Digital Whisper
Technologic Papers

הוכחות באפס ידע

מאת אריק פרידמן

הקדמה

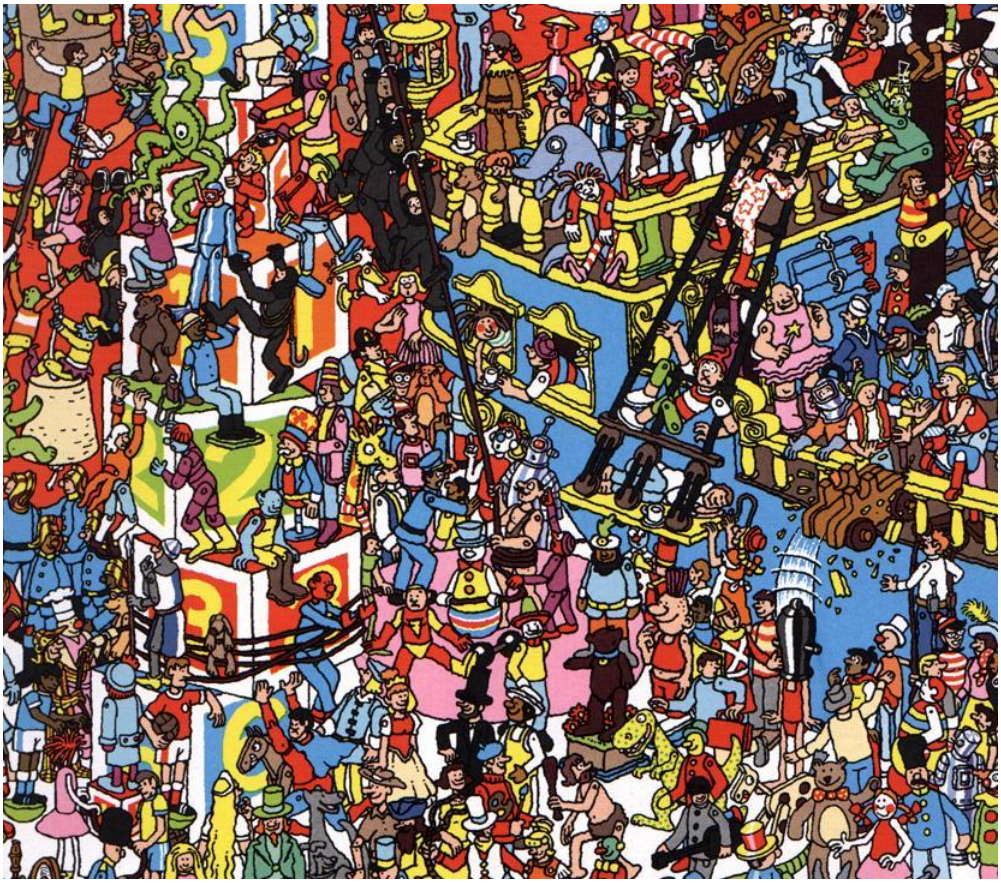
בעשורים האחרונים הגיחה הקריפטוגרפיה מתחומי המודיעין והאקדמיה, והפכה לגורם מרכזי המאפשר, בין השאר, מסחר אלקטרוני בטוח ברשת. כשמדברים על קריפטוגרפיה הדבר הראשון שעולה לראש הוא בדרך כלל "הצפנה" או "חתימות דיגיטליות", אולם התחום כמובן רחב בהרבה והקריפטוגרפיה מציעה שלל של כלים נוספים , חלקם משיגים מטרות שלכאורה סותרות את ההגיון ואת האינטואיציה האנושית לגבי איך דברים עובדים. אחד מכלים אלה הוא הכלי של הוכחה באפס ידע.

בניגוד למה שאולי מרמז השם, אין מדובר על האתגר העומד בפניהם של תלמידי התיכון המתמודדים עם שאלה בבחינת בגרות במתמטיקה, אלא במנגנון המאפשר להוכיח טענה מסויימת בלי לגלות דבר מעבר לעצם נכונות הטענה. על-פניה, נראה כי זו משימה בלתי אפשרית – כשאנחנו חושבים על הוכחות אנחנו מתארים בדרך כלל מצב בו מציגים עובדות כלשהן, או מספקים מידע שיתמוך בטענה. איך אפשר להוכיח דבר מה באופן שכזה? למנגנון של הוכחות באפס ידע תרומה רבה לקריפטוגרפיה. לדוגמה, הוא מאפשר לכפות על משתתפים זדוניים בפרוטוקול קריפטוגרפי לפעול על פי כללי הפרוטוקול. דוגמה אחרת שתוצג בהמשך היא יישומן של הוכחות באפס ידע להזדהות של משתמש בלי שיהיה ניתן ללמוד דבר על הסוד שלו, שבאמצעותו הוא מזדהה.

איך להוכיח איפה אפי בלי לגלות איפה הוא?

ראשית, בכדי להמחיש כיצד ניתן להוכיח דבר מה מבלי לגלות מידע נוסף, נפתח בדוגמה פשוטה מחיי היום-יום. בסדרת הספרים "איפה אפי" (או בגרסה האמריקאית Where's Waldo), נדרש הקורא לאתר את דמותו של אפי, בחור חביב בחולצת פסים.

והנה אתגר. במקום כלשהו בציור שלהלן נמצא אפי . אם הצלחתם למצוא את אפי , מאוד קל להוכיח את זה למישהו אחר – אפשר פשוט להצביע על אפי בציור . עם זאת, זה יהיה "ספוילר" אם הצד השני גם רוצה לחפש את אפי. האם אפשר להוכיח שמצאתם את אפי בלי לחשוף את מקומו?



ובכן, מסתבר שכן. הנה פתרון אפשרי: לקחת נייר אטום וגדול מאוד (הרבה יותר גדול מהד פים בספר), ולגזור בנייר פתח קטן שיהיה ניתן לראות דרכו אך ורק את פניו של אפי ולהניח אותו מעל דף הספר , כך שכל שאר הציור יהיה מוסתר. במידה והנייר מספיק גדול כך שלא יהיה ניתן להסיק ממיקום הגזירה היכן אפי נמצא בדף הספר, ובמידה ואף אחד לא הציץ בזמן שהנחתם את הדף, כל מה שיראו זה את פניו של אפי בפתח (אותם ממילא מכירים) ואכן לא ניתן יהיה ללמוד דבר על מיקומו של אפי. המדקדקים יבחינו כי נדרשים אמצעי זהירות נוספים. למשל, יש לוודא שאתם לא מרמים באמצעות דפדוף לדף הקודם שאותו פתרתם לפני רגע, והנחת הנייר הגזור עליו. המתעניינים מוזמנים להציץ ברשימת המקורות כדי להעמיק בפתרון הבעיה. דוגמה נהדרת נוספת ממחישה את העקרונות של הוכחות באפס ידע באמצעות סיפור על מערת הקסמים של עלי באבא, והקישור מופיע גם הוא ברשימת המקורות.

מערכות הוכחה אינטראקטיביות

על הוכחות באפס ידע מדברים בעיקר בהקשר של "מערכות הוכחה אינטראקטיביות". מערכת הוכחה אינטראקטיבית מוגדרת בהקשר של שפה כלשהי, שאפשר לחשוב עליה כעל משפחה של טענות (למשל, משפחת הטענות "אני יודע איפה אפי נמצא" עבור ציורים של אפי), כאשר בהוכחה נתונה רוצים להוכיח או להפריך את שייכותה של טענה למשפחה זו. במערכת הוכחה אינטראקטיבית יש שני צדדים: המוכיח (prover) והמוודא (verifier). לרוב אנו מניחים כי למוודא יש כוח חישובי מוגבל, בעוד המוכיח אינו מוגבל בכוחו. אפשר לחשוב על הוכחה אינטראקטיבית כעל סוג של משחק בו המוכיח נדרש לשכנע את המוודא בתקפותה של טענה כלשהי. שני הצדדים מקבלים פרמטר משותף, ובסוף התהליך המוודא צריך להחליט האם הוא אכן מקבל את הטענה (accept) או שהוא דוחה אותה (reject).

בהינתן האלגוריתמים המוכיח והמקבל, ישנן שתי דרישות ממערכת הוכחה: דרישת השלמות היא שעבור טענה נכונה, בסוף התהליך, המוודא יקבל את הטענה. דרישת הנאותות היא שלכל טענה שקרית ולכל מוכיח שהוא (כולל מוכיחים רמאים), המוודא ידחה את הטענה בהסתברות גבוהה.

במערכת הוכחה אינטראקטיבית באפס ידע קיימת דרישה נוספת של סודיות. אינטואיטיבית, הרעיון הוא שכל מה שניתן לחשב מתוך תמליל ההוכחה ניתן לחשב גם מהטענה (הנכונה) עצמה בלבד, והמשמעות היא שהמוכיח לא "הדליף" בזמן תהליך ההוכחה שום פרט חדש שלא היה ניתן לחשב ביעילות עוד קודם. דרישת הסודיות היא דרישה שחלה על המוכיח וצריך לוודא שהיא תקפה על כל מוודא שהוא, כולל מוודא שאין לו מטרה אמיתית לגלות אם ההוכחה נכונה או לא, וכל מה שהוא רוצה זה רק "לחלוב" מידע כלשהו מהמוכיח.

באופן פורמלי מנסחים את הדרישה הזו במונחים של סימולציה:
לכל מוודא שהוא, קיים אלגוריתם יעיל (קרוי "סימולטור"), כך שלכל טענה בשפה, האלגוריתם יכול לייצר "תמלילים" של הוכחות שיהיו דומים לאינטראקציות של אותו מוודא עם המוכיח. מידת הדמיון הנדרשת נגזרת באופן ישיר ממידת הסודיות הנדרשת. עבור אפס ידע מושלם, האלגוריתם צריך להיות מסוגל לייצר תמלילים זהים של השיחות.

הדרישה עבור "אפס ידע חישובי" היא, שאף גורם, בעזרת כל חישוב יעיל לא יוכל להבחין בין התמלילים המדומים לבין הה וכחות האמיתיות (משמעות הסודיות כאן, היא שלא ניתן יהיה לחשב שום דבר חדש ביעילות בעזרת האינטרקציה של המוודא עם המוכיח, אולם, במידה ויהיה לנו את כל הזמן שבעולם אולי כן נצליח לדלות אינפורמציה מהאינטראקציה).

לפני הצגת דוגמה להוכחה באפס ידע, נבחן כלי קריפטוגרפי נוסף – סכמות התחייבות.

להטיל מטבע בטלפון

נתאר את הסיטואציה הדמיונית הבאה: אי-שם בתחילת שנות ה-2000, באישון לילה אחד, אריק שרון ובוש משוחחים בטלפון במטרה להביא לסיומה של מסכת דיונים ארוכה הנוגעת לסיוע אמריקאי ומחוות ישראליות כאלה ואחרות. נראה שכל הדיונים נתקלים במבוי סתום, אבל חייבים למצוא פתרון. בראשו של אריק מבליח רעיון: "תראה, בוש", הוא אומר, "אנחנו לא מצליחים להתקדם, נכון? נראה לי שאין ברירה. בוא נערוך הגרלה. אני אטיל מטבע, אם יוצא עץ- נלך בדרך שלי, אם יוצא פאלי נלך בדרך שלך. מה אתה אומר?". אולם, בוש אינו בחור תמים. "איך אוכל לדעת שאתה לא עובד עלי? הרי אני לא יכול לראות מה קיבלת". אריק לא מתבלבל: "תראה, אין בעיה, גם אתה תטיל מטבע, כך שהדבר יהיה מאוזן. אם יצא לנו את אותה התוצאה, נלך בדרך שלי, אחרת נלך בדרך שלך, כן?". בוש מטיל מטבע, "יצא לי עץ". אריק מטיל מטבע, "גם לי". בוש נאנח, "מה שהוגן הוגן".

האם בכלל שני צדדים יכולים לבצע הגרלה כזאת כאשר אינם סומכים אחד על השני?
ובכן, הקריפטוגרפיה מספקת פתרון באמצעות מנגנון המכונה סכמת התחייבות. הרעיון הוא פשוט ביותר: צד אחד מתחייב מראש על הטלת מטבע בלי לגלות אותה, ואחרי שהצד השני מכריז על הטלת המטבע שלו, הצד הראשון חושף מה התוצאה שהתחייב אליה. ההתחייבות הזאת מזכירה את אותו קוסם החוזה מראש את תוצאת הבחירות/ הלוטו/ כוכב נולד, כותב את התוצאה על נייר ונועל את הדף בכספת. לאחר מעשה, מוציאים את הדף מהכספת ומאמתים את תחזית הקוסם. כמובן, הפתרון הקריפטוגרפי יקשה על הקוסם לבצע אחיזת עיניים בעת חשיפת ההתחייבות, אם כי שימוש בכלים קריפטוגרפים, לא מהימנים, איפשר בעבר לחוקרים לחזות מראש את הזוכה בבחירות לנשיאות האמריקאית באמצעותפלייסטשן 3.

סכמת התחייבות

בסכמת התחייבות יש שני צדדים – הצד שולח והצד המקבל, וישנם שני שלבים: שלב התחייבות ושלב גילוי. נתמקד בהתחייבות של הצד שולח על ביט יחיד (על מחרוזות ארוכות יותר ניתן להתחייב באמצעות התחייבויות נפרדות על ביטים). סכמת התחייבות צריכה לקיים שני תנאים: סודיות (secrecy) ומחוייבות (binding, או לחלופין חד משמעיות – non-ambiguity). משמעות הסודיות היא שלא יהיה ניתן להבחין בין התחייבות על ביט '0' לבין התחייבות על ביט '1'; כלומר, ההתחייבות עצמה לא תלמד את הצד מקבל מהו הערך עליו התחייב הצד השולח. המשמעות של מחוייבות היא שבשלב הגילוי יהיה ניתן "לפתוח" את ההתחייבות רק לערך חוקי אחד, מה שמבטיח לנו שהשולח לא יוכל לרמות ולהחליט לאחר מעשה לאיזה מבין הביטים לפתוח את ההתחייבות.

כדי להדגים סכמת התחייבות, אציג את בעיית הלוגריתם הדיסקרטי: נניח כי נתון לנו מספר ראשוני p גדול מאוד, ונתבונן על החבורה Z^*_p (מכילה את כל המספרים מ- 0 עד p-1). בכל חבורה כזאת קיים לפחות מספר אחד g (generator, יוצר) שבאמצעות חזקות שלו מודולו p ניתן לקבל את כל המספרים בחבורה. לדוגמה, עבור המספר הראשוני הבא: (הקטן יחסית) 13, המספר 6 הוא יוצר ($6^0 \bmod 13 = 0$, $6^1 \bmod 13 = 6$, $6^2 \bmod 13 = 10$, $6^3 \bmod 13 = 8$, …). בהינתן מספר כלשהו, נניח: x, קל לחשב $y=g^x \bmod p$. אולם לא ידוע פתרון יעיל לבעיה ההפוכה, המכונה "בעיית הלוגריתם הדיסקרטי": בהינתן

מספר y, מצא x כך ש-$y=g^x \bmod p$ (קיים פתרון פשוט שאינו יעיל: עבור על כל ה-x-ים האפשריים עד שימצא אחד אשר מקיים את המשוואה. חייבים לבחור p מספיק גדול כדי להפוך פתרונות מסוג זה ללא מעשיים).

בהנחה כי אכן אין פתרון יעיל לבעיית הלוגריתם הדיסקרטי, ניתן לנצל זאת בכדי לייצר סכמת התחייבות. בשלב ההתחייבות, הצד השולח בוחר באקראי מספר כלשהו r בין 0 ל-p-2 כך שהזוגיות של המספר היא הביט אליו רוצים להתחייב. השולח מחשב ושולח את $g^r \bmod p$. בשלב הגילוי השולח ישלח את הביט שאליו התחייב ואת r. המקבל מוודא שהזוגיות של הביט ושל r תואמות, וכן ש-$g^r \bmod p$ תואם למספר שקיבל בשלב ההתחייבות. המחוייבות של השולח במקרה זה היא מושלמת – מהרגע שנשלח $g^r \bmod p$ אין לשולח שום יכולת למצוא איזשהו r' עם זוגיות השונה מ-r כך ש-$g^r \bmod p = g^{r'} \bmod p$. פשוט לא קיים מספר כזה. מבחינת סודיות, על סמך הנחת הקושי של בעיית הלוגריתם הדיסקרטי אין ביכולתו של המקבל לגלות את r ולחשוף את הביט. זוהי סודיות חישובית, והיא אינה סודיות מושלמת; אם היה לצד המקבל את כל הזמן שבעולם, היה ביכולתו לבצע בדיקה עבור כל הערכים האפשריים ל-r עד שהיה מוצא את הערך הנכון.

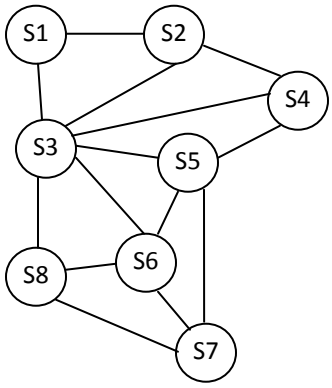
קיימות גם סכמות בהן יש סודיות מושלמת ומחוייבות חישובית (כלומר הופכים את ההנחות לגבי הכוח החישובי גם של השולח וגם של המקבל), אולם לא ניתן להשיג סכמה בה גם הסודיות וגם המחוייבות מושלמות, מאחר והמטרות הללו סותרות אחת את השנייה באופן מחייב: סודיות מושלמת דורשת שפלטי ההתחייבויות האפשריים עבור הביטים 0 ו-1 יהיו זהים, בעוד מחוייבות מושלמת דורשת שפלטים אלה יהיו זרים.

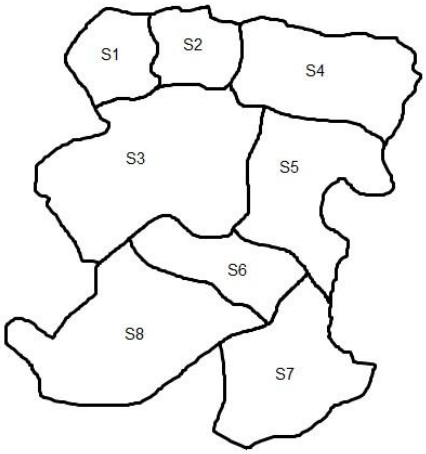
לאחר שראינו מהי סכמות התחייבות, נחזור לנושא הוכחות באפס ידע, ונראה יישום של סכמת התחייבות להוכחה כזו.

צביעת מפות באפס ידע

נפליג שוב על כנפי הדמיון, הפעם אל ימי הביניים, עת גילדות של קרטוגרפים התחרו זו בזו במטרה להפיק מפות איכותיות. עולם הקרטוגרפיה נקלע לסערה, בעת שאחד מחברי הארגון מכריז כי הצליח לצייר מפה של כל הנחלות בממלכה באמצעות שלושה צבעים בלבד. הקרטוגרפים נהגו להשתמש במגוון רחב של צבעים לצורך צביעת המפות (למעשה מספיקים ארבעה צבעים), אך עד כה אף אחד לא הצליח להפיק מפה מוצלחת באמצעות שלושה צבעים בלבד, כך שאף זוג נחלות שכנות לא יהיו צבועות באותו צבע (מאות שנים מאוחר יותר מדעני מחשב יאפיינו את הבעייה כ-*NP-שלמה*). למעשה, הקרטוגרפים נטו להאמין כי הדבר אינו אפשרי עבור מפת הממלכה. לכן, לאור הכרזתו של חברם, הקרטוגרפים טענו מייד כי לא רק שההכרזה היא עזת מצח, אלא שהיא גם חצופה, ודרשו מהקרטוגרף הסורר להוכיח בו במקום את טענתו או להתפטר. אותו קרטוגרף נקלע למצוקה – נראה כי כדי להוכיח את טענתו הוא צריך להציג את המפה ולחשוף את סודו בפני קהילת הקרטוגרפים, ובכך ימנע ממנו להציע את המפה המיוחדת לכל המרבה במחיר. ואולי לא?

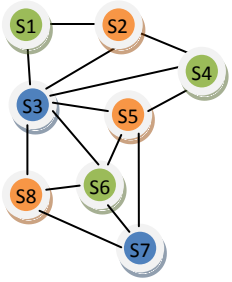
את המפה ניתן לייצג כגרף, בו כל נחלה היא צומת ושכנות בין נחלות מיוצגת באמצעות קשת. צביעת המפה בשלושה צבעים כך שכל זוג נחלות שכנות צבועות בצבעים שונים שקולה לצביעה של צמתי הגרף כך שאף קשת לא מחברת שני צמתים בעלי אותו צבע (בעיה זו ידועה בשם "בעיית 3-צביעה"). לדוגמה, להלן חלק קטן ממפת הקרטוגרף:



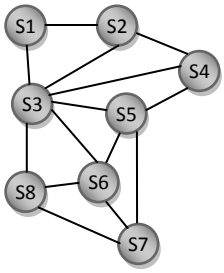


כדי להוכיח את יכולתו לצבוע את המפה בשלושה צבעים, הקרטוגרף יכול לנקוט בסדרת הצעדים הבאה:

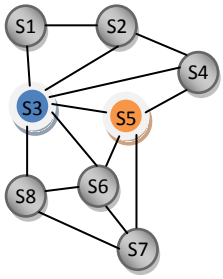
1. להגריל איזושהי פרמוטציה על הצבעים של הגרף. לדוגמה:



2. לייצר התחייבות על הצבע של כל אחד מהצמתים, ולהציג אותה לחבריו הקרטוגרפים. עקב תכונת הסודיות של סכמת ההתחייבות, הם לא יוכלו לגלות מתוך ההתחייבות מה הצביעה שבה השתמש:



3. בשלב הבא, חברי הגילדה בוחרים באקראי שני צמתים סמוכים, ודורשים ממנו לחשוף אותם. למשל, S3 ו-S5.



4. הקרטוגרף פותח את ההתחייבות על אותם שני צמתים שנבחרו.
5. אם הקרטוגרף לא פתח את ההתחייבות בהצלחה או אם מתברר כי שני הצמתים שנבחרו הם בעלי אותו צבע, חברי הגילדה מכלים את זעמם בקרטוגרף. אחרת, הם נאלצים להסכים שלפחות בסיבוב הזה הקרטוגרף הוכיח את יכולתו ל-3-צביעה.

על סדרת צעדים זו ניתן לחזור שוב ושוב עד שחברי הגילדה יתרצו ויגיעו למסקנה כי הקרטוגרף אכן הצליח לצבוע את המפה עם שלושה צבעים בלבד.

למה הסכמה הזו מהווה הוכחה באפס ידע? ההסברים שלהלן לא מהווים הוכחה (בספר של גולדרייך המופיע ברשימת המקורות ההוכחה מתפרשת על שבעה עמודים!), אך מטרתם להעביר את הרעיון הכללי. נבחן את שלושת הקריטריונים:

א) קריטריון השלמות דורש שאם בידיו של הקרטוגרף יש אכן 3-צביעה של המפה, אז הוא יוכל להוכיח זאת לחבריו. דרישה זו מתקיימת – שימוש ב-3-צביעה מבטיח כי לאף זוג צמתים סמוכים לא יהיה את אותו צבע, כך שאם הקרטוגרף פועל לפי ההנחיות, בשלב החמישי הוא תמיד יעבור את המבחן בהצלחה.

ב) קריטריון הנאותות דורש שאם אין בידי הקרטוגרף 3-צביעה, אז חברי הגילדה יעלו עליו בהסתברות גבוהה. כדי להבטיח זאת, יש לחזור על סדרת הצעדים מספיק פעמים. נניח שיש k קשתות בגרף (כלומר k זוגות צמתים שאותם חברי הגילדה יכולים לדרוש לגלות). אם לקרטוגרף אין 3-צביעה, המשמעות היא שלפחות אחת מאותן קשתות מחברת צמתים מאותו צבע, ולכן בהסתברות לפחות 1/k הקרטוגרף יידרש לפתוח קשת בעייתית והשקר ייחשף (מכיוון שבהוכחות אפס ידע המוכיח אינו מוגבל בכוחו חשוב להשתמש בסכמות עם מחוייבות מושלמת, אחרת המוכיח יוכל לרמות בעת פתיחת ההתחייבות). באמצעות חזרה על סדרת הצעדים מקטינים את ההסתברות שיתמזל מזלו של הקרטוגרף והשקר לא יתגלה.

ג) קריטריון הסודיות דורש ששום פרט חדש לא ידלוף מההוכחה כאשר בידי הקרטוגרף יש 3-צביעה של המפה. אינטואיטיבית, מאחר ובכל פעם שמבצעים את סדרת הצעדים הקרטוגרף מגריל מחדש את הקצאת הצבעים לצמתים, אז לא נלמד מהצבעים שנחשפו דבר מעבר לנכונות הטענה. ניתן לייצר "תמלילים" של הוכחות לכל מוודא גם ללא ידיעת הצביעה האמיתית: נגריל באקראי צבע לכל צומת ונייצר התחייבות. לאחר שהמוודא בחר זוג צמתים, נבדוק אותם: אם הם בצבעים שונים, אפשר לחשוף אותם ונקבל תמליל שנראה כמו אינטראקציה עם המוכיח האמיתי. אם קיבלנו צמתים באותו צבע, נגנוז את התמליל. אופי הסודיות שמקבלים כאן הוא סודיות חישובית (אין סודיות מושלמת כיוון שבהינתן כוח חישובי בלתי מוגבל אפשר לחשוף את ההתחייבויות ולגלות צמתים שכנים בעלי אותו צבע).

סכמת זיהוי באפס ידע (פיאט-שמיר)

אחד השימושים המעניינים להוכחות באפס ידע הוא לצורך פרוטוקולי הזדהות. משתמש מסוים מחזיק איזשהו סוד- s שרק הוא יודע, והוא מוכיח את זהותו למישהו אחר באמצעות הוכחה שהוא יודע את s. היינו מעוניינים לאפשר לעשות זאת, כך שמוודא הזהות או מישהו שמצותת לתעבורה לא ילמדו דבר על הסוד. דוגמה לפרוטוקול הזדהות כזה הוא פרוטוקול פיאט-שמיר, שהוצע על ידי עמוס פיאט ועדי שמיר ב-1986. פרוטוקול זה מתבסס על הקושי של בעיית הפירוק לגורמים ראשוניים. בפועל הפרוטוקול אינו יעיל מספיק, אולם הוא מהווה בסיס למספר סכמות זיהוי אחרות באפס-ידע, והוא מועיל להבהרת הרעיון.

כשלב מקדים, גוף מסוים שכולם סומכים עליו בענייני זיהוי (לצורך העניין, משרד הפנים) בוחר מספרים ראשוניים גדולים p ו-q ומחשב את n=pq, בדומה למה שקורה באלגוריתם RSA. את הראשוניים p ו-q

חשוב לשמור בסוד. כל גורם שמעוניין להנפיק "תעודת זהות" בוחר כסוד מספר s בין 1 ל-n (לא כולל) שהינו זר ל-n, מחשב $v=s^2 \bmod n$, ורושם את v במשרד הפנים תחת זהותו, כך שכולם יכולים לראות שהמספר v שייך לו.

כעת, לצורך הזדהות, חוזרים על הצעדים הבאים t פעמים (כאשר את t ניתן לקבוע על-פי ההסתברות שבה נרצה לתפוס רמאים):

1. המוכיח (הצד שמזדהה) בוחר מספר אקראי r בין 1 ל-n (לא כולל) ושולח $x=r^2 \bmod n$.
2. המוודא בוחר באקראי ביט e (0 או 1) ושולח למוכיח.
3. אם המוודא שלח 0, המוכיח ישלח בחזרה y=r. [נועד לתפוס רמאים]
   אם המוודא שלח 1, המוכיח ישלח בחזרה $y=rs \bmod n$. [נועד להוכיח זהות]
4. אם נשלח y=0 המוודא דוחה את ההזדהות (זה נועד לתפוס רמאות שבה המוכיח בחר r=0).
5. אם $y^2=xv^e \bmod n$ המוודא מקבל. אחרת הוא דוחה.

אם כל t הסיבובים התקבלו בהצלחה, ההזדהות הסתיימה בהצלחה.

זוהי סכמת הזדהות באפס ידע. שלמות מתקיימת כאן מכיוון שהמשתמש האמיתי תמיד יצליח לעבור את כל הבדיקות במידה והוא יפעל לפי ההנחיות: אם הצד המוודא דרש את הבדיקה הראשונה (e=0), אין למשתמש שום בעיה לשלוח את המספר r שבחר בחלק הראשון, ואם המוודא דרש את הבדיקה השניה (e=1), הידיעה של הסוד s מאפשרת למשתמש לשלוח את $rs \bmod n$ גם במקרה זה. בכל מקרה, הבדיקה בשלב 5 תעבור בהצלחה. לעומת זאת, מתחזה ייתפס בהסתברות גבוהה, ולפיכך מתקיימת דרישת הנאותות: אם פעל בשלב הראשון לפי ההנחיות, אז במידה והמוודא בחר e=1 המתחזה לא יוכל להחזיר תשובה נכונה כיוון שאינו יודע את s. אולם יש לו גם אפשרות לרמות, ולשלוח בשלב 1 את הנתון $x=r^2/v$. במקרה זה, כאשר המוודא בוחר e=1 יוכל לשלוח y=r ולעבור את הבדיקה, אולם אז הוא מסתכן בכך שהמוודא יבחר e=0, ובשלב 3 המוכיח יצטרך לשלוח $y=\sqrt{r^2/v} \bmod n$. כמובן שמשימה זאת אינה מעשית כיוון שנדרש לפתור שורש ריבועי שמודולו n (בעיה השקולה חישובית לפירוק של n לגורמים ראשוניים). הסודיות מתקיימת מכיוון שבכל הרצה של הפרוטוקול, או שנחשף ערכו של r, שהוא מספר אקראי, או שנחשף ערכו של rs, שגם הוא מספר אקראי. יש אפשרות לייצר תמלילי הוכחה על ידי בחירה אקראית של y, והגדרת $x=y^2$ או $x=y^2/v$ בהתאם לבחירת המוודא.

מילות סיכום

הוכחות באפס ידע הן כלי שימושי ומועיל בפיתוחים בתאוריה של הקריפטוגרפיה. כמובן שהמידע שהוצג כאן הוא רק קצה המזלג וישנן הרחבות רבות לתחום זה: מהו אפס-ידע סטטיסטי? איך מטפלים ב"הרכבה" של הוכחות באפס ידע (שרשור של טענות)? מה קורה כשמבצעים מספר הוכחות באפס ידע במקביל? (מתברר שמקביליות עשויה לשבור אפס-ידע) רשימת המקורות שלהלן היא נקודת פתיחה מועילה למי שמעוניין ללמוד עוד על תחום זה.

מקורות

1. להוכיח איפה אפי באפס ידע:

Applied Kid Cryptography by Moni Naor, Yael Naor and Omer Reingold.
http://www.wisdom.weizmann.ac.il/~naor/PUZZLES/waldo.html

2. מערת הקסמים של עלי-באבא:

How to explain zero knowledge to your kids, by Quisquater Jean-Jacques, Guiollou Louis and Tom Berson: http://www.springerlink.com/content/uebe1l72w9n9m8f8/ (also possible to access copies here and here)

3. מבוא לאפס ידע:

Zero-Knowledge: a tutorial by Oded Goldreich.
http://www.wisdom.weizmann.ac.il/~oded/zk-tut02.html

4. למידע נרחב יותר על אפס ידע:

Oded Goldreich: Foundations of Cryptography, Volume 1 (Basic Tools), Chapter 4, Cambridge University Press, 2001. An early draft of the chapter is available online:
http://www.wisdom.weizmann.ac.il/~oded/PSBookFrag/part4N.ps