קריפטוגרפיה 2

הרצאה 9: Zero Knowledge Proofs

Textbook: Katz and Lindell. Introduction to Modern Cryptography.

מרצה: אורי שטמר

הנושא הבא שלנו זה הוכחות באפס מידע.

דוגמה אבסטרקטית: נניח שבתרגיל הבית אתם צריכים להוכיח טענה מסויימת. סטודנט בקורס ניסה ולא הצליח והוא משוכנע שהטענה לא נכונה. הסטודנט מגיע למרצה לשעות הקבלה ואומר שהטענה שביקשו ממנו להוכיח לא נכונה בכלל. איך המרצה יכול מצד אחד להוכיח לסטודנט שהטענה נכונה, אבל מצד שני לא לגלות לו שום דבר על הפתרון?

דוגמה נוספת: נניח שילדה מנסה לחפש את אפי באחד מהציורים של"איפה אפי?" ולא מוצאת אותו. הילדה אומרת להורים שלה שהיא לא מאמינה שאפי נמצא בתמונה בכלל. איך ההורים יכולים לשכנע את הילדה שאפי נמצא בתמונה מבלי לגלות לה שום דבר על המיקום שלו בתוך התמונה?

לפני שנדבר על הוכחות באפס מידע, נגדיר קודם מהי מערכת הוכחה. נדבר על שפה $L \subseteq \{0,1\}^*$ ונרצה להוכיח טענות מהצורה $x \in L$.

לדוגמה:

$L = \{$כל הגרפים שאין להם צביעה חוקית ב 4 צבעים$\}$

בהינתן גרף G אני רוצה להוכיח לכם שאין לו צביעה ב- 4 בצעים. איך אפשר להוכיח דבר כזה...?

יהיו לנו 2 שחקנים: מוכיח (prover) ומוודא (verifier).

מה נדרש ממערכת הוכחה?

שלמות: לכל $x \in L$ ניתן להוכיח כי $x \in L$

נאותות: לכל $x \notin L$ לא ניתן להוכיח כי $x \in L$

יעילות: ניתן לוודא את נכונות ההוכחה בצורה יעילה (אולם לא חשוב כמה זמן נידרש כדי ליצור את ההוכחה)

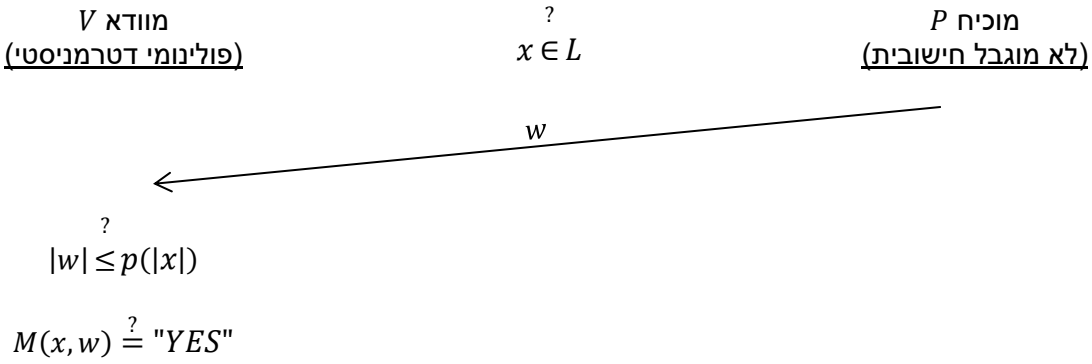
בניסוח הזה, מערכת הוכחה דומה להגדרת החלקה NP. תזכורת:

שפה L שייכת למחלקה NP אם קיים אלגוריתם פולינומי דטרמניסטי M ופולינום p כך ש:

(1) לכל $x \in L$ קיים עד w כך ש- $|w| \leq p(|x|)$ כך ש- $M(x,w) = \text{"YES"}$

(2) לכל $x \notin L$ ולכל w מתקיים $M(x,w) = \text{"NO"}$.

לפי הגדרת המחלקה NP, לכל שפה $L \in NP$ נוכל לבנות מערכת הוכחה באופן הבא:



כדי להגדיר מהי מערכת הוכחה בצורה פורמלית, נחזק את התהליך הזה בשתי צורות:
(1) נרשה אינטראקציה (שאלות של המוודא ותשובות של המוכיח)
(2) נרשה למוודא להיות אקראי ונדרוש שההסתברות שהוא טועה היא קטנה

<u>הגדרה:</u>
פרוטוקול הוכחה מוגדר ע"י 2 אלגוריתמים P ו- V כאשר:
- P הוא אלגוריתם (לא מוגבל חישובית) אשר בסיבוב ה- i מקבל קלט $x, q_1, a_1, \dots, q_{i-1}, a_{i-1}, q_i$ ומחזיר תשובה a_i.
- V אלגוריתם אקראי שרץ בזמן פולינומי ב- $|x|$. על קלט $x, r, a_1 q_1, \dots, q_{i-1}, a_{i-1}$ מחזיר את q_i (השאלה ה-i-ית). כאן r הם המטבעות האקראיים של V.

שימו לב שמכיוון ש- V פולינומי אז מספר הסיבובים בפרוטוקול, אורך השאלות ואורך התשובות פולינומיים ב- $|x|$.

דרישות:
- שלמות: לכל $x \in L$ מתקיים $\underbrace{\Pr[(V,P)(x) = "YES"]}_{\text{ההסתברות ש } \boldsymbol{V} \text{ משתכנע בסיום ריצת הפרוטוקול בין } \mathbf{V} \text{ ל } \boldsymbol{P} \text{ על קלט } x} \geq \frac{3}{4}$
- נאותות: לכל $x \notin L$ <u>ולכל מוכיח</u> P^* מתקיים $\Pr[(V,P^*)(x) = "YES"] \leq \frac{1}{4}$

הערות:
- ניתן להחליף את ההסתברות בשלמות מ- $3/4$ ל- 1, כלומר לכל $x \in L$ המוודא יקבל בהסתברות 1.
- ניתן להקטין את השגיאה בנאותות מ- $1/4$ ל- $1/|x|^c$
- בלי הגבלת הכלליות אפשר להניח ש- P דטרמניסטי
- מחלקת כל השפות שיש להם מערכת הוכחה כזאת נקראת $IP\ (Interactive\ Proofs)$

דוגמה לפרוטוקול: איך אני יכול להוכיח לכם שאני יודע להבחין בין פפסי קולה לקוקה קולה?

<u>דוגמה למערכת הוכחה אינטראקטיבית:</u>

נסתכל על השפה הבאה:
$$QR = \{(N,x) : x \in \mathbb{Z}_N^*,\ \exists y \text{ such that } x = y^2 \bmod N\}$$

הוכחה אינטראקטיבית פשוטה $(QR \in NP)$:
המוכיח שולח למוודא את y והמוודא בודק ש- $x \in \mathbb{Z}_N^*$ ובודק ש- $y^2 \equiv x \bmod N$.

עכשיו נראה מערכת הוכחה יותר מסובכת שבה המוודא לא לומד שום דבר מעבר לכך ש- $(N,x) \in QR$. בפרט, לא נרצה שהמוודא ילמד שורש של x...

קלט: (N,x)
- המוכיח: מגריל $r \in \mathbb{Z}_N^*$ ושולח למוודא את $z = r^2 \bmod N$
- המוודא: מגריל $c \in \{0,1\}$ בהתפלגות אחידה ושולח את c למוכיח
- המוכיח: אם $c = 0$ אזי המוכיח שולח את r למוודא
  אם $c = 1$ אזי המוכיח שולח $r' = r \cdot y \bmod N$ (כך ש $x \equiv y^2 \bmod N$)
- המוודא: אם $c = 0$ בודק כי $z \equiv r^2 \pmod N$
  אם $c = 1$ בודק כי $(r')^2 \equiv (ry)^2 \equiv r^2 y^2 \equiv z \cdot x \pmod N$

<u>שלמות:</u>
אם $x \in QR_N$ אזי המוודא תמיד יקבל.

<u>נאותות:</u>
נניח $x \notin QR_N$. אזי ישנם 2 אפשרויות:

(א) המוכיח שולח $z \notin QR_N$, כלומר ל- z אין שורש, ואז אם המוודא יגריל $c = 0$ אז המוכיח יתפס. המוכיח נתפס בהסתברות לפחות $1/2$.

(ב) המוכיח שולח $z \in QR_N$, כלומר קיים r כך ש- $r^2 \equiv z \pmod N$. נניח בשלילה כי במקרה בו $c = 1$ המוכיח הצליח למצוא r' כך ש- $(r')^2 \equiv z \cdot x \pmod N$ כלומר $(r')^2 \equiv r^2 \cdot x \pmod N$ כלומר $x = \left(\frac{r'}{r}\right)^2 \bmod N$. כלומר x הוא שארית ריבועית, בסתירה להנחה ש- $x \notin QR_N$. שוב המוכיח יתפס בהסתברות לפחות $1/2$.

<u>הערה:</u> ניתן להקטין את השגיאה ע"י חזרות.

נרצה כעת להוסיף למערכת הוכחה אינטראקטיבית את הדרישה שאם $x \in L$ והמוכיח הוא הגון אזי כל מוודא לא ילמד מידע (פרט לכך ש- $x \in L$).

מה זה מידע??? לא נגדיר. נתחמק מלהגדיר מה זה <u>מידע</u>. במקום זה נגדיר רק תנאי מספיק לכך שהמוודא לא לומד מידע:

מוודא לא לומד מידע מהמוכיח אם הוא יכול לחשב <u>בעצמו</u> את מה שהוא רואה בפרוטוקול.

דוגמה שבה כן דולף מידע: מוכיח שרוצה להוכיח שבגרף נתון קיים מסלול המילטוני ולצורך כך הוא נותן למוודא מסלול המילטוני בגרף. מוודא שרץ בזמן פולינומי לא יכול למצוא מסלול המילטוני בעצמו (אם $BPP \neq NP$).

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

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

(2) כל מוודא V^* לא לומד מידע:
לכל אלגוריתם אקראי פולינומי V^* קיים אלגוריתם אקראי פולינומי (בתוחלת) S^{V^*} שנקרא סימולטור כך ש- $S^{V^*}(x) \equiv (V^*, P)(x)$. כלומר, התפלגות הפלט נראית בדיוק אותו דבר.
(ישנם הגדרות שקולות המנוסחות קצת אחרת בעזרת מה שנקרא ה- VIEW של V^*)

<u>משפט:</u> $QR \in PZK$

<u>הוכחה:</u> נראה כי (V, P) שהגדרנו קודם היא מערכת הוכחה באפס מידע. (זה שזה מערכת הוכחה כבר ראינו...)

עובדה מתורת המספרים: לכל $x \in QR_N$, אם $r \in \mathbb{Z}_N^*$ הוא איבר אקראי מ- $\mathbb{Z}_N^*$ אזי $z = r^2 \in QR_N$ הוא איבר אקראי מ- QR_N וגם $\left(\frac{x}{z}\right) \in QR_N$ הוא איבר אקראי מ- QR_N.

כלומר, שני הצעדים הבאים שקולים:
* P מגריל $r \in \mathbb{Z}_N^*$ ושולח $z = r^2 \pmod N$ ל- V.
* P מגריל $r \in \mathbb{Z}_N^*$ ושולח $z = \frac{x}{r^2} \pmod N$ ל- V.

<u>הסימולטור:</u>

(1) הגרל $x \in \{0,1\}$ בהתפלגות אחידה.

(2) אם $c = 0$ הגרל $r_0 \in \mathbb{Z}_N^*$ ושלח $z = r_0^2 \bmod N$ ל- V^*.
אם $c = 1$ הגרל $r_1 \in \mathbb{Z}_N^*$ ושלח $z = \frac{r_1^2}{x} \bmod N$ ל- V^*.

(3) קבל ביט b מ- V^*. אם $b = c$ שלח r_b ל- V^* והחזר את הפלט של V^*.
אחרת $(b \neq c)$ לך לצעד (1).

<u>הסבר:</u> יהי V^* מוודא כלשהו (אולי רמאי) ונראה שאפשר לסמלץ אותו. מכיוון שאנחנו לא יודעים איך הוא יתנהג (כלומר באיזה התפלגות הוא בוחר את הביט b שלו, ואיך הוא מחשב את הפלט שלו), אנחנו נשתמש בו כקופסא שחורה.

V^* מצפה לקבל 2 הודעות מ- P והוא יקבל אותם מ- S^{V^*}. לכן, אם ההודעות מתפלגות אותו דבר, אז V^* יתנהג אותו דבר ויפלוט את אותו הפלט.

<u>טענה 1:</u> גם בפרוטורול וגם בסימולטור, מתקיים ש- z הוא איבר אקראי ב QR_N.
(טענה 1 נובעת מהעובדה הקודמת...)

<u>המסקנה:</u> גם בסימולטור וגם בפרוטוקול, מתקיים ש- b נבחר באותה התפלגות כאשר בסימולטור התפלגות b בלתי תלויה ב- c. לכן, $\Pr[b = c] = \frac{1}{2}$.
אם $b = c = 0$ אזי גם בפרוטוקול וגם בסימולטור מתקיים ש- V^* מקבל שורש אקראי של z ואם $b = c = 1$ אזי V^* מקבל שורש אקראי של $z \cdot x$.

<u>נסכם:</u> אם $b = c$ אזי V^* מקבל בשני המקרים (גם בפרוטוקול וגם בסימולטור) אותה התפלגות של הודעות ולכן הפלט שלו זהה בשני המקרים. נשים לב כי טענה זו לא תלויה במספר הפעמים שהרצנו את צעד (1) ונכשלנו, כי כל פעם מפעילים את V^* מחדש ללא תלות בהיסטוריה.

זמן הריצה של S^{V^*}: מכיוון שהסימולטור יצליח בהסתברות $1/2$ אזי תוחלת מספר הריצות שלו היא 2.

מטרה בפעם הבאה: להראות מערכת הוכחה באפס מידע עבור כל שפה ב- NP.