יסודות הקריפטוגרפיה שיעור #11

t-out-of-n secret sharing:

תזכורת: ברשות דילר אמין סוד $S \in U$ המחלק את הסוד ל-n חלקים. הדרישות הם ש-t חלקים מאפשרים שחזור ו-$t-1$ (ופחות) לא נותנים שום אינפורמציה על S. ראינו שיטה לחלוקת סוד בסכמה זו (שיטת שמיר): בונים פולינום מדרגה t $f[x] = \sum_{i=1}^{t} f_i[x]$ מעל $\mathbb{Z}_p$ שכל מקדמיו אקראיים פרט למקדם חפשי S. החלק של i: $f_i[x] = y_i \frac{(x-x_2)}{x_i-x_2} \cdot \ldots \cdot \frac{(x-x_t)}{x_i-x_t}$.

<u>הערה חשובה טכנית</u>: בהינתן t חלקים $s_{i_1}, \ldots, s_{i_t}$, הסוד S ניתן לשחזור כפונקציה לינארית של החלקים: יש קבועים $b_{i_1}, \ldots, b_{i_t}$ כך ש-$S = \sum_{j=1}^{t} b_{i_j} s_{i_j}$ כך ש-b_{i_j}. הכל כמובן מעל $\mathbb{Z}_p$.

Threshold PKC:

פענוח t-out-of-n: דילר קובע מערכת, מגריל מפתחות (ציבורי ופרטי), ומפרסם את כל המידע הציבורי. הוא מבצע את הסכמה של שמיר על המפתח הפרטי וכל אחד מ-n המשתתפים מקבל חלק s_i (כאן הדילר סיים את תפקידו).

אליס שולחת הודעה מוצפנת $C = E(m)$ (מוצפנת עם המפתח הפומבי), כל אחד מ-n המשתתפים מחשב "פיסה" של ההודעה המפוענחת: $m_1, \ldots, m_n$. t מתוכם מאפשרות שחזור m.

<u>Elgamal PKC - תזכורת</u>: יהיו $p = 2q + 1$. בוב בוחר $a \in [0, \ldots, p-2]$ והמידע הפומבי שמפרסם הוא $\beta = g^a$ (g יוצר), והמפתח הפרטי שלו הוא a. אליס מצפינה ע"י בחירת מפתח $k \in [0, \ldots, p-2]$ ומחשבת את $g^k \pmod p$, ושולחת $E(m) = (g^k, m \cdot \beta^k)$. בוב מפענח: $(g^k)^a = \beta^k \pmod p$. זה מאפשר היפוך כפלי ל-$\beta^k$ מבלי לדעת את k, ואז $\beta^{-k} \cdot m \cdot \beta^k = m$.

המודיפיקציה שמבצעים על אלגמל המקורי הוא שינוי $\beta = g^{2a}$, ואליס שולחת את $(g^{2k}, m \cdot \beta^k)$. ניתן להראות כי סכמת אלגמל החדשה חזקה כמו המקורית (רדוקציה: אם אפשר לשבור את החדשה, אפשר לשבור את המקורית).

החלקים של המפתח הפרטי $2a$ לפי שמיר יסומנו $a_1, \ldots, a_n$ הניתנים אחד למשתתף. נשים לב כי החזקות g^d "חיות" ב-$\mathbb{Z}_{p-1}$, אבל הוא כלל אינו שדה ($p-1 = 2q$). נסמן $(c_1, c_2) = (g^{2k}, m \cdot \beta^k)$ ואז פענוח: c_1, c_2 מחשבים $c_1^a = (g^{2k})^a = (g^{2a})^k = \beta^k$.

[נניח נתון $g^r, g^s \pmod p$, כאשר r, s לא ידועים ו-b, c קבועים. מה אפשר לעשות איתם? לחשב את $g^{r \pm s}$, $g^{br} = (g^r)^b$ - כלומר אפשר לחשב פעולות לינאריות בחזקות, ונשתמש בזה.]

אז כעת רוצים לחשב את $c_1^{a_i \pmod{p-1}} = (g^k)^{a_i \pmod{p-1}}$. נרצה לבצע אינטרפולציה על החזקה, אך $p-1$ אינו ראשוני ויותר מכך הוא זוגי כי הוא שווה ל-$2q$. מה עושים? לכן עובדים עם <u>חזקות זוגיות</u> של g (לכן בחרנו $2a$ כמפתח). QR (הריבועים) הם תת חבורה של $\mathbb{Z}_p^*$. $p-1 = 2q$ ולכן כל תת חבורה היא בת 2 איברים או q איברים מ-QR. חלוקת הסודות תהיה ב-$\mathbb{Z}_q$. בהינתן מפתח a המחלק בונה $f[x]$ מדרגה t. ניזכר כי $c_1 = g^{2k}$ ולכן הוא שארית ריבועית (איבר ב-QR), ולכן כל $c_1^{a_i}$ הוא גם ב-QR. נניח t הראשונים הם $c_1^{a_1}, \ldots, c_1^{a_t}$ ומתוך זה רוצים לשחזר את c_1^a. מתוך הסכמה של שמיר קיימים $b_1, \ldots, b_t$ כך ש: $a = \sum_{i=1}^{t} b_i a_i$ ואז מחשבים את $c_1^a = c_1^{\sum_{i=1}^{t} b_i a_i} = \left(c_1^{a_1}\right)^{b_1} \cdot \ldots \cdot \left(c_1^{a_t}\right)^{b_t} \pmod p$ וזוהי m.

<u>למה threshold RSA קשה יותר?</u>

ראשית, בהעלאה בחזקה ניתן בקלות לחבר ולכפול, ב-RSA רק לכפול. כמו כן חזקה ב-RSA היא מודולו $(p-1)(q-1)$. נניח שהיה ניתן להפטר מחזקות של 2. לו היינו עובדים ישירות עם $\frac{p-1}{2} \cdot \frac{(q-1)}{2}$ זה מאפשר פירוק pq - ומזה רוצים להימנע. בקיצור – מסובך יותר אם כי אפשרי.

ובזה תם הנושא threshold cryptography.

הוכחות אינטראקטיביות והוכחות באפס מידע:

מהי הוכחה ומהי הוכחה יעילה?

הוכחה קלאסית: תשתית (אקסיומות, כללי היסק), טענה מאורך n והוכחה: סדרה באורך $p(n)$ של אקסיומות, טענות שנגזרות וכו', המסתיימת בטענה המקורית. הוכחה יעילה כאן היא פולי'.

הוכחה ספציפית: טענות שייכות לשפה L נתונה, x טענת קלט המקיימת $x \in L$. הוכחות יעילות כאן יהיו ב-NP.

רכיבים שהוספו:

- אינטראקציה בין prover שיודע הכל ואינו מוגבל חישובית, ו-verifier שאינו מוגבל חישובית והוא ספקן.
- הטלת מטבעות.

<u>שאיפות</u>:

- בסוף ההוכחה, אם הטענה נכונה V ישתכנע בהסתברות $1-\varepsilon$.
- אם הטענה אינה נכונה, ההסתברות ש-V ישתכנע קטנה מ-ε.

<u>בעית non isomorphism</u>:

בעיה זו כנראה לא ב-NP; עדיין יש לשפה זו הוכחות אינטראקטיביות יעילות. איזומורפיזם בגרפים: גרפים זהים עד כדי renaming של הצמתים.

נניח שיש בגרפים נתונים n קודקודים. נתון זוג G_1, G_2, P מעוניין לשכנע את V ששניהם לא איזומורפיים. המוודא V בוחר באקראי $i \in \{1,2\}$ ומבצע G_i תמורה אקראית של שמות הקודקודים. התוצאה $G = \pi(G_i)$ מוחזרת למוכיח. המוכיח צריך לחשב מה היה i שנבחר. אם $G_1 \cong G_2$ אז P טועה בהסתברות $\frac{1}{2}$. חוזרים על כך 200 פעמים; אם P מצליח בכולם אז V משתכנע, אחרת V דוחה.

Zero knowledge proofs:

דוגמא: הכרעה האם גרף הוא 3-צביע. אליס רוצה לשכנע את בוב שהגרף צביע. רוצים שאליס תוכל להוכיח זאת לבוב מבלי שידע איך היא עושה את זה ומבלי שיוכל להוכיח זאת לאחרים. אז תחילה אליס עושה פרמוטציה על צביעת הגרף; לאחר מכן מבצעים הצפנה על צביעת הגרף, כך שלכל צומת יש מפתח אחר המצפין את הצבע שלו.

בוב יכול לבקש הוכחה על קשת, וזאת יעשה ע"י כך שאליס תשלח לבוב את שני צמתי הקשת מוצפנים. כלומר, בכל בדיקה נתונה רואים את צבעי שני צידי הקשת. בכל סיבוב יש הסתברות של $\frac{1}{|E|}$ שאם הגרף אינו 3 צביע, בוב יעלה על כך (אז נעשה את זה הרבה פעמים): לפני כל בקשת קשת, אליס עושה פרמוטציה על הצבעים ומצפינה אותם, ושולחת לבוב את הקשת שמבקש – אם אליס מרמה אז הסיכוי שבוב יבקש קשת שתהיה הקשת האחת (לפחות) שבשני צדדיה אותו צבע הוא $\frac{1}{|E|}$. הצפנת הצבעים היא בכדי לשמור עליהם בפני בוב. הפרמוטציות דואגות שבוב לא יוכל לצבור מידע מפעם לפעם.

אם נחזור על זה מספיק פעמים (k), הסיכוי שאליס מרמה הוא $\left(1-\frac{1}{|E|}\right)^k$. המשך ההסבר במסמך.