תרגול מס' 7 במבוא לקריפטוגרפיה מודרנית

27 בנובמבר 2013

(Partially) Homomorphic Encryption

- מוטיבציה: מעוניינים כי אמזון יבצעו עבורנו חישובים על־גבי מידע רגיש. האם ניתן לחשב ע"ג מידע מוצפן?

הגדרה 0.1 תהי $\odot : \{0,1\} \times \{0,1\} \to \{0,1\}$ פעולה בינארית. נאמר כי מערכת הצפנה (עבור ביטים) הומומורפית ביחס ל־$\odot$ אם קיימת פעולה בינארית על צפנים $\tilde{\odot}$ כך ש:

$$E(b_1)\tilde{\odot}E(b_2) = E(b_1 \odot b_2)$$

- עבור הצפנה סימטרית / אסימטרית
- עבור הצפנה הסתברותית: $\forall r_1, r_2 \exists r_3 : E(b_1; r_1)\tilde{\odot}E(b_2, r_2) = E(b_1 \odot b_2; r_3)$

Example from Class: the Goldwasser-Micali QR System

- מפתח פרטי: $p, q \equiv 3 \mod 4$ (במקרה זה $-1 \in J^+ \setminus QR$)
- מפתח פומבי $N = pq$
- הצפנה של ביט b: דוגמים $r \leftarrow Z_N^*$ ומצפינים $(-1)^b r^2$.
- פענוח: בודקים האם הצופן שארית ריבועית.
- הומומורפית ל־$\oplus$ (חיבור מודולו 2): $(-1)^{b_1} r_1^2 \cdot (-1)^{b_2} r_2^2 = (-1)^{b_1+b_2 \mod 2}(r_1 r_2)^2$

Private Information Retrieval

- Chor-Goldreich-Kushilevitz-Sudan
- מטרה: מעוניינים למשוך מידע מ־DB בגודל N מבלי לחשוף את השאילתא בפני השרת.
- מה ניתן לדרוש לגבי סודיות השאילתא? האם אפשר לקבל סודיות מושלמת?
- פתרון אחד: מודל בו יש כמה שרתים שאינם יכולים לתקשר.
- פתרון אחר: סודיות רק נגד שרתים הרצים בזמן פולינומי.
- באופן כללי מערכת PIR תכלול שלושה אלגוריתמים:
  - E מצפין בעזרת מפתח סודי sk שאילתא $1 \leq i \leq N$: $c = E_{sk}(i)$
  - A בהנתן שאילתא מוצפנת מחשב תשובה: $a = A(DB, c)$
  - D מפענח בעזרת sk את התשובה: $DB[i] = D_{sk}(a)$
- דרישת הבטיחות, לכל $i, j \in [N]$

$$E_{sk}(i) \approx_{c,\epsilon} E_{sk}(j)$$

- המטרה: למזער את התקשורת עם השרת.

בנייה מהצפנה הומומורפית עם סיבוכיות $\sqrt{N}$

- Kushilevitz-Ostrovsky
- תהי (E, D) הצפנה הומומורפית ביחס ל $+ \mod 2$
- חימום: בהנתן N הצפנות של ביטים $E(b_1) \dots E(b_N)$ ו־N ביטים (לא מוצפנים): $a_1 \dots a_N$, כיצד נחשב $E(\sum_{j=1}^{N} a_j b_j \mod 2)$?
- נניח כי רק מעוניינים כי התשובה של השרת a תהיה קצרה (בעוד שהשאיתא יכולה להיות ארוכה).
  - שאילתא עבור כניסה $i \in [N]$: N הצפנות $E_{sk}(b_1) \dots E_{sk}(b_N)$ כאשר $b_j = \begin{cases} 1 & j = i \\ 0 & j \neq i \end{cases}$.

- תשובה: השרת יחשב $E(\sum_{j=1}^{N} DB[j] \cdot b_j)$
- תשובת השרת קצרה כגודל k של הצפנת ביט יחיד ובאופן טיפוסי $k \ll N$. אולם התקשורת הכוללת $\Omega(N \cdot k)$

- מעוניינים במערכת עם תקשורת כוללת $O(\sqrt{N} \cdot k)$
- נסדר את ה־DB במטריצה בגודל $\sqrt{N} \times \sqrt{N}$.
- נשתמש בפתרון הקודם על כל אחת משורות המטריצה על־מנת ללמוד את העמודה ($i \mod \sqrt{N}$) במטריצה שבה נמצאת הכניסה ה־i .
- תקשורת כוללת: $2\sqrt{N} \cdot k$.
- ניתן להכליל ולקבל פתרון $O(d \cdot \sqrt[d]{N} \cdot k^{d-1})$ - בתרגיל בית.

More from Partially Homomorphic Encryption

- כיצד ניתן לבנות CRH מהצפנה הומורפית?
- כיצד ניתן לבנות CRH מ־PIR?