תרגול מס' 12 במבוא לקריפטוגרפיה מודרנית

1 בינואר 2014

Oblivious Transfer

- אינטואיציה: הפונקציונליות האידאלית.
- מתברר כפונקציונליות "שלמה" לחישוב בטוח של פונ'. בהנתן TP המממש OT באופן אידיאלי, ניתן לחשב כל "פונ' רבת משתתפים" באופן בטוח.
- ישנן כמה דרכים להגדיר בטיחות, ההגדרה החזרה ביותר מבוססת על סימולציה, ניתן הגדרה חלשה (ופשוטה) יותר.

הגדרה 0.1 (OT): פרוטוקול OT כולל שני משתתפים שולח S, ונמען R.

- הקלט של השולח S: שתי הודעות m_0, m_1
- הקלט של הנמען R: ביט b
- נכונות: בסוף הפרוטוקול, R לומד את m_b.
- בטיחות עבור משתתפים "ישרים אך סקרנים":
  - S אינו לומד דבר על b: לכל m_0, m_1

$$View_S(S(m_0, m_1), R(0)) \approx_c View_S(S(m_0, m_1), R(1))$$

  - R אינו לומד דבר על m_{1-b}: עבור $b = 0$ ולכל m_0, m_1, m_1'

$$View_R(S(m_0, m_1), R(0)) \approx_c View_R(S(m_0, m_1'), R(0))$$

    וכנ"ל לגבי $b = 1$.

OT from TDPs (*Even – Goldreich – Lempel*)

- תזכורת (TDP) : במשפחה F של TDPs ניתן לדגום $pk, sk \leftarrow K$:
  - בעזרת pk ניתן לחשב את הפרמוטציה $F_{pk} : \{0,1\}^n \to \{0,1\}^n$.
  - בעזרת sk ניתן להפוך ביעילות $D_{sk}(F_{pk}(x)) = F_{pk}^{-1}(F_{pk}(x)) = x$
  - בהנתן $pk, F_{pk}(x)$ עבור $pk \leftarrow K$, $x \leftarrow U_n$, "קשה" לחשב את x.
- תהי $HCB\ B : \{0,1\}^n \to \{0,1\}$ עבור F, כלומר

$$pk, F_{pk}(x), B(x) \approx_c pk, F_{pk}(x), U_1$$

- הפרוטוקול
  - קלט ל-S: $m_0, m_1 \in \{0,1\}$
  - קלט ל-R: $b \in \{0,1\}$
  - $S \to R$: S דוגם $pk, sk \leftarrow K$ ושולח ל-S את pk.
  - $S \leftarrow R$: דוגם $x_b \leftarrow U_n$ ומחשב $y_b = F_{pk}(x)$, דוגם $y_{1-b} \leftarrow U_n$. שולח ל-R את (y_0, y_1)
  - $S \to R$: מחשב $x_0 = F_{pk}^{-1}(y_0)$,$x_1 = F_{pk}^{-1}(y_1)$, ושולח $e_0 = B(x_0) \oplus m_0, e_1 = B(x_1) \oplus m_0$
  - S: מחשב $m_b = e_b \oplus B(x_b)$.
- מדוע הפרוטוקול בטוח נגד יריבים ישרים אך סקרנים?
  - האם S לומד על b?

$$View_S(S(m_0, m_1), R(b)) = y_0, y_1$$

שתי מחרוזת $F(x_b), y_{1-b}$ - אקראיות ללא תלות בערך של b.

  - האם R לומד על m_{1-b}?
  -

$$\begin{aligned} View_R(S(m_0, m_1), R(b)) &= y_{1-b}, B(F_{pk}^{-1}(y_{1-b})) \oplus m_{1-b} \text{ (and } x_b, m_b \text{ etc.)} \approx \\ & F_{pk}(x_{1-b}), B(x_{1-b}) \oplus m_{1-b} \approx \\ & F_{pk}(x_{1-b}), u \oplus m_{1-b} \equiv \\ & F_{pk}(x_{1-b}), u \end{aligned}$$

כאשר $u \leftarrow U_1$ אקראי ובלתי תלוי.

- האם הפרוטוקול בטוח נגד S^* רשע? כן, בהנחה שניתן לבדוק ש- F_{pk} אכן פרמוטציה.
- האם הפרוטוקול בטוח נגד R^*רשע? מה הבעיה המרכזית? וכיצד תציעו לפתור אותה?