תרגול מס' 5 במבוא לקריפטוגרפיה מודרנית

14 בנובמבר 2013

Collision-Resistant Hash Functions

הגדרה 0.1 (CRH). פונ' $h : \{0,1\}^{n+s} \to \{0,1\}^n$ היא $\epsilon - CRH$, אם לכל יריב פולינומי

$$\Pr_A[x \neq x' \leftarrow A(h) : h(x) = h(x')] \leq \epsilon$$

(עבור n מספיק גדול)

- יותר בכלליות ניתן לדבר על משפחה $\{h_k\}$ ולדרוש

$$\Pr_{A,k}[x \neq x' \leftarrow A(k) : h_k(x) = h_k(x')] \leq \epsilon$$

(עבור n מספיק גדול) הגיוני גם במודל שבו ליריב יש מידע קודם (נקרא "לא יוניפורמי")

- מוטיבציה - אותנטיקציה קצרה של מידע.
- בעיה מהעולם האמיתי: רוצים לאכסן DB גדול אצל גוגל, למשל את הציונים של כל תלמידי האוניברסיטה.
- בעת משיכת המידע: רוצים לוודא שאכן מדובר במידע ששמרנו. המידע יכול להשתנות:
  - באופן תמים: כתוצאה מכשל מקרי.
  - באופן זדוני: ע"י אחד התלמידים, ע"י גוגל (אולי על-מנת לחסוך מקום).

- פתרון נאיבי: בהנתן DB $d \in \{0,1\}^N$ נשתמש ב־CRH : $h : \{0,1\}^N \to \{0,1\}^K$ עבור K קטן למשל $\sqrt{N}$, או אפילו $\log^2 N$ (הנחה חזקה יותר. כמה זמן יקח לשבור האש עם תמונה בגודל K בכוח?). נשמור רק את $h(d)$.
- בעת משיכת מידע עתידית מגוגל, כיצד נבדוק שאכן קיבלנו את המידע שאכסנו?
- האם הפתרון פרקטי? (כמה זמן נדרש למשיכת $N \ll 10$ ביטים מסוימים? כמה זמן יקח לעדכן מס' דומה של ביטים.
- פתרון טוב יותר : (Merkle Hash): נניח בה"כ $N = 2^n$, ניקח $h : \{0,1\}^{2K} \to \{0,1\}^K$, עבור $K = 2^k$ "קטן".
- נבנה עץ אותנטיקציה בינארי (ציור). $\frac{N}{K} = 2^{n-k}$ בלוקים. עומק העץ $n - k \leq \log N$.
- כיצד מוודאים בלוק? עלות: $O(K \log N)$.
- אם גוגל מצליחה לרמות, אז היא יודעת למצוא התנגשויות ב־h.
- האם אפשר לעדכן?
- הערה: לא צריך CR מלא, דרישה חלשה יותר ־ TCR.

Keyed CRH from DL

- יהי $g \in Z_p^*$ יוצר.
- נגדיר משפחה של פונ' $\{h_z : z \in Z_p^*\}$כאשר : $h_z : Z_p^* \times Z_p^* \to Z_p^*$ באופן הבא:

$$(x, y) \longmapsto z^x \cdot g^y = g^{wx+y} \text{ where } z = g^w$$

טענה 0.2 יהי A יריב המוצא התנגשויות

$$\Pr_{z \leftarrow Z_p^*}[(x, y) \neq (x', y') \leftarrow A(z) : z^x \cdot g^y = z^{x'} g^{y'}] \geq \epsilon$$

אז אפשר לבנות יריב ששובר DL בהס' דומה.

הוכחה: בהנתן g^w עבור w אקראי נריץ $A(z)$ כאשר $z = g^w$ (מדוע לדגום $z \leftarrow Z_p^*$ ולדגום $z = g^w$ עבור $w \leftarrow Z_p^*$ זה אותו הדבר?). נמצא $(x, y) \neq (x', y')$ כך שך $xw + y = x'w + y'$. ■

OWF vs. CRH

- מה יותר חזק?
- האם אפשר לבנות OWF מ־ CRH ולהפך?

טענה 0.3 נניח כי $H : \{0,1\}^{2n} \to \{0,1\}^n$ היא CR, אז היא גם OW.

הוכחה: נניח ראשית הנחה מפשטת, הפונ' רגולרית. לכל איבר בתמונה בדיוק 2^n איברים בתמונה ההפוכה. נניח כי Aמוצא התנגשויות בהס' ϵ, נראה A' שהופך בהס' $\epsilon(1-2^{-n})$ ■