קריפטוגרפיה 2

הרצאה 6: CPA

Textbook: Katz and Lindell. Introduction to Modern Cryptography.

מרצה: אורי שטמר

היום נראה איך אפשר להשתמש ב PRF כדי לבנות מערכת הצפנה בטוחה כנגד הצפנה של הודעות מרובות.
בנוסף, מערכת ההצפנה שנבנה תהייה בטוחה גם אם היריב יכול לבקש הצפנות של מסרים כרצונו.

בטיחות כנגד מתקפת הודעות נבחרות — CPA – Chosen Plaintext Attack

עד עכשיו, היריבים שדיברנו עליהם בהקשר של מערכות בצפנה היו פסיביים. נחזק את היריב ע"י כך שניתן לו גישה פונקציונלית ל- $Enc_k(\cdot)$. הגישה היא אדאפטיבית, כלומר המסר ה- i שהיריב מבקש להצפין יכול להיות תלוי בהצפנות של i-1 המסרים הקודמים.

משחק הבחנה CPA עבור מערכת הצפנה $\Pi = (Gen, Enc, Dec)$

(1) $k \leftarrow Gen(1^n)$

(2) היריב $\mathcal{A}$ מופעל על קלט 1^n עם גישת אורקל ל- $Enc_k(\cdot)$
היריב בוחר זוג מסרים m_0, m_1.

(3) בחר ביט $b \in \{0,1\}$ באקראי בהתפלגות אחידה
$c \leftarrow Enc_k(m_b)$
הצופן c נמסר ליריב.

(4) היריב (עדיין עם גישת אורקל ל- $Enc_k(\cdot)$) פולט $\hat{b}$.
היריב מנצח אם $b = \hat{b}$.

הגדרה: מערכת הצפנה Π תקרא בטוחה-CPA אם לכל יריב $\mathcal{A}$ פולינומי הסתברותי קיימת פונקציה זניחה $negl$ כך ש-

$$\Pr\left[\begin{matrix}\text{מנצח במשחק } \mathcal{A} \\ \text{ההבחנה עם } \Pi\end{matrix}\right] \leq \frac{1}{2} + negl(n)$$

ההסתברות היא מעל Enc, Gen, בחירת b, ומעל האקראיות של $\mathcal{A}$.

הערות:

1. ליריב יש גישה פונקציונלית בלבד ל- $Enc_k(\cdot)$. היריב אינו לומד תוצאות ביניים, זמן ריצה, צריכת חשמל... בפרט, היריב אינו מקבל את k!
2. אלגוריתם ההצפנה חייב להיות הסתברותי.
אחרת היריב יכול לבקש הצפנות של m_0, m_1 ואח"כ בהסתברות 1 להבחין בין ההצפנות שלהם...
3. הגדרת הבטיחות הזאת חזקה יותר מההגדרה הקודמת שראינו (EAV-בטיחות)
כי הוספנו ליריב כח – גישת אורקל ל- $Enc_k(\cdot)$. היריב לא חייב להשתמש בגישת האורקל...
4. זמן הריצה של היריב חוסם מלמעלה את מספר הגישות שלו לאורקל.

בניית מערכת הצפנה CPA-בטוחה מתוך פונקציה פסאודואקראית

משפט: אם קיימת פונקציה פסאודואקראית אזי קיימת מערכת הצפנה CPA-בטוחה.

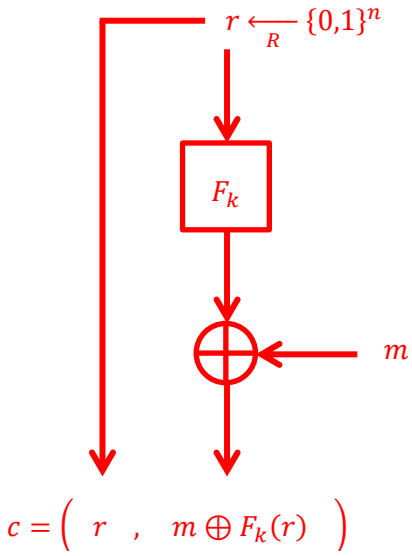
הוכחה: תהי F פונקציה פסאודואקראית. נבנה מתוך F את מערכת ההצפנה הבאה Π, אשר מקבלת פרמטר בטיחות 1^n ומצפינה הודעות בנות n ביטים (אם צריך להצפין הודעות ארוכות יותר נוכל לפרק לבלוקים באורך n).

נגדיר $\Pi = (Gen, Enc, Dec)$ באופן הבא:

Gen: קבל קלט 1^n. בחר והחזר $k \in \{0,1\}^n$ בהתפלגות אחידה

Enc: קבל קלט $k \in \{0,1\}^n$ והודעה $m \in \{0,1\}^n$. בחר $r \in \{0,1\}^n$ בהתפלגות אחידה. החזר את הצופן
$$c = \left(r, m \oplus F_k(r)\right)$$

Enc בציור:



נשים לב ש- Enc שבנינו כאן הוא אקראי. אם נצפין פעמיים את אותו המסר אז ככל הנראה לא נקבל את אותו הצופן כי הסיכוי שנקבל את אותו ה r פעמיים הוא פיצפון.

Dec: קבל קלט $k \in \{0,1\}^n$ וצופן $c = (r, s)$. החזר
$$m = F_k(r) \oplus s$$

נכונות הפענוח:
$$F_k(r) \oplus s = F_k(r) \oplus \left(m \oplus F_k(r)\right) = m$$

הוכחת בטיחות של Π

תהי $\widetilde{\Pi} = \left(\widetilde{Gen}, \widetilde{Enc}, \widetilde{Dec}\right)$ מערכת הצפנה זהה ל- Π פרט לכך שמשתמשים בפונקציה אקראית f במקום בפונקציה הפסאודואקראית F. כלומר $\widetilde{Gen}$ פולט פונקציה אקראית f ואז $\widetilde{Enc}$ מצפין בדיוק כמו Enc רק עם f במקום F_k.

(זאת אמנם לא מערכת הצפנה יעילה, אבל אנחנו עדיין יכולים להגדיר אותה לצורך ההוכחה...)

יהיה $\mathcal{A}$ יריב פולינומי הסתברותי למשחק CPA מול Π. נסמן ב $q(n)$ חסם עליון על מספר השאילתות ש- $\mathcal{A}$ מבצע למערכת ההצפנה. נראה 2 דברים:

$$\left|\Pr\left[\begin{matrix}\text{מנצח במשחק } \mathcal{A}\\ \Pi \text{ עם CPA}\end{matrix}\right]-\Pr\left[\begin{matrix}\text{מנצח במשחק } \mathcal{A}\\ \widetilde{\Pi} \text{ עם CPA}\end{matrix}\right]\right|\le negl(n) \qquad ((\text{א}))$$

$$\Pr\left[\begin{matrix}\text{מנצח במשחק } \mathcal{A}\\ \widetilde{\Pi} \text{ עם CPA}\end{matrix}\right]\le\frac{1}{2}+\frac{q(n)}{2^n} \qquad ((\text{ב}))$$

משילוב $((\text{א}))$+$((\text{ב}))$ נקבל

$$\Pr\left[\begin{matrix}\text{מנצח במשחק } \mathcal{A}\\ \Pi \text{ עם CPA}\end{matrix}\right]\le\frac{1}{2}+\underbrace{\frac{q(n)}{2^n}+negl(n)}_{\text{זניח}}$$

ולכן Π היא CPA-בטוחה.

<u>הוכחת $((\text{א}))$ – הוכחה ברדוקציה</u>

מתוך $\mathcal{A}$ (שהוא יריב למשחק ההבחנה מול Π) נבנה יריב $\mathcal{A}'$ שמנסה לשבור את הפונקציה הפסאודואקראית F.

היריב $\mathcal{A}'$

קלט: 1^n וגישת אורקל לפונקציה $O:\{0,1\}^n\to\{0,1\}^n$

(1) הרץ $\mathcal{A}(1^n)$. כאשר $\mathcal{A}$ מבצע שאילתת הצפנה על הודעה $m\in\{0,1\}^n$ נענה על השאילתא באופן הבא:
   (א) הגרל $r\in\{0,1\}^n$ בהתפלגות אחידה
   (ב) $y\leftarrow O(r)$
   (ג) החזר את הצופן $\langle r, y\oplus m\rangle$ ל- $\mathcal{A}$

(2) כאשר $\mathcal{A}$ פולט זוג מסרים $m_0,m_1\in\{0,1\}^n$, הגרל ביט $b\in\{0,1\}$ בהתפלגות אחידה ובצע:
   (א) הגרל $r\in\{0,1\}^n$ בהתפלגות אחידה
   (ב) $y\leftarrow O(r)$
   (ג) החזר את הצופן $\langle r, y\oplus m_b\rangle$ ל- $\mathcal{A}$

(3) המשך לענות על שאילתות הצפנה ל- $\mathcal{A}$ כמו בשלב (1) עד אשר $\mathcal{A}$ פולט ביט $\hat{b}$. אם $\hat{b}=b$ אז החזר 1 ואחרת החזר 0.

כעת נשים לב שמתקיים:

$$\Pr_{f,\mathcal{A}'}\left[\mathcal{A}'^{\,f(\cdot)}(1^n)=1\right]=\Pr\left[\begin{matrix}\text{מנצח במשחק } \mathcal{A}\\ \widetilde{\Pi} \text{ מול CPA}\end{matrix}\right]$$

$$\Pr_{k,\mathcal{A}'}\left[\mathcal{A}'^{F_k(\cdot)}(1^n)=1\right]=\Pr\left[\begin{matrix}\text{מנצח במשחק } \mathcal{A}\\ \text{מול CPA } \Pi\end{matrix}\right]$$

מה שמוכיח את (א), כי

$$\left|\Pr_{f,\mathcal{A}'}\left[\mathcal{A}'^{f(\cdot)}(1^n)=1\right]-\Pr_{k,\mathcal{A}'}\left[\mathcal{A}'^{F_k(\cdot)}(1^n)=1\right]\right|\leq negl(n)$$

מכיוון ש- F היא פסאודואקראית.

<u>הוכחת (ב):</u>

נזכור שבכל פעם שמסר m מוצפן, נבחרת מחרוזת אקראית r וההצפנה היא הצמד $\langle r, f(r)\oplus m\rangle$. אם היריב יודע מהו m הוא יכול לחשב ממהצפנה את $f(r)$. נסמן ב- $\hat{r}$ את האקראיות בה משתמשים להצפנת m_b. ההצפנה היא

$$\langle \hat{r}, \underbrace{f(\hat{r})\oplus m}_{\text{נסמן } \hat{s}}\rangle$$

נבחן 2 מקרים:

מקרה 1: $\hat{r}$ לא היה בשימוש בהצפנת מסרים אחרים שהיריב ביקש להצפין.

לכן, מכיוון ש- f היא פונקציה אקראית, המחרוזת $f(\hat{r})$ איתה הצפנו את m_b היא אקראית לחלוטין ובלתי תלוייה בכל שאר המשחק. לכן ההסתברות שהיריב מנצח במקרה זה היא בדיוק חצי (כמו בניתוח של One Time Pad).

מקרה 2: $\hat{r}$ היה בשימוש בהצפנת אחד המסרים אותם היריב ביקש להצפין.

במקרה זה היריב יכול לחשב

$$\hat{m}=\hat{s}\oplus f(\hat{r})$$

ולבדוק האם $\hat{m}=m_0$ או $\hat{m}=m_1$.
(כלומר במקרה זה היריב יכול לנצח בהסתברות 1)

אבל, מכיוון ש- $\mathcal{A}$ מבצע לכל היותר $q(n)$ שאילתות, אז לאורך המשחק ישנם לכל היותר $q(n)$ ערכים של r שהשתמשנו בהם. מכיוון ש- $\hat{r}$ נבחר באקראי מתוך $\{0,1\}^n$, אז ההסתברות ש- $\hat{r}$ היה בשימוש היא לכל היותר $\frac{q(n)}{2^n}$.

נחשב:

$$\Pr\left[\begin{matrix}\text{מנצח במשחק } \mathcal{A}\\ \text{מול CPA } \tilde{\Pi}\end{matrix}\right]=\underbrace{\Pr\left[\begin{matrix}\mathcal{A}\\ \text{מנצח}\end{matrix}\middle|\begin{matrix}\hat{r}\text{ היה}\\ \text{בשימוש}\end{matrix}\right]}_{\leq 1}\cdot\underbrace{\Pr\left[\begin{matrix}\hat{r}\text{ היה}\\ \text{בשימוש}\end{matrix}\right]}_{\leq q(n)/2^n}+\underbrace{\Pr\left[\begin{matrix}\mathcal{A}\\ \text{מנצח}\end{matrix}\middle|\begin{matrix}\hat{r}\text{ לא היה}\\ \text{בשימוש}\end{matrix}\right]}_{=1/2}\cdot\underbrace{\Pr\left[\begin{matrix}\hat{r}\text{ לא היה}\\ \text{בשימוש}\end{matrix}\right]}_{\leq 1}$$

$$\leq\frac{q(n)}{2^n}+\frac{1}{2}$$

מה שמוכיח את (ב) ומסיים את הוכחת המשפט, כלומר מראה ש- Π היא *CPA*-בטוחה.

מ.ש.ל.

<u>תרגיל:</u> נגדיר משחק הבחנה *non-adaptive-CPA* באופן הבא:

(1) $k \leftarrow Gen(1^n)$

(2) היריב $\mathcal{A}$ מופעל על קלט 1^n ופולט וקטור של מסרים
$m_0, m_1, m_2, \dots, m_\ell$

(3) נגריל $b \in \{0,1\}$ בהתפלגות אחידה ונצפין $c \leftarrow Enc_k(m_b)$.
בנוסף נחשב הצפנות
$$c_2 \leftarrow Enc_k(m_2)$$
$$\vdots$$
$$c_\ell \leftarrow Enc_k(m_\ell)$$
וניתן ליריב את $c, c_2, c_3, \dots, c_\ell$
(כלומר אנחנו מצפינים אחת מבין m_0, m_1 ומצפינים את כל שאר ההודעות)

(4) היריב פולט $\hat{b}$ ומנצח אם $b = \hat{b}$.

נאמר כי מערכת Π היא non-adaptive-CPA בטוחה אם כל יריב פולינומי אחקראי מנצח במשחק הנ"ל עם Π בהסתברות לכל היותר $\frac{1}{2} + negl(n)$.

הוכיחו/הפריכו: מערכת הצפנה Π היא non-adaptive-CPA בטוחה אם ורק אם היא CPA-בטוחה.

* נראה את הפתרון בכיתה. נסו לחשוב על הפתרון מראש.