



על Bulletproofs, הוכחה באפס ידיעה ושאר ירקות

מאת אופק שוחט

הקדמה

קריפטוגרפיה היא נושא רחב בו, בין השאר, חוקרים כיצד ניתן להעביר מידע ממקום למקום בדרך "מאובטחת". השיטות אשר פותחו עם השנים התחילו משיטות פשוטות כמו צופן שחלוף ("צופן קיסר"), וכעת השיטות המפותחות הן חזית המחקר העכשווית. העברת מידע היא חשובה, והיא בסיס של האינטרנט כיום. כחלק מהעברת המידע באופן מאובטח, לעיתים עלינו להוכיח כי בידינו מידע כלשהו או שטענה מסוימת היא נכונה, אך מבלי שנרצה להציג את המידע שברשותנו. זה נשמע מעט פרדוקסלי - וזהו אחד הדברים שהכניסו אותי לתחום הקריפטוגרפיה בפרט ולעולם המתמטיקה בכלל.

הוכחות כאלה מכונות "Zero Knowledge Proofs", או בעברית צחה: "הוכחות באפס ידיעה", והן הרבה יותר שימושיות ממה שחשבתם - כנראה. בשיטות האלה ניתן לבצע דברים מגניבים מאוד: לדוגמה, ניתן לבצע חישוב מבוצר בקבוצה בלי הצורך לסמוך על שאר המשתתפים בחישוב, או לפחות על רובם (תחום המכונה MPC - "חישוב מרובה משתתפים"), לדוגמה לטובת הצבעות אלקטרוניות. דוגמה נוספת היא היכולת לחתום דיגיטלית על הודעה, כך שנדע אם היא שונתה בדרך; וגם, הדבר שחייבתם לו... Range Proofs - להוכיח שערך קיים בתוך טווח ערכים מסוים. על השימושים האחרים של Bulletproofs לא אדבר פה.

מטרתי במאמר זה היא לתת לכם את הבסיס הנדרש להבנת המאמר "[Bulletproofs: Short Proofs for Confidential Transactions and More](#)" - מאמר ידוע מאוד בתחום ה-Zero Knowledge Proofs ובעל השפעה בהיסטוריה של התחום (אחד מכותבי המאמר הוא [דן בונה](#), ישראלי, ופרופסור באוניברסיטת טסנפורד וזוכה פרס גדל). את ההסברים אתחיל מהבסיס, כך שאין דרישות לידע מוקדם בקריפטוגרפיה. אני אנסה לגרום לכם לחשוב ואולי להמציא מחדש כמה דברים, ובכלל ללמוד על ה-'שדה' הזה ☺. אני מבטיח שיהיה - לפחות קצת - מעניין.

הענף עצמו והשם הנלווה לו פותח ופורסם ב-1985 על ידי Goldwasser, Micali ו-Rackoff, במאמר "[The knowledge complexity of interactive proof-systems](#)"¹ (אחת מכותבות המאמר היא [שפי גולדווסר](#), חוקרת ישראלית-אמריקאית המתגוררת בישראל, ובין השאר, היא פרופסור למתמטיקה במכון וייצמן), שם

¹ <https://dl.acm.org/doi/pdf/10.1145/22145.22178>



הם הגדירו פורמלית את הפרימיטיב "הוכחה באפס ידיעה", עם מכונות טיורינג "אינטראקטיביות" (ממליץ לקרוא אם מעניין אתכם), אבל ההגדרות המודרניות הרבה יותר קלות להבנה.

הוכחות באפס ידיעה מוסיפות שכבה נוספת על הדרישות שראינו עד כה: אסור שה-"אויב" יבין משהו על העד. אפשר להגדיר את ההוכחות האלה עם שלושה תנאים:²

1. שלמות (completeness): אם מוכיח הגון נתן למאמת הגון הוכחה - המאמת ישוכנע שהטענה נכונה;
2. תקפות (soundness): אם מוכיח לא-הגון נתן למאמת הגון הוכחה - המאמת לא ישוכנע שהטענה נכונה; וגם
3. אפס-ידיעה (zero-knowledgeness): אם מוכיח נתן למאמת הוכחה, המאמת לא ילמד שום דבר על העד.

התנאים הללו הגיוניים והכרחיים, ואולי אפילו טבעיים, אבל פורמליזם הוא חשוב. משם, בעצם, פרץ ענף ה-zero knowledge.

"A proof is whatever convinces me." - Shimon Even (1935-2004)³

קצת רקע

הרקע המתמטי יהיה קצר ככל שניתן:

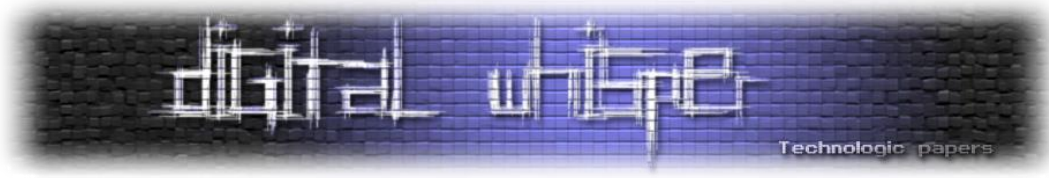
שדות הם ממש כמו המספרים הממשיים שאנחנו מתעסקים איתם ביום-יום, המספרים המרוכבים, הרציונליים ועוד. או, יותר נכון, אלו הם דוגמאות לשדות. הפעולות עליהם, כפל וחיבור, מקיימות כמה אקסיומות והם נוחים לעבודה. הפעולות קיבוציות וחילופיות, ומשם התכונות הנחמדות של המבנים הללו. לכל איבר בקבוצה המגדירה את השדה, קיים איבר המקיים: $a \otimes (a^{-1}) = 1$, כאשר $a \neq 0$ וגם $a \oplus -a = 0$, כאשר $0, 1$ מוגדרים להיות האיברים הניטרליים⁴ של הקבוצה. כאשר 'מכפילים' (\otimes) ב-1 נקבל את אותו האיבר, וכש'נחבר' (\oplus) עם 0 נקבל אותו האיבר.

חבורות הן כמו שדות מוגבלים: עליהם מוגדרות רק פעולה בינארית אחת. לרוב בקריפטוגרפיה נשתמש בחבורות ציקליות⁵, כך שקיים איבר g , שעם מכפלות חוזרות אפשר לייצר את כל החבורה. נקרא לכל g העונה להגדרה "מחולל". תזכורת חשובה: $g^a g^b = g^{ab}$. שימו לב שכל פעולה באברי חבורה גוררת

² אפשר להגדיר את תנאים 1 ו-2 עם: ... בהסתברות זניחה\מכריעה. לפעמים מוסיפים עוד תנאי של יעילות, כך שאימות והוכחה אמורים להיות בזמן פולינומי.

³ <https://www.wisdom.weizmann.ac.il/~oded/VO/foc.pdf>

⁴ איבר נייטרלי הוא איבר בקבוצה שכאשר מבוצעת עליו פעולה בינארית עם איבר אחר, היא איננה משנה את האיבר האחר
⁵ גם שדות סופיים הם ציקליים ובהם משתמשים בשביל להגדיר הרבה דברים אחרים, כמו הנקודות על עקומים אליפטיים, נקודות על סריגים ודברים אחרים. פשוט קל להשתמש בהם.



פעולות נוספות כמו מודולו, אבל אלו לא חשובות בשביל הבנת הנושא, רק הבעיה הגוררת את סיבוכיות הפתרון (שזה חשוב, ללא ספק ©).

המכפלה הפנימית (inner product) שדיברתי עליה קודם מוגדרת כך⁶: בהינתן שני וקטורים a, b עם n איברים:

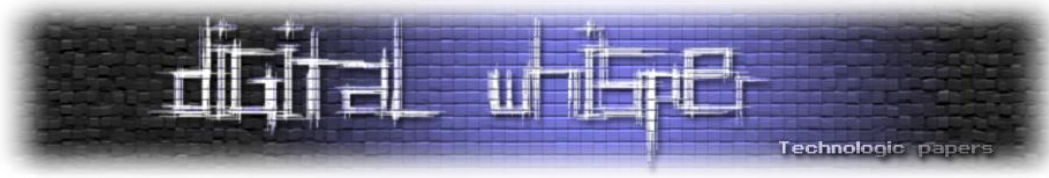
$$\langle a, b \rangle = \sum_{i=1}^n a_i \cdot b_i, b = (b_1, b_2, \dots, b_n), a = (a_1, a_2, \dots, a_n)$$

אסמן מפתחות ציבוריים באות גדולה, פרטיים באות קטנה. במאמר משתמשים בנוטציה שהוצגה על ידי Stadler-I Camenisch:

$\{(w) : \mathcal{L}(w, x)\}$ מייצגת את המטרה של ההוכחה. ההוכחה צריכה להיות בשפה \mathcal{L} עם העד w וההצהרה x . ההצהרה היא מידע שידוע גם למוכיח וגם למאמת; העד הוא מידע (לרוב סודי), שרק המאמת יודע. למשל הוכחה שמנסה לשכנע את המאמת בכך שאיזשהו x (העד) כפול G שווה ל- Y (בתוך ההצהרה) תיוצג כך: $\{(x) : Y = xG\}$ (זו הנוטציה ל- discrete logarithm problem בעקומים אליפטיים). לרוב משתמשים בבעיות בתוך NP, כך שלפעמים קוראים לשפה "NP-relation".

בעיית הלוגריתם הדיסקרטי/בדיד: נניח שקיימים מבנים מתמטיים בהם קשה מאוד למצוא את x מהערך g^x , ונניח שהמבנה בו אנחנו משתמשים הוא כזה בהמשך המאמר. זו ההנחה הבסיסית במאמר והיא סטנדרטית להרבה מהקריפטוגרפיה כיום⁷. אני אשתמש בסימון של המספרים הטבעיים (לנו) בשביל לייצג את בעיית הלוגריתם הבדיד ($g^a = b$), אבל תמיד אפשר לייצג אותה גם כ- $aG = b$, למשל בשביל עקומים אליפטיים.

⁶ זו ההגדרה שמשתמשים בה במאמר, אבל מכפלה פנימית היא מושג יותר כללי, שלרוב מדבר על פונקציה מהצורה $V \times V \rightarrow F$ המקיימת כמה אקסיומות.
⁷ עכשיו מנסים להחליף אותה עם בעיות אחרות מגניבות לא פחות! ראו: [הספר הזה](#).



Bulletproofs

Bulletproofs⁸ היא שיטה קריפטוגרפית (ממש מגניבה) שמאפשרת לעשות מספר דברים. בין השאר, הוכחות טווח ומעגלים אריתמטיים (אל חשש, עדיין לא צריך לדעת כלום ☺).

היא אינה מצריכה הכנה מוקדמת כמו חלק מה-ZK-SNARKS⁹, כך שהיא מאוד אטרקטיבית, ובנוסף לזאת היא גם לוגריתמית במקום. אז למה בעצם צריך אותה?

מה זו התחייבות? התחייבות זו פונקציה שהתוצאה שלה מחייבת את המתחייב לערך מסויים (binding) ומסתירה אותו (hiding).

ניקח את הדוגמה הנפוצה ביותר: מטבעות קריפטוגרפיים. נניח כי אנו מנסים לתכנן מערכת שבה יהיה ניתן להעביר סכום כסף מ-Alice ל-Bob בלי שאף אחד אחר ידע. פרטיות כזו היא מחויבות של המדינה ו/או הבנקים בעולם שלנו, אבל אם אנו רוצים להיפטר מהתלות הזו, החברים ברשת צריכים לשכנע את עצמם שלא יצרנו כסף חדש, בלי לדעת את הסכומים. אנחנו נשתמש בהתחייבות C שתיתן לנו להחביא וקטור של ערכי כסף, ולהתחייב אליו. כאילוץ נוסף, נצטרך שההתחייבות תהיה הומומורפית, כלומר: $C(a) \otimes C(b) = C(a \oplus b)$ כאשר \oplus ו- \otimes מסמלות פעולות.

אנחנו בעצם מנסים למצוא שיטה שתיתן לנו לבדוק שכל הכסף הנקלט לעסקה מהשולח, הוא אותו הסכום כמו הכסף שנכנס לחשבון המקבל (פחות עמלה מסויימת שנשארת ציבורית; דבר כזה הוא לרוב רצוי); כך שיהיה נחמד אם הפעולות יהיו חיבור. אבל רגע אחד, אנחנו מכירים פונקציה כזו - כזו שהנחנו שלא נוכל לשבור(!): בעיית הלוגריתם הבדיד g^v -¹⁰. אבל אם נשתמש רק ב- g^v , תוקף ידע מישהו השתמש באותו הערך פעמיים, או, אם המידע קל לניחוש, הוא יוכל לנסות ולמצוא את הערך. אם נכפיל את התוצאה בעוד ערך מוסכם, בחזקת ערך שנקרא לו גורם הסתרה (אנשי האקדמיה ללשון העברית, דברו איתו!), נוכל לקבל פונקצית התחייבות, בה הפעולה ההומומורפית נשמרת - היא כפל, וחיבור! כך שכאשר נכפיל: $Com(a, s_1) \cdot Com(b, s_2)$ נקבל: $Com(a + b, s_1 + s_2)$.

הפונקציה $g^x h^v$, אותה פיתחנו למעלה, נקראת התחייבות Pederson. היא מחביאה בצורה מושלמת (Perfectly Hiding; כמו OTP מי שמכיר), כך שגם עם מחשב קוונטי לא אוכל למצוא את הערך. שימו לב:

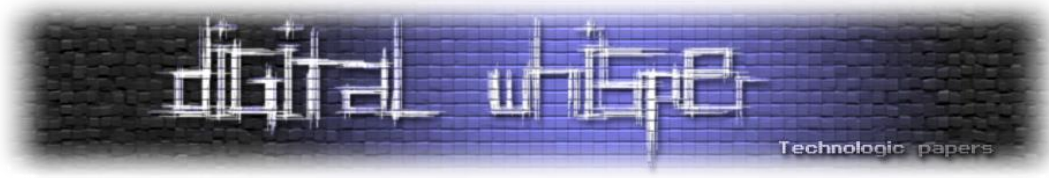
1. ההכללה לוקטורים פשוטה: ניקח g וקטור ונחשב: $Com(V, s) = g^s \prod_{i=1}^n h_i^{V_i}$, וגם,

2. אי אפשר סתם לחשב s חדש בשביל למצוא ערך ספציפי מהתחייבות קודמת, מכיוון שנצטרך לשבור את בעיית הלוגריתם הבדיד - זו שהנחנו שלא פתירה.

⁸ <https://eprint.iacr.org/2017/1066.pdf>

⁹ לא בהכרח מצריכות אותה, אבל לרוב (לא שמעתי על אחת שלא משתמשת באחת). שיטה אחרת להוכחות באפס ידיעה - גם הן ריקורסיביות. הן יותר קטנות, אבל לרוב גם מחייבות אותנו לסמוך על איזושהי setup ceremony המייצר כמה ערכים משותפים. הן מחייבות איזשהו שלב יסודי כזה - "כננו מהימן" ("trusted setup") - בשביל לעבוד.

¹⁰ DLP - discrete logarithm problem



נחזור בחזרה: אז נשלח התחייבות לערכים עם גורמי הסתרה המבטלים זה את זה (את זה לא קשה לעשות, פשוט צריך לבחור כאלה שסכומם שווה ל-0), ופתרנו את הבעיה לא?:

$$\prod_{i=1}^n h^{in_i} \cdot \prod_{i=1}^n g^{si} = \prod_{i=1}^n h^{out_i} \cdot \prod_{i=1}^n g^{S_{n+i}} \cdot h^{fee}$$

$$\Leftrightarrow \prod_{i=1}^n h^{in_i} = \prod_{i=1}^n h^{out_i} \cdot h^{fee}$$

הוכחנו שלא יצרנו או השמדנו כסף, נכון? נכון? ... אז זהו, שלא.™

הבעיה נוצרת מהמבנה המתמטי בו אנחנו משתמשים: החבורה. נתון שלכל איבר יש הופכי, כך שאם נשתמש בערך המייצג 1-, נוכל לייצר מטבע מאוויר. למשל: $h^1 h^2 = h^2 h^1$, אבל גם: $h^{-1} h^3 = h^2$.

אז בעצם, מה צריך לעשות? אנחנו צריכים משהו שיוכיח שכל מה שנכנס, וכל מה שיוצא יהיו בגודל מסויים; נגיד בין 0 לבין 2^{64} .¹¹ נקרא להוכחות כאלה הוכחות טווח.

ההיסטוריה של הוכחות הטווח

הוכחות טווח - או Range Proofs - עושות בדיוק את זה: מוכיחות שערך שהתחייבנו אליו בתוך טווח מסויים. במאמר המקורי של מה שאנחנו קוראים לו היום Monero, השתמשו ב-Borromean ring signatures. אתאר אותו בתמצית.

Ring Signatures - חתימות מעגליות

נתחיל בחתימות רגילות¹². נגדיר H להיות פונקצית גיבוב (hash); נגדיר k הוא המפתח הפרטי ו-K הוא המפתח הציבורי, שהוא שווה ל-m; g^k זו ההודעה שעליה אנחנו חותמים; || זו פונקצית שרשור בבייטים. זהו מוטיב חוזר בהוכחות האלה: אנחנו צריכים למצוא פונקציה שאפשר לחשב את ערכה רק עם המפתח הפרטי - התחייבות כזו - ובאותו הזמן, עם פרמטר ציבורי ועוד מידע אופציונלי מהמוכיח, נוכל למצוא את ערכה, ולבדוק.¹³

¹¹ הדרישה היחידה היא שלא נעשה overflow.

¹² זו מה שנקראת schnorr signature.

¹³ שימו לב: עקומים אליפטיים עם פרמטרים מתאימים נותנים "רמת אבטחה" של 2^{128} כאשר הגודל של החבורה הוא λ . הוא פרמטר אבטחה. בחבורות שלא משתמשות ב-ECDLP, גודל החבורה צריך להיות הרבה יותר גדול. בנוסף, נצטרך שהחבורה תהיה ציקלית.

בואו ננסה לבנות בעצמנו אחת כזו. זכרו שאנחנו צריכים שהמערכת שלנו תוכל להיבדק על ידי כולם, כך שנשתמש ב-K באימות. בשביל שנוכל להתעסק ב-"עולם" של K, אנחנו צריכים להעלות את g באיזשהו ערך הקשור להודעה שלנו, גם אם היא ארוכה יותר מאברי החבורה. נשמע מוכר, לא? נקרא לערך הזה ה-"אתגר". כך שיש לנו: $c = H(m)$, $s = kc$. אבל את c אנחנו יודעים לחשב, ו-s הוא רק צעד אחד קדימה! בשביל זה אנחנו משתמשים ב-"nonce", מספר שנשתמש בו פעם אחת (בלבד!) בשביל להסתיר את המפתח שלנו.

המוכיח יחשב:

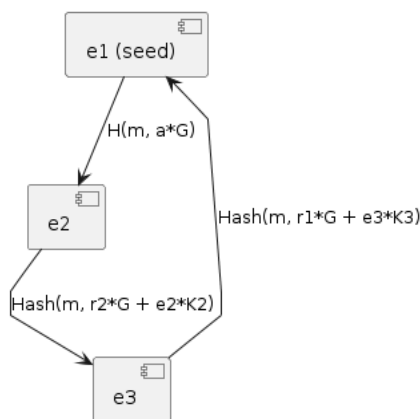
$$r = g^\alpha$$

$$c = H(r || m)^{14}$$

$$s = \alpha - kc$$

והמאמת, שקיבל (r, s) , יבדוק אם $r = g^s K^c$. נזכור: $K = g^k$ ונראה במעריך: $\alpha - kc + kc = \alpha$. נתון לנו r, כך שאנחנו יכולים לבדוק. כשיעורי בית אופציונליים, שכנעו את עצמכם שאי אפשר לבנות את החתימה בלי המפתח הפרטי בהינתן הודעה מסוימת שאתם רוצים לזייף.

חתימות מעגליות עובדות על אותו העיקרון, אבל הן עובדות יותר כהוכחת OR: הן מוכיחות שאנחנו יודעים את הפתרון הברידי לאחד מתוך המפתחות הנכללים במעגל. המעגל נסגר עם מספרים רנדומליים שמתפקדים כמו האתגר בחתימה הרגילה, עם קשר בין חוליות השרשרת כאשר לפחות אחד מהם צריך להיות עם קשר אמיתי בשביל שהאחרים יצליחו להיקשר.



בהתחייבות Pedersen, אנחנו יכולים להשתמש בגורם ההסתרה כמפתח פרטי (במה שקראתי לו s). ניזכר שבהתחייבות הזו, אם הערך אליו אנחנו מתחייבים הוא אפס, אנחנו צריכים רק את הפתרון הברידי. אז בעצם, אם אנחנו רוצים להוכיח שהתחייבנו ל-1, נצטרך פשוט להוכיח שיש לנו את הפתרון הברידי

¹⁴ יכול להיות שתראו מקומות אחרים שמוסיפים גם את המפתח הציבורי. אולי גם עם + ולא -. הרעיון הוא אותו רעיון.

להתחייבות כפול ההופכי של h . אז אם ניקח חתימה מעגלית, נוכל להוכיח שהערך אליו התחייבנו הוא, למשל, 1 או 2, וכן הלאה. אם היינו יכולים לתאר את המספר אחרת, אולי היינו יכולים להוכיח את הדברים בנפרד. נגיד, בינארי?

בעצם נוכל בעצם לבנות מערכת של משוואות 'או' המגבילות את טווח המספר. למשל בשביל להגביל את המספר ל- $[0, 2^{64}]$ נבנה: $b_1 \in \{0,1\}, b_2 \in \{0,2\}, \dots, b_{64} \in \{0, 2^{63}\}$.

עכשיו "באמת" - Bulletproofs

הוציאו את המאמר ב-2017, כשהוא מתבסס על [המאמר הזה](#) מ-2016. הוא משתמש במה שהמאמר הקודם הציג, טענת המכפלה הפנימית בשילוב עם הוכחה רקורסיבית, בשביל לייצר הוכחה הרבה יותר קטנה: עד אז, סיבוכיות התקשורת הייתה $O(\sqrt{n})$, והם שיפרו אותה ל- $O(\log n)$.

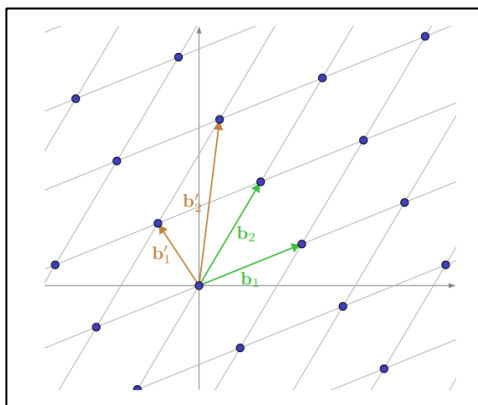
טענת המכפלה הפנימית (the inner product argument) מוגדרת כך (שימו לב, g, h, a, b הם וקטורים! g, h צריכים להיות בתוך הקבוצה הציקלית שבחרתם. פעולת החזקה כאן דומה למכפלה הפנימית):

$$\langle a, b \rangle = c \wedge P = g^a h^b$$

ההגדרה נראית מפחידה, אבל היא לא באמת. בעצם, היא מאוד קרובה לבעיית הפתרון הבדיד: בהינתן התחייבות P ומספר c , אנחנו צריכים להוכיח שהמכפלה הפנימית של הפתחים ל- P - הפתרונות שלה a ו- b שווה ל- c . במאמר שלהם הם הציגו טענה פשוטה יותר, שאפשר לשכנע את עצמכם שהיא נותנת את אותו הפתרון (אבל עם פחות מידע שצריך להעביר):¹⁵

$$P = g^a h^b \cdot u^{\langle a, b \rangle}$$

למי שלמד ליניארית, הרעיון כאן הוא בעצם להשתמש במשתנה בלתי תלוי " u " להיות כמו בסיס אורתוגונלי g -ו- h . חשבו על זה כר u ,¹⁶ מייצר חבורה שונה.



¹⁵ ראו עמוד 13 [במאמר](#). המאמר כתוב טוב!

¹⁶ [נלקח מכאן](#). זה לא נראה ככה, אבל הרעיון הוא אותו רעיון. עוד על סריגים (מקורות מגניבים [כאן](#), [כאן](#), [כאן](#) ו**כאן**)

ההוכחה

בואו נסכם מה אנחנו רוצים בעצם:

1. להוכיח שאנחנו יודעים את הפתחים ל- P ,
2. לעשות זאת במינימום מקום.

ניקח שני וקטורים a, b - שניהם בגודל של חזקה של $2, n$. נסמן $n' = n / 2$ ונחלק את a ו- b לשני וקטורים באמצע ונסמן: $a_1 = a_{[1:n']}, a_2 = a_{[n':n]}$; $b_1 = b_{[1:n']}, b_2 = b_{[n':n]}$. כך גם נעשה לנקודות המחוללות שלנו g ו- h . נחשב את L ו- R , התחייבויות לערבוב שני הוקטורים:

$$L = g_2^{a_1} h_1^{b_2} \cdot u \langle a_1, b_2 \rangle$$

$$R = g_1^{a_2} h_2^{b_1} \cdot u \langle a_2, b_1 \rangle$$

שימו לב שאם היינו משתמשים באותו החצי, היינו יכולים לשלוח את L ו- R , והמאמת היה יכול להשוות את מכפלתם ל- P , אך לא היינו מוכיחים דבר. ובכל זאת, נשלח למאמת את L ו- R . כמו בהתחייבות לחתימה, גם פה אנחנו - או במקרה הזה המאמת - בוחרים מספר x בשביל להסתיר את הידע שלנו. בעצם, הפרמטר הזה מאפשר למוכיח "לערבב" את a ו- b בצורה כזו שהמאמת באמת ידע לבדוק. המספר גם נועד לבדוק שהיחס אותו אנו מוכיחים אינו מקרי, כי זהו משתנה בלתי-תלוי. לחלק הבא, זכרו שאנחנו עובדים עם פונקציות הומומורפיות, כאשר הכפל באותו המחולל הוא הומומורפי בזכות חוקי החזקות. נגדיר:

$$a' = x \cdot a_1 + x^{-1} \cdot a_2$$

$$b' = x^{-1} \cdot b_1 + x \cdot b_2$$

ונשלח אותם למאמת. הוא לא יכול לקבל את a או b מפני שאפשר לקבל אותם משילובים שונים של וקטורים שונים. אפשר כאן לראות למה חישבנו כך את L ו- R : הפרדנו את החצאים למחוללים השונים, ובו בזמן נראה:

$$\langle a_1, b_2 \rangle x^2 + \langle a_2, b_1 \rangle x^{-2} + \langle a, b \rangle = \sum_{i=1}^{n'} (x a_{1_i} + x^{-1} a_{2_i})(x^{-1} b_{1_i} + x b_{2_i}),$$

סכום החזקות של u ב- $L(x^2)$ ו- $R(x^{-2})$.

החצאים המעורבבים נשלחים למאמת. הוא יחשב את $P' = L(x^2) P R(x^{-2})$, ונראה שאם הדבר חושב נכונה, הוא יראה כך:

$$g_1^{x^{-1} a'} g_2^{x a'} h_1^{x b'} h_2^{x^{-1} b'} u \langle a', b' \rangle$$

כבר כאן אנחנו יכולים לראות את הסגולות הרקורסיביות של ההוכחה הזו: אנחנו לוקחים שני וקטורים, ובשביל ההוכחה שולחים וקטורים שהם מחצית מגודלם ההתחלתי וגם מספר x . אפשר להיפטר מתקשורת עם המאמת בכך שנשתמש בהריסטיקת פיאט-שמיר, המחליפה תקשורת בפונקצית גיבוב או Random Oracle.



סיכום: אפשר להוכיח רקורסיבית לכל חצי ולתת את הערכים a', b' האחרונים, שלא נותנים שום מידע על הוקטורים המקוריים. כך מקבלים הוכחה בגודל $2 + \log_2(n)$ איברי קבוצה כש- n הוא מספר האיברים בפתחים המקוריים. בהמשך המאמר, הרעיון הוא להכניס איזושהי טענה לתבנית הזו של טענת המכפלה הפנימית.

אני לא אמשיך מכאן כי ההמשך כולל שימוש נבון בדברים קודמים, ואני חושב שהמאמר כתוב מספיק טוב. אתם תראו דברים מוכרים גם מהעמודים הקודמים, ואני מקווה שהכנתי אתכם טוב. קראו מעמוד 12 - ההנו!¹⁷

הנה כמה תובנות פשוטות שיחסכו לכם מאמץ:

1. משתמשים במשתנה של הפולינום בעצם להפריד לשכבות של טענות שונות אפילו אם הם באותה הטענה (בשביל להכניס אותם לטענה אחת, בעצם), וכדי להוכיח לעצמנו, כמאמתיים, שהיחס אינו מקרי;
2. לא צריך לפחד מפולינומים וקטוריים (vector polynomials, במאמר), הם כנראה מה שאתם חושבים שהם.

3. [rust dalek-cryptography notes](#)¹⁸

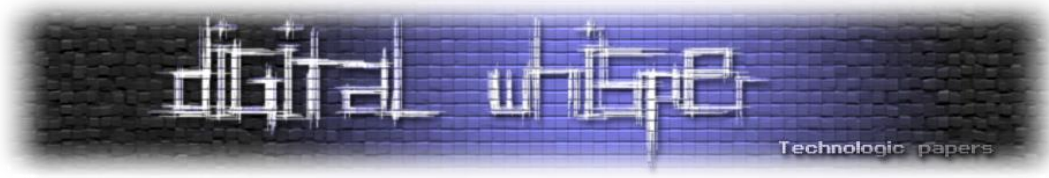
סיכום

דיברנו על הוכחות באפס ידיעה ושיטות שונות שהשתמשו בהן או משתמשים גם עכשיו לאורך השנים. אני חושב שהנושא הזה מרתק: הוא משלב בין מדעי המחשב למתמטיקה ולפעמים גם תורת המשחקים, כמה מופשט שאפשר לקחת את זה. במאמר המשך אוכל להסביר את המשך המאמר ואולי מאמרים אחרים - כמו curve trees, השדרוגים של bulletproofs ועוד. שימו לב שכל מה שכתוב במאמר הוא הבנתי שלי - תלמיד תיכון רנדומלי - כך שאם משהו לא נשמע לכם הגיוני אשמח שתפנו אלי, גם אם זו סתם שאלה או בקשה:

ofeksh.oss @ gmail.com

תודה רבה!

¹⁷ כן, זו צורת הציווי של תהנו. גם אני לא ידעתי. המידע יהיה גבולי בכל מה שצריך ב-arithmetic circuits, אבל אפשר!
¹⁸ האתר שלהם כזה מגניב! dalek.rs



ביבליוגרפיה

רוב הקישורים בגוף המאמר, חלקם שמתים גם פה:

<https://eprint.iacr.org/2009/211.pdf>

<https://www.cs.cornell.edu/courses/cs6810/2009sp/scribe/lecture18.pdf>

<https://soc1024.ece.illinois.edu/teaching/ece598am/fall2016/zkproofs.pdf>

<https://www.cs.jhu.edu/~susan/600.641/scribes/lecture10.pdf>

https://www.boazbarak.org/cs127spring16/chap14_zero_knowledge.pdf

<https://www.wisdom.weizmann.ac.il/~oded/VO/foc.pdf>

https://nt4tn.net/tech-notes/201505.confidential_values.txt

<https://eprint.iacr.org/2017/1066.pdf>

<https://dankradfeist.de/ethereum/2021/07/27/inner-product-arguments.html> - Borromean Ring

Signatures

<https://eprint.iacr.org/2004/027.pdf> - LSAG

<https://cronokirby.com/posts/2022/03/on-moneros-ring-signatures/>

Appendix 1 - סתם דברים מגניבים

הזכרתי זאת מאוד בחופזה, אז אדבר על זה שוב כאן: בשביל להעביר את הדברים כאן לעקומים אליפטיים, בעצם צריך להשתמש בפעולות של העקום. אז חיבור במקום כפל, כפל במקום חזקה. שימו לב ל-cofactor ©, אגב, ristretto.

- [lattice based zero knowledge stuff](#)
- [recent kerfuffle in lattice based cryptography](#)
- [guide for manipulating elliptic curves](#)