**<u>בין שיתוף לסודות: קריפטוגרפיה בעידן המודרני – פרופ' מוני נאור, 22.11.2016</u>**

פרופ' מוני נאור: צהריים טובים. אני מוני נאור, מהמחלקה למדעי המחשב, פרופסור למדעי המחשב, בפורמט הזה אני מבין שלא מציגים אותי אז הצגתי את עצמי. אני הולך לדבר על קריפטוגרפיה בעידן המודרני. באופן מסורתי מה זה קריפטוגרפיה? היא עוסקת בשמירה על חשאיות בתקשורת. נניח שיש שני שחקנים, אליס ובוב, שרוצים לדבר, וישנה איב שרוצה להאזין,. הם רוצים לדבר בלי שאיב תצליח להבין מה הם אומרים. זו בדרך כלל הצורה שהשתמשו בה בקריפטוגרפיה במשך השנים.

קריפטוגרפיה זה בעצם עיסוק עתיק מאוד, גם בתנך יש רמזים לכך. בספר ירמיהו יש פסוק "איך נלכדה ששך ותתפש כל הארץ; איך היתה לשמה בבל, בגויים". מה זה ששך? זה בבל. פשוט בבל בא"ת ב"ש. ירמיהו, כיוון שהוא אומר במפורש את השם בבל בהמשך הפסוק, לא מתכוון להסוות כלום. יש לו כבר את הצופן, הוא מבין שזה לא צופן טוב, כי אפשר להבין מה זה ששך. גם בכתבי החרטומים אפשר לראות הדים לקריפטוגרפיה, סימנים בעלי צורה מיוחדת. סביב מלחמת בעולם בשנייה יש ספרים וסרטים סביב פיצוח האניגמה.

אם אתם רוצים ללמוד יותר, יש ספר של דייויד קהאן על הנושאים האלה, אבל לא אעסוק יותר מדי בהיסטוריה.

מה קרה בעידן המודרני? השינוי הגדול חל בשנות ה-70, עד אז עיקר השימושים היו ביטחוניים. זה לא היה תחום מחקר, לא התפרסמו כמעט מאמרים על קריפטוגרפיה, עד סוף ה-70 יש מאמר מפורסם אחד של קלוד שאנון, ואז שקט המון שנים. משנות ה-70 חל גידול אדיר, ההצפנה נכנסה לשימושים מסחריים, היתה התפתחות במחשוב ויותר צורך בקריפטוגרפיה. אותנו מעניין מחקר אקדמי, במיוחד התפתחות המחקר בסיבוכיות של חישובים. מאמרים חשובים בתקופה זהם של דיפי-הלמן שהעלו את הרעיון של קריפטוגרפיה במחקר וקיבלו את פרס השנה. יש מאמר של ריבסט-שמיר-אדלמן שלנו, ועוד התפתחות חשובה זו DES, מפתח משותף להצפנת נתונים. אבל לאור זאת שזו היתה שיטה טובה, או לפחות לא גרועה וכולם יכלו להשתמש בה, היה ברור שיש פה משהו משמעותי.

באופן כללי, המודלים שמדברים עליהם הם יותר מורכבים ממה שראינו קודם. המודלים מדברים על משימות יותר מגוונות ויותר מאשר התעסקות בשיתוף. דרך להגדיר קריפטוגרפיה זה דרכים לשמירה על חשאיות, פרטיות ואמינות במערכות מחשוב.

מאז התפשטות האינטרנט, ב-25 השנים האחרונות, קריפטוגרפיה היא רלוונטית לכולם ושומעים עליה המון. בחדשות יש המון דברים שקשורים לקריפטוגרפיה, בדרך כלל בהקשרים שליליים, חולשות ופריצות שמתגלות, אבל ברור שזה דבר שאמור לעניין אנשים.

יש לזה השלכות חברתיות. מסחר אלקטרוני זו דוגמא מובהקת, קשה לראות את ההתפתחות שלו בחברות כמו אמזון בלי אפשרות להצפנה וחתימה דיגיטלית. מערכות בחירה – נדבר איך אפשר לעשות מערכת שאפשר להצביע בה בלי שניתן לכפות על אנשים להצביע כרצונך, איך לוודא שהמערכת עובדת כמו שצריך. איך להדליף סודות ואיך לא להדליף – על זה לא נדבר, רק אם יהיו שאלות מהקהל. יש גם הנושא של פרטיות – כשמציעים שבמקום לשלם מיסים גבוהים על כלי רכב, תשלם לפי שימוש בכלי הרכב למשל, שימוש לפי השעה שאתה נוסע, הכביש והעומס עליו; ואז מיד עולה השאלה איך זה ייעשה. האם יתבצע עליך מעקב, האם אפשר לבנות מערכת תשלומים שלא תפגע בפרטיות ועדיין

אנשים ישלמו לפי שימוש? יש הסוגיה של מניעת ניצול לרעה של משאבים, אחת הדרכים להיאבק בכך זה מבחן טיורינג אוטומטי.

בכל אופן יש סיבוכיות, קיים הנושא של סיבוכיות החישובים. באופן כללי מדברים על חקר המשאבים החישוביים הדרושים לביצוע משימות. משאב זה זמן חישוב, כמות הזיכרון הדרושה, התקשורת. כשמדברים על בעיה חישובית, הכוונה היא לכפל של שני מספרים שרוצים למצוא את המכפלה שלהם. אפשר לדבר על בעיה כמו בחירת הצעד הבא במשחק שח או מציאת מסלול הקצר ביותר עובר באוסף ערים נתון. אלה דוגמאות לבעיות חישוביות שהסיבוכיות שלהם שונה. אנחנו רוצים למצוא בעיות שלא ניתנות לפתרון על ידי שום מחשב מציאותי. הבעיה סיווג הבעיות הדורשות משאבי חישוב דומים. האם P שווה ל-NP? זו בעיה חשובה שמוצגת ושואלת האם את כל הדברים שניתנים לחישוב בצורה יעילה, ניתן גם לוודא. למשל הערכת יצירת אמנות אי אפשר להעריך על ידי היצירה עצמה.

בעיית הסוכן הנוסע – אני רוצה למצוא את המסלול הקצר ביותר שעובר בין שתי ערים, זה קל לוודא בהינתן מסלול, ואז אתה יכול לוודא את אורך המסלול. אבל למצוא אותו זה קשה. אפשר לראות שזה קשה כמו כל בעיה אחרת. והנה בעיה עוד יותר קשה – מציאת מסלול בין הרבה ערים.

בעיה שימושית בקריפטוגרפיה זה פירוק מספרים גדולים. כשנותנים לנו שני מספרים גדולים, אני יכול לייצר את המספר שהוא מכפלה שלהם, גם אם אתן לכם מספרים של 500 ספרות ואבקש לכפול אותם – זה יהיה קצת קשה אבל כנראה שתצליחו אחרי כמה שעות. אבל בהינתן מכפלה של שני מספרים ראשוניים גדולים, אין אלגוריתם יעיל שמוצא את אותם מספרים. האלגוריתם יכול למצוא את המכפלה, אבל לא לשות פירוק לגורמים. זה לא בדיוק זמן ריצה אקספוננציאלי, אבל מעל אלף וקצת ביטים זה כבר קשה לחישוב. פירוק לגורמים הוא אחת הבעיות החשובות ביותר בקריפטוגרפיה - כאשר RS הומצא לראשונה, הפירוק לגורמים והידע על אלגוריתמים היה איטי יותר. כיוון שהבעיה הזאת חשובה, הרבה התחילו להסתכל עליה ברצינות, וב-15-20 השנים האחרונות היתה התפתחות משמעותית מאוד ביכולות ובהבנת הקושי של פירוק לגורמים. זו דוגמא טובה להפריה הדדית.

עוד נקודה מעניינת – שמחשב קוונטי שלא יודעים לבנות אותו, זה מודל חישובי שעוד לא נבנה, אפשר לחשב בעזרתו פירוק לגורמים. העובדה הזו היא אחת המוטיבציות לנסיונות לבנות מחשב כזה.

הרעיון המרכזי בקריפטוגרפיה הוא שדווקא בעיות שקשה לחשב, למשל שקשה למצוא את המסלול הקצר ביותר בין ערים, שחושבים שזה חדשות לא טובות, דווקא החדשות הרעות האלה הן טובות בקריפטוגרפיה. בעובדה שיש בעיות שלא ניתנות לפתרון יעיל, אפשר להשתמש כדי לייצר מערכות קריפטוגרפיה בטוחות. זה הרעיון הבסיסי.

יש דוגמאות לזה, בפרט דוגמא שאראה היום בהרצאה, שלא דורשת שימוש ברעיון הזה – מה אני מתכונן לעשות? בהרצאה אספר על שיתוף סודות, אתן דוגמאות, ואחר כך אציין מה לדעתי הדברים המרכזיים בקריפטוגרפיה, שאלות ותהיות.

אוקיי. הבעיה זה שיתוף, לפעמים אדם קשיש או נוטה למות רוצה לספר לילדיו איפה האוצר, או מה הסיסמה לכספומט, והוא לא רוצה שכולם ידעו על כך. אחת השאלות היא איך להגדיר את זה, איך לממש את זה. אז בעצם מה יש לנו? מי הנפשות הפועלות? יש קבוצת משתתפים, אסמן אותם ב-P1, P2 והלאה, יש מי שמכיר את הסוד, בעל הסוד S, הוא רוצה לשתף אותו בין השחקנים, הוא הולך לייצר

N חלקים, לתת חלק לכל אחד מהשחקנים. שחקן P1 יקבל את החלק פאי 1, שחקן P2 יקבל את החלק פאי 2. וכן הלאה. הוא לא ייקח את הסוד ויקרע אותו לגזרים, אלא יְיַצֵר את החלקים בצורה מתוחכמת, בצורה הסתברותית כפונקציה של הסוד. החלק פאי 1 ייגזר מהסוד אבל לא בצורה דטרמיניסטית אלא באמצעות מחרוזת אקראית שנשתמש בה.

לגבי כל קבוצת שחקנים חושבים האם היא כשירה, האם רוצים שהיא תוכל לשחרר את הסוד על בסיס החלקים שלה או לא. אם הקבוצה קטנה מדי, או מתחת לקו מסוים, היא לא אמורה לשחזר. רוצים שקבוצות הכשירות יוכלו לשחזר את הסוד, וקבוצות לא כשירות לא יֵדעו כלום. איך להגדיר את זה כך שהם לא ידעו כלום? להגיד שלא חשוב מה היה הסוד, התפלגות החלקים שהקבוצה הלא כשירה רואה איננה תלויה בסוד. לא חשוב מה הסוד, אם יש קבוצה שלא אמורה ללמוד את הסוד, מה שחברי הקבוצה רואים בלתי תלוי בסוד.

הרעיון הזה הוצג על ידי עדי שמיר ובלייקלי בסוף שנות ה-70. נתחיל עם דוגמא פשוטה – יש לנו בסך הכל שני שחקנים, רק שניהם ביחד יכולים לשחזר את הסוד. הקבוצות הכשירות כוללות את שני השחקנים אלה, כל שאר הקבוצות הן לא כשירות. כל שחקן בפני עצמו לא לומד שום דבר על הסוד, רוצים שלכל ערך אפשרי של הסוד תהיה אותה התפלגות על פני החלקים.

מה הפתרון? הפתרון דומה מאוד לרעיון של פנקס. נגיד שזה קוד לכספומט. בעל הסוד בוחר מספר אקראי בן ארבע ספרות. נותן ל-P1 את Z ול-P2 הוא נותן את 4 הספרות האחרונות של Z + S.

איך זה נעשה? פעם היו לי פה תשובות במצגת ומחקתי אותן. איך נעשה השחזור? לוקחים את הערך שניתן ל-P1, מורידים ממנו את ערך של P2, ומקבלים חזרה את הקוד. תמיד מסתכלים רק על 4 הספרות האחרונות. שחזור הוא פשוט על ידי חיסור (בטעות כתוב פה במצגת חיבור, זה צריך להיות חיסור).

בכל אופן, למה השיטה הזאת בטוחה? מה ש-P1 מקבל זה מספר אקראי שלא קשור לסוד. P2 גם הוא מקבל מספר אקראי שלא קשור לסוד, כי לכל ערך אפשרי שהוא יכול לקבל יש רק בחירה אחת של Z שתוביל אותו לערך. לכן מה שהוא מקבל לא מוביל לסוד, למרות שלכאורה יש לו פונקציה, אבל Z הוא אקראי. לכן כל שחקן מקבל ערך אקראי לגמרי, ורק ביחד הם יוכלו לשחזר.

אם רוצים לעשות הכללה ל-K מתוך K, על ידי זה שנבחר Z1, Z2 עד ZK, נחבר את כולם ל-S (בעל הסוד). זה נותן שיטה 2 מתוך 2, באופן כללי K מתוך K. אם כל השחקנים צריכים להיות נוכחים, הבעיה היא פשוטה. עד פה החדשות הטובות.

מה קורה אם אנחנו רוצים עכשיו משהו טיפה יותר מורכב? אני מחלק עכשיו דפים לכל המשתתפים כאן. יש לנו הרבה שחקנים, הקבוצות הכשירות מכילות שני שחקנים, שני שחקנים ביחד יכולים לשחזר את הסוד, אחד לבד לא יכול. נראה דוגמא שהסוד הוא רק ביט אחד. כל חלק בפני עצמו לא אמור למסור מידע על הביט שהוא או אפס או 1, כל שני חלקים ביחד יכולים. כלומר, כל שני אנשים שלא פגשו זה את זה, ביחד הם אמורים להיות משחזרים של הסוד.

אז אולי עכשיו תתחלקו לזוגות ותפתחו את המעטפות הסודיות. ההוראות שאתם מקבלים – אם המספר שלך שווה למספר של חברך, הסוד המשוחזר הוא אפס. אם שני המספרים שונים, הסוד המשוחזר הוא 1. מה הסוד? אף אחד לא שיחזר? הסוד הוא אפס.

איך עשינו את זה? באמצעות יצירת החלקים על ידי בעל הסוד. אם הביט הוא אפס, הוא בוחר מספר אקראי Z בין 1 ל-N ונותן אותו בתור החלק לכל השחקנים. אם הביט הוא 1, הוא בוחר מספר אקראי R בין 1 ל-N ונותן לשחקן ה-I את המספר R+I. מה שקורה כאן מבטיח לנו שאין שני שחקנים שמקבלים את אותו המספר. אם הביט הוא 1, לקחנו מספר R ונתנו לשחקן I את המספר R+1. זה אומר ששני השחקנים I ו-J לא יקבלו את אותו הדבר. לכן כאשר הם יפתחו את המעטפה, הם יראו שני מספרים שונים וישחזרו נכון. פה נתנו אותו ערך לכולם, אז אם המספר שלך שווה לזה של חברך, ברור שכולם ישחזרו לאפס. למה זה בטוח? כי בכל מקרה אחר של כל שחקן, זה מספר אקראי בין אפס ל-1. אם המספר האקראי הוא B, החלק שלך הוא מספר אקראי B. פה, מאותה סיבה של הסיפור הקודם, קיבלנו מספר אקראי, בחרנו מספר אקראי לשחקן I ונתנו את R+I שזה מספר אקראי בין 1 ל-N. ואז מקבלים את מה שרצינו – כאן כל השחקנים מקבלים מספר אקראי, פה אין שחקן שמקבל אותו מספר, כל מספר הוא אקראי. לכן מכל חלק בפני עצמו לא לומדים כלום, רק משני חלקים ביחד.

זו דוגמא פשוטה למשימה שלא ברור איך לעשות אותה אחרת. אם הייתי בפורום אינטימי ומציע לכם רעיונות – יש כאלה שמכירים שיטות קריפטוגרפיה, אבל אני לא חושב שהיה פשוט לעלות על שיטה פשוטה שתעשה זאת.

בואו נראה משהו טיפה יותר מורכב. חלוקה של 3 מתוך N. כאן שוב, הקבוצות הכשירות הן אלה שמכילות 3 או יותר מתוך N שחקנים, הקבוצות הלא כשירות מכילות פחות מ-3 שחקנים. רואים שהסוד הוא גדול; קודם הוא היה רק ביט אחד, עכשיו נניח שיש לו 40 ביטים, סוד באורך 4 ספרות נניח. השיטה מתחילה מצביעה של המשתתפים בשלושה צבעים. זה אוסף של צביעות בשלושה צבעים, כך שלכל שלושה משתתפים קיימת צביעה בה הם צבועים בשלושה צבעים שונים. הצביעה היא לא סודית, בוחרים אותה, היא קבועה ומכירים אותה. בשקף אתם רואים את הצביעות, אתם רואים את אוסף הצביעות של השחקן הראשון, אוסף הצביעות של השחקן השני ואוסף הצביעות של השחקן השלישי. כל טור כאן הוא צביעה אפשרית. מה התכונה שאנחנו רוצים? אנחנו רוצים שלכל שלשה של שחקנים אפשריים יהיה טור שבו יש שלושה צבעים שונים. כאן אתם רואים את הטור שני, כל שאר הטורים זה צביעות אחרות. גודל האוסף זה מספר טורים, מספר השורות כמספר השחקנים, אנחנו רוצים למצוא אוסף צביעות שבו לכל שלוש השורות יהיה טור של כל שלושת הצבעים.

ברגע שיש לנו צביעה כזאת, מה אנחנו עושים? על כל טור בפני עצמו עושים חלוקת סוד של שלושה מתוך שלושה. אם אין בטור שלושה צבעים מתוך שלושה, אין בעיה, לא מסרנו בכלל מידע, כי שני שחקנים לא מוסרים מידע. אם יש פחות משלושה שחקנים, לא יהיו שתי שורות עם שלושה צבעים, אז בעצם יש יותר צבעים מאשר שחקנים. אבל הצביעה הבטיחה שיהיה טור שבו מופיעים כל שלושת הצבעים. מה ששלושת החברים צריכים לעשות, זה למצוא ביחד בחלקים שלהם, את הטור שבו מופיעים כל הצבעים – סגול, חום וירוק - לחבר את שלושת המספרים שמופיעים בטור ולקחת את ארבע הספרות האחרונות. זה הסוד המשוחזר. בואו נראה מי השלשה הראשונה שתגלה את הסוד.

הנה כך נראית הצביעה (מראה בשקף). כלומר בצביעה ראשונה 1 2 3 צבועים ירוק, 4 5 6 צבועים אדום, 7 8 9 צבועים סגול, וכן הלאה. לא נדבר איך משיגים את הצביעה אבל היא קיימת.

השחזור הוא 8578 בדיוק. הסוד הוא 8578, ממנה יצרנו את הצביעות האלה (מראה בשקף), כל מי שהיה ירוק קיבל את החלק הזה, מי שהיה אדום קיבל את החלק זה, מי שהיה סגול בטור הראשון קיבל את החלק הזה, זה איפשר את השחזור.

אוקיי. מה אנחנו יודעים באופן כללי? באופן כללי אם יש לנו K שחקנים מתוך N, הקבוצות הכשירות מכילות K שחקנים או יותר מתוך N שחקנים. הקבוצות הלא כשירות מכילות פחות מ-K שחקנים. מה שרואים כאן בשקף זו בנייה שעדי שמיר הציע במאמר. הפתרון הוא לבחור מספר ראשוני שבו Q גדול או שווה ל-N+1. השאלה אם יודעים כמה שחקנים הולכים להיות או לא, בדרך כלל הבעיה קשה אם לא יודעים מה גודל הקבוצה.

זו עבודה שעושים תלמידי אילון יוגב ואילן קומרגודסקי. הם עובדים על השאלה מה עושים כשלא יודעים מראש כמה שחקנים יש. עכשיו נניח שיודעים מהו N, בוחרים מספר ראשוני של לפחות N+1, ואז בוחרים פולינום שהוא P(X), זה יהיה פולינום אקראי. המדרגה היא K פחות 1, הערך של פולינום בנקודה אפס הוא S, כל שאר המקדמים אקראיים. אז החלק של השחקן Pi הוא P(i), ואז מסתכלים מה השאריות ב-Q. את השחזור אפשר לעשות בעזרת אינטרפולציה של פולינומים. בהינתן K ערכים שבהם Y שווה ל-P(i) – קיים פולינום יחיד שמקיים את האילוצים. אם יש רק שתי דוגמאות, יכולים להיות הרבה פולינומים. הנקודה היא שכל עוד לא קיבלנו בדיוק K ערכים, לא למדנו שום דבר על מקדם חופשי. מקדם חופשי יכול להיות כל אחד, בדיוק אותה הסתברות, בדיוק אותו מספר פולינומים. אם מקבלים פחות מ-K ערכים, יש אותו מספר פולינומים של ערך אפשרי בנקודה אפס. לכן כל השחקנים לא קיבלו את הערכים, ומה שהם יודעים לא תלוי בסוד. זה רעיון חשוב. אפשר לעשות הרבה מניפולציות, למשל אם יש לי חלוקה לסוד S1, חלוקה לסוד S2, ואני רוצה ליצור חלוקה של S1 ועוד S2, כל אחד יכול בקלות לייצר את החלק הזה.

זה בסיס להרבה אפשרויות של חישוב בטוח על ידי כמה שחקנים שלכל אחד יש ערך שהוא קיבל, והם רוצים לחשב פונקציה משותפת בלי לגלות יותר מדי מה הערכים שלה.

מה השימושים של חלוקת הסוד? אתן לכם דוגמא פשוטה לשימוש אפשרי של חלוקת סוד. אמרנו שמספר השחקנים הכולל, ה-N, כמעט לא משפיע. צריך לבחור מספר ראשוני מספיק גדול. עכשיו תארו לכם שאתם רוצים לעשות עצומה, רוצים להוכיח שהרבה אנשים חתמו והם תומכים בנושא מסוים אבל לא רוצים לחשוף מי חתם, ורוצים שהוכחה תהיה קצרה.

נניח שיש גוף ניטרלי – והשאלה גם מה זה ניטרלי – שהוא מחלק לכל האנשים הרלוונטיים חלק של סוד בסכמה של K מתוך N. הרעיון הוא שמי שתומך בעצומה אמור לתת את החלק שלו למארגן העצומה. כדי להוכיח שלפחות K אנשים תומכים, מארגן העצומה משחזר את הסוד. הוא יכול להוכיח שלפחות K אנשים תומכים בו כי הוא הצליח לשחזר את הסוד, אבל לא יודעים מי האנשים שתמכו, רק כמה. הוא שמר לחלוטין על האנונימיות של K האנשים אלה.

עכשיו עולה השאלה מתי מחלקים, מה קורה אם רוצים לעשות חישוב ולחזור על זה, לבצע משימות שונות, לדעת שלא גונבים סודות לאנשים. לכן זה רק חלק מהסיפור, אבל זו דוגמא. אם אתם אומרים שהרבה אנשים תומכים בהם בלי שאתם מגלים מיהם, בלי שאתם עושים משהו ארוך במיוחד, זה לא ברור.

דוגמא לשימוש בחלוקת סוד – חישובי MPC, יש שמות באינטרנט והם משתמשים בחלוקת סוד. למשל יש אתר של מכון ויצמן עם עץ ושורש של העץ. לכל אחד מ"ההורים" בעץ הזה יש מפתח, זהו מפתח השורש, והם מאשרים באמצעותו את "הילדים" שלהם. מפתח השורש של רשם השמות באינטרנט, ה-DNS, מחולק בין שבעה אנשים, כך שאם תהיה שריפה או משהו אפשר יהיה לשחזר. כל חמישה מתוך שבעה אנשים יכולים לשחזר. אם אתם גולשים, אתם משתמשים ב-DNS שמאובטח על ידי שורש של DNS, אז כל אחד מכם משתמש בחלוקת סוד.

הזכרתי שימוש ב-MPC. באופן כללי יש לנו שחקנים, לכל אחד יש ערך, רוצים לעשות חישוב כלשהו של הערכים שלהם, ולא רוצים לגלות אותם. הדבר הבסיסי ביותר שצריך זה חלוקת הסוד שראינו, זו אחת הפרוצדורות שמשתמשים בה.

הזכרנו בחירות ממוחשבות. אפשר להבין למה רוצים את זה, אפשר לשאול האם זה טוב או רע, אבל הבסיס לבחירות ממוחשבות יהיה משהו דומה לחלוקת הסוד שראינו. זה יהיה כמובן יותר מורכב, אבל זה הרעיון.

אני פוסח פה על כמה דוגמאות, ועובר לדבר על האתגרים שעומדים בפנינו כשחוקרים קריפטוגרפיה. בכוונה אני מדגיש מחקר של קריפטוגרפיה, כי יש גם שאלה של שימוש. הדברים האלה תלויים אחד בשני, אדבר גם על איך לגרום להשתמש בקריפטוגרפיה. אני חוזר למה שהתחלתי בו, לקריפטוגרפיה יש קשר הדוק עם התפתחות המחקר בסיבוכיות של חישובים.

האם P שווה ל-NP? מה קורה עם חישוב שקל לחשב ולוודא. אם יש לי שני מספרים שאני רוצה לכפול אותם, אחשב את המכפלה, אראה שהיא מה שהיא צריכה להיות. אבל בהינתן מכפלה אנחנו לא יודעים לעשות חזרה את הפירוק לגורמים. אם P שווה ל-NP, כל מה שאני יכול להעריך אני יכול לחשב. אולי אוכל לעשות סימולציה של כל אחד מהם. אבל זו לא תהיה קריפטוגרפיה, רק פנקס חד פעמי, כל שאר העניינים קשורים לקריפטוגרפיה – כמו מפתח פומבי – ייעלמו.

עולם אפשרי אחר זה יוריסטיקה, שם זה כמעט אותו דבר. אולי יש בעיות קשות, אבל קשה למצוא את הבעיות הקשות. כדי לא להיות אופטימיים, יש גם עולם שאפשר לקרוא לו Pessiland, זה עולם שבו גם יש קריפטוגרפיה וגם אפשר לגלות. זה עולם רע מאוד. יש עולמות שונים שיש בהם קריפטוגרפיה. אנחנו לא יודעים באיזה עולם אנחנו נמצאים, אני מעריך שאנחנו נמצאים איפה שהוא באמצע. בעולם המיניסקריפט יש חלקים מעניינים של קריפטוגרפיה, למשל מפתח מסוים, בקריפטוגרפיה של מפתח פומבי לא יודעים מה זה. פה חייבים לעשות את החישובים שהראיתי, ובשביל כל אחד מאלה צריכים הנחות שונות. נגיד בהנחה שקשה לקבל את הגורמים, אם באמת קשה לפרק לגורמים, אנחנו נמצאים בקריפטומניה.

אולי העולם האחרון שכדאי להזכיר, זה אובפוסטופיה, כאן ההנחה היא שאפשר לקחת תוכנית כלשהי, לעמעם אותה כך שאי אפשר להבין מה התוכנית עושה, לשמור על הפונקציונליות שלה, אבל בלי להבין מה היא עושה. אגיד בצורה קצת גסה – לא יהיה הבדל בין לתת לך את התוכנית לבין לתת לכם תוכנית על ידי קופסה שחורה. גם זה אפשרי, ואם זה אפשרי אז המון דברים אחרים אפשריים.

זו תמונת העולם הכללית, אנחנו לא יודעים איפה אנו נמצאים, כל אחת מההנחות מתאימה לעולם אחר. פה צריכים הנחות כלליות לעולם של מיניסקריפט, צריכים פונקציות חד כיווניות, שקל לחשב בכיוון אחד וקשה לחשב בכיוון שני.

המחקר שואל מה היחס בין העולמות האלה, איזו הנחה גוברת ומה אפשר לעשות. בפרט אחת השאלות החשובות היא מה ההנחות שמאפשרות קריפטוגרפיה – הצפנת מפתח ציבורי וחתימות – מה ההנחות שצריכים כדי לקבל פתרונות יעילים של העולם הזה.

יש תחום מאוד מתפתח בשנים האחרונות, הצפנה הומומורפית, שמאפשרת לנו לבצע חישובים על פני דברים מוצפנים בלי שיודעים מה הערכים שלהם. אני מקבל הצפנה, עושה חישוב, שולח לכם חזרה, אני לא למדתי כלום על הנתונים שלכם ואתם יודעים רק את הערך שאני החזרתי לכם.

יש הצעות לבניות כאלה, אפילו הצעות לא רעות, אבל עדיין לא ביעילות של מה שצריכה הצפנת המפתח הציבורית. כאמור, מה שלא כל כך פשוט זה אולי להתנחל בלבבות. חלקים מהקריפטוגרפיה הצליחה, גם HTTP משתמשים בהצפנת מפתח ציבורי. יש חלקים שעוד לא זכו להצלחה גדולה. השאלה אם בגלל חוסר מודעות, אולי מנסים לפתור בעיה שלא קיימת, או אולי הפתרונות עדיין לא מספיק טובים. זו השאלה. ובפרט התחום המעניין של מה קורה בבחירות.

ואולי פשוט אסיים פה ואענה על שאלות. תודה רבה.

מחיאות כפיים.

שאלה: מה הדבר הכי מרשים שראית שקרה בקריפטוגרפיה שהפך לשימושי, שהפתיע אותך?

פרופ' מוני נאור: קשה להפתיע אותי...

אם שאלת, אז אדבר על פרטיות דיפרנציאלית, שזה על גבול הקריפטוגרפיה. בפרטיות דיפרנציאלית רוצים לשחרר מידע משותף על הרבה אנשים, רוצים לטעון שזה לא פוגע בפרטיות שלך. אני מספר על ממוצע המשכורות בחדר וזה לא פוגע בפרטיות של כל אחד. השאלה היא איך להגדיר את זה. ההגדרה הטובה ביותר היא פרטיות דיפרנציאלית שהוצעה לפני עשר שנים, עם קובי ניסים שהוא תלמיד שלי לשעבר. ההגדרה אומרת: מתי לא פגעתם בפרטיות של מישהו? אם אני מסתכל על נתונים כוללים, מסתכל על אותו בסיס נתונים ורק שיניתי את אחד הנתונים, ואז יש התפלגויות, יש מכניזם שמשחרר מידע, אותו מכניזם שמופעל על זה, והמרחק בין שתי ההתפלגויות הוא מרחק קצר. זה משהו שיש לו פוטנציאל גדול להצלחה, כבר יש דוגמאות לזה שמשתמשים בהן בגוגל כרום. גם חברת אפל יצאה בהכרזה שישתמשו בזה כדי לעודד את כל המפרסמים שלהם, כי כל מידע שיתנו יהיה מפורסם בצורות האלה.

שאלה: האם יש דרכים לסמן סוד בצורה כזאת שאדע למי יש אותו? למשל לחזור לאניגמה, שלא רצו לפעול עם הסודות?

פרופ' מוני נאור: האם אני יכול לסמן סוד כך שאדע למי הועבר? יש דרכים לכך, בהחלט כן. למרבה הפלא זה קשור לפרטיות דיפרנציאלית, הרעיון של לגלות את המדליפים. אפשר לראות בזה את ההיפך מפרטיות. במה שהצגתי אני משחרר משהו, איזשהו מידע משותף לכולם, ולא יכול לדעת מה הנתונים שנמצאים אצל מישהו מסוים. בבעיה ששאלת זה הפוך, מישהו הפיץ סודות, מסמכים, ואז יכול להיות שהיה איחוד של כמה אנשים, השאלה אם מסוגלים לגלות מי האנשים האלה. יש שיטות שונות לעשות זאת, בהחלט. יש אפשרות לגלות מי האיש או האנשים.

שאלה: רוב מה שדובר כאן זה על המידע המועבר אחרי שהוא הוצפן. אבל יש שלבים קודמים. אני מקיש על המקלדת, המחשב לא מיד מצפין את זה, יש כל מיני בַּאפֶרִים שבהם אני יכול ללכת ולקרוא את זה מבחוץ.

פרופ' מוני נאור: בהחלט, זו אחת הבעיות.

שאלה: אם ניכנס לחומרה, האם יהיו דברים שיצפינו את המידע באיזה אופן?

פרופ' מוני נאור: זו נקודה חשובה. כדאי להפעיל את כל אמצעים קריפטוגרפים, כמה שיותר מהר. אמרתי שכמעט לא התפרסמו מאמרים בנושא של קריפטוגרפיה, הנה דוגמא למאמר שפורסם על ידי קרקהופס, שידוע בגלל השורה הזאת – מערכת להצפנה צריכה להיות בטוחה גם אם כל החלקים במערכת ידועים, פרט למפתח הסודי. זה מאמר מ-1883. מה שאתה מניח שנבחר באקראי זה המפתח, וזה לא ידוע. איך שהמערכת פועלת, זה כן ידוע. הנקודה השישית שלו היתה שהמערכת צריכה להיות כל כך קלה לשימוש שלא תהיה בעיה להשתמש בה והיא לא צריכה לגרום למשתמשים שלה לעקוב אחרי אוסף גדול של חוקים. זו אחת הבעיות המוכרות, לא רוצים לפגוע בחוויית המשתמש, רוצים שכל הדברים ייעשו בשלב מוקדם מאוד ואוטומטית, אבל אין לנו דרכים לכפות את זה.

שאלה: בנוגע ליישומים של שיתוף סיגנלים שהם לא בהכרח מחשבים, אולי יש מחשוב בדרך, אבל לא בהכרח מחשבים. למשל גוף מנהל של חברה, שהחלטות לא יוכלו להתבצע על ידי אדם אחד אלא על ידי X חברים ביחד.

פרופ' מוני נאור: זה בהחלט שימוש אפשרי לזה. אולי זה יהיה משהו ממושקל, למשל שאם מדובר בבעלי מניות ההחלטות שיוכלו לקבל יהיו יחסית לכוחם כבעלי מניות. כל הדברים האלה בהחלט יכולים להיות רלוונטיים.

שאלה: יישומים פופולריים גם?

פרופ' מוני נאור: לא. למרות שרעיונות אלה קיימים כמה עשרות שנים, חלק מהדברים תפסו מאוד, חלק לוקח להם הרבה זמן.

שאלה: אחשוב על שתי דרכים ללמידת הסוד, אחד זה N ו-K. אם אני מגדיל את N, כשהסוד מתגלה הוא מתגלה להרבה אנשים. אם אני רוצה סוד יותר סודי, אני רוצה ש-N יהיה מצומצם יותר. מצד שני אם אני רוצה להגן על הסוד, אני רוצה שכמות האנשים שיש להם את המפתח תהיה כמה שיותר גדולה, אם אני רוצה להגן על הסוד אני רוצה K כמה שיותר גדול. יש הגדרה פורמלית מה הרצוי?

פרופ' מוני נאור: למשל בדוגמא של שימוש שהזכרתי, הרבה פעמים יש גבול של שליש. יוצאים מתוך הנחה שאין קואליציה גדולה יותר משליש מהשחקנים, ואז שם K גדול ומניחים שהם לא משתפים פעולה, מספיק להניח שאין רוב שיודעים. ואז חלוקת הסוד תהיה משהו כמו N חלקי 3 מתוך N, או משהו כזה, אבל זה תלוי בהשלכה.

עוד שאלות? תודה רבה.

מחיאות כפיים.