Digital Whisper
Technologic Papers

הצפנה מבוססת עקומים אליפטיים

מאת: גדי אלכסנדרוביץ'

הקדמה

בשנת 1993 רעדה האדמה בעולם המתמטי כשאנדרו ווילס הכריז כי הוכיח את המשפט האחרון של פרמה - בעיה פתוחה בת 350 שנים שהייתה אחת מהבעיות הפתוחות המרכזיות במתמטיקה. ווילס הוכיח השערה מודרנית יחסית, שממנה (בזכות עבודתם של כמה מתמטיקאים שקדמו לו) נבעה ההוכחה למשפט האחרון של פרמה, שעסקה בשני אובייקטים מתמטיים מודרניים - עקומים אליפטיים ותבניות מודולריות. בעקבות ההוכחה, והרבה יותר ממנה בזכות הספר שכתב סיימון סינג על הנושא, הפכו שני המושגים הללו למילות קסם עבור העולם הלא-מתמטי; למרות שגם סטודנטים למתמטיקה עשויים שלא להיתקל בהם כלל בלימודיהם, יוצא לי לראות אותם מוזכרים שוב ושוב בידי הדיוטות.

אבל לעקומים אליפטיים ותבניות מודולריות יש חיים בפני עצמם, כל אחד בתחומו שלו. עקומים אליפטיים נחקרים כבר במשך עשרות שנים ועוסקת בהן אחת מההשערות המפורסמות ביותר במתמטיקה כיום - השערת בירץ' וסווינרטון-דייר (שהיא אחד מ"שבע בעיות המילניום", לצד שאלת P=NP למשל), אבל כל התורה העשירה שלהם לא ממש זמינה עבור ההדיוט המתמטי. למרבה המזל, עקומים אליפטיים הצליחו גם להסתנן לתחום הרבה יותר ידידותי למתחילים - קריפטוגרפיה. במאמר הזה אני מקווה לתת טעימה כלשהי מהנושא - לסייע לקורא להבין "מה זה" - גם מה זה עקום אליפטי, וגם מה זו הצפנה שמבוססת על עקומים אליפטיים. דרך ההצגה שלי תהיה שטחית - כאמור, להציג את העקומים האליפטיים במלוא יופיים זו משימה קשה למדי; אבל אני מקווה שהיא תהיה מעניינת גם כך.

נתחיל בהצפנה. אני מניח שהקוראים מכירים את המושג של הצפנת מפתח ציבורי; אם לא, מומלץ ללכת ולקרוא על הנושא כעת. למרות שהצפנה היא בת אלפי שנים, מפתח ציבורי הוא המצאה חדשה יחסית, בת פחות מ-40. המאמר המוקדם ביותר שעסק בה היה זה של דיפי והלמן מ-1976; מאמר שבו הם לא הציגו מערכת הצפנה פומבית (היו אלו ריבסט, שמיר ואדלמן שעשו את זה ב-1977 עם פרסום RSA) אבל הם הציעו שיטה לשיתוף מפתחות באופן פומבי: שיטה שבה שני צדדים מסוגלים ליצור יש מאין מפתח סודי שישמש את שניהם באופן כזה שגם מי שמצותת לכל שיחתם לא מסוגל לדעת מה יהיה המפתח. מכיוון שזה יהיה חשוב מאוד להמשך, אתאר פורמלית את השיטה.

פרוטוקול דיפי-הלמן מתרחש ב"עולם" של המספרים השלמים מודולו ראשוני p; מודולו פירושו שאחרי כל ביצוע פעולת חיבור או כפל, מחלקים ב-p ולוקחים את השארית (אם p=7 אז 1= 4 x 2 כשהחשבון הוא מודולו p). העולם הזה הוא בעל תכונות מתמטיות יפות מאוד - למשל, לכל p קיים מספר $1 \leq g < p$ כלשהו כך שכל מספר בין 1 ו- p-1 מתקבל כחזקה של g (מודולו p). ל-g כזה קוראים יוצר. לאוסף המספרים מ-1 ועד p-1, עם פעולת הכפל מודולו p, קוראים "החבורה הכפלית מודולו p" ומסמנים אותה ב-$\mathbb{Z}_p^*$. אני לא סתם זורק עליכם סימונים מפחידים - בהמשך יהיה ברור למה כדאי להכיר את השמות הללו.

פרוטוקול דיפי הלמן פועל כך: ראשית כל דיפי והלמן מסכימים איכשהו באופן פומבי על מספר ראשוני גדול p ועל g שיוצר את $\mathbb{Z}_p^*$. לאחר מכן דיפי מגריל לעצמו מספר a והלמן מגריל לעצמו מספר b והם שומרים את המספרים הללו בסוד לעצמם, אבל דיפי מחשב את g^a ושולח להלמן; והלמן מחשב את g^b ושולח לדיפי. כעת, דיפי מקבל מהלמן את ה-g^b שלו, ואת כל המספר הזה הוא מעלה בחזקת a ומקבל $(g^a)^b = g^{ab}$; והלמן מקבל מדיפי את ה-g^a שלו ומעלה בחזקת b ומקבל $(g^a)^b = g^{ab}$. כעת יש להם מפתח משותף - g^{ab}; ואילו כל מי שצותת להם לא יודע מהו g^{ab} שכן הוא ראה רק את g^a ואת g^b.

דיפי והלמן מסתמכים כאן על קושי של בעיה מתמטית מוכרת - בעיית הלוגריתם הדיסקרטי. האם, אם אנחנו יודעים מהו g ומהו g^a, אנחנו מסוגלים לגלות מהו a? התשובה היא כן, ולא. כן, כי יש דרכים לגלות את זה (אפשר למשל לעבור על כל ה-a-ים האפשריים ב-$\mathbb{Z}_p^*$ ולנסות אחד אחד), אבל לא, כי השיטות שאנו מכירים דורשות יותר מדי זמן (כלומר, יותר זמן מאשר חלף מאז תחילת היקום). תיאורטית, ייתכן שמחר בבוקר יגלו דרך לפתור ביעילות בעיות לוגריתם דיסקרטי; בפרט מחשבים קוונטיים, אם יצליחו לבנות אותם אי פעם, יפתרו את הבעיה הזו. בינתיים, בעולם האמיתי, זוהי בעיה קשה ודיפי-הלמן מיושם בהצלחה במקומות רבים (חשוב לציין שדיפי-הלמן כפי שהוצג כאן פגיע מאוד להתקפות מסויימות, ובפרט להתקפת Men-in-the-middle; זה ממש לא סוף הסיפור).

ההצפנה הפומבית של RSA לא מסתמכת על הקושי של לוגריתם דיסקרטי אלא של פירוק לגורמים, אבל יש שיטות אחרות להצפנה פומבית שכן מתבססות על לוגריתם דיסקרטי - אולי המוכרת שבהן היא השיטה של אל-גאמל שגם אותה אני רוצה להציג במהירות. כמקודם, גם כאן ה"עולם" שבו ההצפנה מתרחשת הוא $\mathbb{Z}_p^*$ כאשר p ויוצר כלשהו g ידועים לכולם. בנוסף, דיפי בונה לעצמו זוג של מפתח פרטי d ומפתח פומבי e כך ש-$e = g^d$ ומפרסם לעולם את e, אך d נשאר סודי (ואנו מאמינים שהוא אכן נשאר סודי גם למי שיודע את g^d ואת g בגלל שזוהי בדיוק בעיית הלוגריתם הדיסקרטי).

מה שקורה באל-גאמל הוא הדבר הבא: בהינתן הודעה m, המצפין שרוצה לשלוח לדיפי את ההודעה מגריל לעצמו איזה שהוא מספר k, שולח לדיפי את g^k, ובנוסף לכך שולח לו את $m \cdot y^k$ (כלומר - הוא שולח את m) כשהיא "ממוסכת" על ידי e^k, שהיא ערבוב של המידע הפומבי של דיפי עם המספר k שהמצפין הגריל; ובנוסף לכך הוא שולח לדיפי את g^k כדי שלדיפי יהיה מושג כלשהו על k.

כעת כדי לשחזר את ההודעה המקורית דיפי מחשב את $\left(g^k\right)^{-d}\left(m \cdot e^k\right) = g^{-kd} \cdot m \cdot g^{kd} = m$ זה חישוב שרק דיפי יכול לעשות כי הוא כולל העלאה של משהו בחזקת d- הסודי.

מה שאני רוצה שתזכרו מדיפי-הלמן ומאל-גאמל הוא שבשניהם התבססנו על פעולות חשבוניות פשוטות בעולם של $\mathbb{Z}_p^*$. השתמשנו רק בכפל ובהעלאה בחזקה, שהיא בעצם קיצור להרבה פעולות כפל; לא השתמשנו כלל בחיבור. זה אומר ששתי השיטות שהצגנו ניתנות, באופן תיאורטי, לשימוש בכל עולם מתמטי שבו קיימת פעולה חשבונית שמתנהגת נחמד כמו כפל. פורמלית, כל מה שצריך הוא שהעולם שלנו יהיה חבורה; למי שלא מכיר את המושג, לא נורא - לא אציג אותו במפורש כי אין זה הכרחי.

העקומים האליפטיים נכנסים למשחק

כעת אפשר סוף סוף להסביר איך כל זה קשור לעקומים אליפטיים. כל עקום אליפטי (ואסביר אוטוטו מה זה בכלל) מהווה חבורה בעצמו - מוגדרת על איבריו פעולת "כפל" (שהיא שונה מאוד בהגדרתה מכפל של מספרים) שמתנהגת יפה. זה אומר שאפשר לקחת את דיפי-הלמן ואת אל-גאמל ועוד שלל שיטות דומות ולהשתמש בהן כמעט ללא שינוי גם בתוך היקום של העקום האליפטי. ההבדל הוא שהעולם של העקומים האליפטיים הוא יותר מורכב ועשיר וכתוצאה מכך החבורות שצצות בו הן יותר "קשות לפיצוח" מאשר $\mathbb{Z}_p^*$.

מבלי להיכנס לכל הפרטים, השיטה החזקה ביותר הידועה כיום לפתרון (לא יעיל אבל גם לא גרוע עד כדי כך) של בעיית הלוגריתם הדיסקרטי - תחשיב אינדקסים - לא עובדת על עקומים אליפטיים (בהערת אגב למתקדמים אציין שלעתים קרובות החבורות שצצות בעקומים אליפטיים איזומורפיות לחבורות כמו $\mathbb{Z}_p^*$; רק שאת האיזומורפיזם הזה קשה לחשב ובכך נעוץ הקושי. זה ממחיש יפה עד כמה ייצוגים שונים לאותו דבר הם בעלי חשיבות במתמטיקה).

אם כן, במאמר הזה לא אציג לכם כלל שיטות להצפנה מבוססת עקומים אליפטיים כי מה שראינו עד כה - דיפי-הלמן, אל-גאמל - הן בעצמן שיטות להצפנה מבוססת על עקומים אליפטיים! מה שבאמת חשוב להבין הוא מהם עקומים אליפטיים וכיצד הם מגדירים חבורה; וכשיש לנו בראש את המוטיבציה המעשית לכך, אני מקווה שיהיה יותר קל לעכל את ההגדרות.

עקומים אליפטיים שייכים לתחום מתקדם למדי במתמטיקה - גאומטריה אלגברית - וככאלו יש להם הגדרה מורכבת ומחוכמת שלא אציג פה בכלל. במקום זאת אציג פה הגדרה פשוטה שגם תלמידי בית ספר יכולים להבין, במחיר אי דיוקים קטנים (שאמנם, חלקם רלוונטיים למי שבאמת רוצה לממש מערכת הצפנה עם עקומים אליפטיים אבל אלוהי המתמטיקה יסלח לי).

גאומטריה אלגברית היא אמנם תחום עמוק מאוד ומורכב מאוד, אבל את נקודת המוצא שלה רואים כבר בשיעורי גאומטריה אנליטית - הרעיון שאובייקטים גאומטריים ניתנים לתיאור באמצעות משוואות. כך למשל קו ישר בזווית של 45 מעלות מתואר על ידי המשוואה הפשוטה $y = x$. יותר במפורש, זה אומר שאוסף הנקודות (x, y) במישור שמקיימות את היחס $y = x$ בין הקואורדינטות שלהן מהוות את הישר המדובר.

אובייקט יותר מחוכם שמוגדר באמצעות משוואה הוא מעגל: אוסף כל הנקודות (x, y) במישור שמקיימות את המשוואה $x^2 + y^2 = 1$ הוא מעגל שרדיוסו 1 ומרכזו בראשית הצירים. אם רוצים לתאר מעגל מחוכם יותר, שמרכזו בנקודה (x, y) ורדיוסו R מקבלים את המשוואה $(x - a)^2 + (y - b)^2 = R^2$ בדומה לומדים בתיכון (לפעמים) לייצג גם כמה אובייקטים גאומטריים מורכבים יותר - אליפסה, היפרבולה, פרבולה... אבל כאן זה בערך נגמר.

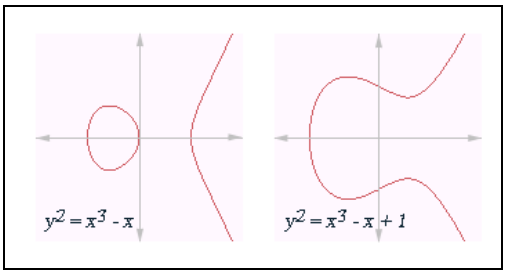
בגאומטריה אלגברית, תחת שנחפש משוואות שמתארות אובייקט גאומטרי שאנחנו כבר מכירים, אנחנו מנסים להבין פתרונות למשוואות כלשהן באמצעות חשיבה עליהם בתור אובייקטים גאומטריים ותקיפה שלהם מכל כיוון אפשרי - גם אלגברי וגם גאומטרי וגם שניהם יחד. עקומים אליפטיים הם מאותם יצורים שצצים כך: אוספי פתרונות למשוואה מסויימת שתכונותיהם הגאומטריות היפות מלמדות אותנו משהו עליהם.

המשוואה שמגדירה עקום אליפטי נראית בדרך כלל כך:

$$y^2 = x^3 + ax + b$$

במקרים פרטיים מסויימים המשוואה מסובכת יותר אבל אמרתי שלא אכנס לכך כאן. במובן מסויים עקום אליפטי הוא אך במרחק צעד אחד מרמת הסיבוך של מעגל או אליפסה - שם היו לנו x^2 ו-y^2 ומקדמים ממעלות נמוכות יותר, וכאן הגדלנו רק קצת את המעריך של x כך שגם x^3 ישתתף במשחק. בפועל, השינוי הקטן הזה כבר משנה לחלוטין את המשחק כולו.

הנה תמונה של איך נראה עקום אליפטי טיפוסי:



(במקור: http://upload.wikimedia.org/wikipedia/commons/5/5b/ECexamples01.png)

כפי שאפשר לראות, היצור הזה סימטרי סביב ציר x (זה נובע מכך שיש לנו y^2 באגף שמאל של המשוואה) ופרט לכך הוא לא נראה מרשים או יפה במיוחד. קרוב לודאי שאתם תוהים למה להתחיל להסתכל מלכתחילה על יצורים שכאלו. התשובה היא שבהקשרים מתמטיים מסויימים הם צצים באופן טבעי יחסית, אבל קשה להביא דוגמאות פשוטות שאפשר להציג בשורה אחת.

דוגמה אחת שאני כן רוצה להזכיר כאן היא בעיית המספרים הקונגרואנטיים. מספר קונגרואנטי (שם איום ונורא שאני לא מבין מהיכן צץ) הוא מספר טבעי n כך שקיים משולש ישר זווית שאורכי צלעותיו כולם רציונליים, ושטחו הוא בדיוק n. השאלה אילו מספרים הם קונגרואנטיים העסיקה כבר את היוונים הקדמונים - מסתבר ש-2, למשל, אינו קונגרואנטי, 5, 6 ו-7 כן, 11 לא, 13 כן, ועוד ועוד. בקיצור, זו לא שאלה טריוויאלית. למעשה, עד היום לא ידועה שום שיטה להכריע בודאות, בהינתן n, האם הוא קונגרואנטי או לא (אם הוא קונגרואנטי אפשר בתיאוריה על ידי חיפוש סדרתי למצוא משולש מתאים עבורו; אבל אם הוא אינו קונגרואנטי לא ידועה כיום דרך להכריע זאת).

והנה, בעזרת להטוטים אלגבריים מסתבר שקריטריון שקול לכך שמספר n יהיה קונגרואנטי הוא שלמשוואה של העקום האליפטי $y^2 = x^3 - n^2x$ יהיה פתרון רציונלי שאיננו $(0,0)$ כאן נשלפים כלים כבדים שעוסקים בעקומים אליפטיים ומניבים לבסוף קריטריון (שלא אתאר כאן) שמאפשר להכריע חד משמעית האם לעקום הזה יש פתרון רציונלי שכזה או לא; אבל הנכונות של הכלים הללו מסתמכת על אותה השערת בירץ' וסווינרטון-דייר שהזכרתי בתחילת הפוסט ולכן הבעיה טרם נחשבת פתורה.

אבל מהי הפעולה?

נחזור לענייננו. כדי שאפשר יהיה להשתמש בעקומים אליפטיים להצפנה, צריך להבין מהי פעולת ה"כפל" שאפשר לבצע עליהם. מכיוון שההגדרה מוזרה, אני רוצה להסביר מהיכן היא מגיעה. אם E מייצגת את המשוואה של עקום אליפטי, זה עדיין לא אומר לנו מיהו העקום; יש חשיבות אדירה לשאלה מהיכן נלקחים הפתרונות של המשוואה. אם אנו דורשים שהם יהיו מספרים רציונליים, זה עקום מעל המספרים הרציונליים $\mathbb{Q}$, ומסמנים זאת $E/\mathbb{Q}$. אם לעומת זאת אנחנו מרשים לפתרונות להיות מספרים מרוכבים, זה מסומן $E/\mathbb{Q}$ ואנחנו מקבלים אובייקט שונה למדי באופיו. מעל המרוכבים, ניתן לחשוב על אוסף הפתרונות של עקום אליפטי כעל טורוס ,או בשמו הפחות פורמלי - בייגלה. להסביר איך בדיוק קורה הדבר המוזר הזה אי אפשר כרגע, אבל חשוב מה שנובע מכך: במרוכבים אפשר להגדיר פעולת חיבור בקלות רבות על איברים מתוך הטורוס - זהו החיבור הרגיל במספרים מרוכבים ועוד פעולת מודולו (רק שבניגוד למודולו p שדיברנו עליו בהתחלה, כאן המודולו הוא של שני איברים שמייצגים "כיוונים" שונים). פעולת החיבור הכמעט-טבעית הזו בטורוס משרה על העקום האליפטי פעולת "כפל" כלשהי, שהיא מה שאני עומד לתאר כאן. אותה הגדרה של פעולת הכפל עובדת גם עבור עקומים אליפטיים מעל שדות אחרים, ובפרט אלו שמשמשים אותנו בהצפנה ואתאר בקרוב. כדי לבלבל אתכם עוד יותר אני אפסיק לקרוא לפעולה הזו "כפל" ואסמן אותה דווקא ב-$+$(למרות שהיא ממש לא פעולת חיבור) כי זה הסימון הנהוג בספרות.

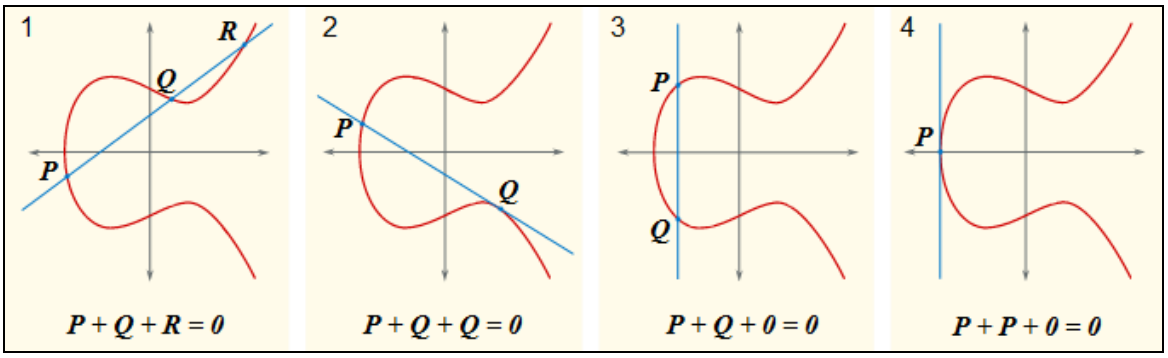
הדרך הפשוטה ביותר לחשוב על הפעולה היא באופן גאומטרי, וכדאי להסתכל שוב על התמונה של עקום אליפטי מעל הממשיים כדי להבין מה בדיוק קורה. בהינתן שתי נקודות על העקום, אנו מעבירים קו שמחבר אותן וממשיכים אותו עד שיחתוך את העקום בנקודה שלישית. את אותה נקודה שלישית אנו משקפים ביחס לציר x, והתוצאה היא תוצאת פעולת החיבור. כלומר, אם A, B הם שתי נקודות על העקום $A + B$, היא מה שמקבלים אחרי העברת קו, חיתוך עם העקום בנקודה שלישית, ואז שיקוף.

אולי השאלה הראשונה שאפשר לשאול היא מה קורה אם כשמעבירים קו בין A, B הוא כלל לא חותך את העקום בנקודה שלישית. זה קורה בדיוק כאשר A, B מחוברים על ידי קו אנכי. במקרה הזה אומרים - לנשום עמוק - שהקו חותך את העקום ב"אינסוף". מה שבאמת מדהים פה הוא שיש פורמליזם מתמטי מדויק לחלוטין שמתאר את זה (משהו שמכונה "מישור פרוייקטיבי") אבל אין צורך להבין אותו כאן. מה

שחשוב הוא שכל עקום אליפטי כולל נקודה נוספת $\mathcal{O}$ שהיא התוצר של חיבור שתי נקודות שמחוברת בידי קו אנכי. בנוסף, ל-$\mathcal{O}$ התכונה ש-$A+\mathcal{O}=A$ לכל נקודה על העקום: $\mathcal{O}$ הוא "אדיש חיבורי" כמו 0 במספרים השלמים הרגילים. בנוסף, אם $A+B=\mathcal{O}$ אז מסמנים זאת בתור $B=-A$. פורמלית, אם A היא הנקודה (x,y), אז $-A$ היא הנקודה $(x,-y)$, אותה קואורדינטת x, אבל קואורדינטת y בעלת סימן הפוך (זהו שיקוף ביחס לציר x).

כעת אפשר לתת ניסוח אחר לפעולת החיבור: אם A,B,C הן שלוש נקודות של העקום האליפטי שנמצאות על אותו קו ישר, אז $A+B+C=\mathcal{O}$. חשבו רגע מדוע ההגדרה הזו זהה להגדרה שנתתי קודם, שבה גם מבצעים שיקוף כלשהו.

כאן רואים דוגמאות לאופן שבו מוגדרת הפעולה:



עוד משהו שלא ברור עדיין הוא מה קורה כאשר מחברים נקודה עם עצמה. כלומר, מהי $A+A$? במקרה הזה מה שעושים הוא להעביר קו שמשיק לעקום האליפטי בנקודה A, ואז כרגיל מוצאים את נקודת החיתוך הנוספת של המשיק הזה עם העקום, משקפים ביחס לציר x וקיבלנו את $A+A$. כדי שיהיה לעקום משיק יחיד בנקודה A נדרש שהוא יהיה "חלק" - מבחינה מתמטית זוהי הדרישה שהנגזרת על פי x והנגזרת על פי y של המשוואה שמגדירה את העקום לא תתאפסנה בו זמנית.

טוב, הזהרתי אתכם שהפעולה הזו היא מוזרה למראה במבט ראשון. התחושה העיקרית שלי כשראיתי אותה הייתה "אוקיי, אבל איך לעזאזל עושים את החישובים הללו בפועל?" והתשובה לכך, למרבה המזל, היא "בקלות". לא עד כדי כך קשה להגיע ישירות למשוואות שמגדירות את הפעולה. אם $(x_1,y_1)+(x_2,y_2)=(x_3,y_3)$ ואנו מניחים ש-$x_1\neq x_2$ (כי אם $x_1=x_2$ הנקודות על אותו קו אנכי ואז סכומן הוא פשוט $\mathcal{O}$) אז הנקודה (x_3,y_3) מתוארת על ידי הנוסחאות:

$$x_3 = \left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - x_1 - x_2$$
$$y_3 = -y_1 + \left(\frac{y_2-y_1}{x_2-x_1}\right)(x_1 - x_3)$$

ואילו אם $(x_1, y_1) = (x_2, y_2)$, כלומר הסכום מוגדר בעזרת המשיק, אז הנוסחה היא:

$$x_3 = \left(\frac{3x_1^2+a}{2y_1}\right) - 2x_1$$
$$y_3 = -y_1 + \left(\frac{3x_1^2+a}{2y_1}\right)(x_1 - x_3)$$

כאשר a הוא חלק מהמשוואה שמגדירה את העקום $y^2 = x^3 + ax + b$.

בעזרת הנוסחאות הללו, אפילו אם לא מבינים מהיכן הן באות (וכאמור - זה לא מורכב כל כך והמתמטיים שבכם אולי ירצו לנסות ולפתח אותן בעצמם) אפשר לבצע את פעולות החשבון בעקום אליפטי באופן קונקרטי לחלוטין. אנחנו רואים שביצוע פעולת חיבור הוא תובעני יותר מאשר חיבור של שני מספרים רגילים - יש כאן הרבה חיבורים, וכפל, וחילוק וכו'; זו הסיבה שעקומים אליפטיים הם תובעניים יותר מבחינת זמן ריצה מאשר חשבון ב-$\mathbb{Z}_p^*$ למשל. הרבה מהמחקר על הצפנה מבוססת עקומים אליפטיים עוסק באופן שבו ניתן לשפר את הביצועים הללו.

סיכום

לסיום, אעיר שלא התייחסתי כלל לדבר המעניין ביותר - איך בכלל מייצרים עקומים אליפטיים? לכאורה אפשר פשוט להגריל a,b ולעבוד עם העקום $y^2 = x^3 + ax + b$, אבל המציאות אף פעם אינה כה פשוטה. ראשית, לא בטוח שלכל a,b אכן נקבל עקום (זכרו את הדרישה שהעקום יהיה "חלק" שהזכרתי קודם), אבל שנית - לא כל עקום שמגרילים ברחוב יהיה בטוח. דרישה חשובה אחת היא שכמות הנקודות שעל העקום תהיה מספר גדול בלי יותר גורמים ראשוניים קטנים, וזה מעלה את השאלה - בהינתן עקום, איך יודעים כמה נקודות יש עליו? זו בעיה מעניינת מאוד בזכות עצמה, שמעידה אולי על כך שגירדתי לבינתיים רק את קצה הקרחון.

על המחבר

גדי אלכסנדרוביץ, בעל תואר ראשון במתמטיקה ותואר שלישי במדעי המחשב מהטכניון, כותב את הבלוג "לא מדויק" העוסק במתמטיקה ובמדעי המחשב:

http://www.gadial.net