תרגול מס' 1 במבוא לקריפטוגרפיה מודרנית

17 באוקטובר 2013

1 מנהלה

- ניר ביטנסקי.
- תרגולים: יום ה' 10:00,11:00.
- שעת קבלה: תיאום במייל nirbitan@tau.ac.il.

2 הנחות חישוביות

- הנחת בסיס: קיימות בעיות חישוביות שלא ניתן לפתור "ביעילות" (בזמן פולינומי).
- דוג' טבעית לבעיות קשות הנן בעיות NP־קשות, אבל אלו בד"כ לא מספיקות (לפחות לא ידוע). מעוניינים בבעיות שקשה לפתור לא רק במקרה הקיצוני (Worst-Case), אלא גם במקרה הממוצע (Average-Case), בפרט רוצים שניתן יהיה לייצר בקלות מקרים קשים. דוג' בהמשך.
- נדון בשני סוגי הנחות:

1. הנחות כלליות (פרימיטיבים): פונ' חד־כיווניות (One-Way Functions), פונ' חד־כיווניות עם דלת־אחורית (Trapdoor One-Way Functions).
2. הנחות ספציפיות: בעיות בתורת המספרים (Factoring), בעיות קומבינטוריות (Subset-Sum), בעיות למידה (Learning Parity with Noise).

- היררכיה של הנחות, $P \neq NP \rightarrow OWFs \rightarrow TDOWFs \rightarrow \ldots$.

One-Way Functions 3

- איך לחשוב על OWF בציור.

הגדרה 3.1 תהי f פונ' חח"ע כך ש $f : \{0,1\}^n \to \{0,1\}^m$ לכל $n \in N$. נאמר ש־f OWF (חלשה) אם:

1. ניתן לחשב אותה בזמן פולינומי.
2. כל יריב פולינומי A "אינו הופך את f על קלט אקראי, אלא בהסתברות קטנה":

$$\Pr_{x \leftarrow \{0,1\}^n}[A(f(x)) = x] \leq 1/100$$

(לכל $n \in N$ מספיק גדול).

<u>הערות</u>

1. ניתן להגדיר גם עבור פונ' שאינן חח"ע. דורשים שקשה למצוא תמונה הפוכה x' כלשהי כך ש $f(x) = f(x')$.
2. בד"כ חושבים על הגדרה חזקה יותר שבה ההסתברות להפוך "זניחה". ניתן לבנות פונ' חזקה מחלשה.

טענה 3.2 אם קיימות OWFs אז $P \neq NP$.

הוכחה: נראה שלכל f (מועמדת ל־OWF), יש שפת NP, L_f, שאם ניתן להכריע אותה אז ניתן להפוך את f (בהסתברות 1). ■

אינטואיציה: בהנתן קלט $y = f(x)$ היינו רוצים לעשות חיפוש בינארי. יורדים בעץ החיפוש, בכל רמה שואלים האם יש תמונה הפוכה בהמשך (ציור). זו שאלת NP.

$$L_f = \{(y, x_{pre}) \in \{0,1\}^n \times \{0,1\}^k : \exists x_{suf} \in \{0,1\}^{n-k} \text{ s.t. } y = f(x_{pre}x_{suf})\}$$

דוג' לפונ' חד־כיוונית מקושי של לוגריתם דיסקרטי

- תהי Z_p^* החבורה הכפלית מודולו ראשוני p. מורכבת מהאיברים $\{1, 2, \ldots, p-1\}$, עם כפל מודולו p, ויהי g יוצר של החבורה, כלומר $Z_p^* = \{g^i : 0 \leq i < p-1\}$.
- בעיית הלוגריתם הדיסקרטי בחבורה:

- קלט: $y = g^x$ עבור $x \in \{0, \ldots, p-2\}$, אקראי.
- אתגר: מצא את $x = \log_g y$.

- מגדיר מועמד טבעי ל־OWF: $f(x) = g^x$.
- הנחה מקובלת: פונ' זו היא אכן OWF (לא נכון במודל קוונטי).
- מניחים גם בחבורות נוספות, נתקל בחלקן בהמשך הקורס.
- אינטואיציה חלקית לכך שהבעיה קשה: נסתכל על הפונ' $x = \log_g y$ עבור $p = 11$ עם היוצר $g = 2$:

x	0	1	8	2	4	9	7	3	6	5
y	1	2	3	4	5	6	7	8	9	10

- אם מסתכלים על $\log_2 y$ מעל השלמים Z, הפונ' הנה מונוטונית וקלה לחישוב. ב־Z_p^* לעומת זאת היא איננה מונוטנית וקשה לחזות את התנהגותה.