תרגול מס' 4 במבוא לקריפטוגרפיה מודרנית

6 בנובמבר 2013

Hardcore Bits

- דיברנו על פסאודו־אקראיות כמוטיב מרכזי בקריפטוגרפיה.
- ראינו שאפשר שפסאודו־אקראיות נובעת מהנחות קושי מסוימות כמו DDH.
- באופן די מדהים, ניתן לקבל פסאודו־אקראיות ישירות מ־OWF (למעשה מכל OWF).

הגדרה 0.1 (Hardcore Bit (HCB)). תהינה $f : \{0,1\}^n \to \{0,1\}^m$ ו־$B : \{0,1\}^n \to \{0,1\}$ פונ'. נאמר כי B היא $\epsilon - HCB$ עבור f, אם

$$f(x), B(x) \approx_{c,\epsilon} f(x), u$$

כאשר $x \leftarrow U_n$ (בשתי ההתפלגויות) ו־$u \leftarrow U_1$ בלתי תלוי ב־x.
או באופן שקול, לכל יריב פולינומי A

$$\Pr_{x \leftarrow U_n}[A(f(x)) = B(x)] \leq \frac{1+\epsilon}{2}$$

- כיצד בונים PRG מ־HCB?
- מקרה פרטי: נניח כי f פרמוטציה. נגדיר

$$PRG(x) = f(x), B(x)$$

- מה אם רוצים למתוח ביותר מביט יחיד?

משפט 0.2 ($Goldreich - Levin$) לכל OWF יש HCB.

Hardcore Bit for DL in Z_p^*

- נזכר ב־פונ' : $EXP : Z_p^* \to Z_p^*$ (אפילו פרמוטציה), בהנתן יוצר $g \in Z_p^*$

$$x \overset{EXP}{\longmapsto} g^x$$

- האם בהניחנו קושי של DL יש לפונ' HCB?
- למשל $PARITY(x) = x \mod 2$, האם הנה HCB? (רמז:QR)

טענה 0.3 ($Blum - Micali$) נגדיר $Half : Z_p^* \to \{0,1\}$ באופן הבא

$$Half(x) = 1 \text{ iff } x \in \left[1, \frac{p-1}{2}\right]$$

אז $Half(x)$ הנה HCB עבור EXP.

- נפתח כלים, ונוכיח מקרה פשוט. את המקרה הכללי נוכיח באופן מודרך בשיעורי הבית.

תזכורת: שאריות ריבועיות

- תת החבורה של השאריות הריבועיות ב־Z_p^*: $QR = \{g^{2s} : 1 \leq s \leq \frac{p-1}{2}\}$
- אמרנו שלכל ריבוע g^{2s} יש שני שורשים g^s ו־$-g^s$, דרך אחרת לכתוב את השורש השני $g^{s+\frac{p-1}{2}}$, השורש הראשון נקרא "השורש העיקרי".
- אינטרפטציה ל־$Half(x)$: "האם g^x הוא השורש העיקרי של g^{2x}?"
- <u>עובדה:</u> ב־Z_p^* , ניתן לבדוק האם ריבועיות ביעילות. ניתן לחשב ביעילות שורשים, **אבל לא תמיד מקבלים את השורש העיקרי**. (בתרגיל בית: נראה עבור $p = 3 \mod 4$.)
- <u>מטרה:</u> להראות כי אם $A(g, g^x)$ מחשב את $B(x)$ בהס' טובה (גדולה מ־$1/2+\delta$) על פני $x \leftarrow Z_p^*$ אקראי, אז אפשר לפתור DL בהסתברות טובה (הקשורה ל־δ).

טענה 0.4 (חימום) אם $A(g, g^x) = Half(x)$ בהס' 1 (כלומר לכל x), אז אפשר לפתור DL בהס' 1.

אסטרטגיה: בהנתן g^y נשתמש ב־$Half$ בשביל למצוא את $y = \sum_0^{n-1} b_i 2^i =$ "$b_{n-1} \dots b_0$" בעזרת חיפוש בינארי (יש שתי דרכים לחיפוש בינארי).

- כיצד נמצא את b_0? נבדוק QR
- כיצד נצא את b_1?
  - נעבור מ־g^{y_0},כאשר $y_0 = y$, ל־g^{y_1} כאשר "$y_1 = "b_{n-1} \dots b_1 0$ ע"י כפל ב־g^{-1} בהתאם ל־b_0.
  - נעבור מ־g^{y_1} ל־$g^{y_1'}$ כאשר "$y_1' = "b_{n-1} \dots b_1$. כיצד?
  - נחשב שורש ? מה מקבלים? (ציור) כיצד נחליט את מי לקחת?
- אתגר: כיצד נשתמש בפונ' $Half$ "רועשת" - טועה הרבה, אבל רוב הפעמים צודקת?