מבוא לקריפטוגרפיה ואבטחת תוכנה
תרגיל 2

רן שחם - 203781000

27 באפריל 2017

שאלה 1

עבור כל ניסוי, נסמן ב־$\mathcal{Q}$ את קב' השאילתות של היריב את האורקל $\mathrm{Mac}(\cdot)$.

סעיף 1

נבנה יריב $\mathcal{A}$ הפועל כך: בהינתן קלט 1^n וגישת אורקל ל־$\mathrm{Mac}_k(\cdot)$ עבור $k \leftarrow \mathrm{Gen}(1^n)$ כלשהו, יחשב את $t = \mathrm{Mac}_k(0^n \| 1^n)$ ויפלוט (m,t) כאשר $m = 1^n \| 0^n$. נשים לב ש־$m \notin \mathcal{Q}$ כי $\mathcal{Q} = \{0^n \| 1^n\}$. כמוכן, $t = F_k(1^n) \oplus F_k(0^n) = F_k(0^n) \oplus F_k(1^n)$ ולכן t הוא תיוג תקף עבור m - כלומר $\mathrm{Vrfy}(k,(m,t)) = 1$. לכן $\Pr\left[\mathrm{MacForge}_{\mathcal{A},\Pi}(n) = 1\right] = 1$ ולכן המערכת אינה בטוחה.

סעיף 2

בהינתן קלט 1^n וגישת אורקל, $\mathcal{A}$ יחשב את $t = \mathrm{Mac}\left(0^{n/2} \| 1^{n/2}\right)$. נגדיר $t' = t[0 \ldots n-1]$ כלומר t' הוא n הביטים הראשונים ב־t. $\mathcal{A}$ יפלוט $\left(0^{n/2}, t'\right)$. ברור ש־$0^{n/2} \notin \mathcal{Q}$ וכן ש־$t' = t[0 \ldots n-1] = F_k\left(\langle 1 \rangle \| 0^{n/2}\right)$ הוא תיוג תקף עבור $0^{n/2}$ ולכן $\Pr\left[\mathrm{MacForge}_{\mathcal{A},\Pi}(n) = 1\right] = 1$ והמערכת אינה בטוחה.

סעיף 3

בהינתן קלט 1^n $\mathcal{A}$ יחשב $(r,t_1) = \mathrm{Mac}_k(0^n)$ ו־$(s,t_2) = \mathrm{Mac}_k(0^n)$ ויפלוט $(r,(s,t_3))$ כאשר $t_3 = t_1 \oplus t_2$.
כמובן ש־$r \notin \mathcal{Q} = \{0^n\}$. כמוכן $t_1 = F_k(r) \oplus F_k(0^n)$ ו־$t_2 = F_k(s) \oplus F_k(0^n)$ ולכן:

$$t_3 = t_1 \oplus t_2 = (F_k(r) \oplus F_k(0^n)) \oplus (F_k(s) \oplus F_k(0^n)) = F_k(r) \oplus F_k(s)$$

ומכאן ש־$\mathrm{Vrfy}(r,(s,t_3)) = 1$ בסיכוי 1 - לכן המערכת אינה בטוחה.

שאלה 4

המערכת אינה בטוחה. יהי H PRG מכפיל אורך. נגדיר:

$$G(s_1 \| s_2) = H(s_1) \| H(s_2)$$

כאשר $s_1 \in \{|s_2|, |s_2|+1\}$. מהתרגיל הקודם, G הוא PRG וכן ברור ש־G מכפיל אורך.
יהי $k \leftarrow \mathrm{Gen}(1^n) \in \{0,1\}^n$. נבנה יריב $\mathcal{A}$ הפועל כך: בהינתן קלט 1^n וגישת אורקל ל־$\mathrm{Mac}_k(\cdot)$, יחשב את $t = \mathrm{Mac}_k(0^n)$ וכן את $H(1^n)$. נגדיר $t' = t[0 \ldots 2n-1]$ כלומר t' הוא $2n$ הביטים הראשונים של t. לבסוף $\mathcal{A}$ יפלוט $(1^n, t' \| H(1^n))$.
נשים לב:

$$\begin{aligned}
t &= \mathrm{Mac}_k(0^n) = G(k \| 0^n) = H(k) \| H(0^n) \\
t' &= t[0 \ldots 2n-1] = H(k) \\
t' \| H(1^n) &= H(k) \| H(1^n) = G(k \| 1^n) = \mathrm{Mac}_k(1^n) \\
1^n &\notin \mathcal{Q} = \{0^n\}
\end{aligned}$$

ולכן $\mathcal{A}$ מצליח בסיכוי 1, כלומר המערכת אינה בטוחה.

שאלה 5

נגדיר את האלגוריתמים הבאים:

- Gen מקבל 1^n ומחזיר $k = k_1 \| k_2$ עבור $k_i \leftarrow \mathrm{Gen}_i(1^n)$ ל־$i = 1, 2$
- Mac מקבל הודעה m ומפתח $k_1 \| k_2$ ומחזיר $t = t_1 \| t_2$ כאשר $t_i = \mathrm{Mac}_{k_i}(m)$
- Vrfy מקבל $(m, t_1 \| t_2)$ ומפתח $k_1 \| k_2$ ומחזיר 1 אם"ם $\mathrm{Vrfy}_1(k_1, (m, t_1)) = \mathrm{Vrfy}_2(k_2, (m, t_2)) = 1$

נראה שהמערכת Π המוגדרת על ידי האלג' הנ"ל היא בטוחה. נניח בשלילה שלא, כלומר שקיים יריב $\mathcal{A}$ ופולינום p כך ש:

$$\Pr\left[\mathrm{MacForge}_{\mathcal{A},\Pi}(n) = 1\right] > \frac{1}{p(n)}$$

לאינסוף ערכי $n \in \mathbb{N}$. מובטח שלפחות אחת מ־Π_1, Π_2 היא בטוחה ונניח בה"כ ש־Π_1 היא בטוחה. נגדיר יריב $\mathcal{A}_1$ שפועל כך: בהינתן קלט 1^n וגישת אורקל ל־$\mathrm{Mac}_1(k_1, \cdot)$ עבור $k_1 \leftarrow \mathrm{Gen}_1(1^n)$ (שלא ידוע ל־$\mathcal{A}_1$), ידגום $k_2 \leftarrow \mathrm{Gen}_2(1^n)$ ויריץ את $\mathcal{A}$ עם 1^n. לכל בקשה של $\mathcal{A}$ עבור הצפנה של m, $\mathcal{A}_1$ יחזיר לו $\mathrm{Mac}_1(k_1, m) \| \mathrm{Mac}_2(k_2, m)$ (הראשון מתקבל מהאורקל והשני ניתן לחישוב יעיל לפי הנחה). לבסוף $\mathcal{A}$ יפלוט $(m^*, t_1 \| t_2)$ ו־$\mathcal{A}_1$ יפלוט (m^*, t_1).

נשים לב ש־$\mathcal{A}_1$ מסמלץ בדיוק את הניסוי $\mathrm{MacForge}_{\mathcal{A},\Pi}(n)$ עבור $\mathcal{A}$, לכל $n \in \mathbb{N}$. נניח ש־$\mathcal{A}$ הצליח בניסוי כלומר ש־$\mathrm{MacForge}_{\mathcal{A},\Pi}(n) = 1$ ־ לכן לפי הגדרה: $\mathrm{Vrfy}(k_1 \| k_2, (m^*, t_1 \| t_2)) = 1$. בפרט, לפי הגדרת Vrfy, מתקיים:

$$\mathrm{Vrfy}_1(k_1, (m^*, t_1)) = 1$$

ולכן $\mathrm{MacForge}_{\mathcal{A}_1,\Pi_1}(n) = 1$. מכאן: [1]

$$\Pr\left[\mathrm{MacForge}_{\mathcal{A}_1,\Pi_1}(n) = 1\right] \geq \Pr\left[\mathrm{MacForge}_{\mathcal{A},\Pi}(n) = 1\right] > \frac{1}{p(n)}$$

לאינסוף n, בסתירה לכך ש־Π_1 בטוחה.

שאלה 6

נניח בשלילה ש־Π אינה בטוחה, כלומר שקיימים יריב $\mathcal{A}$ ופולינום p כך ש:

$$\Pr\left[\mathrm{MacForge}_{\mathcal{A},\Pi}(n) = 1\right] > \frac{1}{p(n)}$$

לאינסוף $n \in \mathbb{N}$. מובטח שאחת מהמערכות Π_1, Π_2 היא בטוחה. נניח בה"כ ש־Π_1 היא מערכת בטוחה, ונראה יריב $\mathcal{A}_1$ ש"שובר" אותה בסיכוי לא זניח.

$\mathcal{A}_1$ יפעל כך: בהינתן קלט 1^n וגישת אורקל ל־$\mathrm{Mac}_1(k_1, \cdot)$ עבור $k_1 \leftarrow \mathrm{Gen}_1(1^n)$, ידגום $k_2 \leftarrow \mathrm{Gen}_2(1^n)$ ויסמלץ את ריצת $\mathcal{A}$ עם הקלט 1^n. עבור בקשה לגישת אורקל של $\mathcal{A}$ להצפנת ההודעה m, יחזיר לו $t = \mathrm{Mac}_1(k_1, m) \oplus \mathrm{Mac}_2(k_2, m)$, כאשר החלק הראשון מתקבל מהאורקל של $\mathcal{A}_1$ והשני מחושב על ידו באופן ישיר. לבסוף, $\mathcal{A}$ יפלוט צמד (m^*, t^*). $\mathcal{A}_1$ יחשב את $t' = t^* \oplus \mathrm{Mac}_2(k_2, m^*)$ ויפלוט (m^*, t').

נניח ש־$\mathcal{A}$ מצליח בניסוי, כלומר ש־$t^* = \mathrm{Mac}(k_1 \| k_2, m^*)$, לכן מהגדרת המערכת:

$$t^* = \mathrm{Mac}_1(k_1, m^*) \oplus \mathrm{Mac}_2(k_2, m^*)$$

ולכן מתקיים:

$$t' = t^* \oplus \mathrm{Mac}_2(k_2, m^*) = \mathrm{Mac}_1(k_1, m^*)$$

כי $\mathrm{Mac}_2(\cdot)$ הוא אלגוריתם דטרמיניסטי, לכן כל הרצה שלו על (k_2, m^*) תיתן את אותו ערך. לכן $\mathrm{Vrfy}(k_1 \| k_2, m^*, t') = 1$ ולכן בכל פעם ש־$\mathcal{A}$ מצליח בניסוי, כך גם $\mathcal{A}_1$. אם כך:

$$\Pr\left[\mathrm{MacForge}_{\mathcal{A}_1,\Pi_1}(n) = 1\right] > \frac{1}{p(n)}$$

לאינסוף n, בסתירה לכך ש־Π_1 בטוחה.

[1] ייתכן ש־$\mathrm{MacForge}_{\mathcal{A}_1,\Pi_1}(n) = 1$ ו־$\mathrm{MacForge}_{\mathcal{A},\Pi}(n) = 0$ ־ למשל אם $\mathcal{A}$ נכשל בגלל ש־ $\mathrm{Vrfy}_2(k_2, (m^*, t_2)) = 0$, לכן אי שווין מתקיים.

שאלה 7

יהיו $\ell_1, \ell_2 : \mathbb{N} \to \mathbb{N}$ כך ש־$H^{(i)} : \{0,1\}^* \to \{0,1\}^{\ell_i(n)}$.
נבנה מערכת בטוחה באופן הבא:

- Gen מקבלת 1^n ומחזירה $s = s_1 \| s_2$ כאשר $s_1 = \mathrm{Gen}^{(1)}(1^n)$ ו־$s_2 = \mathrm{Gen}^{(2)}(1^n)$
- H היא פונקצייה שבהינתן קלט $s = s_1 \| s_2$ ומספר x פולטת $H^{(1)}_{s_1}(x) \| H^{(2)}_{s_2}(x)$

נניח בשלילה שהמערכת אינה בטוחה, כלומר שקיים יריב $\mathcal{A}$ ופולינום p כך שמתקיים:

$$\Pr\left[\mathrm{HashColl}_{\mathcal{A},\Pi}(n) = 1\right] > \frac{1}{p(n)}$$

לאינסוף n. נניח בה"כ ש־$\mathcal{H}^{(1)}$ היא בטוחה. נבנה יריב $\mathcal{A}_1$ הפועל כך: בהינתן קלט s_1, דוגם $s_2 \leftarrow \mathrm{Gen}^{(2)}(1^n)$ ומריץ את $\mathcal{A}$ עם $s_1 \| s_2$.
לבסוף $\mathcal{A}$ פולט x, x' וכך גם $\mathcal{A}_1$.
נניח ש־$\mathcal{A}$ מצליח, כלומר ש־$x' \neq x$ ו־$H_s(x) = H_s(x')$ כאשר $s = s_1 \| s_2$. אם כך:

$$H_{s_1}(x) \| H_{s_2}(x) = H_{s_1}(x') \| H_{s_2}(x')$$

ובפרט, $H_{s_1}(x) = H_{s_1}(x')$. לכן

$$\Pr\left[\mathrm{HashColl}_{\mathcal{A}_1,\Pi_1}(n) = 1\right] \geq \Pr\left[\mathrm{HashColl}_{\mathcal{A},\Pi}(n) = 1\right] > \frac{1}{p(n)}$$

לאינסוף n, בסתירה לכך ש־Π_1 עמידה בפני התנגשויות.