9.03.2021 *קריפטוגרפיה 2*

הרצאה 2: בטיחות סמנטית

Textbook: Katz and Lindell. Introduction to Modern Cryptography.

מרצה: אורי שטמר

המוטיבציה שלנו בהגדרה של EAV-בטיחות הייתה שרצינו לדרוש שיריב יעיל לא יוכל "ללמוד שום מידע" על ההודעה מתוך הצופן. בפועל מה שההגדרה שלנו אמרה זה שיריב לא יכול להבחין בין הצפנה של הודעה א' להצפנה של הודעה ב'.

- האם השגנו את המטרה? האם זה אומר שאי אפשר ללמוד כלום על המסר?
- היום נכיר הגדרת בטיחות נוספת (הנקראת בטיחות סמנטית) שתופסת את האינטואיציה הזאת שלא ניתן ללמוד כלום על המסר ואז נראה שההגדרה מהשיעור שעבר גוררת את ההגדרה הזאת.

איזו דרישות בטיחות נרצה ממערכת הצפנה?

נסיון 1: בהינתן צופן לא ניתן לפענח (ללא המפתח הסודי)
ברור שאנחנו רוצים שלא יהיה אפשר לפענח, אבל זה לא מספיק. האם מערכת שמאפשרת לתוקף לשחזר חצי מההודעה היא בטוחה?

נסיון 2: בהינתן צופן לא ניתן ללמוד אף ביט מההודעה (ללא המפתח הסודי)
זה עדיין לא מספיק. מה לגבי תוקף שלומד ששני הביטים הראשונים שווים מבלי ללמוד אף אחד מהם?

נסיון 3: בהינתן צופן לא ניתן לחשב אף פונקציה של ההודעה (ללא המפתח הסודי). אינטואיטיבית, זה אומר שלא ניתן ללמוד כלום על ההודעה מתוך הצופן.
זאת דרישה הרבה יותר טובה שתהווה את הבסיס להגדרה של **בטיחות סמנטית**. אבל, כפי שנראה בהמשך, זה לא כל כך פשוט לפרמל את הדרישה הזאת וההגדרה בפועל תהייה שונה.

היום נפרמל את ההגדרה הזאת של בטיחות סמנטית ונראה שלכל מערכת EAV-בטוחה עומדת בהגדרה הזאת.
אבל לפני כן – חימום: נראה שבתנאים מסויימים לא ניתן ללמוד אף ביט בהודעה.

משפט לחימום: תהי Π מערכת הצפנה EAV-בטוחה עבור הודעות באורך קבוע ℓ. אזי לכל יריב פולינומי אקראי $\mathcal{B}$ ולכל $i \in \{1,2,\dots,\ell\}$ קיימת פונקציה זניחה $negl$ כך ש-

$$\Pr\left[\mathcal{B}\left(1^n, Enc(m,k)\right) = m[i]\right] \leq \frac{1}{2} + negl(n)$$

כאשר $m[i]$ הוא הביט ה- i ב- m וכאשר ההסתברות היא מעל הגרלת $m \in \{0,1\}^\ell$ בהתפלגות אחידה, מעל בחירת המפתח k, מעל האקראיות של Enc ומעל האקראיות של היריב $\mathcal{B}$.

למה זה רק חימום?

- מדובר רק על הודעות מתחום באורך קבוע (בלתי תלוי בפרמטר הבטיחות n)
- מדובר רק על התפלגות אחידה על הודעות. מה לגבי התפלגויות אחרות?
- כמו שאמרנו, לא מספיק לדרוש שאי אפשר לנחש כל ביט בודד.

הוכחה: ההוכחה היא על ידי רדוקציה. לכל יריב $\mathcal{B}$ כנ"ל נבנה יריב $\mathcal{A}$ שמנסה להבחין בין הודעות. נראה שאם $\mathcal{B}$ מצליח לנחש את הביט ה- i בהסתברות משמעותית יותר גדולה מ $1/2$ אז $\mathcal{A}$ מצליח להבחין בין הודעות בהסתברות משמעותית יותר גדולה מ $1/2$, מה שלא יתכן מכיוון שהמערכת היא EAV-בטוחה.

נקבע i ויהי $\mathcal{B}$ יריב שמנסה ללמוד את הביט ה- i.
עבור $b \in \{0,1\}$ נסמן ב- I_b את אוסף כל ההודעות שהביט ה- i שלהם הוא b. כלומר,

$$I_b = \left\{m \in \{0,1\}^\ell : m[i] = b\right\}$$

שימו לב ש- $|I_b| = \frac{2^\ell}{2}$.

נבנה את היריב $\mathcal{A}$ באופן הבא:

1) הגרל $m_0 \in I_0$ והגרל $m_1 \in I_1$ בהתפלגות אחידה והחזר m_0, m_1
($\mathcal{A}$ הוא יריב למשחק $\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}$ ולכן אחרי שהוא קובע m_0, m_1 המאתגר בוחר מפתח k וביט $b \in \{0,1\}$, מצפין $c \leftarrow Enc(m_b, k)$ ונותן את c ליריב $\mathcal{A}$)

2) קבל צופן c, הרץ $b' \leftarrow \mathcal{B}(1^n, c)$ והחזר b'
(b' הוא הניחוש של $\mathcal{A}$ ל- b)

שימו לב ש- $\mathcal{A}$ אכן רץ בזמן פולינומי מכיוון שצעד 1 פולינומי ומכיוון ש- $\mathcal{B}$ פולינומי.

ננתח את ההסתברות ש- $\mathcal{A}$ מצליח.

$$\Pr\left[\begin{matrix}\text{מנצח במשחק } \mathcal{A} \\ \text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}(n)\end{matrix}\right] = \Pr\left[\mathcal{B}\left(1^n, Enc(m_b, k)\right) = b\right] =$$

$$= \frac{1}{2} \cdot \Pr\left[\mathcal{B}\left(1^n, Enc(m_b, k)\right) = b \middle| b = 0\right] + \frac{1}{2} \cdot \Pr\left[\mathcal{B}\left(1^n, Enc(m_b, k)\right) = b \middle| b = 1\right]$$

$$= \frac{1}{2} \cdot \Pr_{m_0 \in I_0}\left[\mathcal{B}\left(1^n, Enc(m_0, k)\right) = 0\right] + \frac{1}{2} \cdot \Pr_{m_1 \in I_1}\left[\mathcal{B}\left(1^n, Enc(m_1, k)\right) = 1\right]$$

$$\begin{aligned} &= \Pr[m \in I_0] \cdot \Pr\left[\mathcal{B}\left(1^n, Enc(m, k)\right) = m[i] \middle| m \in I_0\right] \\ &\quad + \Pr[m \in I_1] \cdot \Pr\left[\mathcal{B}\left(1^n, Enc(m, k)\right) = m[i] \middle| m \in I_1\right] \end{aligned}$$

$$= \Pr\left[\mathcal{B}\left(1^n, Enc(m, k)\right) = m[i]\right]$$

כלומר:

$$\Pr\left[\begin{matrix}\text{מנחש את } \mathcal{B} \\ \text{הביט ה } i \text{ ב } m\end{matrix}\right] = \Pr\left[\begin{matrix}\text{מנצח במשחק } \mathcal{A} \\ \text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}(n)\end{matrix}\right] \underset{*}{\leq} \frac{1}{2} + negl(n)$$

כאשר המעבר המסומן ב * נובע מכך ש- Π היא EAV-בטוחה.
מ.ש.ל.

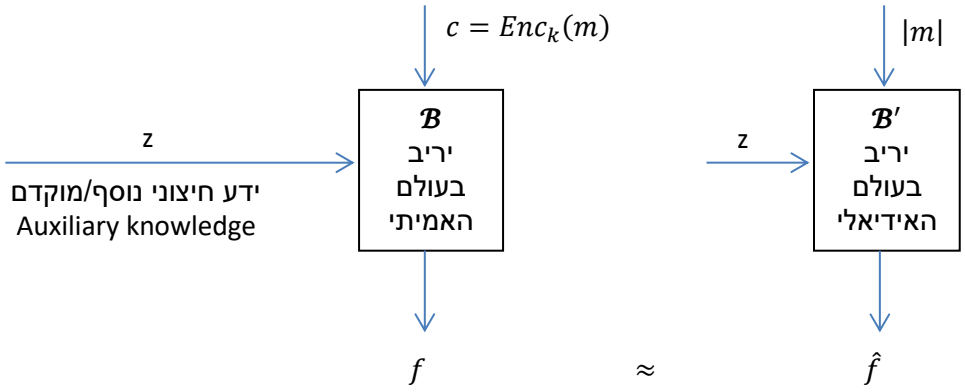
מה שראינו עד עכשיו זה שאם ההודעות מתפלגות באופן אחיד אזי במערכת EAV-בטוחה היריב לא יכול ללמוד אף ביט מההודעה. אנחנו צריכים להכליל את זה גם להודעות באורך לא קבוע, להתפלגויות אחרות, ולפונקציות של ההודעה. הכללה נוספת שנדבר עליה: ייתכן שליריב יש מידע חיצוני בנוסף לצופן. האם זה עוזר לו?

שאלה: אינטואיטיבית רצינו לדרוש שמתוך הצופן לא ניתן לחשב אף פונקציה של ההודעה. האם באמת אפשר להשיג הבטחה כזאת?

תשובה: לא בדיוק. למשל, מתוך הצופן ניתן אולי לחשב את האורך של ההודעה.
דוגמה נוספת לבעייתיות: אמרנו שאנחנו רוצים להכליל את הדרישה האחרונה להתפלגויות אחרות. למשל, נניח שההתפלגות היא אחידה על פני קבוצה S של הודעות מסויימות ונניח שהיריב יודע את זה. אז "מתוך הצופן" היריב יכול "לחשב" שההודעה הגיעה מתוך הקבוצה S. האם היריב באמת חישב כאן משהו מתוך הצופן? איך נפרמל מה בסדר שהיריב יחשב ומה לא בסדר?

בדוגמה האחרונה היריב לא באמת היה צריך את הצופן כדי לדעת שההודעה הגיע מתוך הקבוצה S (הוא כבר ידע את זה מראש...). לכן, מה שאנחנו באמת רוצים לדרוש זה שכל מה שהיריב יכול לחשב מתוך הצופן הוא היה יכול לחשב גם בלי הצופן.

<u>איך נפרמל את זה?</u>
אינטואיטיבית, נדרוש שלכל יריב $\mathcal{B}$ שמקבל צופן c ומידע חיצוני כלשהו z ומנסה לחשב "תובנה" כלשהי f על המסר המוצפן, קיים יריב $\mathcal{B}'$ שמקבל רק את האורך של המסר ואת z ומצליח לחשב את "אותה תובנה" f. בציור:



היריב $\mathcal{B}$ נקרא "יריב בעולם האמיתי" אשר רואה צופן c ומנסה לחשב משהו. היריב $\mathcal{B}'$ נקרא "יריב בעולם האידיאלי" כי הוא בכלל לא מקבל את הצופן. ההגדרה של בטיחות סמנטית אומרת שכל מה שאפשר לחשב בעולם האמיתי (מתוך הצופן) אפשר לחשב גם בעולם האידיאלי (בלי הצופן בכלל) ולכן גם בעולם האמיתי לא מפיקים בעצם שום תועלת מהצופן.

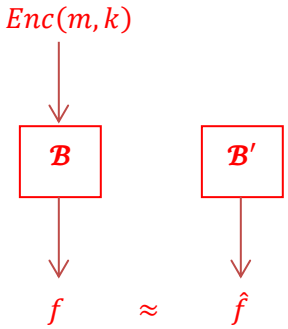
נעשה חימום נוסף לפני ההגדרה הפורמלית:

<u>משפט נוסף לחימום:</u> תהי Π מערכת הצפנה EAV-בטוחה עבור הודעות באורך קבוע ℓ. אזי לכל יריב פולינומי אקראי $\mathcal{B}$ קיים יריב פולינומי אקראי $\mathcal{B}'$ כך שלכל $S \subseteq \{0,1\}^\ell$ ולכל פונקציה $f: \{0,1\}^\ell \to \{0,1\}$ הניתנת לחישוב באופן יעיל קיימת פונקציה זניחה $negl$ כך ש-

$$\left|\Pr\left[\mathcal{B}\left(1^n, Enc(m,k)\right) = f(m)\right] - \Pr[\mathcal{B}'(1^n) = f(m)]\right| \leq negl(n) \qquad ((1))$$

כאשר ההסתברות השמאלית היא מעל <u>הגרלת המפתח k</u>, הגרלת $m \in S$ בהתפלגות אחידה, <u>האקראיות של Enc</u>, והאקראיות של $\mathcal{B}$. ההסתברות הימנית היא מעל הגרלת $m \in S$ בהתפלגות אחידה ומעל האקראיות של $\mathcal{B}'$.

בציור, לכל יריב $\mathcal{B}$ קיים יריב $\mathcal{B}'$ כך ש-



למה זה עדיין רק חימום?

- עדיין מדובר רק על הודעות באורך קבוע $m \in \{0,1\}^\ell$
- אמנם ההתפלגות היא כבר לא בהכרח אחידה על $\{0,1\}^\ell$, אלא על תת קבוצה, אבל זה עדיין לא מספיק כללי. מה לגבי התפלגויות אחרות?
- עדיין אין auxiliary knowledge.

הוכחה: יהי $\mathcal{B}$ יריב פולינומי אקראי. עלינו להראות כי קיים יריב פולינומי אקראי $\mathcal{B}'$ עבורו מתקיים תנאי (1) (לכל S ולכל f...).

רעיון ההוכחה: אנחנו צריכים להשתמש ב $\mathcal{B}$ ולבנות בעזרתו יריב $\mathcal{B}'$ שלא מקבל הצפנה כקלט ועדיין מתנהג כמו $\mathcal{B}$. איך נבנה אלגוריתם $\mathcal{B}'$ כזה? מכיוון ש- Π היא EAV-בטוחה, אנו יודעים שאף אלגוריתם יעיל לא יכול להבחין בין $Enc(m,k)$ לבין $Enc(1^\ell,k)$. לכן כדי לסמלץ את $\mathcal{B}$ ללא $Enc(m,k)$ פשוט ניתן לו במקום את $Enc(1^\ell,k)$, ואז הוא אמור להתנהג אותו דבר...

נגדיר את היריב $\mathcal{B}'$ באופן הבא:

1) הגרל k באקראי וחשב $c \leftarrow Enc(1^\ell,k)$
2) הרץ $\mathcal{B}(1^n,c)$ וענה כמוהו

תהי $f:\{0,1\}^\ell \to \{0,1\}$ פונקציה הניתנת לחישוב בצורה יעילה ותהי $S \subseteq \{0,1\}^\ell$. נרצה להראות שדרישה (1) מתקיימת עבור $\mathcal{B},\mathcal{B}',f,S$. לצורך כך נגדיר יריב $\mathcal{A}$ למשחק ההבחנה $\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}$:

1) היריב $\mathcal{A}$ מגריל $m_0 \in S$ בהתפלגות אחידה, ופולט את m_0 ואת $m_1 = 1^\ell$.
(המאתגר בוחר מפתח k וביט b, מחשב $c \leftarrow Enc(m_b,k)$ ושולח את c ל- $\mathcal{A}$)
2) אם $\mathcal{B}(1^n,c) = f(m_0)$ אז החזר $b' = 0$. אחרת החזר $b' = 1$.

מכיוון ש- Π היא EAV-בטוחה אנו יודעים כי $\Pr[\text{מנצח } \mathcal{A}] \le \frac{1}{2} + negl(n)$. מצד שני,

$$\frac{1}{2} + negl(n) \ge \Pr[\text{מנצח } \mathcal{A}] = \frac{1}{2}\cdot \Pr[\text{מנצח } \mathcal{A} | b=0] + \frac{1}{2}\cdot \Pr[\text{מנצח } \mathcal{A} | b=1] =$$

$$= \frac{1}{2}\cdot \Pr[\mathcal{B}(1^n, Enc(m_0,k)) = f(m_0)] + \frac{1}{2}\cdot \Pr\left[\mathcal{B}\left(1^n, Enc(1^\ell,k)\right) \ne f(m_0)\right]$$

$$= \frac{1}{2}\cdot \Pr[\mathcal{B}(1^n, Enc(m_0,k)) = f(m_0)] + \frac{1}{2}\left(1 - \Pr\left[\mathcal{B}\left(1^n, Enc(1^\ell,k)\right) = f(m_0)\right]\right)$$

$$= \frac{1}{2} + \frac{1}{2}\left(\Pr[\mathcal{B}(1^n, Enc(m_0,k)) = f(m_0)] - \Pr\left[\mathcal{B}\left(1^n, Enc(1^\ell,k)\right) = f(m_0)\right]\right)$$

$$= \frac{1}{2} + \frac{1}{2}\left(\Pr[\mathcal{B}(1^n, Enc(m_0,k)) = f(m_0)] - \Pr[\mathcal{B}'(1^n) = f(m_0)]\right)$$

כלומר הוכחנו ש- (1) מתקיים (ללא הערך המוחלט) עבור הפונקציה הזניחה $2\cdot negl$.

כדי לקבל את הכיוון השני של הערך המוחלט נחליף את אי השיוויון

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

באי השיוויון

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

(אי השיוויון השני נכון מכיוון שכל יריב יעיל מנצח במשחק ההבחנה בהסתברות לכל היותר ½ פלוס משהו זניח. בפרט זה נכון עבור היריב שעונה הפוך מ- $\mathcal{A}$, מה שאומר שההסתברות ש- $\mathcal{A}$ מפסיד היא לכל היותר ½ פלוס משהו זניח, כלומר ההסתברות שהוא מנצח היא לפחות ½ פחות משהו זניח.)

מדוע היריב $\mathcal{A}$ שהגדרנו הוא פולינומי?

- מכיוון ש- $S \subseteq \{0,1\}^{\ell}$ היא קבוצה סופית (כי ℓ בלתי תלוי ב- n) אז ניתן להגריל $m_0 \in S$ ביעילות
- ההפעלות של $\mathcal{B}$ ושל f יעילות כיוון ש- $\mathcal{B}, f$ יעילים.

מ.ש.ל.

אמרנו שאנחנו רוצים להכליל את הדבר הזה גם להתפלגויות יותר כלליות. אבל אנחנו רואים כאן שאנחנו חייבים לדבר רק על התפלגויות שאפשר לדגום מהן בצורה יעילה, אחרת היריב $\mathcal{A}$ שהיינו מקבלים כאן לא היה פולינומי...

אז עכשיו נכליל את הדיון שלנו ב 3 דרכים:

1. נדבר על מערכת הצפנה עבור תחום הודעות כלשהו
2. במקום לדבר רק על התפלגות אחידה על תת קבוצה, נדבר על כל הפלגות שניתנת לדגימה בצורה יעילה
3. נאפשר לתת מידע חיצוני על m

<u>הגדרה:</u> למערכת הצפנה עם מפתח פרטי יש *בטיחות סמנטית כנגד מאזין* אם לכל יריב פולינומי אקראי $\mathcal{B}$ קיים יריב פולינומי אקראי $\mathcal{B}'$ כך שלכל אלגוריתם פולינומי אקראי $Samp$ ולכל פונקציות f, h שניתנות לחישוב בזמן פולינומי קיימת פונקציה זניחה $negl$ כך ש-

$$\left|\Pr\left[\mathcal{B}\left(1^n, Enc(m,k), h(m)\right) = f(m)\right] - \Pr\left[\mathcal{B}'\left(1^n, |m|, h(m)\right) = f(m)\right]\right| \leq negl(n)$$

כאשר ההסתברויות הן מעל בחירת m על ידי $Samp(1^n)$, האקראיות של $\mathcal{B}$ ושל $\mathcal{B}'$, מעל הגרלת המפתח k ומעל האקראיות של Enc.

<u>משפט:</u> מערכת הצפנה Π עם מפתח פרטי היא EAV-בטוחה אם"ם יש לה בטיחות סמנטית כנגד מאזין.

<u>הוכחה (נראה רק כיוון אחד: בטיחות כנגד הבחנה ⇐ בטיחות סמנטית)</u>

ההוכחה כמעט זהה להוכחה האחרונה. מתוך $\mathcal{B}$ נגדיר את $\mathcal{B}'$ כך:

קלט: $1^n, |m|, h(m)$
1) הגרל k באקראי וחשב $c \leftarrow Enc\left(1^{|m|}, k\right)$
2) הרץ $\mathcal{B}\left(1^n, c, h(m)\right)$ וענה כמוהו

ואת היריב $\mathcal{A}$ נגדיר כך:

1) היריב $\mathcal{A}$ דוגם $m_0 \leftarrow Samp(1^n)$

ומגדיר $m_1 = 1^{|m_0|}$

2) לאחר שהיריב $\mathcal{A}$ מקבל צופן c מהמאתגר הוא מבצע:
אם $\mathcal{B}(1^n, c, h(m_0)) = f(m_0)$ אז החזר $b' = 0$. אחרת החזר $b' = 1$.

נשים לב ש- $\mathcal{A}$ יעיל חישובית כי $f, h, Samp$ יעילים. שאר ההוכחה בדומה:

$$\frac{1}{2} + negl(n) \geq \Pr[\text{מנצח } \mathcal{A}] = \frac{1}{2} \cdot \Pr[\text{מנצח } \mathcal{A} | b = 0] + \frac{1}{2} \cdot \Pr[\text{מנצח } \mathcal{A} | b = 1] =$$

$$= \frac{1}{2} \cdot \Pr[\mathcal{B}(1^n, Enc(m_0, k), h(m_0)) = f(m_0)] + \frac{1}{2} \cdot \Pr\left[\underbrace{\mathcal{B}\left(1^n, Enc(1^{|m_0|}, k), h(m_0)\right)}_{\mathcal{B}'(1^n, |m_0|, h(m_0))} \neq f(m_0)\right]$$

$$= \cdots$$