digital whisper
Technologic Papers

השפעת המחשוב הקוונטי על הצפנה

מאת דניאל רואי

הקדמה

המחשב הקוונטי משנה את כללי המשחק. במשך עשרות שנים הסתמכנו על הצפנה מתמטית כדי לשמור על סודיות של הודעות, מסמכים, שיחות ומידע עסקי. אבל פיתוחים מואצים בתחום המחשוב הקוונטי מציבים איום ממשי: היכולת לפרוץ את מערכות ההצפנה הנפוצות ביותר בעולם תוך שעות או ימים בודדים.

אלגוריתמים כמו RSA ו-EC, שנחשבו במשך שנים לבלתי חדירים, עלולים לקרוס מול יכולות העיבוד המקבילי והעצום של מחשבים קוונטיים. ההשלכות רחבות: אבטחת מידע, פרטיות, תקשורת, מסחר מקוון, הגנה צבאית, ואפילו אמון בסיסי באינטרנט - כל אלה עומדים בפני טלטלה.

אז מה הופך מחשב קוונטי לכל כך שונה וחזק? האם החשש מפני "Q-Day" - היום שבו מחשב קוונטי ישבור את ההצפנה - מוצדק? ומה עושים כבר היום כדי להתכונן לעולם שבו הפיזיקה עצמה משחקת תפקיד במלחמת הסייבר?

במאמר זה נסקור את הבסיס המדעי של המחשוב הקוונטי, נבין כיצד הוא מאיים על שיטות ההצפנה הקיימות, ונציג את המירוץ שמתקיים עכשיו כדי להמציא את הקריפטוגרפיה מחדש.

מהו מחשב קוונטי?

מחשב קוונטי הוא מחשב שבנוי על יחידות חישוב הנקראות קיוביטים (qubits) במקום ביטים רגילים. בניגוד לביט קלאסי, שיכול להיות באחד משני המצבים 0 או 1, קיוביט הוא מערכת קוונטית ולכן יכול להיות במצב 0, 1, או בסופרפוזיציה קוונטית של מצבים, ועשוי להיות שזור עם קיוביטים אחרים. במילים אחרות, קיוביט יכול לייצג בשלב חישוב אחד מספר מצבים בו זמנית, בעוד שביט קלאסי מייצג רק ערך בודד בכל רגע נתון. בנוסף, קיוביטים יכולים להיות קשורים אחד לשני במרחק (תכונת שזירה קוונטית), כך שהמדידות עליהם מקושרות זו לזו באופן לא קלאסי. כתוצאה מכך, מחשבים קוונטיים מסוגלים לבצע חישובים מקביליים בהיקפים עצומים.

נוספים על היתרונות הללו, השוני הבסיסי במבנה המחשב: במקום שערים לוגיים של ערכים בינאריים, פועלים במחשב הקוונטי שערים קוונטיים (יחידות מטריציאליות יחידתיות שפועלות על הקיוביטים). מחקר תאורטי הראה שמחשב קוונטי יכול להיות לפחות טוב כמו מחשב רגיל, אך מוערך שבפועל יהיו בעיות שהמחשב הקוונטי יפתור בהרבה פחות משאבים.

המחקר בפועל החל בשנות ה-70 של המאה ה-20, ומאז נבנו מחשבים קוונטיים מצומצמים (בגידול הדרגתי בכמות הקיוביטים). למשל, כבר בשנת 2001 הצליחו לפרק לגורמים את המספר 15 עם מחשב קוונטי[1]. עם זאת, נכון להיום (2025) המחשבים הקוונטיים שפיתוחם ידוע עדיין קטנים מדי כדי לבצע פריצה מלאה להצפנות פופולריות. ההתקדמות המדעית מתמקדת כיום בהגדלת מספר הקיוביטים היציבים, בהפחתת שיעור השגיאות ובפיתוח אלגוריתמים חדשים. למשל, בשנת 2024 גוגל טענה שהשיגה עליונות קוונטית (כלומר ביצוע חישוב כזה שלמחשב הקלאסי אין סיכוי לבצע בזמן סביר) והצליחה ב-5 דקות של השבב הקוונטי Willow לבצע חישוב שיקח למחשב קלאסי 10 ספטיליון שנים.[2]

יתרונות של מחשב קוונטי על מחשב רגיל: איך מודדים מהירות של אלגוריתם?

סיבוכיות זמן ריצה - מושג יסוד באלגוריתמים

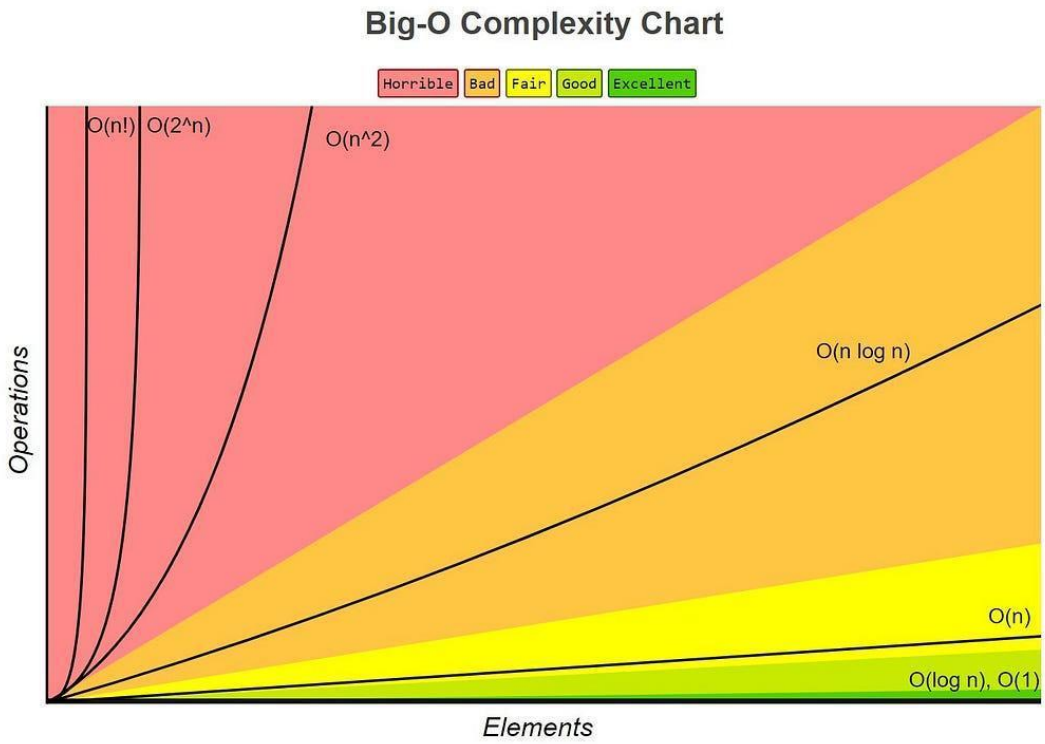
כאשר אנו מעוניינים להעריך את היעילות של אלגוריתם, אנו בוחנים לרוב את סיבוכיות זמן הריצה שלו - מדד שמעריך כמה פעולות האלגוריתם מבצע כתלות בגודל הקלט. מקובל להתמקד במקרה הגרוע ביותר של זמן הריצה, כלומר - כמה פעולות יידרשו כאשר התנאים אינם לטובתנו. את סיבוכיות זמן הריצה מסמנים באמצעות הסימון O() שנקרא Big O notation כאשר בתוך הסוגריים נרשמת פונקציה המתארת את מספר הפעולות הדרושות ביחס לגודל הקלט אותו נהוג לסמן כ-N.

לדוגמה, נניח שעלינו לבדוק האם מספר מסוים מופיע ברשימה. הדרך הפשוטה ביותר לעשות זאת (במחשב קלאסי) היא לעבור איבר אחר איבר, להשוות כל אחד מהם למספר המבוקש, ולהפסיק אם נמצא התאמה. ייתכן שהמספר המבוקש יופיע כבר במקום הראשון, אך מכיוון שאנחנו בוחנים את המקרה הגרוע ביותר נניח שהוא איננו מופיע כלל. במקרה כזה נצטרך לעבור על כל **N** האיברים ולבצע עבור כל אחד מהם שתי פעולות: קריאה והשוואה. כלומר, מספר הפעולות הכולל יהיה בקירוב **2N**. עם זאת, כשאנו מחשבים סיבוכיות, אנו מתעלמים מקבועים כמו 2 - משום שהם אינם משפיעים משמעותית על הקצב שבו מספר הפעולות גדל עם גודל הקלט. לכן, את סיבוכיות זמן הריצה של אלגוריתם זה נבטא כ-**O(N)**

[1] Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance
[2] Meet Willow, our state-of-the-art quantum chip

סוגי סיבוכיות נפוצים

ישנם מספר סוגים עיקריים של סיבוכיות זמן ריצה, שכל אחד מהם מייצג קצב גידול שונה של מספר הפעולות הדרושות ככל שהקלט גדל:



- **O(1)** - זמן קבוע: האלגוריתם מבצע מספר קבוע של פעולות, ללא תלות בגודל הקלט. לדוגמה, גישה לאיבר במערך לפי אינדקס.
- **O(log N)** - לוגריתמי: מספר הפעולות גדל בצורה איטית מאוד ככל שהקלט גדל. דוגמה לכך היא חיפוש בינארי ברשימה ממוינת - בכל שלב חותכים את הרשימה לחצי.
- **O(N)** - לינארי: מספר הפעולות גדל בקצב ישר עם גודל הקלט. הדוגמה מהחיפוש ברשימה אינה ממוינת שייכת לסוג זה.
- **O(N log N)** - לינארי-לוגריתמי: שכיח באלגוריתמים יעילים למיון, כמו Merge Sort או Quick Sort בממוצע. זהו סיבוך מעט גרוע יותר מלינארי, אך עדיין נחשב יעיל.
- **$O(N)^2$** - פולינומי: כל איבר בקלט נבדק מול כל איבר אחר - למשל, בחירה של זוגות. מופיע לעיתים קרובות באלגוריתמים נאיביים למיון או לחישובים על גרפים.
- **$O(2^N)$** - מעריכי: מספר הפעולות מוכפל בכל הוספת איבר לקלט. מופיע לרוב בבעיות קומבינטוריות, כמו חישוב כל תת-הקבוצות של רשימה.

- **O(N!)** - עצרת: גרוע במיוחד - מספר האפשרויות גדל במהירות עצומה עם גודל הקלט. מופיע בבעיות כמו מציאת כל הסדרים האפשריים (Permutations).

כמובן שהרבה מאוד פעמים סיבוכיות זמן הריצה של אלגוריתם הוא מורכב בהרבה מהדוגמאות פה, אבל אפשר לנסות להשוות אותו לסיבוכיות הקרובה אליו ביותר ברשימה כדי לדעת בערך את היעילות שלו.

הערות חשובות

סיבוכיות זמן ריצה היא מדד חשוב, אך אינה חזות הכול. ייתכן שדווקא אלגוריתם עם סיבוכיות גבוהה יעבוד טוב יותר במקרים מסוימים או בקלטים קטנים. בנוסף, סיבוכיות אינה מתארת את זמן הביצוע בפועל, אלא את הקצב שבו מספר הפעולות הדרושות גדל עם גודל הקלט. לכן, במאמר זה אנו נתבסס על סיבוכיות הזמן ככלי עיקרי להשוואה בין אלגוריתמים משום שזהו המדד המקובל והמדעי ביותר להשוואת יעילותם.

היתרונות העיקריים של מחשבים קוונטיים נוצרים מהאפשרות לנצל סופרפוזיציה ושזירה כדי לבצע חישובים מקבילים בכמויות אדירות.

אלגוריתמים קוונטיים

אלגוריתם שור (התגלה לראשונה ב-1994)

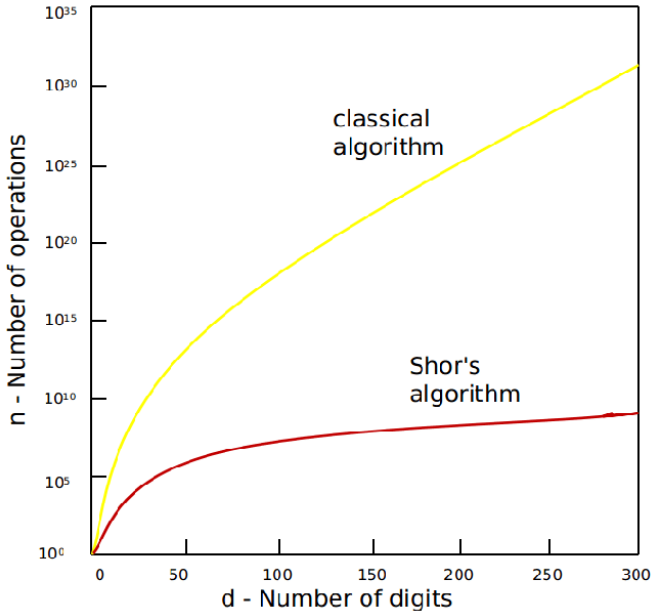
אלגוריתם קוונטי לפירוק מספרים לגורמים ראשוניים. בעוד שבמחשב רגיל אין אלגוריתם פולינומי (יעיל) ידוע לפירוק, במחשב קוונטי השילוב של כמה אלגוריתמים נותנים לנו את היכולת לגלות את הגורמים בצורה יעילה. כתוצאה מכך, ניתן לפצח בקלות יחסית את שיטת ההצפנה RSA (המבוססת על פירוק) - חישובים שנמשכים עשרות אלפי שנים במחשב רגיל יתבצעו בשעות או ימים בודדים במחשב קוונטי עם שור. הערכות קודמות הראו צורך במיליוני קיוביטים בקוונטי כדי לפצח RSA-2048, אך מחקר עדכני של חברת גוגל אף הציע יכולת פחות חזקה - להמשך בפסקה החמישית.

במחשב קלאסי, האלגוריתם היעיל ביותר הידוע לנו יכול לפרק לגורמים בסיבוכיות זמן ריצה של:

$$O\left(e^{\frac{4}{\sqrt[3]{9}}\cdot(ln\,N)^{1/3}\cdot(lnln\,N)^{2/3}}\right)$$

שזה נכנס לקטגוריה מיוחדת בין פולינומי למעריכי שזה נחשב איטי, בעיקר כשמריצים את האלגוריתם על מספרים גדולים כמו המספרים שמשתמשים בהם בשביל הצפנות כיום, שהם מספרים עם לפחות 2048 סיביות (ביטים) שזה יוצא בערך 600 ספרות. לעומת זאת, סיבוכיות הריצה של אלגוריתם שור היא בסך הכל $O(\ln(N)^3)$ שזה הרבה יותר קטן ונכנס לקטגוריה זמן פולינומי. אומנם השינוי יכול להיראות לא גדול במיוחד, אבל הוא גדול מאוד כשהמספר שצריך לפרק הוא גדול מאוד.

להלן גרף שמראה את הגידול בכמות הפעולות שהאלגוריתם הקלאסי צריך לעשות ביחס למספר הפעולות שהאלגוריתם הקוונטי (שור) צריך:



אפשר לראות בקלות שככל שהקלט (המספר שאנחנו צריכים לפרק) גדול יותר ככה הפער בין האלגוריתם הקלאסי לאלגוריתם הקוונטי גדל יותר ויותר, ובזמן שלמחשב שמשתמש אלגוריתם הקלאסי יכול לקחת אלפי שנים לפרק מספרים גדולים במיוחד מחשב קוונטי יוכל לעשות זאת במהירות יחסית.

אלגוריתם גרובר (1996)

אלגוריתם לחיפוש/בדיקת אפשרויות במקביל. החיפוש באלגוריתם גרובר עובר על כל המרחב המפתחות בבת אחת באמצעות סופרפוזיציה ומצמצם את מספר הצעדים הנדרשים לכמעט השורש הריבועי של מספר האפשרויות. המשמעות היא גדולה, כי היכולת הגמישה של האלגוריתם (למען האמת האלגוריתם עושה משהו קצת יותר כללי, אבל נוותר על זה בשביל הפשטות) זה בעצם אותו הדבר כמו לנסות מתקפת brute force. לדוגמה, כדי לפרוץ מנעול עם מיליון קודים אפשריים (כלומר, 10 בחזקת 6 קומבינציות שונות) במחשב רגיל אנחנו נצטרך במקרה הכי גרוע מיליון ניסיונות, ובמקרה הממוצע 500,00 ניסיונות במתקפת brute force קלאסית. לעומת זאת, אלגוריתם גרובר יוכל למצוא את הקוד הנכון בכ-1,000 צעדים בלבד, כלומר בערך השורש הריבועי של מיליון. זהו שיפור גדול בקנה מידה חישובי. היתרון של האלגוריתם הוא שהוא לא מוגבל לחישוב אחד ספציפי כמו אלגוריתם שור, אלא הוא יכול להיות יעיל נגד כל הצפנה שאפשר לנסות פתור אותה בעזרת brute force - כמעט כל הצפנה, אבל החולשה שלו הוא שגם אם יהיה אפשר לפרוץ בעזרתו הצפנה יהיה אפשר מאוד בקלות "לחזק" את ההצפנה ככה שהיא תהיה חזקה מדי עבור האלגוריתם.

כמו שכבר ראינו מקודם, הסיבוכיות לאלגוריתם הקלאסי היא O(N), והפעם הסיבוכיות הקוונטית היא O(√N), שזה שיפור משמעותי אבל לא מספיק כדי לפרוץ לגמרי הצפנות אלא רק להחליש אותם מעט.

לדוגמא, אם אתה מחפש מילה במילון של מיליון ערכים, אז האלגוריתם הקוונטי יוכל לעשות את זה ב(בערך) 1000 צעדים, אבל אם יש במילון 10^{20} ערכים, אז לאלגוריתם הקוונטי ייקח כ-10^10 צעדים, שזה עדיין הרבה. כל מה שצריך כדי להגן מפני אלגוריתם גרובר הוא להגדיל את גודל הקלט שעליו אפשר לעשות brute force בחזקת 2, ככה שאם המפתח היה מורכב פעם מ-256 סיביות (256^2) אז עכשיו הוא יהיה מורכב מ-512 (512^2).

אלגוריתמים קוונטיים מנצלים עקרונות חשובים בפיזיקה קוונטית שמאפשרים (בפשטות) לחלקיקים להיות בכמה מקומות בו זמנית להשפיע אחד על השני באופן מיידי כדי לבצע חישובים במקביל ולשלוט בהסתברויות של תוצאות רצויות. בניגוד לאלגוריתמים קלאסיים, שבהם בודקים אפשרות אחת בכל שלב, המחשב הקוונטי מייצג את כל האפשרויות בבת אחת, מפעיל על כולן חישוב מקבילי, ואז מכוון את המערכת כך שהתוצאה הנכונה תהיה בעלת הסתברות מדידה גבוהה.

יתרונות אלו הפכו את המחשבים הקוונטיים לכלי עתידי רב עוצמה, אך חשוב לזכור שבמובן התאורטי המחשב הקוונטי לא יכול לפתור כל בעיה באופן יעיל. ההבדל העיקרי הוא בסיבוכיות החישובית של בעיות מסוימות. בשימוש מעשי חשוב להדגיש שהטכנולוגיה כיום עדיין בתחילת דרכה - עדיין יש מעט קיוביטים יציבים ושגיאות גבוהות.

סוגי הצפנה הפגיעים לאלגוריתמים קוונטיים - הצפנה אסימטרית

הצפנות אסימטריות הם הצפנות המשתמשות בזוג מפתחות: אחד ציבורי שאפשר לגלות ולפרסם ואחד פרטי שצריך להיות בלתי אפשרי לגלות בעזרת המפתח הציבורי והם מהוות את הבסיס לרוב מערכות ההצפנה המודרניות באינטרנט. הצפנות אלו מסתמכות על בעיות מתמטיות מסוימות הנחשבות קשות מאוד לפתרון במחשב קלאסי, ולכן נחשבו לבטוחים במשך עשרות שנים. הופעת המחשוב הקוונטי מערערת הנחות יסוד אלו, משום שהיא מאפשרת פתרון מהיר של אותן בעיות שבעבר היו כמעט בלתי אפשריות לפיצוח.

אחת ההצפנות הנפוצות ביותר היא **RSA**, המבוססת על פירוק לגורמים ראשוניים. בשיטה זו, לוקחים שני מספרים ראשוניים גדולים במיוחד ומכפילים אותם. את התוצאה (שהיא המפתח ציבורי) ניתן לפרסם, מתוך ההנחה שקשה מאוד לחזור ממנה ולמצוא מהם שני המספרים הראשוניים שיצרו אותה. ואכן, במחשב קלאסי פירוק של מספרים באורך מאות או אלפי ביטים נחשב לבלתי ישים מעשית ואפילו למחשבים רבי עוצמה זה עלול לקחת אלפי שנים, אלא שמחשב קוונטי שמריץ את אלגוריתם שור מסוגל לבצע פירוק כזה בעזרת אלגוריתם שור במהירות גבוהה בהרבה. המשמעות היא שמחשב קוונטי גדול יוכל לגלות את המפתח הפרטי המשויך למפתח הציבורי ולפענח את המידע המוצפן בקלות. לכן RSA אינו בטוח בעולם קוונטי.

גם שיטות מבוססות לוגריתם בדיד (בעיה במתמטיקה שאומרת שקשה מאוד למצוא חזקה של מספר בהינתן התוצאה במצב מסוים[3]) חשופות לאותו סוג איום. אלגוריתם דיפי הלמן (Diffie Hellman), למשל, מאפשר לשני צדדים להחליף מפתחות בצורה מאובטחת על גבי ערוץ פתוח או במילים אחרות להצליח להחליט על מפתח הצפנה סודי שאף אחד, אפילו לא מישהו שקורא את כל ההודעות בין הצדדים יוכל לשחזר . בעיית הלוגריתם הבדיד שעליה האלגוריתם מסתמך קשה מאוד לפתרון במחשב קלאסי, ולכן השיטה הייתה בטוחה במשך שנים. אך מחשב קוונטי יכול לפתור גם את הבעיה הזו בעזרת אותו אלגוריתם שור, וכך לחשוף את המפתח המשותף בלי שאף צד ירגיש בכך.

כנ"ל לגבי חתימות דיגיטליות בשיטת **DSA** (שיטה שמאפשרת לך להוכיח שאתר שאתה נכנס אליו הוא באמת האתר הנכון ולא מתחזה) והצפנות על בסיס עקומים אליפטיים (ECC). גם הן מסתמכות על גרסאות של בעיית הלוגריתם הבדיד וגם הן ניתנות לפתרון על ידי מחשב קוונטי גדול בפרק זמן קצר. משמעות הדבר היא שחתימות, הצפנות וחילופי מפתחות המבוססים על אלגוריתמים אלו עלולים להפוך ללא בטוחים כלל עם התפתחות מחשוב קוונטי.

אחת ההשלכות הקריטיות ביותר לכך היא על פרוטוקול **TLS** (Transport Layer Security) - הפרוטוקול שמאבטח את רוב התעבורה באינטרנט, כולל דפדפני אינטרנט, שירותי מייל, אפליקציות ועוד. TLS עושה שימוש באלגוריתמים אסימטריים בשלב ההתחברות הראשונית (handshake), לצורך אימות זהות השרת וחילופי מפתחות סודיים. ברגע שאלגוריתמים כמו RSA, DSA או ECC כבר אינם בטוחים כל חיבור TLS יכול להיחשף בפני תוקף שמסוגל ללכוד את התקשורת ולהריץ עליה מתקפה קוונטית.

כל זה לא אומר שכל סוגי ההצפנות פגיעות למתקפה קוונטית. הצפנות סימטריות (כמו AES) ופונקציות גיבוב (כמו **SHA 256**) לרוב חסינות יותר מפני התקפה קוונטית ישירה כי האלגוריתם הקוונטי החזק ביותר (שור) לא משפיע עליהם. מצד שני, אלגוריתם גרובר אכן מקצר משמעותית את חיפוש המפתח, כך שיש להתאים את אורך המפתח - למשל אלגוריתם AES שמשתמש במפתח הצפנה בגודל של 256 ביטים עדיין מספק ביטחון שערכו המקביל בקנה מידה קוונטי יהיה כ-128 ביטים. באופן כללי, הסכמת הקריפטוגרפים היא כי רק הצפנה א-סימטרית מהווה איום קריטי בטווח הרחוק, ואילו הצפנה סימטרית חזקה (עם מפתחות ארוכים) תוכל לעמוד אף בעידן הקוונטי.

לסיכום, כל שיטת הצפנה ציבורית נפוצה כיום עלולה להישבר על ידי מחשב קוונטי עתידי, בעוד שההגנות הסימטריות דורשות שינויים וחיזוקים קטנים בלבד. הכרה זו היא הגורם המרכזי לפיתוח פתרונות קריפטוגרפיים אלטרנטיביים, הנקראים הצפנה פוסט-קוונטית, שמתאימים לשימוש גם מול התקפות קוונטיות.

[3] בעיית הלוגריתם הבדיד

פתרונות פוסט קוונטיים - קריפטוגרפיה עמידה למחשבים קוונטיים

בשנת 2016 פתח המכון האמריקאי לתקנים וטכנולוגיה NIST בתהליך מקיף וגלובלי לבחינת אלגוריתמים פוסט קוונטיים. לאחר בחינה של עשרות מועמדים מכ-25 מדינות, התקבלו ארבעה אלגוריתמים עיקריים לקראת תקן רשמי[4], שעתיד להחליף (או לשלב) את האלגוריתמים הקיימים:

- **CRYSTALS-Kyber** - מנגנון להצפנת מפתחות (Key Encapsulation Mechanism) המבוסס על בעיית הסריגים. זהו האלגוריתם שנבחר לשמש כתקן הרשמי להחלפת מפתחות, והוא נחשב למהיר, יציב וקל ליישום.
- **CRYSTALS-Dilithium** - סכמת חתימה דיגיטלית מבוססת על אותה משפחת בעיות סריגים. נבחר לשמש כתקן המרכזי לחתימות פוסט-קוונטיות בשל האיזון בין מהירות, גודל מפתח ורמת אבטחה.
- **FALCON** - סכמת חתימה אלטרנטיבית ל-Dilithium, גם היא מבוססת סריגים. מציעה גודל חתימה קטן יותר, אם כי יישומה מורכב יותר. תיכנס לתקנים מאוחרים יותר ככלי משלים.
- **SPHINCS+** - אלגוריתם חתימה מבוסס על פונקציות גיבוב בלבד (hash-based). יתרונו העיקרי הוא בביטחון התאורטי הגבוה שהוא מספק, גם מול תוקף קוונטי עתידי, אם כי ביצועיו פחות יעילים.

רוב האלגוריתמים הפוסט-קוונטיים שנבחרו על ידי NIST כמו Kyber, Dilithium, FALCON מבוססים על בעיה מתמטית הנקראת בעיית הסריגים (Lattice Problem), כי זוהי בעיה שקשה במיוחד לפתרון אפילו במחשב קוונטי. הסיבה לכך שסריגים נחשבים בטוחים היא שאין אלגוריתם קוונטי או קלאסי יעיל לפתרונם, בניגוד לפירוק לגורמים או לוגריתמים בדידים שעליהם מתבססים רוב ההצפנות האסימטריות כיום. בנוסף, הם מתאימים לחומרה קיימת, והיישום שלהם מהיר - מה שהופך אותם לבחירה מועדפת ליישום בפועל. למי שרוצה לקרוא עוד על הצפנה באמצעות סריגים מוזמן לקרוא פה.

מעבר לאלגוריתמים מבוססי סריגים, קיימת גם גישה שונה לחלוטין להתמודדות עם איום קוונטי והיא להשתמש בפיזיקה הקוונטית עצמה כדי להחליף את שלב חילופי המפתחות. חשוב להבין כי ברוב השימושים בהצפנה אסימטרית (כמו RSA או ECC) תפקידה העיקרי הוא לשתף מפתח סודי בין שני צדדים לצורך הצפנה סימטרית בהמשך. כלומר, עיקר האיום הקוונטי הוא בשלב הראשוני - שלב "לחיצת היד" (handshake) שבו שני הצדדים מחליטים על מפתח הצפנה שבעזרתו יצפינו את השיחה שלהם. כאן נכנסת לתמונה שיטת QKD (Quantum Key Distribution) - טכנולוגיה המאפשרת לשני צדדים לשתף מפתח סודי תוך שימוש בחלקיקים קוונטיים (לרוב פוטונים). היתרון של QKD הוא עקרוני: לפי חוקי תורת הקוונטים, כל ניסיון ריגול על הקו הקוונטי גורם לשיבוש במדידה ולכן ניתן לדעת האם המפתח נצפה או שונה. כך ניתן לבנות ערוץ בטוח לחלוטין לשיתוף מפתח בלי להסתמך כלל על בעיות מתמטיות קשות או הנחות תאורטיות לגבי חוסן אלגוריתמים. אומנם QKD עדיין מוגבל מבחינת מרחק, עלות ותשתית פיזית, אך הוא מציע חלופה

[4] NIST Releases First 3 Finalized Post-Quantum Encryption Standards

קונספטואלית מרתקת וייחודית למודל הקריפטוגרפי כולו: במקום לסמוך על חישוב - לסמוך על פיזיקה. אפשר לקרוא על הצפנה כזאת במאמר המצוין של גדי אלכסנדרוביץ קריפטוגרפיה קוונטית

מעבר הדרגתי ופתרונות מעשיים

המעבר לקריפטוגרפיה פוסט-קוונטית אינו מתבצע בבת אחת. כיום ממליצים גופי תקינה ומדינות שונות ליישם שיטות היברידיות שבהן נעשה שימוש משולב גם באלגוריתמים הקלאסיים וגם באלגוריתמים פוסט קוונטיים, בעיקר בפרוטוקולים קריטיים כמו TLS.

כיום מתבצע מעבר הדרגתי לשימוש ב-TLS היברידי, שהוא פרוטוקול המאבטח את התקשורת באינטרנט גם בפני תוקפים עם מחשב קוונטי. ב-TLS רגיל, החלפת המפתחות מתבצעת לרוב בשיטה כמו X25519 (שמבוססת על עקומים אליפטיים ולכן פגיעה לאלגוריתם שור), אבל היא עלולה להישבר על ידי מחשב קוונטי. לכן, ב-TLS היברידי משלבים שני אלגוריתמים: האחד קלאסי (כמו X25519), והשני פוסט קוונטי (כמו Kyber). שני האלגוריתמים פועלים במקביל: כל אחד מהם יוצר מפתח זמני, ובסוף מחברים את המפתחות יחד כדי ליצור את מפתח ההצפנה הסופי. כך, גם אם תוקף מצליח לשבור את אחת השיטות (למשל בעזרת מחשב קוונטי), המפתח המשותף עדיין יהיה בטוח בזכות האלגוריתם השני. שיטה זו כבר נתמכת בגרסאות מתקדמות של דפדפני Chrome ובשירותים כמו Cloudflare.

אתגרים ועתיד התחום

חרף ההתקדמות המרשימה, חשוב להבין: אף אלגוריתם פוסט-קוונטי אינו "בטוח לחלוטין". האבטחה מבוססת על ההנחה שלא קיימת מתקפה יעילה אך אין הוכחה פורמלית לכך. לכן, ארגונים ממשלתיים, צבאיים ופרטיים שואפים לשמור על גמישות קריפטוגרפית - שילוב של מספר אלגוריתמים ויכולת מעבר הדרגתית.

מדינות רבות מקדמות תוכניות לאומיות להיערכות:

- בארה"ב, בשנת 2022 נחתם חוק פדרלי (Quantum Computing Cybersecurity Preparedness Act) שמורה לסוכנויות הפדרליות להתחיל להיערך למעבר לפוסט-קוונטום בהתאם להנחיות שיפרסם ה-NIST.[5]
- בבריטניה, ה-NCSC פרסם תוכנית שלפיה מערכות קריטיות יידרשו להשלמת המעבר עד 2035.[6]
- מרכז הסייבר הקנדי (Canadian Centre for Cyber Security) פרסם ב-2025 המלצה לכל הגופים הממשלתיים להיערך למעבר להפצה פוסט קוונטית עד להשלמת התהליך ב-2035.[7]

[5] Quantum Computing Cybersecurity Preparedness Act
[6] UK cybersecurity agency warns over risk of quantum hackers

מתי מחשבים קוונטיים יהיו חזקים מספיק ולמה לעבור עכשיו

על אף ההבטחות הדרמטיות של המחשוב הקוונטי, התחום עדיין רחוק ממימוש מלא בקנה מידה שישבור את ההצפנות הנפוצות. רמת אי הוודאות גבוהה, וההערכות משתנות במהירות ככל שהמחקר באלקטרוניקה, באופטיקה ובאלגוריתמיקה מתפתח.

לפי הערכות מוקדמות, כדי לפרק מפתח RSA-2048 (כ-617 ספרות) יידרשו מחשבים קוונטיים בעלי כמה מיליונים קיוביטים יציבים, בשילוב עם תיקון שגיאות חזק. מחקר שפורסם על ידי Google בשנת 2025 טוען כי ייתכן שכמה מאות אלפי קיוביטים יספיקו כדי לבצע את הפריצה בפחות משבוע[8] - ירידה דרמטית מההערכה הקודמת של כ-20 מיליון. אולם גם המספרים "האופטימיים" הללו מתייחסים למערכות שנמצאות כיום הרחק מעבר ליכולת התעשייתית, ודורשות לא רק כמות עצומה של קיוביטים אלא גם מערכות תומכות עם אמינות וחוסן שטרם הושגו.

מחשב קוונטי לא פועל בשקע בקיר, אלא במתקן מורכב שפועל בטמפרטורות קיצוניות (לרוב כ-0.01 קלווין, כמעט באפס המוחלט), בבידוד מלא כמעט מכל רעש אלקטרומגנטי או תנועה מכנית. כל קיוביט, בין אם הוא מבוסס על מלכודת יונים, זרם על-מוליך או פוטונים, הוא רכיב רגיש להפליא. אחת הבעיות הגדולות ביותר היא decoherence שזה תהליך שבו הקיוביט מאבד את מצבו הקוונטי בעקבות אינטראקציה עם הסביבה. המשמעות היא שמשך הזמן שבו אפשר לבצע חישוב מדויק מוגבל מאוד (לעיתים נמדד במילישניות), ולעיתים קצר מדי כדי להשלים אלגוריתם מלא.

כדי להתגבר על כך, נדרש מנגנון של תיקון שגיאות קוונטי, המבוסס על רעיון של ייצוג קיוביט "לוגי" בעזרת קבוצה של קיוביטים פיזיים. מעריכים שלצורך קיוביט לוגי יציב אחד, יידרשו כ-1,000 קיוביטים פיזיים, תלוי בשיטת התיקון ובאיכות המערכת. כלומר, גם אם היום מדברים על "1,000 קיוביטים", בפועל זה אומר בסך הכל קיוביט אחד או שניים שפועלים בלי שגיאות. מדובר על רמה שאינה מספיקה להריץ אלגוריתם משמעותי כמו שור על מספרים שאפילו מתקרבים למספרים שמשתמשים בהם בהצפנה אמיתית, אלא לכל היותר להדגמות או ניסויים בסיסיים.

כיום (2025), החברות המובילות - IBM, Google, Rigetti, Quantinuum ואחרות - מחזיקות מערכות בטווח של מאות עד אלפי קיוביטים, אך רובם אינם מתוקנים, ושיעור השגיאות עדיין מהווה צוואר בקבוק קשה. זמן הפעולה בין שערים קוונטיים קצר, אך מספר השערים הרציפים שניתן לבצע לפני שהמערכת "מתפרקת" נמוך מאוד, ולכן קשה להריץ חישוב עמוק בלי לאבד את המידע בדרך.

---

[7] Roadmap for the migration to post-quantum cryptography for the Government of Canada
[8] How to factor 2048 bit RSA integers with less than a million noisy qubits

Q-Day באופק? לא בהכרח בקרוב

למרות האתגרים, מוסדות עולמיים עוקבים בדריכות אחר האפשרות של מה שמכונה **Q-Day** - היום שבו מחשב קוונטי חזק מספיק יוכל לפרוץ מערכות הצפנה קלאסיות (כמו RSA, ECC). הערכות שונות נעות בין תרחישים אופטימיים מאוד לבין תחזיות שמרניות: אנליסטים מ-Gartner טוענים כי כבר בשנת 2029 מערכות הצפנה אסימטרית ייחשבו "בלתי בטוחות", ובשנת 2034 יתבצעו פריצות בפועל[9]. לעומתם, גופי מחקר ומדענים אחרים מעריכים שהשלב הזה יגיע מאוחר יותר, ואין סכנה להצפנה מודרנית בעשור הקרוב.[10]

כיום, רוב המערכות הקיימות כוללות לכל היותר כמה מאות קיוביטים שאינם מתוקנים, עם ערכי שגיאה של 3^10 עד 2^10 - סדרי גודל רחוקים מהמינימום הנדרש לביצוע פריצה ממשית. לשם השוואה, כדי להריץ גרסה מתוקנת של אלגוריתם שור שתפרק 2048-RSA בפרק זמן סביר, יש צורך בכמיליון שערים קוונטיים מדויקים, ברצף, על מערכת עם קיוביטים לוגיים מתוקנים היטב - רמה שטרם הושגה.

הספקנות המדעית: לא כל עליונות קוונטית היא מהפכה

בקהילה המדעית יש גם גישה מפוכחת ולעיתים ביקורתית כלפי ההייפ. מחקרים שמצהירים על "עליונות קוונטית" נבחנים בזהירות: כאשר גוגל הציגה ב-2024 את שבב הקוונטים Willow שביצע חישוב ב-5 דקות שלטענתה ידרוש למחשב קלאסי 10 ספטיליון שנים, חוקרים אחרים טענו שניתן לבצע את אותו חישוב במחשב קלאסי תוך ימים ספורים. כלומר, הפער בין עוצמה תאורטית לעוצמה פרקטית עדיין גדול.

מתקפת "אסוף עכשיו, פענח אחר כך"

גם אם Q-Day יגיע רק עוד עשור, ההיערכות צריכה להתחיל עכשיו. הסיבה פשוטה: מדינות, גופי ביון ושחקנים מתקדמים כבר מבצעים את מתקפת "Harvest Now, Decrypt Later" - כלומר, הם אוספים כיום כמויות עצומות של מידע מוצפן, במטרה לפענח אותו בעתיד כאשר המחשוב הקוונטי יבשיל. מסמכים רפואיים, צילומים פרטיים, דוחות פיננסיים או מידע ביטחוני שנשמר היום בהצפנה קלאסית עשויים להפוך לחשופים לחלוטין בעוד עשור. לכן גובר הקונצנזוס המקצועי כי יש להאיץ את המעבר להצפנה פוסט-קוונטית כבר כעת - לא רק בפרוטוקולים החדשים, אלא גם בהמרת מידע קיים.

[9] Begin Transitioning to Post-Quantum Cryptography Now
[10] Predicting 2037: 2023 Quantum Threat Timeline

הקושי המעשי: תשתיות, תאימות, וכאוס אפשרי

המעבר לפוסט קוונטי אינו פשוט. מערכות קיימות משתמשות במגוון פרוטוקולים, ספריות הצפנה, ותשתיות כמו PKI, TLS ו-IoT. כדי לבצע מעבר הדרגתי ובטוח, יש צורך בתמיכה מקבילה (dual mode), בדיקות תאימות, ויכולת לעבוד עם שני אלגוריתמים במקביל - קלאסי וחדש. הדבר נכון במיוחד בפרוטוקולים כמו TLS 1.3 שהוא, כמו שכבר הבנתם, פגיע במיוחד. מעבר לכך, האלגוריתמים הפוסט קוונטיים נוטים להשתמש במפתחות גדולים יותר ובמבנים מתמטיים מורכבים יותר (למשל, סריגים), מה שמקשה על שילובם במערכות קיימות מבחינת רוחב פס, זמן עיבוד ותמיכה חומרתית. נדרשת השקעה נרחבת מצד יצרני תוכנה, יצרני שבבים וספקי שירות על מנת להתאים מוצרים - וכל זאת תוך שמירה על תאימות לקוד מקור קיים ומגבלות רגולטוריות.

רגולציה והיערכות מוסדית

גופים רגולטוריים ברחבי העולם כבר קובעים יעדים ברורים: בבריטניה, ה-NCSC פרסם מפת דרכים שדורשת מיפוי נכסים קריפטוגרפיים עד 2028, שדרוג מערכות עד 2031, והסרה מוחלטת של תשתיות ישנות עד 2035. ארגונים קריטיים כמו מוסדות פיננסיים, ספקיות תקשורת ויצרני ציוד תעשייתי נדרשים להוביל תהליכים מוקדמים, בעוד שמערכות עם ציוד ישן (כמו ICS או IoT) יצטרכו זמן היערכות ארוך יותר.

שיקול תאורטי: גם הפוסט קוונטי אינו חסין לחלוטין

גם פתרונות פוסט קוונטיים אינם מגיעים עם תעודת ביטוח. כמה מהאלגוריתמים פוסט קוונטיים שנחשבו לבטוחים הוכחו כחלשים גם למחשבים קלאסיים, כמו אלגוריתם Rainbow, אלגוריתם מבוסס שיטת הצפנה בשם UOV[11] שהגיע לשלב הסיום של תחרות מציאת אלגוריתמים פוסט קוונטיים ואז נמצאה לו חולשה שאפשרה לפענח את המפתח ואת ההצפנה בכמה ימים.[12]

אלגוריתמים כמו Kyber, Dilithium, +SPHINCS אומנם נבחרו לאחר בחינה מדוקדקת, אך נכון ל-2025 אין להם הוכחה פורמלית לחסינות קוונטית מלאה. חוקרים רבים מזכירים שבניגוד ל-AES שהוא אלגוריתם קלאסי שנחקר במשך עשרות שנים, האלגוריתמים החדשים נמצאים עדיין בשלבים מוקדמים יחסית של בדיקה. ייתכן שעם הזמן יימצאו להם התקפות חדשות או תקלות תכנוניות.

לכן המעבר מחייב לא רק החלפת מפתחות והתקנת עדכונים, אלא גם זהירות מתמדת, חתירה למחקר אינטנסיבי, ובחינה תקופתית של חוזק האלגוריתמים. בעידן החדש, שמירה על הצפנה טובה דורשת גמישות קריפטוגרפית - היכולת לשלב ולשנות אלגוריתמים בהתאם לצורך.

[11] Unbalanced oil and vinegar scheme
[12] Breaking Rainbow Takes a Weekend on a Laptop

סיכום

תופעת המחשוב הקוונטי עומדת לשנות את כל כללי ההצפנה המוכרים. מחשב קוונטי גדול מספיק יצליח לפתור בעיות של אבטחת מידע שקשה היום, בעיקר באמצעות אלגוריתמים כמו שור וגרובר. המשמעות היא שהצפנות אסימטריות כיום (RSA, ECC וכו') יהיו בעתיד חלשות ולא יוכלו לעמוד במתקפות קוונטיות. בתגובה, נבנו אלגוריתמים חדשים העומדים בפני מתקפה קוונטית (הקרויים פוסט קוונטיים). התהליך כולל מעבר מתמשך של התקנים ומערכות, ומומלץ להתחיל בו כבר עכשיו גם אם המחשבים הקוונטיים החזקים עוד אינם זמינים. כך יושג מצב שבו המידע שיישמר היום יהיה מוגן גם בעתיד הקוונטי.

המחבר

דניאל רואי, מלש"ב.

אשמח לשמוע הערות באימייל: danielroi385@gmail.com

המחבר הוא חבר בקהילת מגשימים נקסט - ארגון הבוגרים של מגשימים, תוכנית הסייבר הלאומית שמטרתה לקדם מצוינות, מקצועיות וציונות באמצעות הנגשת לימודי מדעי המחשב והסייבר לתלמידי הפריפריה.

בוגרי התוכנית משתלבים ביחידות הטכנולוגיות בצה"ל ובגופי הביטחון, והקהילה מהווה עבורם בית חם המאגד מאות סיניורים, עשרות יזמים והצלחות משמעותיות.

מוזמנים להצטרף ולעקוב אחרי הקהילה בסושיאל שלנו:

https://www.linkedin.com/company/magshimim-next

https://www.instagram.com/magshimim.next

לקריאה נוספת

The State of Post-Quantum Cryptography (PQC) on the Web

Post-quantum cryptography: Lattice-based cryptography

Grover's Algorithm: A Simplified Interpretation

Quantum Cryptography - Shor's Algorithm Explained