יסודות הקריפטוגרפיה תרגול 9#

טריידאוף זיכרון מול זמן:

אם רוצים למצוא פתרון ל-$C = E_k(P)$:

- ניתן לעבור על כל מרחב המפתחות, כאשר זמן הריצה הוא מירבי, זיכרון הוא קבוע.
- ניתן לבצע חישוב מוקדם $\forall k. E_k(P_0)$; בהינתן C מבצעים חיפוש ברשימה (נניח ממויינת) המכילה את כל ה- $E_k(P_0)$ האפשריים. כאן נניח שהחישוב המוקדם "מחוץ למשחק", כלומר נעשה בעבר ולא משפיע לי על סיבוכיות האלג'. כעת ניתן בזמן לוגריתמי לבצע חיפוש בכל התוצאות, התופסות מקום רב, או אפילו בזמן קבוע (אם נחזיק ב-*hash table*). בפיתרון זה הזיכרון גדול, הזמן קטן.

אלו שני פתרונות קיצוניים, אחד משתמש בזמן מקסימלי והשני במקום מקסימלי. נרצה כעת לווסת את השניים, כמו למשל ב- *meet in the middle* *attack*, שם עבור מרחב בגודל 2^{112} השתמשנו ב-2^{56} זיכרון ו-2^{56} זמן.

<u>טרייד אוף לבעיית פתרון *Discrete log* לבעיית *DH*</u>:

אם נדע לחשב עבור $y = g^x \pmod p$ מהו x, זהו פתרון *Discrete log*. במקרה זה:

- רק זמן: נחשב g^x לכל $x \in \mathbb{Z}_p$ עד שנקבל את y.
- רק זיכרון: נחשב מראש הכל ונשמור הכל: $\{g, g^2, \dots, g^{p-1} = 1\}$, וכעת חיפוש y הוא מהיא בקבוצה זו.

הצעה: נשמור בזיכרון רק $\sqrt{p}$ איברים: $L = \left\{g^{\lfloor\sqrt{p-1}\rfloor}, g^{2\lfloor\sqrt{p-1}\rfloor}, \dots, g^{p-1}\right\}$ - כאן הזיכרון הנדרש הוא רק $\sqrt{p}$. נגיד שבמקום לחשב את g^x לכל x נחשב את $g^{-x}y$ ונרצה לקבל 1 (זה שקול). כעת נחשב לכל x החל מ- 1 והלאה את $g^{-x}y$ ונעצור כשנקבל איזשהו איבר ב- L. כשעצרנו אנו יודעים שמתקיים: $g^{-x}y = g^{k\lfloor\sqrt{p-1}\rfloor}$ ולכן $y = g^{k\lfloor\sqrt{p-1}\rfloor+x}$ כלומר די לבדוק $x \in [0 \dots \lfloor\sqrt{p-1}\rfloor]$ - כלומר זמן $\sqrt{p}$. גם החישוב המקדים לוקח רק $\sqrt{p}$ (במקרה זה, לא במקרה הכללי).

הסבר: כשהולכים על שיטה ללא זיכרון, בעצם מחפשים x ביחס ל-1. אם מחשבים מראש $\sqrt{p}$ איברים, אז בעצם יש לנו $\sqrt{p}$ "עוגנים" (כמו 1 שהיה עוגן יחיד מקודם), ולכן מספר ה-x האפשריים בין עוגן לעוגן הוא לא p כמו קודם אלא $\sqrt{p}$. אלגוריתם זה נקרא *Baby-step-Giant-step* של *D. Shank*. ניתן לשחק עם חלוקת הזיכרון והזמן, למשל $p^{\frac{2}{3}}$ זיכרון עם $p^{\frac{1}{3}}$ זמן.

<u>מקרה נוסף</u>:

נתונה פרמוטציה $\pi: X \to X$ מקרית מעל X קבוצה סופית. נתון $y = \pi(x)$, רוצים לחשב את x, אך כעת בניגוד לקודם לא ידוע דבר על הפרמוטציה (קודם ידענו שזה מעגל). גם כאן אפשר ללכת על המקרים הקיצוניים: או לרוץ על הכל ולחפש, או לשמור את π^{-1} ולגשת בזמן מהיר. פתרון ביניים: בפרמוטציה יהיה לנו למעשה אוסף מעגלים המורכבים עבור z כלשהו מ-$\{z, \pi(z), \pi(\pi(z)), \dots, \pi^k(z) = z\}$ (מעגל בעל k איברים). אם יש לנו מעגל שהוא יחסית קטן, נניח עד $\sqrt{|X|}$, אין בעיה. עבור מעגל גדול, נרצה להשתמש בשיטה של קודם, שהיא למעשה חלוקה של המעגל. מה שעושים זה כך: נחזור m פעמים על הצעדים הבאים:

- מגרילים נקודת התחלה s
- מחשבים את $e = \pi^t(s)$ ושומרים את הזוג (e, s) בטבלה בזיכרון

לשם הקונקרטיות נקח $m = \sqrt{|X|}, t = \sqrt{|X|}$. כלומר כל פעם לוקחים שרשרת בגודל שורש המרחב ויש לנו שורש המרחב כאלה שרשראות. כן השלב המקדים יקח לנו בניגוד לקודם $|X|$ כיוון שאין לנו ידע מוקדם על π שמאפשר לנו חישובים מהירים (קודם היינו צריכים רק לחשב $g^{\sqrt{p-1}}$ ואז כל השאר זה חזקה k שלו). אם השרשראות מכסות בדיוק את כל X, קיבלנו 100 אחוזי הצלחה, כלומר לכל y נוכל למצוא את x שהוא המקור שלו, וזאת נעשה ב- $\sqrt{|X|}$: בהינתן $y \in X$, נחשב את $\pi^{-1}(y)$ בצורה הבאה:

Repeat $\sqrt{|X|}$ times for $y \to w$:

- $w' := \pi(w)$
- $if\ w' = y, return\ w$
- $if\ w \in \{e_i\}_{i=1}^m, w = s_i$
- $else\ w = w'$

באופן כללי הולכים לחזור על זה t פעמים, כאורך השרשרת. נרצה להראות שכיסינו אחוז קבוע מהמרחב ($1 - \frac{1}{e} \cong 63\%$):

נאמר שעד כה כיסינו לכל היותר $\frac{1}{2}|X|$, ואם כן אז כל שרשרת תתרום בתוחלת לפחות $\frac{\sqrt{|X|}}{2} = \frac{1}{2}t$, ואז יש שקר כלשהו שמגיעים לפיכך לאחוז הנ"ל.

הוכחה מלאה הועלתה לאתר.