SHUTTERSTOCK | ASAP

דוברות אוניברסיטת בר-אילן

מחרוזת צופנת סוד

על שיטה מהירה ליצירת מספרים אקראיים

פרופסור עדו קנטר ופרופסור מיכאל רוזנבלו, חברי סגל במחלקה לפיזיקה באוניברסיטת בר-אילן ותלמידיהם איגור ריידלר ויערה אביעד, פרסמו את תוצאותיו של מחקר לפיתוח מכשיר פשוט אך רב עוצמה שנודעת לו חשיבות רבה בתחומים רבים של מדע, תקשורת ואבטחה – מחולל מספרים אקראיים מהיר במיוחד.

מספר אקראי מושלם הוא מספר שאין כל דרך לנבא את ספרותיו. בפועל, בימים אלה זוהי מחרוזת בינרית, הבנויה כולה מהספרות 0 או 1, באורך בלתי מוגבל למעשה. המספר נקרא "אקראי" משום שגם אם ידועות אחדות מהספרות שלו, אי-אפשר בשום פנים לדעת מראש מה תהיה הספרה הבאה אחריהן.

יש למספרים האקראיים יישומים חשובים במדע, החל ביצירת מדגם אקראי לחלוטין (למשל, בחירת משתתפים בסקר דעת קהל באופן כזה שאין להם שום מכנה משותף מלבד עצם השתייכותם לאוכלוסייה הנבדקת), וכלה בסריקת אותות רדיו וניתוח שלהם. אבל חשיבותם המעשית הגדולה ביותר של המספרים האקראיים מצויה כיום בתחום ההצפנה (קריפטוגרפיה).

בעליו של מידע סודי – צבאי, מדיני, מסחרי, פיננסי – מבקשים לשמור על סודיותו, ולכן הם מצפינים אותו באופן כזה שרק הם עצמם ומי שמקבלים מהם את המידע יוכלו לקרוא אותו. לשם כך צריך להיות להם מַפתח – מחרוזת ספרות הידועה רק לשותפי הסוד, ולא לכל אדם אחר. יש שיטות שונות ליצירת מפתחות הצפנה, אבל ברמה הגבוהה ביותר, המפתח שנמצא יעיל ביותר הוא מחרוזת של מספרים אקראיים, שהרי איש אינו יכול "לפצח" אותה בשיטה יעילה.

כללית, יש שתי דרכים ליצור מחרוזת כזו: מחולל המספרים האקראיים יכול להיות תוכנת מחשב בעלת אלגוריתם ליצירת אקראיות, או תהליך פיזיקלי סטוכסטי (כלומר תהליך שאין שום אפשרות לדעת מראש מה יהיו תוצאותיו המדויקות). בעייתה הגדולה של השיטה האלגוריתמית היא אי-עמידותה בפני מה שנקרא "התקפה בכוח הזרוע": שימוש במחשבים מהירים ביותר על המידע המוצפן עתיד לגלות בסופו של דבר כיצד הוא הוצפן: את מה שמחשב (דטרמיניסטי) אחד יכול לבנות, מחשב אחר יכול לחקות. בתהליכים סטוכסטיים, לעומת זאת, שיטת כוח הזרוע לא תועיל – משום שאין מאחוריהם שום שיטה. ובכל זאת יש להם בעיות משלהם – יש צורך במהירות

קובץ זה נועד אך ורק לשימושם האישי של מורי הפיזיקה ולהוראה בכיתותיהם. אין לעשות שימוש כלשהו בקובץ זה לכל מטרה אחרת ובכלל זה שימוש מסחרי; פרסום באתר אחר (למעט אתר בית הספר בו מלמד המורה); העמדה לרשות הציבור או הפצה בדרך אחרת כלשהי של קובץ זה או כל חלק ממנו.

רבה, והמערכות המייצרות אותם הן בדרך כלל יקרות, מסובכות ולא לגמרי אמינות.

קנטר, רוזנבלו ותלמידיהם התגברו על בעיות אלה ופיתחו מערכת פיזיקלית זולה, מהירה ביותר ואמינה ליצירת מספרים אקראיים, שבמרכזה מכשיר לייזר. הדבר מפתיע בגלל תדמיתו של הלייזר כמכשיר עקבי וקוהרנטי, המפיק אלומת אור אחידה ברמת דיוק גבוהה מאוד. ובכל זאת נמצאה דרך לקבלת אקראיות מלייזר, על-ידי שימוש במשוב חיצוני.

העיקרון המרכזי המונח ביסוד הלייזר הוא התרוצצותה של אלומת אור בתוך המכשיר הלוך ושוב, בין שתי מראות. בדרך זו נוצר משוב חיובי המעלה את רמת האחידות של אלומת האור עוד ועוד, עד שהיא בוקעת לבסוף מהמכשיר כפעימה (פולס) של אור קוהרנטי, באורך גל אחיד ובמופע (פאזה) אחיד. אבל – וזה החידוש – אם האלומה מופנית לעבר מראה חיצונית, ומוחזרת ממנה לתוך הלייזר, יש בו עתה שני סוגי משוב: פנימי וחיצוני. שילוב שניים אלה מחולל כאוס – האות המגיע אל הגלאי של המערכת אינו אחיד עוד, ואין שום שיטה בחוסר האחידות שלו.

הגלאי ממיר את עוצמת הפעימה למספר המאוחסן במונה. תוכנת מחשב מחשבת את ההפרש בין ערכיהן של שתי פעימות רצופות, וליתר ביטחון נוטלת רק מספר שרירותי של ספרות מ"קצה" המספר שהתקבל כהפרש (הספרות הכי פחות משמעותיות מבחינה פיזיקלית), לצורך יצירת המספר האקראי. לדוגמה, אם עוצמתה של פעימה אחת היתה 20.504430 מיליוולט ועוצמת הפעימה השנייה היתה 17.564144 מ"ו, ההפרש הוא 2.940286. אם החליטו המשתמשים במערכת, באורח שרירותי, ליטול רק את שתי הספרות הכי פחות משמעותיות מבחינת המדידה, הם יצרפו למחרוזת שלהם את המספר 8 (בצורתו הבינרית 1000) ואחריו את המספר 6 (0110 בינרי). המפתח שיתקבל יהיה 10000110. בפועל, כמובן, יש הרבה יותר ספרות אחרי הנקודה העשרונית, ואפשר ליטול מספר גדול יותר של ספרות פחות משמעותיות. חשוב מכך, מספר הפעימות הוא עצום, ולכן אורך המַפתח יכול להגיע, בשנייה אחת של פעולת המערכת, למיליארדים רבים של ספרות בינריות.

יתרונותיה של מערכת זו רבים. ראשית, היא אינה מחייבת מתקן מסובך, אלא משתמשת בלייזרים, בגלאים ובממירים שאפשר לקנותם "מעל המדף", ובתוכנת מחשב פשוטה יחסית. שנית, מהירותה עצומה ולכן היא מסוגלת לחולל מספרים אקראיים ארוכים ביותר (כמובן, ככל שהמספר ארוך יותר, כן הסיכוי לפיצוחו בכוח הזרוע קטן יותר). ולבסוף, היא עומדת בדרישה המקובלת ליצירת מספרים אקראיים, כמו זו שפיתח מכון התקנים האמריקני.

ועדיין נשאלת השאלה, כיצד יגיע המַפתח – מחרוזת המספרים האקראיים – מידי מי שיצר אותו והשתמש בו להצפנת מידע, לידי מי שיקבל ממנו את המידע המוצפן ויצטרך לפענח אותו. קנטר ורוזנבלו מוסרים שכבר בחנו את היכולת לפתח שיטת הצפנה במהירות האור והמבוססת על סינכרון בין לייזרים כאוטיים, שיטה שהוכחה כבטוחה. ❖

מאנגלית: עמנואל לוטם

לקריאה נוספת

Reidler, Y. Aviad, Michael Rosenbluh and I. Kanter, Phys. Rev. Lett. 103, 024102 (2009) .

J. Miller, Physics Today, August 2009, pg. 12.

קובץ זה נועד אך ורק לשימושם האישי של מורי הפיזיקה ולהוראה בכיתותיהם. אין לעשות שימוש כלשהו בקובץ זה לכל מטרה אחרת ובכלל זה שימוש מסחרי; פרסום באתר אחר (למעט אתר בית הספר בו מלמד המורה); העמדה לרשות הציבור או הפצה בדרך אחרת כלשהי של קובץ זה או כל חלק ממנו.