

# סיבוכיות

© ארזים

28 במרץ 2017

## 1 קושי חישובי

בשיעור שעבר התחלנו לדבר על החיוביות בקושי חישובי. דיברנו על פרוטוקול RSA: לוקחים  $p, q$  ראשוניים, וקובעים  $N = pq$ . לוקחים  $e$  שזר למכפלה  $(p-1)(q-1)$ , ולוקחים  $d$  המקיים

$$ed = 1 \pmod{(p-1)(q-1)}$$

ההצפנה היא

$$Enc(x) = x^e \pmod{N}$$

כעת נעבור לדון בפרוטוקול רבין.

### 1.1 פרוטוקול רבין

בפרוטוקול זה, לוקחים שני ראשוניים  $p, q \equiv 3 \pmod{4}$ . מגדירים  $N = pq$ , ומצפינים על ידי  $x \mapsto x^2 \pmod{N}$ . פענוח על ידי משפט השאריות הסיני:

**משפט 1.1** (משפט השאריות הסיני) יהיו  $a, b$  מספרים זרים. אזי ההעתקה

$$f : \mathbb{Z}/ab\mathbb{Z} \rightarrow (\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$$
$$f(x) = (x \pmod{a}, x \pmod{b})$$

היא חד־חד־ערכית ועל, ניתנת לחישוב באופן יעיל, וגם ההעתקה ההופכית ניתנת לחישוב באופן יעיל.

**הוכחה:** גודל התחום והטווח זהה, ולכן מספיק להראות חד־חד־ערכיות. נניח כי  $x, y \in \mathbb{Z}/ab\mathbb{Z}$  עם

$$x \equiv y \pmod{a}$$
$$x \equiv y \pmod{b}$$

מכאן

$$a, b \mid x - y$$

ולכן

$$ab \mid x - y$$

כלומר  $x = y$ .  
ברור שחישוב ההעתקה ניתן לביצוע ביעילות. נראה כיצד לחשב את ההעתקה ההופכית.  
 $a, b$  זרים, ולכן ניתן למצוא בעזרת אלגוריתם אוקלידס המורחב מספרים  $\alpha, \beta$  כך שמתקיים  $a\alpha + b\beta = 1$ . כעת,

$$a\alpha \pmod{b} = 1$$

$$a\alpha \pmod{a} = 0$$

$$b\beta \pmod{a} = 1$$

$$b\beta \pmod{b} = 0$$

בהינתן  $(x_1, x_2) \in \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ , ניקח

$$x = x_1 b\beta + x_2 a\alpha \pmod{ab}$$

ומהמשוואות שלמעלה מתקיים בדיוק

$$x \pmod{a} = x_1$$

$$x \pmod{b} = x_2$$

■

כעת אנחנו מוכנים לפענח בפרוטוקול רבין - בהנתן  $y = x^2$ , נחשב את  $y \pmod{p}$ ,  $y \pmod{q}$ , נחשב שורשים

$$x_1^2 = y \pmod{p}$$

$$x_2^2 = y \pmod{q}$$

ואז נשלב בעזרת משפט השאריות הסיני כדי למצוא את השורשים של  $y \pmod{N}$ .

**טענה 1.2** יהי  $p$  ראשוני כך שמתקיים  $p \equiv 3 \pmod{4}$ . בהינתן  $y = x^2$  מתקיים

$$y^{\frac{p+1}{4}} \in \{x, -x\}$$

**הוכחה:** היות ומתקיים  $y = x^2$ , נקבל

$$y^{\frac{p+1}{4}} = x^{\frac{p+1}{2}}$$

נרצה להוכיח כי  $x^{\frac{p+1}{2}} \in \{x, -x\}$  ולשם כך נראה

$$\left(x^{\frac{p+1}{2}}\right)^2 = x^2$$

ואכן

$$\left(x^{\frac{p+1}{2}}\right)^2 = x^{p+1} = x^p \cdot x = x^2$$

■

**הערה 1.3** כל החישובים מתבצעים מודולו  $p$ , ובשדה מתקיים לכל  $x$ :

$$x^p = x$$

כעת, בשביל הפענוח, נמצא  $\alpha, \beta$  המקיימים  $\alpha p + \beta q = 1$ , ונחשב את ארבעת המספרים הבאים:

$$S_1 = x_1 \beta q + x_2 \alpha p \pmod{N}$$

$$S_2 = -x_1 \beta q + x_2 \alpha p \pmod{N}$$

$$S_3 = x_1 \beta q - x_2 \alpha p \pmod{N}$$

$$S_4 = -x_1 \beta q - x_2 \alpha p \pmod{N}$$

**טענה 1.4**  $S_i^2 = x^2$  לכל  $i \in \{1, 2, 3, 4\}$

■

**הוכחה:** נובע ממה שהראינו.

קיבלנו ארבעה פתרונות אפשריים. איך נדע מהו  $x$  המקורי? אין תשובה טובה.

**טענה 1.5** אם יש אלגוריתם שבהינתן  $y = x^2 \pmod{N}$  מחזיר אחד מארבעת הפתרונות האפשריים, אזי בהתסברות גבוהה, נצליח לחשב את  $p, q$ .

**הוכחה:** נבחר באקראי  $x \in \mathbb{Z}/n\mathbb{Z}$ . נחשב  $y = x^2$ , ונבקש מהאלגוריתם שורש. נשים לב שבהסתברות  $\frac{1}{2}$ , נקבל פתרון שאינו  $x$  או  $-x$ . אם קיבלנו פתרון  $z \notin \{x, -x\}$  אז נשים לב כי  $z - x$  או  $z + x$  הוא 0 מודולו  $p$  או מודולו  $q$ , אבל לא מודולו  $N$ . נחשב gcd עם  $N$ , ונקבל את  $p$  או את  $q$ .

■

## 1.2 שימוש של RSA - חתימה דיגיטלית

בהנתן מסמל  $x \in (\mathbb{Z}/N\mathbb{Z})^*$ , כאשר  $N = pq$ , ראשוניים, החתימה שלי עליו תהיה  $x^d \pmod N$ . המפתח הפומבי הוא  $e$ , כמו בפרוטוקול RSA. כדי לוודא שאכן אני חתמתי כראוי, בהנתן חתימה  $y$ , מחשבים את  $y^e \pmod N$ , ובודקים האם קיבלנו את המסמך המקורי (לפי מה שהוכחנו בעבר).

## 2 חישוביות

סיימנו לדון במבוא ובמוטיבציה לקורס. נעבור לדון בחישוביות ובמודלים חישוביים.

### 2.1 ייצוגים/סימונים

מחרוזות או קלטים יוגדרו בדרך כלל מעל האלפבית  $\{0, 1\}$ , אבל נרשה גם (וישמש אותנו) אלפבית כללי, סופי,  $\Sigma$ . כלומר, קלטים יהיו מתוך  $\Sigma^*$ .  
 $\varepsilon$  מסמן את המילה הריקה,  $|x|$  מסמן את האורך של המילה  $x$ .  
לעתים נדבר על קלטים מתוך  $\Sigma^* \times \Sigma^*$  וכדומה. הסימן  $\perp$  משמעו Null.

### בעיה חישובית

- בעיית הכרעה: בהינתן קלט  $x$ , רוצים להכריז איזשהו תנאי. כלומר, יש שפה  $L \subseteq \Sigma^*$  ונרצה להכריע האם  $x \in L$ .
- בעיית חיפוש: בהינתן פונקציה  $f: \Sigma^* \rightarrow \Sigma^*$  וקלט  $x \in \Sigma^*$ , נרצה לחשב את  $f(x)$ .
- באופן כללי יותר, בהנתן יחס  $S \subseteq \Sigma^* \times \Sigma^*$ ,  $x \in \Sigma^*$ , נרצה למצוא  $y \in \Sigma^*$  שמקיים  $(x, y) \in S$ .

### 2.2 מודל החישוב

**הגדרה 2.1** מכונת טיורינג בעלת סרט אחד היא שביעייה סדורה:

$$M = (Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$$

כאשר:

- $Q$  קבוצה סופית (של מצבים).
- $\Sigma$  אלפבית הקלט, שלא מכיל את הסימנים  $\vdash, \dashv$ .
- $\delta: Q \times \Gamma \rightarrow Q \times \Gamma \times \{\leftarrow, \rightarrow\}$  פונקציית מעבר.
- $q_0, q_a, q_r \in Q$ , כאשר  $q_0$  המצב ההתחלתי,  $q_a$  המצב המקבל,  $q_r$  המצב הדוחה.

תהליך החישוב של מכונת טיורינג  $M$ : בהנתן קלט  $x \in \Sigma^*$ , נדמיין שהסרט של  $M$  מאותחל כאשר הוא מתחיל בסימן  $\vdash$ , שמסמן את תחילת הקלט, שאחריו באים כל התווים של  $x$ , ולאחר מכן אינסוף תווי  $\dashv$ . בהתחלה המכונה נמצאת במצב  $q_0$ , ונדמיין ראש קורא שנמצא בתא הראשון בסרט. כעת, כל עוד המכונה לא במצב  $q_a$  או  $q_r$ , מפעילים את  $\delta$  על המצב שלנו כרגע והסימן הכתוב בתא אליו הראש מצביע. פועלים לפי מה שחוזר מפונקציית המעבר:

היא מחזירה  $(q, \sigma, d)$ . משנים את המצב הפנימי למצב  $q$ , כותבים  $\sigma$  בתא הסרט עליו הראש מצביע, ומזיזים את הראש לתא הסמוך בכיוון שאליו  $d$  מצביע. כעת, אם המכונה עצרה במצב  $q_a$ , נאמר כי היא קיבלה את  $x$ , ואם היא עצרה במצב  $q_r$  נאמר שהיא דחתה את  $x$ . בשני המצבים נאמר כי המכונה הכריעה את  $x$ . אם היא לא מכריעה, לפי הגדרתנו, המכונה רצה לנצח.

בהינתן שפה  $L \subseteq \Sigma^*$ , נאמר כי מכונה  $M$  מכריעה את  $L$  אם לכל  $x \in L$ ,  $M$  מקבלת את  $x$ , ולכל  $x \notin L$ ,  $M$  דוחה את  $L$ . עבור מכונה מסויימת  $M$ , נגדיר את  $L(M)$  להיות שפת כל המילים שהמכונה מקבלת.

חישוב יחסים על ידי מכונות טיורינג: בהינתן קלט  $x$ , נאמר שהפלט של מכונת טיורינג  $x$  הוא המחרוזת הכתובה על הסרט של  $M$  אחרי הקלט  $x$ , בעת עצירת המכונה. נאמר כי  $M$  מכריעה את היחס  $R$  אם לכל  $x$  עבורו יש  $y$  עם  $(x, y) \in R$ , מתקיים כי  $M$  בריצתה על  $x$ , עוצרת במצב  $q_a$ , והפלא שלה הוא  $y'$  שמקיים  $(x, y') \in R$ . אם אין  $y$  כזה, נרצה שבריצה על  $M$ ,  $x$  תעצור במצב  $q_r$ .

**טענה 2.2** קיימות שפות שלא ניתנות להכרעה.

**הוכחה:** עוצמת קבוצת כל מכונות הטיורינג היא בת מניה. לעומת זאת, עוצמת קבוצת כל השפות היא כעוצמת קבוצת החזקה של  $\{0, 1\}^*$ , שהיא לא בת מניה. ■

**דוגמאות** לשפות לא כריעות:

$$A_{TM} = \{ \langle M, w \rangle \mid M \text{ is a TM which accepts } w \}$$

$$H_{TM} = \{ \langle M, w \rangle \mid M \text{ is a TM which halts on } w \}$$

$$H_{TM, \varepsilon} = \{ \langle M \rangle \mid M \text{ is a TM which halts on } \varepsilon \}$$

חישוב יוניפורמי - מכונת טיורינג היא מודל חישוב יוניפורמי, במובן שהיא אמורה לעבוד לכל אורך קלט.

### 2.3 חישוב לא יוניפורמי

מודל חישוב שתלוי באורך הקלט.

**הגדרה 2.3** מעגל בוליאני על  $n$  קלטים הוא גרף מכוון חסר מעגלים. כל קודקוד בגרף הוא אחד מבין

1. שער קלט - שערים ללא קשתות נכנסות (דגת כניסה 0).

2. שער לוגי - אחד מבין  $\wedge, \vee, \neg$ .

שער בעל דרגת יציאה 0 נקרא שער פלט. לשער המסומן  $\neg$  יש דרגת כניסה 1.

החישוב בעזרת מעגל בוליאני מתבצע באופן הבא: בהנתן מעגל עם  $n$  שערי קלט, ממוספרים  $1, \dots, n$ , וקלט  $x \in \{0, 1\}^n$ , נתאים את הביט  $i$  של  $x$  לשער הקלט  $i$ . כל שער שידועים הערכים של כל הכניסות שלו יחשב את הפונקציה שכתובה בו (NOT על הכניסה היחידה שלו, AND/OR על הכניסות שלו). כך נמשיך עד שנחשב את הערך של כל שערי הפלט. הפלט של המעגל הוא הערך הכתוב בשערי הפלט (שגם הם ממוספרים).

בהנתן מעגל בוליאני  $C$  עם  $n$  קלטים ושער פלט יחיד, נאמר כי  $C$  מקבל את  $x$  אם על קלט  $x, C$  מוציא 1. אחרת,  $C$  דוחה את  $x$ .  
 נשים לב כי כל  $x \in \{0, 1\}^n$  מתקבל או נדחה על ידי  $C$ . נאמר כי  $C$  מחשב את  $L_n \subseteq \{0, 1\}^n$  אם  $C(x) = 1$  (סימון שאומר שעל  $x$  המעגל  $C$  מוציא 1) אם ורק אם  $x \in L_n$ .  
 נאמר כי סדרת מעגלים  $\{C_n\}$ , כאשר  $C_n$  הוא מעגל בעל  $n$  קלטים, מחשבת שפה  $L \subseteq \{0, 1\}^*$  אם  $C_n$  מחשב את  $L \cap \{0, 1\}^n$ .

**משפט 2.4** (שנוכיח בשיעור הבא) לכל שפה  $L$  יש משפחת מעגלים המחשבת את  $L$ .