יסודות הקריפטוגרפיה תרגול #10

חזרה על שיעור שעבר – *Hellman*: טריידאוף זיכרון וזמן:

רוצים להפוך את הפונקציה $f: X \to X$: מבצעים חישוב מקדים, לשמור זיכרון בגודלm. לרוב השאילתות $y \in X$ בזמן t רוצים לחשב את $x := f^{-1}(y)$ כך ש-$f(x) = y$. שבוע שעבר דיברנו על f שהיא פרמוטציה, ועבורה f אם $m \cdot t = |x|$כ אז ניתן להשיג סיכוי הצלחה קבוע.

<u>מה קורה עם פונקציות שאינן פרמוטציות?</u>

למשל, אם יש לנו $hash$ של ססמא, הססמא לא חייבת להיות בגודל ה- $hash$; דוגמא נוספת היא פונקציה $f(k) = E_k(p^*)$ עבור מפתח k וטקסט p^* קבוע. במקרה כזה הבלוק יכול להיות בגודל 128 והמפתח בכלל 64 – כלומר הפונ' לא מאותו מרחב אל עצמו. עבור פרמוטציה הפעלנו את f על עצמה, וזאת לא ניתן לעשות כאן.

פתרון לדוגמא השניה: כדי להפוך לפונקציה $X \to X$ כאשר $X = \{0,1\}^{64}$ (מרחב המפתחות) נרכיב פונקציה $R: \{0,1\}^{128} \to \{0,1\}^{64}$ שלא חייבת להיות מתוחכמת, כמו למשל לקיחת 64 הביטים הראשונים. כעת: $R \circ f: X \to X$. קיבלנו פונ' שאינה פרמוטציה (בהכרח) כי לא נתון ש- f, R חח"ע. אז איפה העובדה שזו לא פרמוטציה מפריעה לנו?

בפתרון עבור פרמוטציה הסתכלנו על מעגלים, כלומר פרמוטציה היא למעשה אוסף מעגלים. כעת יש לנו מעגלים יחד עם עצים וכל מיני, ובנוסף יכולות להיות נקודות שאין להן מקור. אם כן, עבור y כלשהו שנמצא, נניח, על איזשהו מסלול המוביל למעגל, הגרלת נקודת התחלה כך שנתפוס את אותו y היא בעלת סיכויים נמוכים. ננסה את השיטה הקודמת של$t = m = \sqrt{|X|}$:

נניח שתוך $|X|^{\frac{1}{6}}$ כיסינו $|X|^{\frac{2}{3}} = |X|^{\frac{1}{2}+\frac{1}{6}}|X|$ (היינו צריכים מזל בשביל זה...). אם כבר כיסינו חלק נכבד זה מהמרחב, אז בסיכוי של $|X|^{-\frac{1}{3}}$ נבחר איבר שכבר כוסה ($|X|/|X|^{\frac{2}{3}}|$). בעצם מטילים מטבע וכל פעם יש סיכוי קטן להפסיד, ואם הפסדנו – השרשרת אותה בודקים (השרשרת החדשה) כבר לא משמשת אותנו. בסיכוי $\varepsilon = |X|^{-\frac{1}{3}}$ לא קיבלנו כלום; בסיכוי $(1-\varepsilon)\varepsilon$ קיבלנו מהשרשרת איבר אחד וכן הלאה – התפלגות גיאומטרית. בתוחלת התפלגות גיאומטרית, כל שרשרת תורמת $\frac{1}{\varepsilon} = |X|^{\frac{1}{3}}$ לכל היותר. בסה"כ קיבלנו: $|X|^{\frac{5}{6}} = |X|^{\frac{1}{3}} \cdot \sqrt{|X|}$ וזה אפילו לא כל המרחב. מכאן שקשה לכסות יותר מ-$|X|^{\frac{2}{3}}$ איברים. כמו כן סיכוי ההצלחה שלנו כבר לא קבוע, אלאε שהוא די קטן.

<u>פתרון נוסף</u>:

נבחר $t = m = |X|^{\frac{1}{3}}$, אמנם לא נוכל לכסות יותר מ- $|X|^{\frac{2}{3}}$ מהמרחב אך נוכל להשיג סיכוי קבוע. נדלג עד השלב שאנו מסתכלים על מצב בו כיסינו $|X|^{\frac{2}{3}}$ איברים בשרשראות קודמות. השרשרת האחרונה תורמת בתוחלת $|X|^{\frac{1}{3}}$ איברים חדשים. כמו כן שרשרת זו עושה את העבודה הכי קשה, למצוא בשלב זה איברים שלא נתקלנו בהם קודם. מכאן, שכל שרשרת קודמת תורמת בתוחלת לפחות $\Omega\left(|X|^{\frac{1}{3}}\right)$. בסה"כ כיסינו $\Omega\left(|X|^{\frac{2}{3}}\right)$ מהמרחב. נשים לב שאם נכסה פחות מ-$|X|^{\frac{2}{3}}$ בהתחלה, אז לשרשרת האחרונה יהיה רק יותר קל למצוא איברים שלא נתקלנו בהם (ומכאן נסיק על חסם תחתון לאיברים שכל שרשרת לפניה תורמת).

<u>*Yet another* פתרון</u>:

נסתכל על $R \circ f$ וננית כי נבחר פעמים רבות R_i שונות כך ש-$f_i = R_i \circ f$. כעת נקבל טבלאות שרשראות רבות, נניח $c = |X|^{\frac{1}{3}}$. אז מה הולך עכשיו?

- סה"כ זיכרון לכל טבלה הואm ולכן לכל הטבלאות יחד נשמור $m \cdot c = |X|^{\frac{2}{3}}$. כל $f_i: X \to X$ והן שונות אחת מהשניה בקצת.
- זמן החישוב המקדים לכל טבלה הוא $m \cdot t$ ולכן סה"כ לכל הטבלאות: $m \cdot t \cdot c = |X|$ (גודל כל המרחב).
- זמן חישוב בודד לכל הטבלאות הוא $t \cdot c = |X|^{\frac{2}{3}}$.
- סיכוי ההצלחה: בטבלה בודדת סיכוי ההצלחה הכולל הוא: $1 - \frac{1}{e} = 1 - \left(1 - \frac{1}{|X|^{\frac{1}{3}}}\right)^{|X|^{\frac{1}{3}}}$ וזה קבוע.

אמנם משלמים יותר, $|X|^{\frac{4}{3}}$ אך זה עדיין יותר טוב מהשיטות הקודמות.