



# יש אפשרות להצפנה בטוחה

ההצפנה הקוונטית תגרום לשבירת הצפנים הקיימים אך גם תאפשר לנו לפתח אמצעי הצפנה חדשים כנגד ההאזנות הממשלתיות, אומרים חוקרים שפרסמו מאמר בניצ'ר בסוף מארס

**ה**כרה בעוצמת המעקב של ה-NSA ושל גופים מקבילים בעולם האיר את תחום האבטחה - או יותר נכון העדר האבטחה - של התקשורת הדיגיטלית שלנו. גם המידע המוצפן ביותר פגיע להתפתחות הטכנולוגית. ובכל זאת, האם אפשר לשמור על פרטיות בעולם פרוץ זה? בגיליון ה-27 במארס של כתב העת ניצ'ר, כותבים החוקרים **ארתור אקרט** ו**רנאטו רנר** מהמרכז לטכנולוגיות קוונטיות באוניברסיטה הלאומית של סינגפור וממכון ETH בשוויץ אילו אמצעים פיסיקליים יאפשרו לנו לשמור על הסודות.

בהיסטוריה של התקשורת הסודית, המאמצים של כותבי הקוד המבריקים ביותר התעמתו שוב ושוב עם הסבלנות של פורצי הקודים. לעתים אנו צופים זאת. אנו יודעים כי אחת ההצפנות החזקות והנפוצות ביותר כיום תהפוך ללא בטוחה ברגע שייבנה מחשב קוונטי.

ואולם המעגל לא חייב להימשך לנצח. "ההתפתחויות האחרונות בתחום הקריפטוגרפיה הקוונטית מראות, כי הפרטיות תהיה אפשרות תחת הנחה חלשה על אודות חופש הפעולה שיש לנו ועל מהימנות המכשיר שבו אנו משתמשים" אומר אקרט, פרופ' לפיסיקה קוונטית באוניברסיטת אוקספורד בבריטניה ומנהל המרכז לטכנולוגיות קוונטיות באוניברסיטה הלאומית של סינגפור, שם הוא גם מחזיק בקתדרה. לפני יותר מ-20 שנה הציעו אקרט ואחרים באופן בלתי תלוי דרך

"מלבד היות

התגלית הזאת

אחת ההתפתחויות

המדעיות החשובות

של השנים האחרונות,

נושא ההצפנה יצא

מהצללים. כבר לא

מטורף לדבר על

הנושאים הללו כיום"

להשתמש בתכונות הקוונטיות של חלקיקי אור כדי לחלוק מפתחות סודיים לתקשורת מוצפנת. המפתח היה רצף אקראי של אפסים ואחדים, שנגזר מבחירה אקראית כיצד למדוד את החלקיקים (וכמה צעדים נוספים), כדי להצפין את המסר. במאמר שפרסמו בניצ'ר, מסבירים אקרט ורנר כיצד הקריפטוגרפיה הקוונטית התפתחה מאז לכיוונים מסחריים ולשטחים תיאורטיים חדשים לחלוטין.

אף כי הפרטיות תלויה באקראיות ובאמון, הדבר המפתיע ביותר בממצאים האחרונים הוא, שאנחנו יכולים לתקשר חופשי גם אם יש לנו אמון מוגבל בהתקן הקריפטוגרפי - תארו לעצמכם שאנחנו רוכשים אותם מאויב שלנו, וביכולות שלנו לבצע בחירה חופשית - כאשר האויב מנסה לעשות מניפולציה עלינו. בהינתן גישה לכמה סוגים של מתאמים, בין אם מקורם קוונטי או לא, ועם מעט רצון חופשי, אנו יכולים להגן על עצמנו. יתר על כן, אנו יכולים להגן על עצמנו כנגד יריבים בעלי טכנולוגיה עדיפה ובלתי מוכרת.

"ככל שהבחירות שלנו אינן ניתנות לחלוטין לחיזוי, נוכל יותר לשמור על הסודות שלנו", אומר רנר, פרופ' לפיסיקה תיאורטית ב-ETZ בציריך, שוויץ. תחום זה צמח מתוך תגלית מתמטית של רנר ועמיתיו של "הגברת האקראיות". הם גילו כי טריק קוונטי יכול להפוך כמה סוגים של מספרים אקראיים במידה קטנה למספרים אקראיים לחלוטין. התחום ניתן ליישום בקריפטוגרפיה, שם שיטות כאלה יכולות להשיב לנו את היכולת לקבל החלטות אקראיות יותר ולהבטיח סודיות גם אם מישהו עושה עלינו מניפולציות.

"מלבד היות התגלית הזאת אחת ההתפתחויות המדעיות החשובות של השנים האחרונות, נושא ההצפנה יצא מהצללים. כבר לא מטורף לדבר על הנושאים הללו כיום", אומר אקרט, שעבד וייעץ לכמה חברות וסוכנויות ממשלתיות.

המאמר הפופולרי למחצה מצטט 68 מאמרים ומחקרים, החל מכתביו של **אדגר אלן פו** על הצפנה ב-1841, דרך מאמרי היסוד של תחום ההצפנה הקוונטית ב-1984 ו-1991 ועד לשפע העדויות על ההאזנות בשנת 2013.

החוקרים מסכמים כי "היום שבו נפסיק לפחד מספקי שירותי הצפנה שלא ניתן לסמוך עליהם אינו כה רחוק".

