תרגול מס' 10 במבוא לקריפטוגרפיה מודרנית

18 בדצמבר 2013

Zero-Knowledge Interactive Proofs (GMR)

- מערכת הוכחה אינטרקטיבית לשפה L מורכבת מ"מוכיח" P "ומוודא" פרובבילסטי V.
  - שלמות (Completeness): לכל $x \in L$: $\Pr_V[(P,V)(x) = 1] \geq 1 - \epsilon$ (בד"כ נדרוש $\epsilon = 0$).
  - נאותות (Soundness): לכל $x \notin L$ ולכל P^*: $\Pr_V[(P^*,V)(x) = 1] \leq \epsilon$
    - חישובית: P^* פולינומי,
    - סטטיסטית P^*לא חסום.
- מה אפשר להוכיח בצורה זאת?
  - בעיות NP (למשל "האם גרף שלוש־צביע") קיימת הוכחה **לא** אינטרקטיבית (הצביעה).
  - מתברר שאפשר להוכיח הרבה יותר. למשל "האם גרף **אינו** שלוש־צביע". האם יש הוכחה לא אינטרקטיבית קצרה?
- עד כה השאלה הקריפטוגרפית היחידה התמקדה בכך ש־P^* עשוי להיות "רשע".
- דאגה נוספת הנה "מה V לומד מההוכחה". (להמחיש בבעיית ההזדהות)
- גם כאן אפשר לשאול האם V יכול ללמוד יותר ע"י סטייה מהפרוטוקול.
- ZK: מעוניינים כי המוודא לא יוכל ללמוד דבר מההוכחה, למעט העובדה שהמשפט נכונה
  - נשמע פרודוקסלי

- מאוד שונה מהדרך הרגילה בא אנחנו חושבים על הוכחות - חלק רב מהערך מיוחס למה שלומדים מההוכחה.

הגדרה 0.1 מערכת (P,V) היא ZK אם לכל מוודא פולינומי V^* קיים סימולטור פולינומי S שיכול לייצר בעצמו מטבעות עבור V^* ואוסף הודעות שנראות כמו הוכחה:

$$S(x) \approx_{c,\epsilon} View_{V^*}(P,V^*)(x)$$

כאשר $View_{V^*}(P,V^*)(x)$ מסמן את כל מה ש-V^* רואה בריצה אקראית של הפרוטוקול (מטבעות והודעות).

- ניתן גם לדרוש statistical ZK.
- ניתן לדרוש רק נגד יריבים "חצי ישרים" שעוקבים אחר הפרוטוקול, אבל עדיין מנסים ללמוד משהו.
- שימוש נפוץ: מעוניינים במערכות לבעיות NP בהן המוכיח P רץ בזמן פולינומי בהנתן עד w עבור x.
- דוג' מהכיתה: הוכחה עבור שלוש-צביעות של גרף (GMW) :
- לצייר קליק בגודל 3,4
- בעיה NP שלמה.
  - קלט משותף: גרף $G = V, E$
  - ברשות המוכיח צביעה חוקית: $\varphi : V \to [3]$ כך שלכל $(u,v) \in E$, $\varphi(u) \neq \varphi(v)$.
  - $P \to V$: בוחר פרמוטציה אקראית $\sigma : [3] \to [3]$, ושולח התחייבות $c_v = COM(\varphi'(v))$ לצבע $\varphi'(v) = \sigma(\varphi(v))$ לכל $v \in V$.
  - $P \leftarrow V$: בוחר קשת אקראית $(u,v) \in E$ ושולח למוכיח.
  - $P \to V$: פותח את ההתחייבות לצבעים $\varphi'(u), \varphi'(v)$
  - V: $\varphi'(u) \neq \varphi'(v)$
- $Soundness$ - אם G אינו שלוש-צביע, לכל צביעה $\varphi'(V)$ אליה P^* מתחייב קיימת קשת כלשהי u,v כך ש $\varphi'(u) = \varphi'(v)$, במקרה זה "נתפוס" את P^* בהס' $1/|E|$. (השתמשנו בכך שלא ניתן לפתוח את ההתחייבות באופן דו-משמעי).

- ZK- עבור V שאינו סוטה מהפרוטוקול:
  - נבחר מטבעות אקראיים V, כלומר קשת אקראית $(\tilde{u}, \tilde{v})$.
  - נבחר באקראי שני צבעים שונים $\tilde{\varphi}'(\tilde{u}) \neq \tilde{\varphi}'(\tilde{v})$ ל- $(\tilde{u}, \tilde{v})$, נשלים את הצביעה $\tilde{\varphi}$ באופן שרירותי.
  - הודעה M_1: נחשב התחייבויות $\{c_v\}_{v \in V}$לכל הצבעים.
  - הודעה M_2: הנה $(\tilde{u}, \tilde{v})$
  - הודעה M_3: פותחים את ההתחייבות ל- $\tilde{\varphi}'(u), \tilde{\varphi}'(v)$.
- כיצד נראה כי הסימולטור עובד כראוי?

$$(u,v), \{c_v\}_{v \in V}, \sigma(\varphi(u)), r(c_u), \sigma(\varphi(v)), r(c_v) \approx_c (\tilde{u}, \tilde{v}), \{\tilde{c}_v\}_{v \in V}, \tilde{\varphi}'(\tilde{u}), r(c_{\tilde{u}}), \tilde{\varphi}'(\tilde{v}), r(c_{\tilde{v}})$$

- מתבסס על כך שההתחייבות הנה $hiding$

$$COM(i) \approx_c COM(j)$$

- כיצד נסמלץ V^* שסוטה מהפרוטוקול?
  - כעת $M_2 = (u^*, v^*)$ נבחרת שרירותית ע"י V^*, יתכן באופן תלוי ב- M_1.
  - ננסה לנחש את (u, v).

טענה 0.2 נצליח לנחש בהס' $1/|E| - \epsilon_{COM}$.

- מדוע?
- כמה זמן יקח לסימולטור בתוחלת?