תרגול מס' 11 במבוא לקריפטוגרפיה מודרנית

1 בינואר 2014

Fully-Homomorphic Encryption

הגדרה 0.1 (FHE): מערכת הצפנה הומומורפית (מלאה) מורכבת משלושת האלגוריתמים הרגילים K, E, D ואלגוריתם נוסף $Eval$:

- K דוגם מפתחות (נניח פרטי)
- E אלגוריתם הצפנה הסתברותי $c \leftarrow E_{sk}(m)$.
- D אלגוריתם פענוח $m = D_{sk}(c)$
- Eval אלג' שערוך הומומורפי: בהנתן פונ' $F : \{0,1\}^n \to \{0,1\}^{n'}$ והצפנה $c \leftarrow E_{sk}(m)$, F מחושבת הומומורפית

$$\hat{c} = Eval(F, c) \sim E_{sk}(F(m))$$

- semantic security: כרגיל לכל שתי הודעות: $E_{pk}(m_0) \approx_c E_{pk}(m_1)$
- function-hiding (דרישה שימושית נוספת): לא ניתן ללמוד מ־ $\hat{c}$ דבר על F למעט התוצאה $F(m)$ (לא נפרמל כרגע). **דורש כי** $Eval$ **יהיה הסתברותי.**
- הערות:
  - F אלג' פולינומי (בד"כ מיוצג ע"י מעגל בוליאני).
  - נניח לפשטות כי $\hat{c}$ אכן מתפלג כמו הצפנה של $F(m)$. בפרט אומר שהגודל $|\hat{c}|$ תלוי רק ב $|F(m)|$ ולא למשל בזמן החישוב של F.
  - בד"כ דורשים בנפרד "קומפקטיות": זמן הפענוח אינו תלוי בזמן החישוב של F.
  - זמן הריצה של $Eval$ פרופורציוני לזה של F.

Zero-Knowledge from FHE

- נבנה מערכת ZK לשפת NP שרירותית.
- תזכורת: L ב־NP אם לכל $x \in L$ קיים עד קצר w המוכיח זאת. פורמלית: קיים אלג' וידוא $F_L(x,w)$ שרץ בזמן פולינומי ב־$|x|$, כך ש: לכל $x \in L$ קיים w כך ש $F_L(x,w)=1$, לכל $\bar{x} \notin L$ ולכל $\bar{w}$, $F_L(\bar{x},\bar{w})=0$.
- ראינו מערכת ZK לבעיה מסוימת ב־NP שלוש־צביעה, למעשה בעיה שלמה ב־NP. מאפשר לבנות פרוטורול ZK לכל שפה ב־NP ע"י רדוקציה.
- לעתים הרדורציה מסובכת ולא יעילה, FHE מאפשרת לעקוף שלב זה.
- תזכורת: מעוניינים בפרוטוקול (P,V) עם שלוש תכונות:
  - completeness: לכל $x \in L$, ועד w: $(P(w),V)=1$.
  - (computational) soundness : לכל $x \notin L$ ומוכיח רשע פולינומי P^*, $(P^*,V)=1$ בהס' לכל היותר $3/4$.
  - ZK: כל V^* פולינומי לא לומד דבר מההוכחה - ניתן לבצע סימולציה יעילה של "המבט" של V^*.
- <u>הפרוטוקול</u>: תהי L שפת NP אם אלג' וידוא F_L.
  - קלט משותף: $x \in L$
  - ברשות P עד w: $F_L(x,w)=1$
- נסיון 1:
  - $P \to V$: שולח הצפנה $c=E_{sk}(w)$ של העד.
  - $P \leftarrow V$: מחשב הומומורפית $\hat{c}=Eval(F_L(x,\cdot),c) \sim E_{sk}(F_L(x,w))$ ושולח למוכיח.
  - $P \to V$: המוכיח מפענח $b=D_{sk}(\hat{c})$ ושולח את b.
  - V: מקבל אם $b=1$.
- האם הפרוטוקול $sound$?

- נסיון 2:
  - $P \to V$: שולח הצפנה $c = E_{sk}(w)$ של העד.
  - $P \leftarrow V$: מטיל מטבע b', אם $b' = 1$, מחשב הומומורפית $\hat{c} \leftarrow Eval(F_L(x,\cdot), c) \sim E_{sk}(F_L(x,w))$ ואם $b' = 0$, מחשב $\hat{c} = Eval(F_\phi(x,\cdot), c) \sim E_{sk}(0)$. $(F_\phi \equiv 0)$
  - $P \to V$: המוכיח מפענח $b = D_{sk}(\hat{c})$ ושולח את b.
  - V: מקבל אם $b = b'$.
- האם הפרוטוקול $sound$? לא יעבוד אם $Eval$ דטרמיניסטי - אינטואיטיבית נובע מ- $function - hiding$.
- האם הפרוטוקול ZK? נגד V^* שסוטה מהפרוטוקול?
- נסיון 3:
  - $P \to V$: שולח הצפנה $c = E_{sk}(w)$ של העד.
  - $P \leftarrow V$: מטיל מטבע b', אם $b' = 1$, מחשב הומומורפית $\hat{c} \leftarrow Eval(F_L(x,\cdot), c) \sim E_{sk}(F_L(x,w))$ ואם $b' = 0$, מחשב $\hat{c} = Eval(F_\phi(x,\cdot), c) \sim E_{sk}(0)$. $(F_\phi \equiv 0)$
  - $P \to V$: המוכיח מפענח $b = D_{sk}(\hat{c})$ ושולח התחייבות $COM(b)$.
  - $P \leftarrow V$: שולח את כל המטבעות שלו.
  - $P \to V$: מוודא בעזרת המטבעות של V, כי אכן $\hat{c}$ חושב ע"י שערוך הומומורפי של F_L או F_ϕ על c. אם לא, עוצר, אחרת פותח את ההתחייבות $COM(b)$.
  - V: מקבל אם $b = b'$.
- האם הפרוטוקול עדיין $sound$?
- האם הפרוטוקול ZK? כיצד יעבוד הסימולטור?
- $Rewinding$!: הסימולטור ישלח הצפנה שרירותית למשל של $1^{|w|}$, ולאחר קבלת $\hat{c}$, יחשב התחייבות לביט שרירותי למשל 1. אז לאחר ש-V^* יציג את המטבעות שלו, יגלה הסימולטור איזה מעגל העריך F_L, F_ϕ או מעגל אחר. בשלב זה הוא "יריץ לאחור" את V^* וישלח לו התחייבות לביט המתאים.
- ישנן כמה נקודות עדינות נוספות שלא נגענו בהן.