קריפטוגרפיה 2

הרצאה 11: המשך ZK

Textbook: Katz and Lindell. Introduction to Modern Cryptography.

מרצה: אורי שטמר

נחזור לפרוטוקול עבור $3-Col$

קלט של המוודא: גרף $G=(V,E)$

קלט של המוכיח: גרף $G=(V,E)$ וצביעה $\varphi: V \to \{1,2,3\}$

(1) המוכיח מגריל פרמוטציה $\sigma: \{1,2,3\} \to \{1,2,3\}$

(2) לכל $v \in V$ המוכיח מתחייב על $\sigma(\varphi(v))$. נסמן את ההתחייבות ב- c_v.

(3) המוכיח שולח $\{c_v\}_{v \in V}$

(4) המוודא מגריל $(u,v) \in E$ ושולח למוכיח. (אם $(u,v) \notin E$ אז המוכיח מסיים את ההתקשרות)

(5) המוכיח פותח את c_u, c_v

(6) אם הפתיחות תקינות וההתחייבויות הן לצבעים שונים אז המוודא מקבל ואחרת דוחה.

שלמות:

אם $G \in 3-Col$ והמוכיח הגון אז המוודא תמיד יקבל.

נאותות:

אם $G \notin 3-Col$ אזי לא קיימת צביעה חוקית ולכל לכל סדרה של ערכים שהמוכיח התחייב עליהם קיימת לפחות קשת אחת $(u,v) \in E$ שהצבעים עליה לא תקינים. בהסתברות לפחות $\frac{1}{|E|}$ המוודא יגריל קשת כזאת וידחה.

הסתברות דחייה זו קטנה מאוד. לכן המוודא והמוכיח יחזרו על הפרוטוקול $2 \cdot |E|$ פעמים (באופן סדרתי). המוודא יקבל אם כל הריצות מקבלות. כעת, ההסתברות שיקבל קלט $G \notin 3-Col$ היא לכל היותר

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

הוכחת ZK:

אנחנו נוכיח ZK תחת הנחה לא נכונה שהתחייבות ל- 0 ול- 1 מתפלגות בדיוק אותו דבר

זה לא נכון כי כל מה שמובטח לנו זה שאלגוריתם יעיל לא יכול להבחין בין התחייבות ל- 0 לבין התחייבות ל- 1, אבל זה ממש לא אומר שההתחייבויות מתפלגות אותו דבר...

הסימולטור עבור V^*:

(1) הסימולטור מתחייב לכל $v \in V$ על ערך אקראי ב- $\{1,2,3\}$ ושולח ל- V^* את ההתחייבויות (כלומר, הסימולטור מריץ את V^* עם מחרוזת אקראית r וההתחייבויות)

(2) הסימולטור מקבל קשר (u,v) מ- V^*. אם $(u,v) \notin E$ אז הסימולטור עוצר. אחרת, אם צבעי u,v שונים אז הסימולטור פותח את ההתחייבויות עליהם, שולח ל- V^* ופולט מה ש- V^* פולט.
אם הצבעים שווים אז חזור ל- (1).

הוכחת נכונות:

<u>זמן ריצה:</u> ההסתברות שהצבעים של u, v שונים היא $2/3$ ולכן בהסתברות זאת הסימולציה תצליח. סך הכל תוחלת מספר החזרות על צעד (1) היא לכן $O(1)$.

* אם נרצה שהסימולטור תמיד יעצור אזי אחרי n צעדים נעצור ונדחה. ההסתברות לכך היא זניחה, לכל היותר $(2/3)^n$.

<u>ZK:</u> מכיוון שהנחנו שלא ניתן להבחין בין התחייבויות, אזי התחייבות על צביעה חוקית ועל צביעה אקראית נראות בדיוק אותו דבר. כלומר, V^* רואה בדיוק אותה התפלגות בפרוטוקול ובסימולטור, כלומר בחירת (u, v) מתבצעת באותה התפלגות בפרוטוקול ובסימולטור. אם הסימולטור הצליח אזי הסימולטור יפתח לשני צבעים אקראיים. גם בפרוטוקול, בכלל בחירת הפרמוטציה האקראית, הצבאים מתפלגים בדיוק אותו דבר.

איך מתגברים על ההנחה כי ההתחייבויות מתפלגות אותו דבר?
מראים שאם ההתפלגות של הסימולטור והפרוטוקול ניתנים להבחנה אזי ניתן לשבור את הסודיות החישובית של ההתחייבויות.

<u>הגדרה:</u> נאמר כי $L \in CZK$ (Computational Zero Knowledge) אם קיימים V, P כך ש-

(1) (V, P) מערכת הוכחה ל- L
(שלמות עבור (V, P) הגונים ונאותות עבור V הגון ו- P^* כלשהו. בנוסף V הוא יעיל)

(2) כל מוודא V^* **<u>יעיל</u>** לא לומד מידע:

לכל אלגוריתם אקראי פולינומי V^* קיים אלגוריתם אקראי פולינומי (בתוחלת) S^{V^*} שנקרא סימולטור כך שלכל מבחין D אקראי פולינומי קיימת פונקציה זניחה $negl$ כך שלכל קלט $x \in L$ מתקיים:

$$\left| \Pr[D(\underbrace{S^{V^*}(x)}_{\substack{\text{פלט הסימולטור} \\ \text{על הקלט } x}})=1] - \Pr[D(\underbrace{(V^*,P)(x)}_{\substack{\text{הפלט של } V^* \text{ לאחר} \\ \text{השיחה עם } P \text{ על} \\ \text{הקלט } x}})=1] \right| \leq negl(|x|)$$