בחינה לדוגמה בתיאוריה שמאחורי בלוקצ'יינס

ניר ביטנסקי ואליעד צפדיה

20 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 בהכרח 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 המכווצת n ביטים ל־$n-1$ ביטים. הראו כי פונקציה כזו מאפשרת לבנות פונקציה עם כיווץ שרירותי. תארו בניה והסבירו בקצרה מדוע היא בטוחה.

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.

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 $x, x' \in \mathbb{Z}_N$ כך ש־

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

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

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.

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.