 2:** ניתן להשתמש בשילוב של מערכת הצפנה במפתח פומבי עם מערכת הצפנה במפתח סימטרי.

**דוגמה:** נניח שיש לנו שתי מערכות הצפנה עם הפרטים הבאים:

- מערכת הצפנה במפתח פומבי  $\Pi = (Gen, Enc, Dec)$ . אורך המפתח ואורך פרמטר הבטיחות הוא  $n$ . אורך הצפנת הודעה  $m$  הוא  $|m| \cdot n$ .
- מערכת הצפנה במפתח פרטי  $\Pi' = (Gen', Enc', Dec')$ . אורך המפתח ואורך פרמטר הבטיחות הוא  $n'$ . אורך הצפנת הודעה  $m$  הוא  $|m| + n'$ .

נשתמש ב  $\Pi, \Pi'$  כדי לבנות מערכת הצפנה במפתח פומבי  $\tilde{\Pi} = (\tilde{Gen}, \tilde{Enc}, \tilde{Dec})$  באופן הבא:

- $\tilde{Gen} = Gen$ .
- כדי להצפין הודעה  $m$  בעזרת מפתח פומבי  $pk$  נבצע:
  1. הגרל מפתח  $k \in \{0,1\}^{n'}$  בעזרת  $Gen'$  וחשב  $c \leftarrow Enc_{pk}(k)$
  2. חשב  $c' \leftarrow Enc'_k(m)$
  3. החזר את הצופן  $(c, c')$

כלומר, כדי להצפין הודעה  $m$ , נגריל מפתח  $k$  עבור מערכת ההצפנה הסימטרית, נצפין מפתח זה בעזרת מערכת ההצפנה במפתח פומבי, ואת ההודעה עצמה נצפין עם מערכת ההצפנה הסימטרית (בעזרת המפתח  $k$ ).

נשים לב שאורך הצופן יהיה  $|m| + |c'| = n \cdot n' + n' + |m|$ .

(הערה: ישנן דרכים יעילות יותר לשילוב מערכת ההצפנה הסימטרית עם מערכת ההצפנה במפתח פומבי)