קריפטוגרפיה 2

הרצאה 10: המשך ZK

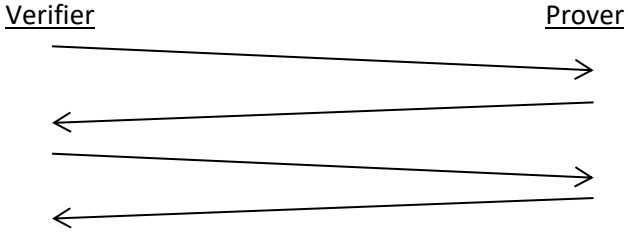
Textbook: Katz and Lindell. Introduction to Modern Cryptography.

מרצה: אורי שטמר

<u>מטרה:</u> להראות מערכת הוכחה עם אפס מידע עבור כל שפה ב- NP.

<u>אבחנה:</u> מספיק להראות עבור שפה NP-שלמה כלשהי B. מדוע?

$$x \overset{?}{\in} A$$
$$\Updownarrow$$
$$f(x) \in B$$



<u>שלמות:</u> אם $x \in A$ אז $f(x) \in B$ ולכן P ישכנע את V ש- $f(x) \in B$, כלומר ש- $x \in A$

<u>נאותות:</u> אם $x \notin A$ אז $f(x) \notin B$ ולכן כל P^* לא ישכנא את V ש- $f(x) \in B$ ולכן כל P^* לא ישכנע את V ש- $x \in A$

<u>אפס מידע:</u> נפעיל את הסימולטור על $f(x)$

<u>נראה מערכת הוכחה עבור 3-Col:</u>

<u>הגדרה:</u> צביעה (חוקית) של גרף $G = (V, E)$ ב- c צבעים היא פונקציה $\varphi: V \to \{1,2,\dots,c\}$ כך שלכל $(u,v) \in E$ מתקיים $\varphi(u) \neq \varphi(v)$.

<u>הגדרה:</u>

$$3\text{-}Col = \left\{ G: \begin{matrix} \text{קיימת צביעה של} \\ G \text{ ב 3 צבעים} \end{matrix} \right\}$$

<u>נסיון 0 לבנות פרוטוקול הוכחה:</u>
המוכיח שולח למוודא צביעה חוקית ב- 3 צבעים.
הבעייה: נותן המון מידע על הגרף.

<u>נסיון 1 לבנות פרוטוקול הוכחה:</u>
המוכיח יגריל פרמוטציה $\Pi: \{1,2,3\} \to \{1,2,3\}$ ויפרסם את $\Pi(\varphi(v))$ לכל $v \in E$.
הבעייה: עדיין צביעה חוקית ומלמדת הרבה מידע.

<u>נסיון 2:</u>

- המוכיח יגריל פרמוטציה Π
- המוודא יגריל קשת $(u,v) \in E$ וישלח אותה למוכיח
- המוכיח ישלח למוודא את $\Pi(\varphi(u))$ ואת $\Pi(\varphi(v))$
- המוודא יקבל אם"ם הצבעים שונים

✓ ZK: המודא מקבל שני צבעים אקראיים שונים ולכל לא לומד מידע

✓ שלמות: אם הגרף 3-צביע אז המודא יקבל

× נאותות: המוכיח יכול לשלוח שני צבעים שונים גם אם הגרף לא 3-צביע...

<u>נסיון 3 – פתרון בעולם הפיזי:</u>

- המוכיח מגריך פרמוטציה Π ולכל צומת $v \in V$ מכניס את $\Pi(\varphi(v))$ למעטפה <u>סגורה</u>
- המודא מגריל קשת (u,v) והמוכיח פותח את המעטפות של u ושל v
- המוודא מקבל אם שני הצבעים שונים ושניהם מהקבוצה $\{1,2,3\}$
  (אם המוכיח לא פותח את המעטפות אז המוודא דוחה...)

✓ שלמות ו- ZK עדיין תקפים

✓ נאותות: אם G <u>לא</u> 3-צביע אזי לכל P^* ולכל אוסף צבעים שהוא שם במעטפות, קיימים שני צמתים שהצבעים במעטפות שלהם לא תקינים. בהסתברות לפחות $1/|E|$ המוודא יגריל קשת כזאת וידחה.

איך נקטין את ההסתברות לשגיאה?
נחזור על הפרוטוקול הנ"ל $2|E|$ פעמים. ההסתברות ש- V לא יגריל קשת לא תקינה בכל $2|E|$ הפעמים היא לכל היותר

$$\left(1-\frac{1}{|E|}\right)^{2|E|} \leq \frac{1}{e^2} \leq \frac{1}{4}$$

בפרוטוקול הזה הסתמכנו על מעטפות סגורות. למעטפות האלו יש 2 תכונות:
(1) המעטפות אטומות: המוודא לא רואה את הצבעים של הצמתים במעטפות שלא נפתחו
(2) אי אפשר לשנות את תוכן המעטפה אחרי שהכנסנו אליה ערך

אנחנו רוצים אנלוג דיגיטלי למעטפות. כלומר אנחנו רוצים בערכת התחייבות (commitment scheme) שמורכבת משני אלגוריתמים:

(א) <u>פרוטוקול התחייבות:</u> המוכיח מחזיק קלט $s \in \{0,1\}$. למוודא אין קלט. הצדדים מנהלים שיחה. בסוף השיחה המודא לא לומד מידע על s.

(ב) <u>פרוטוקול פתיחה:</u> הצדדים מנהלים שיחה שבסופה המוודא אמור ללמוד את s. התכונה: המוכיח לא יכול לגרום למוודא "לטעות" וללמוד $s' \neq s$.

<u>באופן פורמלי:</u>

- **<u>פרוטוקול התחייבות:</u>**
קלט מוכיח: $s \in \{0,1\}$, פרמטר בטיחות 1^n, ומחרוזת אקראית r_P
קלט מודא: פרמטר בטיחות 1^n ומחרוזת אקראית r_V

(הערה: כאן המוכיח והמודא הם אלגוריתמים פולינומיים אקראיים. המחרוזות r_P ו- r_V מסמנות את המחרוזות האקראיות שלהם)

<u>סימון:</u> נסמן ב- $\left(V^*, P(b)\right)$ את פלט המודא V^* אחרי הפרוטוקול כאשר P מחזיק בקלט b.

<u>דרישת סודיות:</u> נדרוש שלכל V^* מתקיים ש- $\left(V^*, P(0)\right)$ ו- $\left(V^*, P(1)\right)$ לא ניתנים להבחנה. כלומר, לכל מבחין D פולינומי אקראי (לא אחיד) קיימת פונקציה זניחה $negl$ כך שלכל n מתקיים
$$\left|\Pr\left[D\left(V^*(1^n), P(1^n, 0)\right) = 1\right] - \Pr\left[D\left(V^*(1^n), P(1^n, 1)\right) = 1\right]\right| \leq negl(n)$$

- **<u>פרוטוקול פתיחת התחייבות:</u>** (באופן כללי אפשר לדבר גם על פרוטוקולים אחרים. אנחנו נראה פרוטוקול ספציפי לפתיחת התחייבויות)

המוכיח שולח r_P ו- b כך שהמוכיח עם r_P ו- b שולח את ההודעות שנשלחו בשלב ההתחייבות (בהתאם להודעות שהמודא שלח).

<u>דרישת פתיחה יחידה:</u> אפשר לפתוח את ההתחייבות בצורה <u>יחידה</u>. כלומר, לכל תקשורת אפשרית c, לא קיימים r_0, r_1 כך שהשיחה c אפשרית עם $r_0, 0$ ועם $r_1, 1$

(במקרה כזה, אפילו מוכיח עם כח חישוב לא מוגבל לא יכול לרמות...)

<u>בניה של פרוטוקול התחייבות מתוך פרמוטציה חד-כיוונית</u>

תהי f <u>פרמוטציה</u> חד-כיוונית ו- h ביט קשה עבורה. כדי להתחייב על ביט b, המוכיח מגריל $x \in \{0,1\}^n$ אקראי ושולח ל- V את
$$\left(f(x), h(x) \oplus b\right)$$

<u>מדוע מתקיימת דרישת הסודיות?</u>
אם V מבחין בין התחייבות על 0 לבין התחייבו על 1 אזי V יכול ללמוד מידע על הביט הקשה $h(x)$:
יהי D מבחין פולינומי אקראי ונסמן
$$\epsilon(n) = \Pr_{x\in\{0,1\}^n}\left[D\left(f(x), h(x) \oplus 0\right) = 1\right] - \Pr_{x\in\{0,1\}^n}\left[D\left(f(x), h(x) \oplus 1\right) = 1\right]$$

נבנה D' שמחשב את $h(x)$ בהסתברות $\frac{1}{2} + \frac{\epsilon(n)}{2}$ (ולכן $\epsilon(n)$ זניח...)

D' מקבל $y = f(x)$ עבור $x \in \{0,1\}^n$ אקראי, מגריל $c \in \{0,1\}$, מריץ $D(y, c)$ ועונה c אם D החזיר 1 ואחרת עונה $\overline{c}$.

נחשב:

$$\Pr\left[D'\left(f(x)\right) = h(x)\right] = \frac{1}{2} \cdot \Pr\left[D'\left(f(x)\right) = h(x) \middle| h(x) = c\right] + \frac{1}{2} \cdot \Pr\left[D'\left(f(x)\right) = h(x) \middle| h(x) \neq c\right]$$

$$= \frac{1}{2} \cdot \Pr\left[D\left(f(x), h(x)\right) = 1\right] + \frac{1}{2} \cdot \Pr\left[D\left(f(x), \overline{h(x)}\right) = 0\right]$$

$$= \frac{1}{2} \cdot \Pr\left[D\left(f(x), h(x) \oplus 0\right) = 1\right] + \frac{1}{2} \cdot \Pr\left[D\left(f(x), h(x) \oplus 1\right) = 0\right]$$

$$= \frac{1}{2} \cdot \Pr\left[D\left(f(x), h(x) \oplus 0\right) = 1\right] + \frac{1}{2} \cdot \left(1 - \Pr\left[D\left(f(x), h(x) \oplus 1\right) = 1\right]\right)$$

$$= \frac{1}{2} + \frac{\epsilon(n)}{2}$$

<u>מדוע מתקיימת דרישה הפתיחה היחידה?</u>

כי f היא פרמוטציה.