מבחן בקורס "מבוא לקריפטוגרפיה מודרנית"

סמסטר א' התשע"ד מבחן חלקי לדוג'

15 בינואר 2014

שאלה 1

בני וניר חולקים מפתח $K \in \{0,1\}^k$ לפונקציית אותנטיקציה $MAC : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$ המתייגת הודעות באורך n ע"י מחרוזות באורך n.

בני מעוניינת לשלוח לניר הודעות מתוייגות באורך $3n$, לשם כך ניר הציע לו לבנות פונ' חדשה $MAC' : \{0,1\}^{3n} \times \{0,1\}^k \to \{0,1\}^n$ המוגדרת ע"י $MAC'(M,K) = MAC(H(M),K)$, כאשר $H : \{0,1\}^{3n} \to \{0,1\}^n$. בני וניר לא מצליחים להסכים כיצד יש לממש את H.

סעיף א'

ניר מציע לממש את H באופן הבא: בהנתן קלט $M \in \{0,1\}^{3n}$, נפרשו כייצוג בינארי של מספר $0 \leq m < 2^{3n}$ נחשב $m' = m \mod 2^n$ ונחזיר את הייצוג הבינארי $M' \in \{0,1\}^n$ של m'.

הראו כי בהנתן הודעה שרירותית $M \in \{0,1\}^{3n}$ ותג $T = MAC'(M,K)$, ניתן לזייף תג חוקי T^* על הודעה חדשה $M \neq M^*$. (הניחו כי, בהנתן K, $MAC(\cdot,K)$ דטרמיניסטית.)

תשובה:
בהנתן M, עבור על $M^* = M + 2^n \mod 2^{3n}$, ההודעות שונות מודולו 2^{3n}, אך זהות מודולו 2^n, ולכן יהיה להן אותו תג T.

סעיף ב'

איזו תכונה ניתן לדרוש מ־H על־מנת לשמור על הבטיחות של המערכת כנגד יריבים חסומים חישובית (בהנחה כי הפונ' MAC בטוחה נגד יריבים חסומים). כלומר יריב חסום היכול לבקש תגים על הודעות $\{M_i\}$ לבחירתו, אינו יכול לזייף תג חוקי עבור הודעה $M^* \notin \{M_i\}$. נמקו תשובתכם בקצרה.

תשובה:
מספיק לבקש כי H תהיה חסינה בפני התנגשויות. אכן יריב המצליח לזייף מבלי ש־$M^*, \{M_i\}$ מכילים התנגשות תחת H יכול לזייף גם עבור ה־MAC המקורי.

שאלה 2

נציע פרוטוקול (S,R) ל-Oblivious Transfer נגד יריבים ישרים אך סקרנים:

קלט של R: ביט b.
קלט של S: שני ביטים $m_0, m_1 \in \{0,1\}$
$R \to S$: **בוחר** $N = pq : p,q = 3 \mod 4$, $r_0, r_1 \leftarrow Z_N^*$, **ושולח את N ואת** $\begin{matrix} c_0 = (-1)^{1-b} r_0^2 \mod N \\ c_1 = (-1)^b r_1^2 \mod N \end{matrix}$.
$S \leftarrow R$: **שולח את** $a = c_0^{m_0} \cdot c_1^{m_1} \mod p$.
S: **אם a הנו שארית ריבועית קובע $m_b = 0$ אחרת קובע $m_b = 1$.**

סעיף א'

נסמן ב־QR_p,QR_q, QR_N את חבורות השאריות הריבועיות ב־Z_p^*,Z_q^* וב־Z_N^* בהתאמה. הראו כי $-1 \notin QR_p \cup QR_q$. הסבירו מדוע מכך נובע כי $-1 \notin QR_N$.

תשובה:
$-1 \mod p = (-1)^{2k+1} = (-1)^{\frac{4k+3-1}{2}} = (-1)^{\frac{p-1}{2}}$, **לכן** $-1 \notin QR_p$, **החישוב עבור q זהה. אם** $-1 = x^2 \mod pq$ **אז** $-1 = x^2 \mod p$.

סעיף ב'

הראו כי בפרוטוקול הנ"ל R אכן יכול לבדוק ביעילות, בהנתן p,q, האם $a \in QR_N$ וכי הוא אכן לומד בסוף את הערך הנכון m_b.

תשובה:
על־מנת לבדוק אם $a \in QR_N$ בודקים האם $a \in QR_p \cap QR_q$. אכן כבר ראינו בסעיף הראשון כי אם $a \in QR_N$ אז $a \in QR_p \cap QR_q$. כמו כן אם $a = x^2 \mod q$ וכן $a = y^2 \mod p$ אז $a = (x,y)^2$ כאשר (x,y) מייצג שארית מודלו N לפי משפט השאריות הסיני.
נראה כעת כי R לומד את m_b. מתקיים:

$$c_0^{m_0} c_1^{m_1} = (-1)^{m_b} r_b^{2m_b} r_{1-b}^{2m_{1-b}} \begin{cases} \in QR_N & m_b = 0 \\ \notin QR_N & m_b = 1 \end{cases}$$

סעיף ג'

הראו כי בפרוטוקול הנ"ל R סקרן יכול גם ללמוד את m_{1-b}. הציעו תיקון לפרוטוקול שימנע זאת (אין צורך בהוכחה).

תשובה:
R פשוט יכול לחלץ מהתשובה את $r_{1-b}^{2m_{1-b}}$ ולהבין מהו m_{1-b}. על־מנת לתקן את הפרוטוקול S יכול להכפיל את התוצאה בשארית ריבועית אקראית r^2, כעת התואה מתפלגת כמו $(-1)^{m_b}u^2$ עבור שארית אקראית.

שאלה 3

בהנתן גרף $G = ([n], M)$ עם קודקודים $[n] = \{1, 2, \ldots, n\}$ ומטריצת שכנויות $M \in \{0,1\}^{n\times n}$ (כלומר, יש קשת (i,j) אמ"מ $M[i,j] = 1$), נאמר כי בגרף **מעגל המילטוני** אם קיים מעגל המורכב מקשתות העובר דרך כל הקודקודים. כלומר, קיימת פרמוטציה של הקודקודים $c : [n] \to [n]$ כך ש־לכל $i \in [n]$, $M[c(i), c(i+1 \mod n)] = 1$.

נציע פרוטוקול אינטרקטיבי (P, V) להוכחה כי בגרף נתון קיים מעגל המילטוני.

<u>קלט משותף</u>: $G = ([n], M)$ גרף עם מעגל המילטוני.
<u>קלט סודי של המוכיח P</u>: מעגל המילטוני $c : [n[\to [n]$

$P \to V$: P שולח n^2 התחייבויות, אחת לכל אחד מערכי מטריצת השכנויות $M[i,j]$.

$P \leftarrow V$: V שולח ביט אקראי b.

$P \to V$: P אם $b = 0$ פותח את כל ההתחייבויות. אם $b = 1$, שולח את c ופותח רק את ההתחייבויות של קשתות המעגל $M[c(i), c(i+1 \mod n)]$.

V: אם $b = 0$, מקבל רק אם ההתחייבויות אכן למטריצה הנכונה M. אם $b = 1$, מקבל רק אם c אכן מתאר מעגל. כלומר, c פרמוטציה ולכל $i \in [n]$, $M[c(i), c(i+1 \mod n)] = 1$.

סעיף א'

הראו כי אם $G = ([n], M)$ **אינו** מכיל מעגל המילטוני, V מקבל בהס' לכל היותר $1/2$. כלומר לפרוטוקול נאותות $1/2$.

תשובה:
ישנן שתי אפשרויות:
הראשונה, P^* שולח התחייבות לגרף האמיתי הנתון ע"י M. במקרה זה, מאחר ואינו יכול לפתוח מעגל המילטוני, נתפוס אותו בהסתברות $1/2$.
השניה, P^* שולח התחייבות לגרף שונה הנתון ע"י M^*. במקרה זה, גם נתפוס אותו בהסתברות $1/2$ כאשר נבקש ממנו לפתוח את הגרף.

סעיף ב'

האם הפרוטוקול הנו פרוטוקול אפס־ידע נגד V^* רשע? נמקו תשובתכם. (הניחו כי לא ניתן לחשב ביעילות מעגל המילטוני.)

תשובה:
בבירור לא. V^* יכול לבקש לפתוח תמיד את המעגל וללמוד מהו המעגל. (V ישר גם מפר אפס־ידע - לומד בהסתברות $1/2$ מעגל).

סעיף ג'

הציעו כיצד להפוך את הפרוטוקול לפרוטוקול אפס־ידע נגד V ישר אך סקרן (ומבלי לפגוע בנאותות או שלמות). נמקו תשובתכם (אין צורך בהוכחה פורמלית). רמז: עבור פרמוטציה שרירותית $c : [n] \to [n]$ ופרמוטציה אקראית $\sigma : [n] \to [n]$, ההרכבה $\sigma \circ c$ מתפלגת כפרמוטציה אקראית.

תשובה:
P לא יתחייב על הקשתות של לפי M המקורית, אלא יפעיל ראשית פרמוטציה אקראית σ על הקודקודים ויתחייב למטריצה $M'[i,j] = M[\sigma^{-1}(i), \sigma^{-1}(j)]$ המתקבלת לאחר הפעלת הפרמוטציה. כאשר יתבק לפתוח את הגרף כולו יציג גם את הפרמוטציה. השלמות והנאותות נשמרים מכיוון ש- M מכיל מעגל אמ"מ $\sigma(M)$ מכיל מעגל. הפרוקטוקול כעת אפס־ידע מכיוון שכאשר V רואה פתיחה של המעגל, הוא פשוט רואה מעגל אקראי שאינו תלוי כלל בגרף המקורי.