02/01/2014

קריפטוגרפיה: תרגיל 5

<u>הגשה</u>: יום ד' 15/1/14 ב 14:10 בהרצאה.

שאלה 1

נגדיר את האופרטור האקראי הבא (הפועל על ביט בודד ומחזיר ביט בודד):

$$\text{flip}_\alpha(z) = \begin{cases} z & , \text{ with probability } (1/2 + \alpha) \\ 1 - z & , \text{ otherwise} \end{cases}.$$

נסמן ב A את האלגוריתם אשר בהינתן database קלט $x = (x_i) \in \{0,1\}$ מחזיר את הפלט $\text{flip}_{\varepsilon/6}(x_i)$. הראו כי אלגוריתם A משמר ε-פרטיות דיפרנציאלית עבור $0 < \varepsilon < 1$.

הערה: הנכם רשאים להשתמש באי שוויון $1 + \varepsilon < e^\varepsilon$ עבור $0 < \varepsilon < 1$.

שאלה 2

נסתכל על הסכמה הבאה לחלוקת סוד t-מתוך-n. יהי p ראשוני כך ש- $p > n$. לחלק סוד $s \in Z_p$, המחלק מגריל t-1 איברים אקראיים $r_0, r_1, ..., r_{t-2}$ מתוך Z_p, מסתכל על הפולינום $Q(x) = (s \cdot x^{t-1} + \sum_{j=0}^{t-2} r_j \cdot x^j) \bmod p$ ונותן למשתתף i את החלק $Q(i)$. שימו לב כי הסוד הוא המקדם של x^{t-1} .

סעיף א

הראו כי כל קבוצה של משתתפים בגודל לפחות t יכולה לשחזר את הסוד בצורה יעילה מתוך החלקים שקיבלה.

סעיף ב

נסתכל על הפולינום $R(x) = (\sum_{j=0}^{t-2} r_j \cdot x^j) \bmod p$. הוכיחו כי אם משתתף i יודע מהו הסוד, אזי הוא יכול לחשב את $R(i)$ מתוך $Q(i)$.

סעיף ג

הוכיחו כי כל קבוצה בגודל t-1 לא מקבלת מידע על הסוד מתוך החלקים שלה, כלומר, בהינתן החלקים כל סוד $s \in Z_p$ אפשרי.

שאלה 3

1. מערכת הצפנה עם מפתח פרטי (E, D, Gen) נקראת <u>נכונה</u> אם כל הודעה m המוצפנת במפתח מפוענחת במפתח ל- m.
2. מערכת הצפנה עם מפתח פרטי (E, D, Gen) נקראת <u>בטוחה</u> אם היא בטוחה על פי ההגדרה שניתנה בכיתה.

סעיף א

נתונות 2 מערכות הצפנה עם מפתח פרטי

$$(E_1, D_1, Gen_1)$$
$$(E_2, D_2, Gen_2)$$

ידוע כי שתיהן נכונות, אך בדיוק אחת מהן בטוחה. לא ידוע מי מהן היא המערכת הבטוחה. בנוסף, נתונה סכמה לחלוקת סוד 2 מתוך 2. מוצעת מערכת ההצפנה הבאה:

- **יצירת מפתחות:**
  הרץ Gen_1 לקבלת k_1, הרץ Gen_2 לקבלת k_2.
  המפתח הסודי: (k_1, k_2).
- **הצפנה של הודעה m:**
  חלק את m על פי סכמה לחלוקת סוד 2 מתוך 2. נסמן את החלקים ב- s_1, s_2.
  חשב $C_1 \leftarrow Enc_1(s_1, k_1)$ ו- $C_2 \leftarrow Enc_2(s_2, k_2)$
  פלוט את ההצפנה $C = (C_1, C_2)$.

הראו כיצד לפענח הודעה במערכת והסבירו מדוע המערכת הנ"ל היא נכונה, ומדוע היא בטוחה.

סעיף ב

נתונות 3 מערכות הצפנה. ידוע שלפחות 2 מהן נכונות ושלפחות 2 מהן בטוחות. לא ידוע איזה מהן בטוחות ואיזה מהן נכונות. הראו מערכת הצפנה העונה על הדרישות הבאות:

1. המערכת משתמשת רק במערכות הצפנה הנתונות ובסכמת חלוקת סוד לפי בחירתכם.
2. המערכת בטוחה.
3. מפענח אשר יודע אילו מבין שלושת המערכות הן הנכונות, יכול לפענח הצפנות (המצפין <u>לא</u> יודע מיהן הנכונות ומיהן הבטוחות).

הסבירו מדוע המערכת שבניתם עונה לדרישות 2 ו- 3.

סעיף ג

נתונות 5 מערכות הצפנה. ידוע שלפחות 4 מהן נכונות ושלפחות 4 מהן בטוחות. לא ידוע איזה מהן בטוחות ואיזה מהן נכונות. הראו מערכת הצפנה נכונה ובטוחה המשתמשת רק במערכות הצפנה הנתונות ובסכמת חלוקת סוד לפי בחירתכם.
<u>שימו לב</u>: כאן גם המצפין וגם המפענח לא יודעים מיהן המערכות הבטוחות ומיהן המערכות הנכונות.

הסבירו מדוע המערכת שבניתם עונה לדרישות.

שאלה 4

סעיף א

נסתכל על הפרוטוקול PIR שתואר בכיתה עם 2 שרתים וסיבוכיות תקשורת $O(n^{1/2})$. הראו כי אם שני השרתים משתפים פעולה אזי הם יכולים ללמוד מידע על הביט שהמשתמש מבקש. הסבירו תשובתכם בקצרה.

סעיף ב

נאמר כי פרוטוקול PIR עם k שרתים הוא $t-$פרטי אם כל t שרתים שמשתפים פעולה לא ילמדו מידע על הביט שהמשתמש מבקש. בסעיפים הבאים נתכנן פרוטוקול PIR 2-פרטי עם 3 שרתים.

תחילה נתכנן פרוטוקול בו סיבוכיות התקשורת מהמשתמש לשרתים היא $O(n)$וסיבוכיות התקשורת מכל שרת למשתמש היא 1. נתאר כיצד המשתמש מכין את השאילתות שלו.

המשתמש רוצה הביט ה- i מתוך מסד נתונים בגודל n.
המשתמש מגריל שתי קבוצות אקראיות $A_1, A_2 \subseteq \{1,...,n\}$.
המשתמש מחשב את הקבוצה $A_3 \subseteq \{1,...,n\}$ הבאה:

1. לכל $j \neq i$ אם j שייך <u>בדיוק</u> לקבוצה אחת מבין A_1, A_2 אזי $j \in A_3$. אחרת, $j \notin A_3$.
2. אם i שייך <u>בדיוק</u> לקבוצה אחת מבין A_1, A_2 אזי $i \notin A_3$. אחרת, $i \in A_3$.
3. המשתמש שולח את הקבוצה A_ℓ לשרת ℓ.

הסבירו מדוע כל שני שרתים שישתפו פעולה לא ילמדו מידע על הביט שהמשתמש מבקש.

סעיף ג

הראו כיצד כל שרת יכול לשלוח ביט אחד למשתמש כך שהמשתמש יכול לשחזר את הביט ה- i. הסבירו כיצד המשתמש מחשב את הביט ה- i, והוכיחו כי חישוב זה נכון.

סעיף ד

תכננו פרוטוקול PIR פרטי עם 3 שרתים כך שסיבוכיות התקשורת הכללית היא $O(n^{1/2})$. תארו את הפרוטוקול והסבירו מדוע הוא נכון, למה הוא שומר על פרטיות ומדוע סיבוכיות התקשורת היא כמבוקש.