

יסודות הקריפטוגרפיה שיעור #10

: Secret sharing schemes contd.

תזכורת: נתון סוד הנתון בידי דילר, וברצוננו לחלק את הסוד בין n אנשים כך ש- n יכולים לשחזר את הסוד אך $n - 1$ ופחות כבר לא יכולים. רוצים שחלקי הסוד המחולק יתפלגו באופן זהה ללא תלות במהו הסוד.

יהי סוד $S \in U$ תחת הנחה שקיים איזושהי התפלגות על U עולם סופי. r הוא גרעין אקראיות. חלוקת הדילר: $F(S, r) = s_1, \dots, s_n$ כאשר s_i הם חלקי הסוד, ו- F היא פונקציה דטרמיניסטית, האקראיות מגיעה מ- r בלבד. המשתתף ה- i מקבל את s_i , ומניחים שהפצת החלקים מתבצעת באופן אמיין.

: n-out-of-n secret sharing

לכל שני ערכים שונים a, b ערכים אפשריים ל- $S \in U$, ולכל $n - 1$ משתתפים, התפלגות החלקים בהינתן $S = a$ זהה לזו אם $S = b$. הגדרה זו שונה מזו שניתנה שיעור שעבר, אך שקולה לה.

• נניח כי $|U| = m$ ובה"כ נניח $\mathbb{Z}_m = \{0, 1, \dots, m - 1\}$.

• הדילר בוחר באקראי, באופן אחיד ובלתי תלוי $r_1, \dots, r_{n-1} \in \mathbb{Z}_m$.

• s_1, \dots, s_{n-1} הם r_1, \dots, r_{n-1} ו- $s_n = S - \sum_{i=1}^{n-1} r_i \pmod{m}$ (XOR אם $m = 2$).

ולידציה לסכמה זו:

טענה: בהינתן ש- $S = a$ יש בדיוק ערך יחיד r_n המקיים את הנ"ל. נקח קואליציה של $\{2, \dots, n - 1, n\}$ משתתפים, ונניח כי $r_2 = c_2, \dots, r_n = c_n$. החלקים הללו נקבעים לפי r_i . מה קורה עם $r_n = a - (\sum_{i=1}^{n-1} c_i) \pmod{m}$. נראה שאכן מתקבל מכך הסוד:

$$s_n = S - \sum_{i=1}^{n-1} r_i = a - \sum_{i=1}^{n-1} c_i \Rightarrow r_1 = a - \sum_{i=1}^{n-1} s_i - s_n = a - \sum_{i=1}^n s_i$$

מה ההסתברות שהוא ייבחר? הסיכוי של כל אחד $\frac{1}{m}$ ולכן הסיכוי שה"כ שיבחר הנכון הוא $\frac{1}{m^{n-1}}$. אם במקום a היה b , ההתפלגות היתה זהה, ולכן לפי התנאי שהגדרנו בהתחלה נשמרת הסודיות והסכמה בטוחה.

: t-out-of-n secret sharing

אותו רעיון, רק שהפעם נרצה לשמור סודיות עבור קואליציות בגודל $t - 1$ ומטה. הרעיון הוא ליצור $\binom{n}{t}$ ת-יות, כלומר תתי קבוצות בגודל t של משתתפים. אם t גדול אז זה מספר גדול - $\frac{2^n}{\sqrt{n}} \approx \binom{n}{t}$. יש פתרון טוב יותר המשתתף באינטרפולציה של פולינומים.

נניח כי בנוסף לכך ש- U סופי, נניח כי הוא שדה סופי. כמו כן נניח כי $|U| \geq n + 1$. נניח כי $f(x) = ax + b$ פולינום בעל משתנה אחד מעל \mathbb{Z}_p . לכל משתתף ניתן את הערך $f(i)$. מה לומד משתתף בודד על $f(0)$? נניח $i = 17$, המשתתף רואה את $17a + b$ שזהו מספר כלשהו בשדה, ולא ידוע דבר על b . אם יהיו במקרה זה של פולינום לינארי שני משתתפים, ניתן יהיה למצוא את b (שתי משוואות עם שני נעלמים). זו האינטואיציה, כאשר $f(0)$ הוא הסוד.

אינטרפולציית לגראנז':

יהיו (x_i, y_i) זוגות, ונתון כי f הוא פולינום העובר דרכם. המטרה של האינטרפולציה היא למצוא את $f(x) = a_{t-1}x^{t-1} + \dots + a_1x + a_0$.

נגדיר: $f_i(x) = y_i \cdot \frac{x-x_2}{x_1-x_2} \cdot \frac{x-x_3}{x_1-x_3} \cdot \dots \cdot \frac{x-x_t}{x_1-x_t}$ שהם t פולינומי עזר כך ש- $f_i(x_j) = y_i$ ו- $f_i(x) = 0$ אחרת. ואז נגדיר: $f(x) = \sum_{i=1}^t f_i(x)$ והוא הפולינום הסופי.

אינטרפולציית פולינומים עובדת מעל כל שדה, סופי ואינסופי כיוון ש- $x_i - x_j \neq 0$ עבור $i \neq j$; ולכל אחד יש הופכי (לכן מעל חוג, שם לא לכל איבר יש הופכי, זה לא בטוח היה עובד).

טענה: יש פולינום יחיד מדרגה $t - 1$ העובר דרך הנקודות הללו. נניח בשלילה כי קיים פולינום $g \neq f$ המקיים את התנאים על כל הנקודות, אז יש לו $t - 1$ שורשים ומתקיים ב- \mathbb{Z}_p ש- $f - g \equiv 0$. פולינום האפס.

: סכמת חלוקת סוד t-out-of-n של Shamir

• הדילר בוחר ערכים ראנדומליים r_1, \dots, r_{t-1} (חלקים מ- \mathbb{Z}_p).

• הדילר מגדיר פולינום: $f(x) = r_{t-1}x^{t-1} + \dots + r_1x + S$.

• s_1, \dots, s_n הם ערכי $f(x)$ בנקודות המתאימות: $s_1 = f(1), \dots, s_n = f(n)$.

וילדציה לסכמה זו:

שחזור אינו בעיה: פשוט מבצעים אינטרפולציה; לא משנה מתוך אילו נקודות נשחזרו, נקבל את אותו פולינום ואז נוכל לחשב את $f(0) = S$.
סודיות בפני קואליציות:

רוצים להראות שכל קבוצה של $t - 1$ משתתפים או פחות לא מלמדת כלום על האיבר החופשי של הפולינום דהיינו על הסוד. נדגים על קואליציה בגודל $t - 1$: נניח כי $S = a$ וניקח $t - 1$ ערכים כלשהם $c_1, \dots, c_{t-1} \in \mathbb{Z}_p$ שהם למעשה ה- s_1, \dots, s_{t-1} חלקים של הסוד שאנו מקבלים.
טענה: יש בחירה אחת בדיוק של $t - 1$ ימים מהם נגזרים $t - 1$ חלקי הסוד. מתקיים: $f(x) = f(1) + \dots + f(t - 1) + a$ כלומר:
 $f(x) = r_{t-1}x^{t-1} + \dots + r_1x + a$ - מכאן שההסתברות לקבל את a היא ההסתברות ש- $s_1 = f(1), s_2 = f(2), \dots, s_{t-1} = f(t - 1)$ והיא בדיוק $\frac{1}{p^{t-1}}$ וזוהי ההסתברות גם עבור $S = b$, כלומר אין הבדל התפלגויות בין a, b ולכן אנו עומדים בתנאי הסודיות.

Threshold Cryptography

הדילר מייצר $N = p \cdot q$ עם e מפתח הצפנה (וידוא חתימה). N, e מפורסמים, d מפתח חתימה.
תהי M הודעה $h(M) = y$ הודעה "מצומצמת" לגביה רוצים לחשב $y^d \pmod{N}$ (זו החתימה).
נהיה מעוניינים ב- y^{s_1}, \dots, y^{s_n} כך שמהם ניתן להרכיב את $y^d \pmod{N}$: $y^{s_1} \cdot y^{s_2} \cdot \dots \cdot y^{s_n} = y^{\sum s_i \pmod{\phi(N)}}$.
מה נרצה מה- S ? s_1, \dots, s_{n-1} יבחרו באקראי ו- $s_n = d - \sum_{i=1}^{n-1} s_i \pmod{\phi(N)}$, והמשתתף ה- i יקבל y^{s_i} .
ב- t -out-of- n יש בעיות טכניות של אינטרפולציה במעריך (כי $(p - 1)(q - 1)$ הוא זוגי).

"הטלת מטבעות דרך הטלפון"Hard core bits of one-way functions

תהי $F: D \rightarrow D$ פונקציה חד כיוונית וחז"ע. נניח כי $p = 2q + 1$, g איבר פרימיטיבי והפוני מוגדרת כך: $F(x) = g^x \pmod{p}$ (והיא חז"ע).
יהי $B: D \rightarrow \{0,1\}$ פרדיקט קל לחישוב. נאמר כי B הוא ביט-קשה עבור F אם בהינתן $F(x)$ קשה למצוא את $B(x)$.
דוגמה לפרדיקט לא קשה ביחס ל- F : הביט התחתון של x , שניתן (כפי שלמדנו) למצוא אותו פשוט ע"י בדיקה האם $F(x) = g^x$ הוא שארית ריבועית.
ברור כי אם פונקציה היא חד כיוונית לא כל הביטים קלים אליה, אחרת היינו יכולים באופן קל לחשב את- F^{-1} .
מתברר כי $HALF(x)$, הביט האמצעי של x , הוא ביט קשה, כלומר הפרדיקט הבודק האם $0 \leq x < \frac{p-1}{2}$ או $\frac{p-1}{2} \leq x < p - 1$ הוא ביט-קשה ל- F .
מציאת $B(x)$ מתוך $F(x)$ לא יכול להיות יותר קשה מלהפוך את F (מהפיכת F מוצאים את כל הביטים שלה, בפרט הקשים).
הגדרה פורמלית:

נאמר כי $B(x)$ קשה ל- F חד כיוונית אם קיימת פרוצדורה P יעילה המקבלת $F(y)$ המצליחה להפוך את F תוך קריאה לפרוצדורה A המחשבת את $B(x)$ מתוך $F(x)$.

נתבונן למשל ב- $HALF(x)$ ביחס ל- $F(x) = g^x \pmod{p}$. נניח נתונה לנו "קופסא" ונתון לנו g^y , ע"י שאלות מהצורה $B(g^y)$ רוצים למצוא את y .
הקופסא מחזירה לנו $0 \leq g^y < \frac{p-1}{2}$ או $\frac{p-1}{2} \leq g^y < p - 1$. המשכים אפשריים אם g^y בחלק הגדול:

- להכפיל את y ב-2: מתוך g^y לחשב את $(g^y)^2 = g^{2y}$.
 - להזיז אותו ב- a ע"י הכפלה $g^y \cdot g^a = g^{y+a}$.
- נניח נכפיל את y ב-2 לפי השיטה הראשונה, נעבור לטווח $[p - 1, 2p]$ (הכל מודולו $p - 1$), אך רק מספרים זוגיים. מעל זה נבצע עוד $half$ וכך הלאה.
זהו חיפוש בינארי.

פרוטוקול אקראיות ברשת באמצעות ביטים קשים:

- אליס בוחרת $F: D \rightarrow D$ פוני חז"ע וקשה להיפוך, ויהי $B(x)$ פרדיקט קשה ל- F .
 - אליס שולחת את F, B לבוב ובוחרת $x \in D$, ומחשבת את $y = F(x)$ ו- $b = B(x)$.
 - היא שולחת לבוב את y וזוהי התחייבות לערך של x .
 - בוב שולח לאליס ניחוש $c \in \{0,1\}$ ל- $B(x)$ לאחר קבלת c , אליס שולחת לבוב את x וכעת הוא יכול לחשב את $b = B(x)$.
 - אם $c = b$ אז בוב מנצח, אחרת אליס מנצחת.
- בחירת x ושליחת $F(x)$ היא התחייבות ל- $B(x)$ (הכנסת x ל"מעטפה אטומה).

