קורס : קודים לתיקון שגיאות ושימושיהם במדעי המחשב
מרצה : ד״ר קלים יפרמנקו
סמסטר : סתיו תשפ״א
תאריך : 24/11/2020

הרצאה 20

Secret Sharing Schemes

<u>הגדרה :</u> ״מערכת לשיתוף סוד״ הינה אוסף פונקציות $s_1, s_2, \dots, s_n$ כך שלכל $1 \le i \le n$ מתקיים : s_i
$\Sigma \to \{(R, s)\}$, כש R הינה מחרוזת מאורך כלשהו מעל הדומיין D, ו s הינו איבר מתוך הדומיין D (במקרה שלנו $D = F_q$). ״מערכת לשיתוף סוד״ מוגדרת ע״י הזוג (l, n) ומקיימת את התנאים הבאים :

א. לכל קבוצה $\{1, \dots, n\} \supseteq T$ כך ש $|T| \ge l$ קיימת פונקציית פענוח המקיימת $D_T(\{s_i : i \in T\}) = s$.
ב. לכל קבוצה $\{1, \dots, n\} \supseteq T$ כך ש $|T| < l$ מתקיים $\Pr[s = x | \{s_i : i \in T\}] = \frac{1}{|D|}$.

במילים פשוטות : כל קבוצה של פחות מ l אנשים ״לא יודעת כלום״ אודות הסוד.

<u>דוגמא :</u>

$$n = 4, \qquad l = 4$$

$$s_1((r_1, r_2, r_3), s) = r_1$$

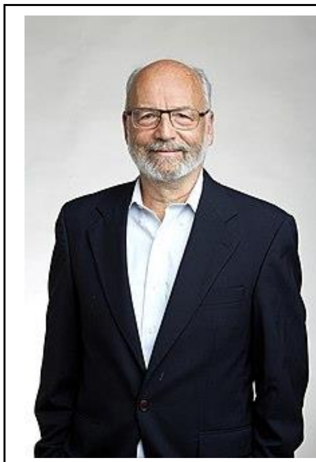
$$s_2((r_1, r_2, r_3), s) = r_2$$

$$s_3((r_1, r_2, r_3), s) = r_3$$

$$s_4((r_1, r_2, r_3), s) = r_1 \oplus r_2 \oplus r_3 \oplus s$$

Shamir's Secret Sharing

SSS הינה מערכת לשיתוף סוד חשובה ביותר אשר מבוססת על אינטרפולציית פולינומים, שהומצאה בשנת 1979 ע״י הקריפטוגרף הישראלי עדי שמיר. אחד מיתרונותיה הבולטים הוא שהינה גמישה וניתנת להרחבה. כלומר, בעל הסוד יכול להוסיף, לשנות או להסיר שותפי סוד בכל פעם שירצה מבלי לשנות את הסוד המקורי.
אלגוריתם זה מקיים את שני התנאים של מערכת לשיתוף סוד ע״י כך שדרושים l שותפי סוד על מנת למצוא אותו, והוא *information theoretically secure*, כלומר עמיד בפני תוקף בעל כוח חישובי בלתי מוגבל.



עדי שמיר

<u>הגדרה:</u> אלגוריתם SSS עבור דומיין F_q כך ש n < $|F_q|$ מוגדר באופן הבא:

1. בחר פולינום אקראי $p(x)\ \sum_{i=0}^{l-1} r_i x^i$ המקיים $r_0 = s,\ r_{l-1} \neq 0,\ r_i \in F_q$.
2. בחר $x_1, x_2, \dots, x_n \in F_q$ $\neq 0$ שונים והגדר לכל $1 \le i \le n$ כי $s_i = (x_i, p(x_i))$.

<u>טענה:</u> SSS מקיים את 2 התנאים של מערכת לשיתוף סוד.

<u>הוכחה:</u>

א. תהי קבוצה $T \subseteq \{1, \dots, n\}$ כך ש $|T| \ge l$. אזי $\{s_i : i \in T\}$ הינה קבוצה של לפחות l נקודות $(x_i, p(x_i))$ על הפולינום. בעזרת אינטרפולציית $Lagrange$ למשל ניתן למצוא את הפולינום $p(x)\ \sum_{i=0}^{l-1} r_i x^i$, ומכאן את $s = r_0$. כלומר קיימת פונקציית פענוח המקיימת $D_T(\{s_i : i \in T\}) = s$.
ב. תהי קבוצה $T \subseteq \{1, \dots, n\}$ כך ש $|T| < l$. אזי $\{s_i : i \in T\}$ הינה קבוצה של פחות מ l נקודות $(x_i, p(x_i))$ על הפולינום. ע"מ אינטרפולציית $Lagrange$ למשל ניתן להסיק כי קיימים לפחות $|F_q|^l$ פולינומים כנ"ל, ומכאן שמספר המקדמים החופשיים האפשריים r_0 הינו לפחות $|F_q|$. מכאן שבמקרה הטוב ניתן להגריל r_0 באקראי ולכן $\Pr[s = r_0 = x | \{s_i : i \in T\}] = \frac{1}{|F_q|} = \frac{1}{|D|}$.

<u>שאלה:</u>

ישנה תת קבוצה של "מורדים", למשל מגודל 3, אשר משקרת בנוגע לאיבר שהיא מקבלת.

1. כמה n אנשים צריך על מנת לגלות את s אם קבוצה זו מכריזה על עצמה כמורדת?
2. כמה n אנשים צריך על מנת לגלות את s אם קבוצה זו אינה מכריזה על עצמה כמורדת?

<u>תשובה:</u>

1. $\boldsymbol{n = l + 3}$: נוכל להסיר מהקבוצה של 3 ה"מורדים", וכך תישאר קבוצה של l שותפי סוד "אמינים", שבעזרתם ניתן לגלות ע"פ הגדרת מערכת לשיתוף סוד את s.
2. $\boldsymbol{n = l + 6}$: מדובר על קוד $RS = [n, k = l, d = n - k + 1]$ בעל $e = 3$ שגיאות. כפי שלמדנו, על מנת לתקן אותן נדרש כי $d = 2 \cdot e + 1 = 7$. מכאן נקבל כי $7 = n - l + 1$, ולכן עבור $n = l + 6$ נוכל לשחזר את הפולינום $p(x)$ ומלצוא את s.

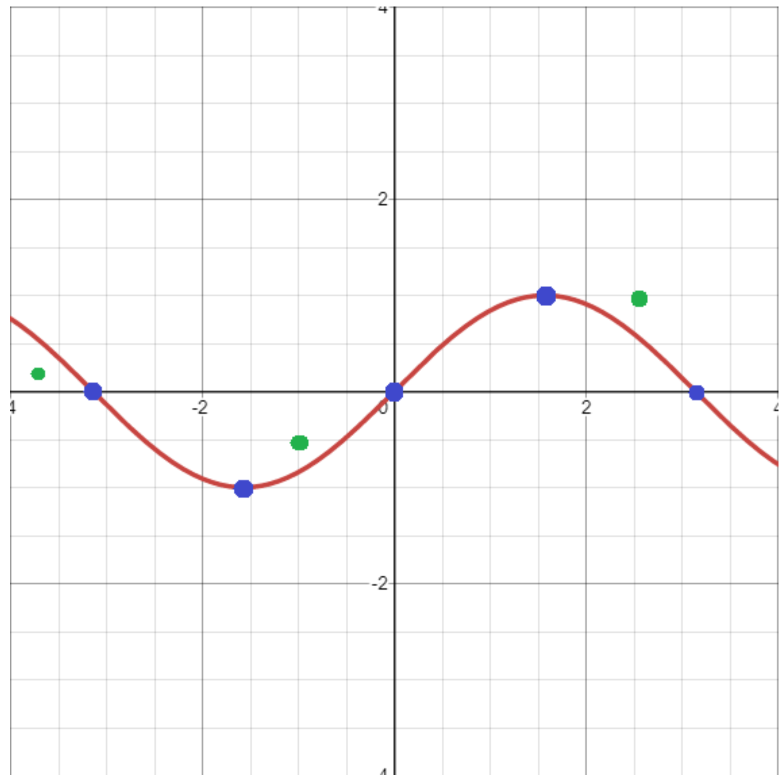
List Recovery

<u>הגדרה:</u> בהינתן הודעה m וקוד C_L כך ש $C_L(m) = (L_1, L_2, \dots, L_n)$ הינה רשימה של n קבוצות מגודל r של סימבולים, כלומר לכל $1 \le i \le n$ מתקיים $L_i = \{y_i^1, y_i^2, \dots, y_i^r\}$, List Recovery הינה הפעולה של שחזור m מתוך רשימת הקבוצות הנ"ל.

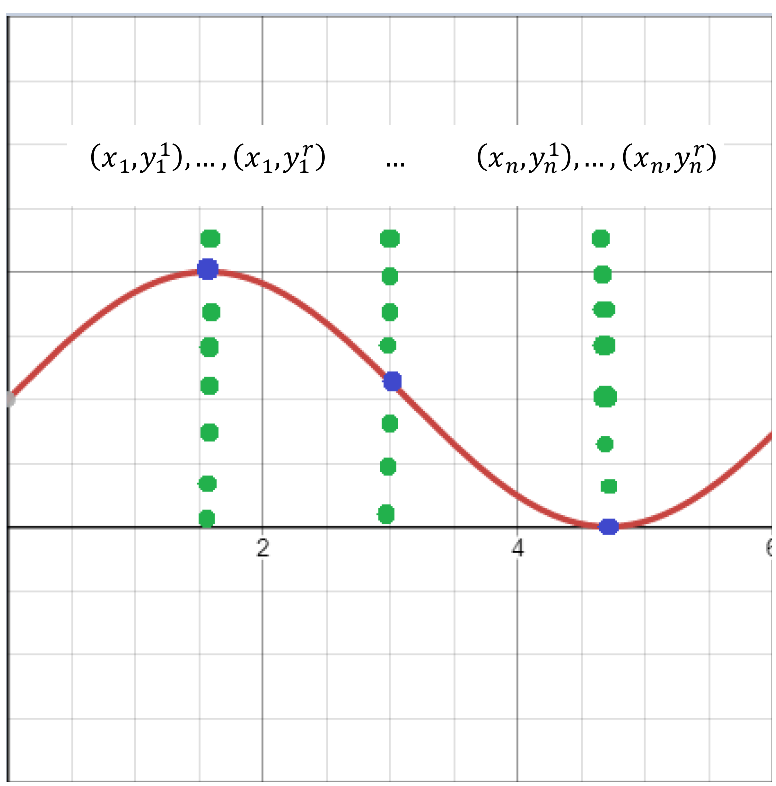
<u>טענה:</u> אם קיים קוד RS כך ש $RS(m) = (y_1, y_2, \dots, y_n)$ כך שלכל $1 \le i \le n$ מתקיים $y_i \in L_i$, אז קיים R כך שאם $r \le R$ אזי ניתן לבצע List Recovery ולהחזיר קבוצה L מגודל $O(poly(n))$ כך ש $m \in L$.

<u>הוכחה:</u> נשתמש באלגוריתם List Decoding לפענוח RS שלמדנו בשיעורים האחרונים.

ניזכר כי עבור List Decoding היו בידינו n נקודות, כאשר ידענו כי $2\sqrt{nk}$ מתוכן על הפולינום אותו חיפשנו:



עבור List Recovery, נסתכל על $r \cdot n$ הנקודות שברשותינו $\{(x_i,y_i^1),(x_i,y_i^2),\dots,(x_i,y_i^r)\}_{i=1}^n$. ידוע כי מתוך $r \cdot n$ הנקודות, n מתוכן נמצאות על הפולינום:



קיבלנו כי:

שיטה	מס' נקודות	מס' נקודות על הפולינום
List Decoding	n	$2\sqrt{nk}$
List Recovery	$n \cdot r$	n

נבחין כי עבור $r = \frac{n}{4k}$ נקבל כי מס' הנקודות שברשותינו הינו $\frac{n^2}{4k}$, ואכן אם $2\sqrt{\frac{n^2}{4k}k} = n$ נקודות מתוכן על הפולינום, נוכל למצוא קבוצה L מגודל $O(poly(n))$ כך ש $m \in L$ בעזרת List Decoding.

כלומר, עבור $R = \frac{n}{4k}$, אם $r \leq R$ אזי ניתן לבצע List Recovery בעזרת List Decoding ולהחזיר קבוצה L מגודל $O(poly(n))$ כך ש $m \in L$ כנדרש.