מבוא לקריפטוגרפיה ואבטחת תוכנה
תרגיל 2

רן שחם - 203781000

25 באפריל 2017

שאלה 1

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

סעיף 1

נבנה יריב $\mathcal{A}$ הפועל כך: בהינתן קלט 1^n וגישת אורקל ל־$\mathrm{Mac}_k\left(\cdot\right)$ עבור $k \leftarrow \mathrm{Gen}\left(1^n\right)$ כלשהו, יחשב את $t = \mathrm{Mac}_k\left(0^n || 1^n\right)$ ויפלוט $\left(m, t\right)$ כאשר $m = 1^n || 0^n$. נשים לב ש־$m \notin \mathcal{Q}$ כי $\mathcal{Q} = \left\{0^n || 1^n\right\}$. כמוכן, $t = F_k\left(1^n\right) \oplus F_k\left(0^n\right) = F_k\left(0^n\right) \oplus F_k\left(1^n\right)$ ולכן t הוא תיוג תקף עבור m - כלומר $\mathrm{Vrfy}\left(k, \left(m, t\right)\right) = 1$. לכן $\Pr\left[\mathrm{MacForge}_{\mathcal{A},\Pi}\left(n\right) = 1\right] = 1$ 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 $t' = t\left[0 \ldots n-1\right]$ 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־$t' = t\left[0 \ldots n-1\right] = F_k\left(\langle 1 \rangle || 0^{n/2}\right)$ הוא תיוג תקף עבור $0^{n/2}$ ולכן $\Pr\left[\mathrm{MacForge}_{\mathcal{A},\Pi}\left(n\right) = 1\right] = 1$ והמערכת אינה בטוחה.

סעיף 3

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

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

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

שאלה 4

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

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

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

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

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

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

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

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־$\mathrm{Mac}_1\left(k_1, \cdot\right)$ עבור $k_1 \leftarrow \mathrm{Gen}_1\left(1^n\right)$ (שלא ידוע ל־$\mathcal{A}_1$), ידגום $k_2 \leftarrow \mathrm{Gen}_2\left(1^n\right)$ ויריץ את $\mathcal{A}$ עם 1^n. לכל בקשה של $\mathcal{A}$ עבור הצפנה של m, $\mathcal{A}_1$ יחזיר לו $\mathrm{Mac}_1\left(k_1, m\right) \| \mathrm{Mac}_2\left(k_2, m\right)$ (הראשון מתקבל מהאורקל והשני ניתן לחישוב יעיל לפי הנחה). לבסוף $\mathcal{A}$ יפלוט $\left(m^*, t_1 \| t_2\right)$ ו־$\mathcal{A}_1$ יפלוט $\left(m^*, t_1\right)$.

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

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

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

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

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:

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

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

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

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

ולכן מתקיים:

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

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

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

לאינסוף n, בסתירה לכך ש־Π_1 בטוחה.

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

שאלה 7

יהיו $\ell_1, \ell_2 : \mathbb{N} \to \mathbb{N}$ כך ש־$H^{(i)} : \{0,1\}^* \to \{0,1\}^{\ell_i(n)}$. נניח בה"כ ש־$\ell_1(n) \le \ell_2(n)$ לכל 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 בהינתן קלט $s = s_1 || s_2$ ומספר x פולטת $H^{(1)'}_{s_1}(x) \oplus H^{(2)}_{s_2}(x)$ כאשר $H^{(1)'}_{s_1} = H^{(1)}_{s_1}(x) || 0^{\ell_2(n) - \ell_1(n)}$, כלומר הפלט שלה זהה לשל $H^{(1)}$ ומרופד ב־0ים כך שיהיה באורך של הפלט של $H^{(2)}$