מבוא לקריפטוגרפיה / תרגיל בית #4

אריאל סטולרמן
ודים סטוטלנד

(1)

(a)

במקרה ומחליפים את סדר השלבים (1) ו-(2) בפרוטוקול, אליס יכולה לנצח בקלות בכל פעם:

- תחילה בוב שולח לאליס את הניחוש שלו ל-$B(x)$ שהוא c.
- אליס מקבלת את הניחוש של בוב ושולחת לו:
  - אם $c = 0$ תשלח לו $y = F(x)$ כך ש-$B(x) = 1$
  - אם $c = 1$ תשלח לו $y = F(x)$ כך ש-$B(x) = 0$

בכל מקרה כיוון שלבוב אין מראש התחייבות של אליס כלפי x (שולחת לו את ה"התחייבות" רק לאחר שיודעת את הניחוש שלו), היא יכולה לשלוח לו y עבור איזה x שתרצה וכך לנצח תמיד.

(b)

במקרה בו $F(x) = g^x$ ברור כי בוב יכול לנצח בסיכוי 1, כיוון שבהינתן $y = g^x$ בוב יכול לבדוק בקלות האם g^x הוא שארית ריבועית כיוון ש-$(g^x)^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\, p)$ והרי g^x שארית ריבועית אמ"מ ה-lsb של x הוא 0. כך בוב יכול תמיד לשלוח את ה-c הנכון ולזכות תמיד.

(c)

הדרישה ש-F תהיה חח"ע אכן נצרכת, אחרת יתכן מצב בו אליס יכולה לרמות. אם נתונים x_1, x_2 כך ש-$B(x_1) = \neg B(x_2)$ ו-$F(x_1) = F(x_2)$ אז אחרי שבוב שולח לאליס את הניחוש שלו c, אליס יכולה לבחור את אחד מבין ה-xים כך שה-lsb שלו הפוך ל-c שקיבלה מבוב, וכך לנצח תמיד.

(אולי אפשר לעדן את הדרישה לכך ש-F אולי לא תהיה חח"ע, אך שכל ה-xים המתמפים לאותו y יתנו את אותו ערך ל-B, וכך אליס לא יכולה לרמות. למקרה זה אנו צריכים הגדרה אחרת למושג ביט-קשה, שכן אנו מכירים את ההגדרה ביחס לפונ' חח"ע – מהגדרה B הוא ביט קשה אם קיימת פרוצדורה שבהינתן $F(y)$ ואלג' המחשב לכל $F(y)$ את $B(y)$ יכולה למצוא את המקור של F - אך המקור הוא ambiguous אם F היא לא חח"ע).

(d)

אליס תבחר e שאינו זר ל-$\phi(N)$ (למשל $e = p - 1$). בתור x אליס תבחר $x \in \mathbb{Z}_N^*$ אי זוגי כלשהו. נגדיר את $x_1 = x$ ו-$x_2 = x \cdot m^d$ כאשר $e \cdot d = \phi(N)$ (ניתן למצוא ע"י xgcd) ו-m הוא מספר זוגי כלשהו מ-D ש-d אינו הסדר שלו. כעת מתקיים:

- $F(x_1) = F(x) = x^e \bmod N$
- $F(x_2) = F(x \cdot m^d) = (x \cdot m^d)^e \bmod N = x^e \cdot \underbrace{m^{de}}_{\equiv 1 (\mathrm{mod}\, N)} \bmod N = x^e \bmod N$

אליס תשלח לבוב את $x^e (\mathrm{mod}\, N)$. עבור תשובת בוב:

- אם $c = 0$ אליס תשלח את $x_1 = x$ שהוא אי זוגי ולכן ה-lsb שלו הוא 1.
- אם $c = 1$ אליס תשלח את $x_2 = x \cdot m^d$ שהוא זוגי (כי m זוגי ו-$m^d \neq 1$) ולכן ה-lsb שלו הוא 0.

כך אליס מרמה ומנצחת את בוב בכל מקרה. הנחה עליה התבססנו: קיים $m \in D$ כך שהסדר שלו ב-$\mathbb{Z}_N^*$ לא מחלק את d).

(e)

אליס תבחר g שאינו איבר פרימיטיבי ב-$\mathbb{Z}_p^*$, כלומר הסדר שלו קטן ממש מ-$p - 1$. נסמן את סדר g כ-d. אליס תבחר $x_1 = x$ כך ש-$x > d$, $x > \frac{p-1}{2}$ ו-$x - d < \frac{p-1}{2}$, ותבחר את $x_2 = x - d$. מתקיים:

- $F(x_1) = g^x (\mathrm{mod}\, p)$
- $F(x_2) = g^{x-d} \bmod p = g^x \cdot g^{-d} \bmod p = g^x \cdot \underbrace{(g^d)^{-1}}_{\equiv 1 (\mathrm{mod}\, p)} \bmod p = g^x \bmod p$

עבור בחירת $B(x) = Half_p(x)$ (כפי שהוגדר בשיעור), נקבל ש-$B(x_1) = \neg B(x_2)$ ואז בהתאם ל-c שיתקבל מבוב, אליס תשלח את ה-x_i שיגרום לה לנצח. התבססנו על ההנחה שניתן למצוא g כזה ואת ה-d בצורה יעילה.

(f)

אם נבחר $F(x)$ להיות cryptographic hash-function אזי היא אינה חח"ע (כיוון שממפה לטווח קטן מהתחום), לבוב יהיה קשה למצוא את המקור של $F(x)$ שאליס תשלח לו, ואליס לא תוכל לרמות כיוון שקשה למצוא x_1, x_2 שונים כך ש-$F(x_1) = F(x_2)$ (מציאת collision קשה בפונ' כאלה).
נציין כי הגדרת הביט הקשה בעייתית כיוון שמההגדרה בכיתה B יהיה ביט קשה ל-F אם קיים אלג' המחשב מתוך $F(x)$ את $B(x)$ שבעזרתו ניתן באופן יעיל לשחזר לכל $F(x)$ את x, אך ב-F שאינה חח"ע הגדרה זו בעייתית. נניח כי קיימת הגדרה מתאימה וכי קיים ל-F כזה B (הגדרה מתאימה יכולה להיות אלג' לא אקראי שמחזיר לכל $F(x)$ איזשהו x במקור שלו. חוסר אקראיות חשוב כדי שיחזיר תמיד את אותו x, כדי שנקבל תמיד את אותו $B(x)$).

(2)

(a)

נניח כי בהינתן $F(x)$ קיים אלג' A כך ש-$A(F(x)) = B(x)$ כאשר $B(x) = Half(x)$ (כפי שהוגדר בשאלה). להלן אלג' יעיל למציאת x בהינתן A עבור $F(x) = g^x \bmod p$. נסמן $y = F(x)$:

- תחילה נבדוק האם $A(y) = 0$. אם כן, ה-msb של x הוא 0, ונמשיך:
  - נכפיל את x ב-2 ע"י העלאת y בריבוע: $y := y^2$.
  - נחזור על התהליך, כאשר בכל שלב מתקבל הביט הבא של x.
- אם הוא 1:
  - נכפיל את x ב-2 ע"י העלאת y בריבוע: $y := y^2$, ובנוסף נחסר ממנו את $\frac{1}{2}p$ ע"י הכפלת y (החדש) ב-$g^{-\frac{1}{2}p}$ (מציאתו ע"י $xgcd$).
  - נחזור על התהליך כך שבכל פעם ההכפלה היא ב-$g^{-\frac{1}{2^k}p}$ כאשר k הוא האיטרציה בה נמצאים.

לאחר $\log p$ איטרציות נקבל את x. הרעיון הוא שבכל איטרציה מקבלים את ה-msb של x ו"מזיזים" את x כדי לקבל באיטרציה הבאה את הביט הבא שלו, תוך נרמול הטווח בו מחפשים.

(b)

נמשיך לפי אותו רעיון של הכפלת x ב-2 ע"י הכפלת x ב-2^e כך ש-$F(x \cdot 2^e) = F(2x)$ (מיידי). נעבוד לפי האלגוריתם הבא:

אם $A(y) = 0$ אז מתקיים ש-$x < \frac{1}{2}N$ (הביט הראשון הוא 0), ואז נכפיל ב-2^e כדי לקבל $F(2x)$: $y_{new} := y_{old} \cdot 2^e$. נסתכל על y_{new}:

- אם $A(y_{new}) = 0$ אז $2x < \frac{1}{2}N$ וזה אומר ש-$x < \frac{1}{4}N$, והביט השני ב-x הוא גם 0.
- אחרת זה אומר ש-$\frac{1}{4}N < x < \frac{1}{2}N$, כלומר הביט השני הוא 1.

אם $A(y) = 1$ אז מתקיים ש-$x > \frac{1}{2}N$ (הביט הראשון הוא 1). נבצע שוב את ההכפלה כדי לקבל את y_{new}:

- אם $A(y_{new}) = 0$ אז $2x \bmod N < \frac{1}{2}N$ וזה אומר ש-$\frac{1}{2}N < x < \frac{3}{4}N$, והביט השני ב-x הוא 0.
- אחרת זה אומר ש-$\frac{3}{4}N < x < N$, כלומר הביט השני הוא 1.

ממשיכים בשיטה זו עד קבלת כל הביטים של x. סה"כ מבצעים כ-$\log N$ איטרציות.

(c)

תחת נתונים אלו, **<u>בהם B הוא אכן פרדיקט ביט-קשה ל-F, ו-F היא אכן פונ' חח"ע וחד כיוונית</u>**, אף אחד מצדי התקשורת לא יכול לרמות:

- אליס לא תוכל לבחור זוג x_1, x_2 שונים המתמפים לאותו ערך ע"י F כיוון שהיא חח"ע, ולכן לא תוכל לרמות את בוב לאחר שישלח לה את הניחוש c שלו, ולשלוח לו x המתאים לה לנצח.
- בוב מצידו לא יהיה בעל יתרון בסיכוי לא זניח על פני אליס למציאת x כיוון ש-B הוא פרדיקט ביט-קשה ל-F ולכן בוב לא יכול למצוא את $B(x)$ מתוך $F(x)$.

(4)

תחילה נחשב את הפולינומים f, g:

```
# calculate f(x) and g(x)
########################
F=GF(7)
R=PolynomialRing(F,'x')
polys = []
for f in R.polynomials(2):
    tmp = 1
    for g in R.polynomials(2):
        # check that they satisfy the demands
        if ((f(0) != g(0)) and (f(1) == g(1)) and (f(2) == g(2))):
            polys += [(p1,p2)]
            tmp = 0
            break
    if (tmp == 0):
        break
# print results
print "f = ",f
print "g = ",g

OUTPUT:
=======
f =  x^2
g =  2*x^2 + 4*x + 2
```

קיבלנו את $f[x] = x^2, g[x] = 2x^2 + 4x + 2$.

נחשב את הפולינומים f_1, f_2, f_3 עבור 1,2,3 בהתאמה ונציב 0:

$$f_1[x] = y_1 \cdot \frac{x-2}{1-2} \cdot \frac{x-3}{1-3} = y_1 \cdot \frac{1}{2}(x^2 - 5x + 6) \underset{in\,\mathbb{Z}_7}{=} y_1 \cdot 4(x^2 - 5x + 6) = y_1(4x^2 + x + 3) \Rightarrow f_1[0] = 3y_1$$

$$f_2[x] = y_2 \cdot \frac{x-1}{2-1} \cdot \frac{x-3}{2-3} = y_2 \cdot -1(x^2 - 4x + 3) = y_2 \cdot (6x^2 + 4x + 4) \Rightarrow f_2[0] = 4y_2$$

$$f_3[x] = y_3 \cdot \frac{x-1}{3-1} \cdot \frac{x-2}{3-2} = y_3 \cdot \frac{1}{2}(x^2 - 3x + 2) \underset{in\,\mathbb{Z}_7}{=} y_3 4(x^2 - 3x + 2) = y_3(4x^2 + 2x + 1) \Rightarrow f_3[0] = y_3$$

$$\Rightarrow h[0] = f_1[0] + f_2[0] + f_3[0] = 3y_1 + 4y_2 + y_3$$

נחשב את y_1, y_2, y_3 עבור כל אחד מהפולינומים f, g:

$$y_1 = f[1] = 1, y_2 = f[2] = 4, y_3 = f[3] = 2$$

$$\Rightarrow h[0] = 3 \cdot 1 + 4 \cdot 4 + 1 \cdot 2 = 3 + 16 + 2 = 21 \underset{in\,\mathbb{Z}_7}{=} 0$$

וזהו אכן הסוד.

$$y_1 = g[1] = 1, y_2 = g[2] = 4, y_3 = g[3] = 4$$

$$\Rightarrow h[0] = 3 \cdot 1 + 4 \cdot 4 + 1 \cdot 4 = 3 + 16 + 4 = 23 \underset{in\,\mathbb{Z}_7}{=} 2$$

וזהו אכן הסוד.

נחשב גם עבור g_1, g_2, g_5 עבור 1,2,5 בהתאמה ונציב 0:

$$g_1[x] = y_1 \cdot \frac{x-2}{1-2} \cdot \frac{x-5}{1-5} = y_1 \cdot \frac{1}{4}(x^2 - 7x + 10) \underset{in\,\mathbb{Z}_7}{=} y_1 \cdot 2(x^2 + 3) = y_1(2x^2 + 6) \Rightarrow g_1[0] = 6y_1$$

$$g_2[x] = y_2 \cdot \frac{x-1}{2-1} \cdot \frac{x-5}{2-5} = y_2 \cdot -\frac{1}{3}(x^2 - 6x + 5) \underset{in\,\mathbb{Z}_7}{=} y_2 \cdot (2x^2 + 2x + 3) \Rightarrow g_2[0] = 3y_2$$

$$g_5[x] = y_5 \cdot \frac{x-1}{5-1} \cdot \frac{x-2}{5-2} = y_5 \cdot \frac{1}{12}(x^2 - 3x + 2) \underset{in\,\mathbb{Z}_7}{=} y_5(3x^2 + 5x + 6) \Rightarrow g_5[0] = 6y_5$$

$$\Rightarrow h[0] = g_1[0] + g_2[0] + g_5[0] = 6y_1 + 3y_2 + 6y_5$$

נחשב את y_1, y_2, y_5 עבור כל אחד מהפולינומים f, g:

$$y_1 = f[1] = 1, y_2 = f[2] = 4, y_5 = f[5] = 4$$

$$\Rightarrow h[0] = 6 \cdot 1 + 3 \cdot 4 + 6 \cdot 4 = 6 + 12 + 24 = 42 \underset{in\,\mathbb{Z}_7}{=} 0$$

וזהו אכן הסוד.

$y_1 = g[1] = 1, y_2 = g[2] = 4, y_5 = g[5] = 2$

$\Rightarrow h[0] = 6 \cdot 1 + 3 \cdot 4 + 6 \cdot 2 = 6 + 12 + 12 = 30 \underset{in\ \mathbb{Z}_7}{=} 2$

וזהו אכן הסוד.

(5)

נניח נתונות לנו שני זוגות של הודעה וחתימה המשתמשות באותו k:

המידע הפומבי שברשותינו: $p, g, y = g^x, H$.

- $(m_1, r, s_1) = \left(m_1, g^k (\mathrm{mod}\, p), (m_1 - g^k x)k^{-1} (\mathrm{mod}\, p-1)\right)$
- $(m_2, r, s_2) = \left(m_2, g^k (\mathrm{mod}\, p), (m_2 - g^k x)k^{-1} (\mathrm{mod}\, p-1)\right)$

נשים לב כי מתקבלות לנו שתי משוואות, שכן החתימות חוקיות:

- $y^r \cdot r^{s_1} = g^{rx} \cdot g^{ks_1} = g^{rx+ks_1} = g^{m_1} (\mathrm{mod}\, p) \Rightarrow rx + ks_1 = m_1 (\mathrm{mod}\, p-1)$
- $y^r \cdot r^{s_2} = g^{rx} \cdot g^{ks_2} = g^{rx+ks_2} = g^{m_2} (\mathrm{mod}\, p) \Rightarrow rx + ks_2 = m_2 (\mathrm{mod}\, p-1)$

קיבלנו 2 משוואות עם שני נעלמים: x, k כאשר כל שאר הנתונים ידועים: r, s_1, s_2, m_1, m_2, p (וניתן לחשב את ההופכיים של אחד מ-s_i ע"י $xgcd$ כי p נתון, כדי למצוא ראשית את k). ההנחות עליהן התבססנו הן ש-$M_1 \neq M_2$ ואין התנגשות ביניהן ע"י H, שזוגות ההודעות עם החתימות שקיבלנו הן חוקיות ושל-s_i שבחרנו למציאת k יש הופכי ב-$\mathbb{Z}_{p-1}$.