תרגול מס' 8 במבוא לקריפטוגרפיה מודרנית

4 בדצמבר 2013

Digital Signatures

- מערכת חתימה מורכבת משלושה אלגוריתמים:
  - K מייצר חתימה סודי sk ומפתח וידוא פומבי vk.
  - $Sign$ בהנתן הודעה m ומפתח החתימה sk מייצר חתימה $\sigma = Sign_{sk}(m)$
  - Ver בהנתן מפתח הוידוא vk, הודעה m, $Ver_{vk}(m, \sigma')$ מוודא את החתימה (בפרט מקבל חתימות חוקיות).
- דרישת הבטיחות ($t-$Time Existential Unforgeability): יריב פולינומי המקבל חתימות על הודעות $m_1 \dots m_t$ הנבחרות אדפטיבית, לא יכול הודעה $m^* \notin \{m_i\}$ עם חתימה מקבלת σ. (באופן כללי t יהיה פולינום שרירותי).
- כיצד בונים חתימות? מאילו הנחות חישוביות?
- דיברנו על־כך שלא יודעים לבנות מערכת הצפנה פומבית מהנחות כגון OWF המספיקות להצפנה פרטית. האם זהו המצב גם עבור חתימות?

משפט 0.1 (Lamport,Goldwasser-Micali-Rivest,Goldreich,Naor-Yung,Rompel) ניתן לבנות חתימות מ־OWF.

סקיצה של הבניה

- חימום: One-Time Signatures מ־OWF : מעוניינים כי יריב המבקש חתימה על הודעה אחת m_1 לבחירתו לא יכול הודעה $m^* \neq m_1$ עם חתימה מקבלת. נניח כי ההודעות באורך חסום k.
- <u>בניה</u>: תהי OWF $f : \{0,1\}^k \to \{0,1\}^k$.

- מפתח סודי $\leftarrow \{0,1\}^k$ $\begin{matrix} x_1^0 \dots x_n^0 \\ x_1^1 \dots x_n^1 \end{matrix}$.
- מפתח פומבי $\begin{matrix} f(x_1^0) \dots f(x_n^0) \\ f(x_1^1) \dots f(x_n^1) \end{matrix}$.
- חתימה על m: $x_1^{m_1} \dots x_n^{m_k}$.
- וידוא ע"י חישוב f והשוואה למפתח הפומבי.

טענה 0.2 בהנתן יריב A המצליח לזייף חתימה בהס' ϵ (לאחר שראה חתימה על הודעה לבחירתו) , ניתן לבנות יריב A' ההופך את הפונ' בהס' $\epsilon/2n$ (בתרגיל בית).

- שתי בעיות עיקריות בסכמה:
  - בטיחות עבור הודעה אחת.
  - אורך החתימה $n \cdot k$ גדל עם אורך ההודעה n (כך גם אורך המפתחות).
- פתרון עבור הבעיה הראשונה: נשתמש ב־CRH: $H : \{0,1\}^* \to \{0,1\}^k$, נחתום על $H(m)$, עד שחתימה תמיד תהיה באורך k^2 ללא תלות ב־n. (בתרגיל בית, עובד לכל חתימה $t-time$ בפרט ל $t=1$.)
- פתרון ראשון עבור הודעות רבות: הרעיון - Chain of Trust.
  - בעת חתימה על ההודעה ה־i, החותם מייצר מפתחות (חד־פעמיים) חדשים (sk_{i+1}, vk_{i+1}) וחותם על (m_i, vk_{i+1}) בעזרת sk_i.
  - החתימה σ_i על m_i כוללת את כל המידע למעט המפתחות הסודיים.
  - החותם צריך לשמור את כל המידע.

טענה 0.3 בהנתן יריב A המצליח לזייף חתימה בהס' ϵ, לאחר שראה t חתימות, ניתן לבנות יריב A' המזייף חתימה בהס' ϵ/t לאחר שראה חתימה אחת (בתרגיל בית).

- בעיות בסכמה:
  - אורך החתימה גדל עם מס' ההודעות.
  - $stateful$
- נתחיל מלפתור את הבעיה הראשונה: נייצר מפתחות במבנה של עץ. (ציור)
- איך נפטר מה־$state$ בעזרת PRF?