בחינה לדוגמה בתיאוריה שמאחורי בלוקצ'יינס

ניר ביטנסקי ואליעד צפדיה

23 ביוני 2019

הוראות

- משך הבחינה: שלוש שעות.
- חומר עזר מותר: 20 דפי A4 כתובים משני הצדדים.
- מותר להשתמש בטענות שהוכחו בכיתה או בשיעורי הבית אך יש לנסח את הטענה בה אתם משתמשים באופן מפורש.
- יש לענות על כל השאלות בבחינה.
- התשובה "אינני יודע/ת" תזכה ב־20% מהנקודות.
- המלצה: התשובה לכל סעיף לא אמורה לקחת יותר ממחצית העמוד. אין צורך להעתיק את השאלות עצמן למחברת הבחינה.
- השאלות אינן בהכרחש מסודרות לפי קושי. במידה ואתם נתקעים, המשיכו הלאה.

שאלה 1

רמי לוי החליט להקים בלוקצ'יין זול במיוחד.

א. במקום להשתמש בפונקציה חסינה מפני התנגשויות עם כיווץ שרירותי הוא משתמש בפונקציה H המכווצת n ביטים ל־$n-1$ ביטים. הראו איך אפשר להשתמש ב־ H כדי לקבל פונקציה חסינה מפני התנגשויות עם כיווץ שרירותי, כלומר הראו איך לכל $t \geq n$ נתון אפשר לבנות פונקציה H_t המכווצת t ביטים ל־ $n-1$ שמבצעת לכל היותר $O(t-n)$ קריאות ל־ H, כך שמכל התנגשות ב־ H_t אפשר יהיה לחלץ התנגשות ל־ H.

ב. במקום להשתמש במערכת חתימה דיגיטלית סטנדרטית, הוא משתמש במערכת חתימה חד־פעמית. כלומר לאחר שהיריב ראה חתימה על הודעה אחת הוא מסוגל לזייף חתימה על כל הודעה אחרת. הציעו דרך להתשמש במערכת החתימה החד־פעמית באופן בטוח כך שעבור כל טרנזקציה מייצר המשתמש זוג מפתחות חדש (פומבי ופרטי) אחד בלבד. אין צורך להוכיח את הבטיחות של הפתרון.

ג. במקום להשתמש בהוכחות אפס ידע ליצירת מטבע אנונימי כדוגמת זירוקוין, הוא משתמש במערכת עם עדים בלתי־ניתנים־להבחנה (WITNESS INDISTINGUISHABLE). האם ניתן להשתמש בזירוקוין במערכת הוכחה שכזו מבלי לבצע שינויים נוספים בפרוטוקול? נמקו בקצרה את תשובתכם.

פתרון

א. בהינתן הפונקציה $H\colon \{0,1\}^n \to \{0,1\}^{n-1}$, נגדיר את הפונקציה $H_t\colon \{0,1\}^t \to \{0,1\}^{n-1}$ לכל t בצורה הבאה: עבור $t = n$ נגדיר $H_n = H$. עבור $t > n$ וקלט $x = x_1, \ldots, x_t \in \{0,1\}^t$ נגדיר

$$H_t(x) = H_{t-1}(H(x_1, \ldots, x_n), x_{n+1}, \ldots, x_t).$$

נשים לב שאם ניתן למצוא לפונקציה התנגשות $H_t(x) = H_t(\tilde{x})$ עבור $x, \tilde{x} \in \{0,1\}^t$ שונים כלשהם, אז יש התנגשות ב־ H_{t-1} עבור $x' = H(x_1, \ldots, x_n), x_{n+1}, \ldots, x_t$ ו־ $\tilde{x}' = H(\tilde{x}_1, \ldots, \tilde{x}_n), \tilde{x}_{n+1}, \ldots, \tilde{x}_t$, כאשר שניהם באורך $t-1$ והם שונים כי אחרת זה שקול למציאת התנגשות ב־ H. ככה אפשר להמשיך עד $t = n$ ולקבל התנגשות ב־ H.

ב. לפני כל חתימה על טרנזקציה, המשתמש יגריל מפתח פומבי ופרטי חד־פעמיים חדשים. בחתימה על הטרנזקציה המשתמש יחתום בפועל עם המפתח הקודם על השירשור של הטרנזקציה עם המפתח הפומבי החדש.

ג. אי אפשר להחליף הוכחת אפס ידע בהוכחה עם עדים בלתי ניתנים להבחנה. בזירוקוין אנחנו מעוניינים להוכיח באפס ידע את הטענה הבאה: "המספר הסיריאלי S מתאים לאחד ה־ ZEROCOIN COMMITMENTS", כאשר העד הוא למעשה המטבעות הרנדומיים שהוגרלו ביצירת ה־ COMMITMENT המתאים. במקרה למשל שהמטבעות הללו נקבעים באופן יחיד מה־ COMMITMENT, אין שום משמעות להוכחה של עדים בלתי ניתנים להבחנה כי יש רק עד אחד וזה למעשה שקול לשליחת המטבעות הרנדומיים שאמורים להיות סודיים.

שאלה 2

יהי $n \in \mathbb{N}$ ו־ $N = 2^n$ ותהי $H\colon \mathbb{Z}_N \to \mathbb{Z}_N$ פונקציית גיבוב הממודלת כפונקציה רנדומית בשאלה זאת, כאשר כל איבר $x \in \mathbb{Z}_N = \{0, \ldots, N-1\}$ מיוצג על ידי מחרוזת בינארית באורך n.

א. נסתכל על הפאזל הבא: בשלב דגימת הפאזל בוחרים $x' \leftarrow \mathbb{Z}_N$ רנדומי ומגדירים פאזל P_y על ידי $y = H(x') - x' \pmod N$. על־מנת לפתור את הפאזל P_y יש למצוא $x \in \mathbb{Z}_N$ כך ש־

$$H(x) = x + y \pmod N.$$

הראו איך לפתור $N > t$ פאזלים $y_1, \ldots, y_t$ בזמן $O(Nn \log t)$ על־ידי $O(N)$ קריאות ל־ H ולכל היותר $O(tn)$ זיכרון. הניחו כי H ניתנת כאורקל, ואינכם משלמים על זמן הריצה שלה.

ב. נסתכל על הפאזל הבא: בשלב דגימת הפאזל בוחרים $x' \leftarrow \mathbb{Z}_N$ רנדומי ומגדירים פאזל P_y על ידי $y = x' - H(x') \pmod N$. על־מנת לפתור את הפאזל P_y יש למצוא $x \in \mathbb{Z}_N$ כך ש־

$$H(x + y) = x \pmod N.$$

הראו איך לפתור $N > t$ פאזלים $y_1, \ldots, y_t$ בסיבוכיות דומה לסעיף הקודם.

ג. כעת נסתכל על הפאזל הבא: בשלב דגימת הפאזל בוחרים $y \leftarrow \mathbb{Z}_N$ רנדומי, כאשר הפאזל P_y שמוגדר על ידי y הוא הבעיה של מציאת $x, x' \in \mathbb{Z}_N$ עם $x' - x \neq y \pmod N$ כך ש־

$$H(x + y) = H(x').$$

הראה שבסיכוי 99% אפשר לפתור פאזל אחד ב־ $O(\sqrt{N})$ קריאות ל־ H בלבד.

פתרון

א. בהינתן $y_1, \ldots, y_t \in \mathbb{Z}_N$ (כאשר כל אחד מיוצג על ידי n ביטים) ממיינים אותם בזמן $O(nt \log t)$ ושומרים אותם ממויינים בזיכרון $O(tn)$. כעת עבור כל $x \in \mathbb{Z}_N$ מחשבים $y = H(x) - x$ ומחפשים בזמן $O(n \log t)$ האם $y = y_i$ עבור איזשהו $i \in [t]$, ונסמן ב־ x את הפתרון לפאזל y_i. עושים זאת עד אשר פגענו בכל $y_1, \ldots, y_t$. ב־ Worst־Case עוברים על כל $\mathbb{Z}_N$ ולכן זמן הריצה הוא $O(Nn \log t)$ ומספר הקריאות ל־ H הוא $O(N)$.

ב. נשים לב שאם $y = x' - H(x')$ אז עבור $\tilde{x} = x' - y$ מתקיים $H(\tilde{x} + y) = \tilde{x}$, כלומר $\tilde{x}$ הוא פתרון לפאזל y. שוב בהינתן $y_1, \ldots, y_t \in \mathbb{Z}_N$ ממיינים אותם ועבור כל $x \in \mathbb{Z}_N$ מחשבים $y = x - H(x)$, מחפשים האם $y = y_i$ עבור איזשהו $i \in [t]$, ואם כן מסמנים ב־ $\tilde{x} = x - y$ את הפתרון לפאזל y_i. הסיבוכיות כמו הסעיף הקודם.

ג. עבור $t = 6\sqrt{N}$ נבחר $t + 1$ ערכים שונים כלשהם $x_1, \ldots, x_{t+1} \leftarrow \mathbb{Z}_N$ ונחפש האם יש $i \neq j$ כך ש־ $H(x_i) = H(x_j)$. כיוון ש־ H פונקציה אקראית, $H(x_i)$ הוא איבר אקראי ב־ $\mathbb{Z}_N$ (באופן בלתי־תלוי ב־ $H(x_j)$ עבור $j \neq i$) נשים לב שהסיכוי ששני איברים אקראיים לא מתנגשים הוא $1 - 1/N$, והסיכוי ששלושה איברים אקראיים לא מתנגשים הוא $(1-1/N)(1-2/N)$ וכך הלאה נקבל שהסיכוי שלא נמצא התנגשות עם $t + 1$ איברים אקראיים הוא

$$(1 - 1/N) \cdot (1 - 2/N) \cdots (1 - t/N) \leq e^{-1/N} \cdot e^{-2/N} \cdots e^{-t/N} \leq e^{-t^2/2N} \leq 0.01$$

כאשר באי־שיוויון הראשון השתמשנו בעובדה ש־ $1 + x \leq e^x$ לכל x. בהינתן שמצאנו x_i, x_j כאלה, הפתרון לפאזל הוא לפחות אחד מבין $(x, x') = (x_i - y, x_j)$, $(x, x') = (x_j - y, x_i)$.

שאלה 3

אליעד, בני, יהודה, וניר מתלבטים האם להגיע השבועאליעד, בני, יהודה, וניר מתלבטים האם להגיע השבוע לשיעור בתיאוריה שמאחורי הבלוקצ'יין. יהודה הציע שלשם כך ישתמשו בפרוטוקול ההסכמה הביזנטית של רבין עם פרמטרים $n = 4, t = 1$. לשם כך, לאחר שבכל סיבוב r כל אחד שלח את הודעותיו, הם מסתכלים השמימה ולפתע מופיע ביט אקראי משותף $c(r)$ עבור סיבוב זה. זכרו כי בכל סיבוב r כל אחד מהששתפים i שולח את הביט $b_i(r)$ שברשותו וקובע את הביט $b_i(r+1)$ לסיבוב הבא בהתאם לביטים שקיבל מהאחרים בסיבוב r ולביט המשותף $c(r)$.

א. תארו את הכלל לפיו משתתף i קובע את הביט $b_i(r+1)$.

ב. הניחו כי אליעד, בני, ויהודה נוהגים בכנות. הוכיחו כי בסוף כל סיבוב הביטים שלהם זהים בהסתברות חצי לפחות וכי אם הביטים שלהם זהים בשלב כלשהו הם ישארו זהים.

ג. יהודה הציע כי במקום להסתכל השמימה, הם יקבעו את הביט המשותף $c(r)$ להיות הביט הראשון של $SHA256(r)$. תארו ביטים התחלתיים עבור שלושת הכנים ואסטרטגיה עבור ניר שתאפשר לו לדאוג לכך שאף סיבוב אינו מסתיים בהסכמה.

פתרון

א. הכלל של המשתמש ה־ i לקביעת $b_i(r+1)$ בסיבוב ה־ r: אם קיבלתי לפחות שלוש הצעות זהות לאותו ביט b (כולל ההצעה שלי $b_i(r)$) אז אגדיר $b_i(r+1) = b$, אחרת אגדיר $b_i(r+1) = c(r)$.

ב. אם הביטים של כל אחד משלושת השחקנים ההוגנים זהים, אז לפי הגדרה כל אחד מהם יקבל שלוש הצעות זהות (כולל של עצמו) ולכן הם ימשיכו להסכים על אותו הביט. אם אף אחד מהשחקנים לא קיבל שלוש הצעות זהות אז עדיין הם כולם יסכימו בסיכוי 1 על הביט $c(r)$. אחרת, אחד השחקנים ראה לפחות שלוש הצעות זהות, לביט מסויים b וכיוון שיש שלושה שחקנים הוגנים, לא ייתכן שמישהו ראה שלוש הצעות לביט ההפוך $\bar{b}$, ולכן במצב הזה תהיה הסכמה אם $c(r) = b$ וזה יקרה בסיכוי חצי.

ג. עבור כל סיבוב r נסמן $b_r = \text{SHA256}(r)$ ונאמר שהמצב הוא בר־תקיפה אם שחקן הוגן אחד מחזיק ב־ b_r (נסמנו בהכ כשחקן מספר 1) ושני השחקנים ההוגנים האחרים מחזיקים בביט ההפוך $\bar{b}_r$ (נסמנם בהכ כשחקנים 3,2). נראה כעת איך השחקן היריב יכול להפוך מצב בר־תקיפה בסיבוב r למצב בר־תקיפה בסיבוב $r+1$ ועל ידי מצב התחלתי שהוא בר־תקיפה עבור $r = 1$ לעולם הפרוטוקול לא יגיע להסכמה. אז בהינתן מצב בר־תקיפה בסיבוב ה־ r נסתכל על $b_{r+1} = \text{SHA256}(r+1)$. אם $b_r = b_{r+1}$, השחקן היריב ישלח את b_r לשחקן 1 ואת $\bar{b}_r$ לשחקנים 3,2 והמצב יישאר זהה גם לסיבוב הבא והוא בר־תקיפה כי $b_r = b_{r+1}$. אחרת, $b_{r+1} = \bar{b}_r$, ופה השחקן היריב ישלח לשחקנים 2,1 את b_r לשחקן 3 את $\bar{b}_r$. בסיום הסיבוב שחקנים 2,1 יחזיקו ב־ $b_r = \bar{b}_{r+1}$ ושחקן 3 יחזיק ב־ $\bar{b}_r = b_{r+1}$, כלומר קיבלנו מצב בר־תקיפה, כדרוש.

שאלה 4

ניר עובד על השקת בלוקצ'יין חדש "ביט־קוינסקי" המשפר את אלגוראנד.

א. השינוי הראשון שהציע באלגוראנד הנו לוותר על שלב בחירת הועדה ופשוט לקחת את הבלוק שמציע המנהיג הנבחר. האם יריב השולט ב־$1/10$ מההון (סטייק) במערכת יכול למזלג את הבלוקצ'יין (כלומר ליצור פיצול)? אם כן, תארו כיצד.

ב. בסופו של דבר שינה ניר את דעתו והחליט שלא לוותר על הועדה. במקום, לכל משתתף ברשת, ייצוג בועדה הפרופרציוני להון (סטייק) שלו. האם הפרוטוקול החדש בטוח? נמקו תשובתכם בקצרה.

ג. נניח כי גודל הועדה הממוצע הוא M ומס' המשתתפים הכולל הוא N. באילו תנאים סיבוכיות התקשורת של הפרוטוקול המקורי עדיפה על ההצעה של ניר. נמקו בקצרה.

פתרון

א. בסיכוי $1/10$ היריב ייבחר למנהיג, והוא יכול להפיץ שני בלוקים שונים לרשת. חלק מהצמתים יקבלו את הבלוק הראשון וחלק את הבלוק השני, ובכך יווצר מזלוג.

ב. הפרוטוקול בטוח. השינוי היחיד הנו שכעת פרוטוקול ההסכמה הביזנטית יבוצע בין יותר משתתפים. ההנחה הרגילה כי למעלה מ $2/3$ מההון ביידיים כנות, מבטיחה את תכונות הבטיחות של פרוטוקול ההסכמה הביזנטית.

ג. סיבוכיות התקשורת של הפרוטוקול המקורי עדיפה כאשר מספר המשתתפים גדול בהרבה מגודל הועדה הממוצעת $M \ll N$. אכן כמות הביטים שכל משתמש מקבל גדלה לינארית במס' חברי הועדה.