תרגול מס' 6 במבוא לקריפטוגרפיה מודרנית

20 בנובמבר 2013

Public-Key Encryption

- מערכת הצפנה פומבית (אסימטרית) מורכבת משלושה אלגוריתמים:
  - K אלג' לדגימת מפתח פומבי $pk \in \{0,1\}^n$ ומפתח סודי $sk \in \{0,1\}^n$.
  - E אלג' הצפנה, בהנתן pk והודעה m, מחשב הצפנה $c = E_{pk}(m)$.
  - D אלג' פענוח, בהנתן sk וצופן c, מפענח $m = D_{sk}(c)$.
- באופן כללי: לא נרצה להניח דבר על ההתפלגות של הודעות. נרצה כי ניתן יהיה להצפין אפילו ביט יחיד $m \in \{0,1\}$.
- אבחנה: (Goldwasser-Micali 82): אלגוריתם ההצפנה E לא יכול להיות דטרמיניסטי. E יקבל אקראיות כקלט נוסף $r \leftarrow \{0,1\}^n$.
- כיצד נגדיר בטיחות?

הגדרה 0.1 . נאמר כי ההצפנה הנה $\epsilon - semantically - secure$ אם:

$$pk, E_{pk}(0;r) \approx_{c,\epsilon} pk, E_{pk}(1;r)$$

כאשר $(sk, pk) \leftarrow K(n)$, $r \leftarrow \{0,1\}^n$.

טענה 0.2 אין הצפנה פומבית עם בטיחות מושלמת (או סטטיסטית) - בתרגיל הבית.

טענה 0.3 גורר בטיחות עבור הודעות ארוכות/רבות. (נראה בהמשך טענה כללית יותר).

El-Gamal Public-Key Encryption from DDH

<u>תזכורת</u>

- תהי G חבורה ציקלית מסדר q עם יוצר g.
- בעיית Diffie-Hellman ב־G:

$$g, g^x, g^y, g^{xy} \approx_c g, g^x, g^y, g^z$$

כאשר $(x, y, z) \leftarrow Z_q^3$.

<u>מערכת ההצפנה</u>

- מפתח פרטי $x \leftarrow Z_q$.
- מפתח פומבי g, g^x.
- הצפנה של $m \in \{0,1\}$: דוגמים $y \leftarrow Z_q$, ומחשבים את ההצפנה $g^y, g^{xy}g^m$.
- פענוח: מחשבים (בעזרת x) את g^{-xy} ואז את g^m ובודקים מהו m.

טענה 0.4 המערכת בטוחה, כלומר:

$$g, g^x, g^y, g^{xy}g^0 \approx_c g, g^x, g^y, g^{xy}, g^1$$

הוכחה: לכל ביט m

$$g, g^x, g^y, g^{xy}g^m \approx_c g, g^x g^y, g^z g^m \equiv g, g^x g^y, g^{z+m} \equiv g, g^x g^y, g^z$$

כאשר $(x, y, z) \leftarrow Z_q^3$. ■

CPA Security

- נשים לב כי במערכת הצפנה פומבית ליריב אפשרות לראות הצפנות של הודעות לבחירתו (מדוע?) ודורשים כי ההצפנה עדיין תהיה בטוחה. מכונה בטיחות כנגד Chosen Plaintext Attack. ניתן להגדיר גם עבור הצפנה סימטרית.

הגדרה 0.5 . נאמר כי מערכת הפנה (פרטית) היא $\epsilon - CPA$, אם כל יריב פולינומי A לא יכול להבחין בין הצפנה של 0 להצפנה של 1 גם בהנתן אורקל הצפנה:

$$\left|\Pr\left[A^{E_{sk}(\cdot)}(c): \begin{array}{c} sk \leftarrow K(n) \\ c \leftarrow E_{sk}(0) \end{array}\right] - \Pr\left[A^{E_{sk}(\cdot)}(c): \begin{array}{c} sk \leftarrow K(n) \\ c \leftarrow E_{sk}(1) \end{array}\right]\right| \leq \epsilon$$

בהצפנה פומבית:

$$\left|\Pr\left[A^{E_{pk}(\cdot)}(c): \begin{array}{c} pk, sk \leftarrow K(n) \\ c \leftarrow E_{pk}(0) \end{array}\right] - \Pr\left[A^{E_{pk}(\cdot)}(c): \begin{array}{c} pk, sk \leftarrow K(n) \\ c \leftarrow E_{pk}(1) \end{array}\right]\right| \leq \epsilon$$

טענה 0.6 מערכת הצפנה פומבית היא $semantically - secure$ אמ"מ היא $CPA - secure$.

טענה 0.7 מערכת CPA (פרטית/פומבית) הבטוחה עבור הצפנות של ביט אחד, בטוחה גם עבור מספר רב של הודעות. לכל יריב פולינומי A ושתי הודעות ארוכות $m, m' \in \{0,1\}^t$

$$\left|\Pr\left[A^{E_{sk}(\cdot)}(c_1, \cdots, c_t): \begin{array}{c} sk \leftarrow K(n) \\ c_i \leftarrow E_{sk}(m_i) \end{array}\right] - \Pr\left[A^{E_{sk}(\cdot)}(c_1, \cdots, c_t): \begin{array}{c} sk \leftarrow K(n) \\ c_i \leftarrow E_{sk}(m'_i) \end{array}\right]\right| \leq \epsilon$$

ההוכחה נשענת על טכניקה שימושית שנקראת $hybird - argument$, בתרגיל הבית.