

## מיחשוב קוונטי - העתיד כבר כאן

יהושע קליסקי | 20 בפברואר, 2024

הפיתוח המואץ של המחשבים הקוונטים, על בסיס רעיונות שהוצעו בשנות ה-80 של המאה הקודמת, מבשר את תחילתה של מהפכה מדעית וטכנולוגית חדשה. זאת מכיוון שהמיחשוב הקוונטי הוא בגדר פריצת גבול בתחום שבו המיחשוב "הרגיל" הגיע כמעט לגבול הפיסי שלו. כוח החישוב של מחשב דיגיטלי תלוי במספר השבבים ליחידת שטח, אך מספר זה מוגבל מסיבות טכנולוגיות ופיזיקליות. תעשיית המחשבים והשבבים משקיעות משאבי תקציב ומחקר במזעור השבבים, אך נראה כי יהיה קשה מאוד להעלות את כוח המיחשוב של המחשבים הנוכחיים על ידי מזעור יחידות החישוב הבסיסיות. המחשב הקוונטי מציע תחלופה מהפכנית בשדה החישוב, עם יכולות בלתי מוגבלות ביישומים אזרחיים וצבאיים.

תיאורית הקוונטים התפתחה לפני כ-120 שנה, והתגבשה לתיאוריה עקבית ומדויקת ומאומתת ניסיונית בשנות ה-20 וה-30 של המאה הקודמת. מחשב קוונטי מיישם תכונות של תופעות המתרחשות בחומר ברמה האטומית או התת-אטומית, כלומר בממדים זעירים ביותר. ברמה זו, תכונות החומר הנמדדות שונות לגמרי מאלו הנמדדות בעולמנו הפיזי והמוכר, ועל כן קשה לתפוש אותן באינטואיציה האנושית שהורגלה בסביבה של עולם מוחשי, בעל שלושה ממדים. התכונות המוזרות של מערכות קוונטיות הטרידו מדענים רבים, כולל האבות המייסדים כאלברט איינשטיין. החוקר הדני הדגול נילס בוהר אף טבע את האמרה: "כל מי שאינו מוכה בהלם על ידי התורה הקוונטית לא הבין אותה".

התכונות הקוונטיות המיוחדות, המיושמות במחשבים קוונטים, הן כדלקמן

- חלקיק תת-אטומי (קוונטי) יכול להימצא במספר מצבים. מצבו הכולל של החלקיק הוא צירוף כל המצבים, או בשפה מקצועית יותר, סופרפוזיציה של מצבים. בהקשר למציאות הפיזיקלית שלנו, ניתן להמחיש את המושג של "צירוף מצבים" למשל למגנט, שבו יש צירוף מצבים של שני קטבים מנוגדים בעת ובעונה אחת. יחידת המידע הקוונטית הבסיסית שהיא צירוף של מספר מצבים נקראת "קיוביט".
- חלקיקים קוונטים זהים משפיעים אחד על מצבו של השני באופן מידי ובכל מרחק שהוא. תכונה זו נקראת "שזירה קוונטית".

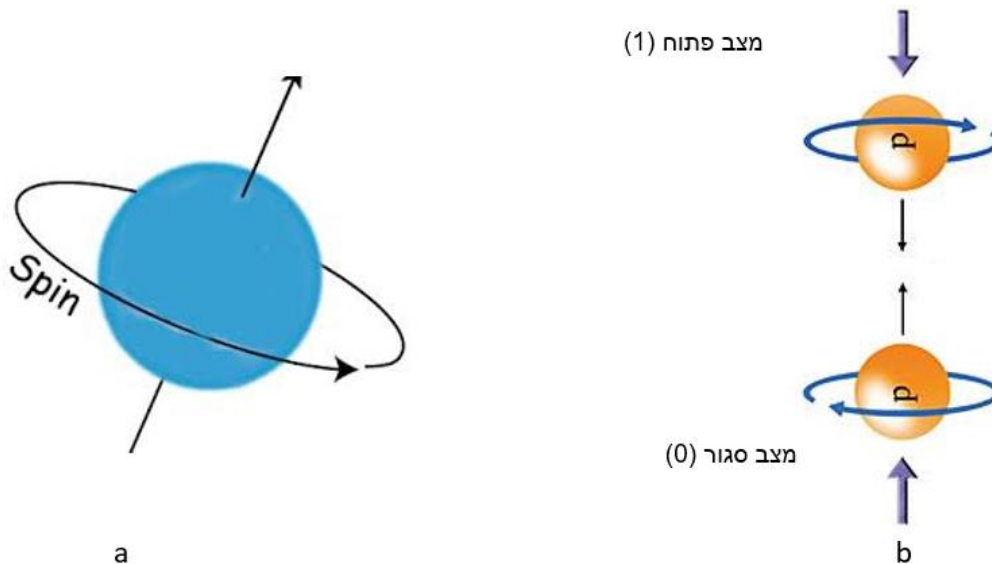
- תהליך כלשהו של מדידה הורס את המצב של סופרפוזיציה (קריסת המצבים) ומביא מידע על אודות מצב קוונטי מסוים.

### עקרון הפעולה של מחשב קוונטי

העיקרון של מחשב קוונטי ויישום התכונות הקוונטיות של חלקיקים אטומיים או תת-אטומים, ועל סמך תכונות אלו בניית דרך חישובית מתאימה. המחשב הדיגיטלי הרגיל פועל בעקרון על צירופים שונים של יחידת חישוב בסיסית, שנקראת גם בשם "ביט", המורכבת מאותות חשמליים הנוצרים בעזרת מתגים חשמליים שנמצאים במצב עובד (או פתוח או "1") או מתג שאיננו פועל (מצב סגור או "0"). פעולת החישוב של המחשב הדיגיטלי המוכר לנו נעשית בכל פעם על ידי בחירת אחד מהמצבים בלבד. לעומת זאת, מחשב קוונטי פועל על פי העקרון שרכיב אטומי או תת-אטומי (קוונטי) הינו בעל תכונה פיזיקלית מסוימת (למשל תכונה מגנטית) המייצגת מתג, ואשר יכולה להיות במצבים המייצגים מצב "פתוח" ומצב "סגור", אך הרכיב הקוונטי נמצא בו זמנית במצבי "פתוח" ו"סגור" כשלמצבים אלו יש משקל סטטיסטי שונה מכיוון שפעולת החישוב נעשית במקביל על מספר רב של מצבים "1" ו-"0" וצירופיהם, מקבלים בעקרון מחשב יעיל, בעל יכולת זיכרון רבה אשר יכול לבצע במקביל מספר רב ביותר של פעולות חישוב בזמן קצר.

כמהחשה להיות חלקיק במספר מצבים (סופרפוזיציה) נדמה את האלקטרון הסובב את גרעין האטום כמעין סביבון המסתובב גם סביב עצמו. סיבוב זה ניקרא בעגה המקצועית "ספין" (**spin**), כמודגם באיור **1a**. הסיבוב סביב עצמו יכול להיות בכיוון סיבוב מחוגי השעון (משמאל לימין ויסומן בחץ יורד  $\downarrow$ ) או בכיוון הפוך לסיבוב מחוגי השעון ויסומן בחץ עולה  $\uparrow$ , כמודגם באיור **1b**. מצבים אלו מייצגים את המתגים החשמליים במחשבים הדיגיטליים הקלאסיים, ולצורך הדיון נגדיר שרירותית מצב  $\downarrow$  כמצב עובד או "מצב פתוח" או מצב "1", ומצב  $\uparrow$  כמצב בו המתג איננו פועל או "מצב סגור".

איור מס' **1a**: דוגמה לאלקטרון המסתובב סביב צירו כסביבון קלאסי; **1b**: דוגמה לאלקטרונים המסתובבים בכיוונים מנוגדים, והמציינים במחשב קוונטי מצבים בו המתג החשמלי עובד (פתוח) או לא עובד (סגור).



בנוסף, תופעת **השזירה הקוונטית (entanglement)** היא ייחודית למערכות קוונטיות עם מספר גישות עיוניות המנסות להבינה ולהסבירה. תופעת השזירה מאפשרת למחשב קוונטי לבצע פעולות שאינן ניתנות לביצוע במחשב דיגיטלי קלאסי. בהינתן שזירה בין שני קיוביטים (יחידת החישוב הבסיסית במחשב קוונטי) הנמצאים במרחק כלשהו אחד מהשני, הם הופכים מיידית תלויים זה בזה. מכאן, שניתן לייצר מתגים קוונטים שזורים זה בזה ואשר מייצגים מצבים קוונטים מסוימים בו זמנית ומבצעים פעולות לוגיות במקביל על מספר רב של קיוביטים שונים – מה שמגביר את יעילות המחשב הקוונטי בביצוע חישובים מסובכים.

לשם ביצוע משימות אלו יש צורך בהתקני זיכרון ובמעגלים לוגיים, אשר מבוססים על תכונות קוונטיות של חלקיקים ברמה האטומית. כך למשל, מערכת של מספר רב של קיוביטים שזורים בתוספת צירופים לוגיים שונים יוצרת "שערים לוגיים" ומעגלי חישוב מורכבים, עם יכולת לבצע חישובים על סופרפוזיציה של מצבים שזורים בניגוד מוחלט למערכות חישוב קלאסיות. אם נניח כי במערכת המחשב הקוונטי יש שני מעגלי חישוב **A** ו-**B** המורכבים מחלקיקים קוונטים שזורים ומתוכננים לבצע פעולות חישוביות מסוימות, ביצוע הפעולה במעגל **A** יגרור מיידית ביצוע פעולת אחרות מוגדרות במעגל **B** ויחסוך משאבי זמן וחמרה.

### יתרונות וחסרונות

היתרון העיקרי של מחשב קוונטי הוא יכולת החישוב המהירה שלו, שהיא בסדרי גודל בלתי נתפשים לעומת מחשב דיגיטלי קלאסי. יתרון זה נובע מעצם העובדה שמחשב קוונטי מבצע מספר רב של פעולות במקביל, בניגוד למחשב הדיגיטלי הקלאסי, שמבצע את פעולות החישוב

שלו בטור. תכונה זו שוברת את הלינאריות של המחשב הקלאסי הפועל על בשיטה בינארית על שני מצבים בלבד, כך שמספר פעולות החישוב ויכולת הזיכרון של מחשב קוונטי מכפילים את עצמם בכל הוספת קיוביט בודד: כך לדוגמה, מדענים מחברת גוגל דווחו בשנת 2019 על כך [שהמחשב הקוונטי](#) שבנו ביצע פעולות מתמטיות סבוכות ב-200 שניות, לעומת 10,000 שנים שהיו נדרשות למחשב דיגיטלי קלאסי לביצוע אותן פעולות.

כפועל יוצא מכך, ניתן להשתמש במחשב קוונטי לפיצוח קודים המבוססים על פירוק מספרים גדולים לגורמים. מדובר בפעולה מתמטית סבוכה, שגוזלת משאבי זמן וחישוב רבים ממחשב דיגיטלי קלאסי, אך אורכת מספר שניות במחשב קוונטי.

מנגד, אחת המגבלות של מחשבים קוונטים היא תוצאה של "רעש קוונטי" - רעשים חיצוניים, למשל חשמליים ומגנטיים וגם חוסגורמים לקיוביטים לשנות או לאבד את המצב הקוונטי במהלך החישוב, בדרך כלל באופן אקראי ובלתי צפוי. ניתן להתגבר על מגבלה זו, אך הדבר מחייב כיום עבודה בתנאים סביבתיים מיוחדים.

## **חברות מובילות**

הפוטנציאל הגלום ביכולות החישוב האדירות של המחשב הקוונטי מהווה גורם מדרבן לחברות וארגונים המתמקדים במאמצי פיתוח עתירי הון אנושי וכספי. המוטיבציה לפיתוח יכולות מיחשוב קוונטיות מוכוונות לפעולות חישוביות סבוכות, שהן מעבר ליכולתו של מחשב קלאסי, קרי מצב של "עליונות קוונטית". למעשה, מדובר בחישובים מורכבים, שלצורך ביצועם נדרש מספר רב של מחשבים קלאסיים, אשר יעבדו במקביל ולמשך זמן לא סביר. סקירה מקיפה על אודות חברות מובילות בנושא נמצאת [במאמר הטכנולוגי הזה](#).

## **המצב בעולם העסקי**

החברות המובילות בתחום הן בעיקר יבמ, גוגל ומיקרוסופט, אשר הדגימו ביצועי מחשב מרשימים.

מדעני חברת [יבמ](#) מעריכים כי המחשבים הקוונטים יבצעו בתוך פרק זמן של שנתיים פעולות חישוב סבוכות מעבר ליכולתם של המחשבים הקלאסיים. כיום, המחשב הקוונטי של יבמ, בן 127 קיוביטים, מסוגל לבצע מיליוני פעולות בלי צורך בתיקון שגיאות [Quantum error correction \(QEC\)](#). המטרה של יבמ הייתה לקבל [מחשב קוונטי בן 1000 קיוביטים בשנת 2023](#), אך בעיות טכנולוגיות הכרוכות [בייצוב הקיוביטים לאורך זמן](#) עיכבו עד לאחרונה מטרה זו.

חברת מיקרוסופט הציגה מחשב קוונטי בעל מבנה פיזיקלי מיוחד, המאפשר [קיוביטים יציבים](#), והמהווה בסיס למחשב-על קוונטי, המסוגל לבצע [כמיליארד פעולות קוונטיות בשנייה](#).

חברת גוגל פרסמה לאחרונה כי [המחשב הקוונטי בן 70 קיוביטים](#) שמדעניה בנו ביצע חישובים שבוכים ב 6.18 שניות, לעומת 47.2 שניות שנדרשו לביצועם על ידי מחשב-על המוצב במדינת טנסי.

לאחרונה פורסם כי האיחוד האירופאי וממשלת צ'כיה יפעילו בשנת 2024 מחשב קוונטי [במרכז החישובים של אוניברסיטת Ostrava](#), ומחשב זה יהיה זמין למשתמשים מתשע מדינות אירופאיות.

בישראל קיימות מספר חברות, קטנות יותר בגודלן כמובן, הנמצאות בחזית הפיתוחים הטכנולוגיים בתחום המיחשוב הקוונטי. אחת מהן, היא חברת [quantum source](#). חברה ישראלית אחרת המובילה בתחום בקרת תהליכים, קרי שליטה בכל מערכות העזר הנדרשות במחשבים קוונטים, היא [קוונטום מאשינס \(Quantum Machines\)](#), שמפתחת מערכות עזר ותמיכה עבור מעבדים קוונטים בעלי אלף קיוביטים.

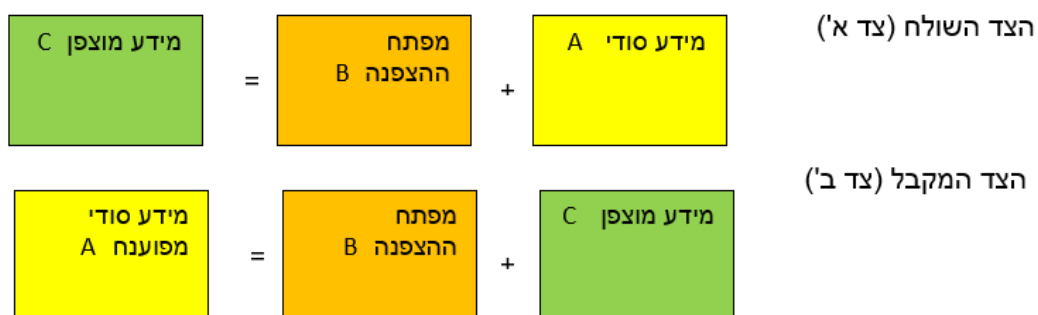
יתרונות המיחשוב הקוונטי ויישומיו הרבים משתקפים בפרמטרים כלכליים. [הערכת שוק](#) העולמי של מיחשוב קוונטי לשנת 2022 הייתה **\$13.67 B** והיא צפויה להגיע לערך של **143.44 B**, עם גידול שנתי ממוצע מורכב (**CAGR**) של 26.5 אחוזים בשנת 2032.

### יישומים של הטכנולוגיה הקוונטית-מבט כללי

למחשב קוונטי עשויים להיות יתרונות רבים בעולם הביטחוני. זאת מכיוון שיהיה מסוגל לערער את הנחות היסוד שעליהן מבוססים היום שימושים רבי חשיבות, ובהם:

פיצוח קודים של הצפנה - שיטת ההצפנה המקובלת כיום פותחה בסוף שנות ה-70 בידי **Rivest, Shamir, Adelman** - להלן צופן **RSA**. איור מס' 1 מדגים את הרעיון העקרוני של פעולת ההצפנה.

### איור מס' 1: תיאור סכמתי של עקרון ההצפנה



נניח כי צד א' מעונין לשלוח מידע סודי מסוים. מידע חסוי זה מקודד לאוסף כלשהו בצורה חבילת אותיות, או מספרים או משפטים. אם אוסף מקודד זה ייחשף לצד כלשהו, שאינו מצויד במפתח הצפנה המאפשר להחזירו לצורתו המקורית, לא יוכל גורם זה לדעת מה הוא מכיל. רק מפתח ההצפנה מאפשר זאת, והוא מורכב ממספר גדול מאוד (כמה מאות) של ספרות, המתקבל מהכפלת שני מספרים ראשוניים, כלומר מספרים שמתחלקים בעצמם וב-1 בלבד, גם הם בני מאות או אלפי ספרות. שני מספרים אלו מהווים את ה"מפתח" והם ידועים למקבל ההודעה בלבד. מציאת זוג מספרים ראשוניים שמכפלתם נותנת מספר בן מאות ספרות הינה משימה בלתי אפשרית על ידי מחשבים קלאסיים. מחשב קוונטי יכול לבצע פעולה זו במהירות וביעילות באמצעות אלגוריתם מיוחד, שפותח בשנת 1994 עבור מחשבים קוונטיים (אלגוריתם **Shor**). כך ניתן לפצח בקלות יחסית את שיטת ההצפנה המקובלת כיום - צופן **RSA** - תוך שניות ספורות, לעומת סדר גודל של אלפי שנים במחשב קלאסי. הערכות חישוביות מראות כי פירוק מספר בן 5000 ספרות לשני גורמים ראשוניים באמצעות המחשבים המוכרים לנו יארך זמן שהוא מסדר גודל של פעמיים גיל היקום, בעוד שמחשב קוונטי יבצע את הפעולה במאות שניות בלבד.

שליטה במסדי נתונים ענקיים - מציאת ערכים שונים אקראיים מתוך מסד נתונים גדול לא ממוין בזמן קצר (אלגוריתם **Grover**). כך למשל, אחת משיטות ההצפנה הידועות (**DES** -

**AES - Advanced Encryption Standard**), או שיטת **Standard**, מניחה קיום של מסד נתונים המכיל מספר רב ביותר של מפתחות הצפנה כשכל מפתח מורכב ממספר רב של ביטים. באמצעות אלגוריתם **Grover**, המחשב הקוונטי מבצע את פעולת חיפוש של המפתח הנכון במקביל על כל המפתחות, תוך קיצור זמן משמעותי לעומת מחשב קלאסי. לדוגמה, למחשב קלאסי שנדרש לחפש בין מאות מיליוני מפתחות מפתח נכון בצופן **DES**, בקצב של מיליון מפתחות בשנייה, יידרשו בקירוב כאלף שנים כדי למצוא מפתח ולפצח את הצופן. לעומת זאת, למחשב קוונטי באמצעות אלגוריתם **Grover** יידרשו בערך ארבע דקות או פחות. הוכח מתמטית שאלגוריתם זה יעיל פחות מאשר אלגוריתם **Shor** לפיצוח קוד ההצפנה השימושי כיום קוד **RSA**.

### קריפטוגרפיה קוונטית

יישום זה מבוסס על התכונה המיוחדת לחלקיקים הקוונטיים, שלפיה כל ניסיון של מאזין כלשהו ליירט (קרי לבצע מדידה) של החלקיקים המרכיבים הודעה המוצפנת באמצעות פרוטוקול המבוסס עליהם, מוביל להפרעות בקליטת המידע עקב קריסת המצבים הקוונטיים של החלקיק, ועל כן גם לגילוי ניסיון היירוט או המדידה באופן מידי. לפיכך, אפשר להעביר באמצעות הצפנה שכזו באמצעות פרוטוקולים מיוחדים שפותחו לצורך זה מידע שאינו ניתן כלל ליירוט או פענוח, והוא חסין לחלוטין מפני חשיפה לצד שלישי.

## בעיות אופטימיזציה מרובת משתנים

מחשב קוונטי הינו בעל יכולות חישוב של אופציית המסלולים הטובה ביותר עבור של מספר רב של מסלולים ומספר רב של כתובות, או באופן כללי יותר - צימוד בין מערכות מרובות משתנים. בשיטה זו המחשב מחפש [את הפיתרון הטוב ביותר האפשרי](#) מבחינת המסלול האופטימלי והוא עושה זאת על ידי חישוב סימולטני של מצבים מצומדים אפשריים (שהם למעשה סידרת פתרונות אפשריים), תוך קבלת הפתרון שזהו המצב שבו הקיוביטים המצומדים, שהם למעשה מצבים פיזיקליים, נמצאים במצב אנרגטי הנמוך ביותר האפשרי. אופציה נוספת לפתרון בעיות אופטימיזציה היא שימוש במחשב אופטי המבוסס על פיזיקת הלייזרים. שיטה זו נקראת **quantum annealing**. מחשב זה שונה מהמחשב הקוונטי שדובר עליו בעיקרון הפעולה שלו. פעולתו מבוססת על עקרונות משולבים של אופטיקה ותורת הקוונטים - נושא שנקרא **quantum optics**. חשוב לציין כי המחשב האופטי איננו מחשב אוניברסלי, אלא מחשב הפותר אך ורק בעיות ספציפיות. בשיטה זו, בעיית האופטימיזציה "נרשמת" על גבי אלמנט אופטי אשר דרכו עוברת קרן הלייזר אשר "מחפשת" סימולטנית ובמהירות האור מכל המסלולים האפשריים מסלול אופטימלי, שהוא המסלול המסתבר ביותר והוא מהווה בעצם את התהליך בעל האנרגיה הנמוכה ביותר במערכת. מבחינת היישום הביטחוני, יכולת זו מאפשרת התמודדות אופטימלית עם תרחישי קיצון בשדה הקרב העתידי, כגון התמודדות רב מימדית עם מספר רב של נחילי תקיפה, תוך שילוב והטמעה של טכנולוגיות ספקטראליות ואלקטרו-אופטיות חדשניות על מנת להשיג הכרעה.

## סימולציות של תהליכים

למחשב קוונטי יתרון מובנה בסימולציות של תהליכים. המדען הנודע ריצ'ארד פיינמן (**Feynman**) הראה ב-1980 כי ביצוע סימולציות במחשב קלאסי הינו תהליך קשה בגלל סיבוכיות החישובים וכוח מחשוב חלש יחסית. לעומת זאת, מחשב המבוסס על מערכות קוונטיות הוא בעל יתרון אינהרנטי בביצוע סימולציות עקב היכולת לבצע חישובים מורכבים תוך יישום תופעת הסופרפוזיציה. למעשה המערכות הקוונטיות (המולקולריות) המרכיבות כל ייצור חי מבצעות סימולטנית פעולות מורכבות ביותר על שום יכולות החישוב של המחשב הקוונטי.

דוגמאות לסימולציית תהליכים הן חיזוי מזג אויר, מידול של תהליכים פיזיקליים סימולטניים ומרובי חלקיקים, סימולציה של תהליכים כימיים מורכבים - כל אלה הינם תהליכים קוונטיים אשר ניתנים לסימולציה במחשבים קוונטיים.

סימולציה ממוחשבת היא חיונית במיוחד כאשר לניסוי פיסי יש עלויות לא סבירות, או סיכונים אחרים - למשל ניסוי הקשור בפיתוחו של נשק גרעיני. מחשב קוונטי יאפשר לעשות זאת במהירות וביעילות, ותוך הימנעות מסיכונים אלה.

## הנדסת חומרים חדשים, יישומים רפואיים

למחשב קוונטי יתרון מובנה לסימולציה של מבנים מולקולריים מורכבי, 'כאמצעי לייצור תרופות כולל תרופות מותאמות אישית או חומרים כימיים חדשים. הדרך המקובלת לסינטזה כימית של תרופות, במיוחד כאלה שמותאמות אישית או תרכובות כימיות מורכבות, כרוכה בעבודה מעבדתית רבה הכוללת שלבים רבים של "ניסוי וטעיה". למחשב הקלאסי אין משאבי זיכרון לביצוע תהליכים אלו ועל כן כל חישוב יארך זמן לא סביר. היתרון בשימוש במחשב הקוונטי ליישומים הניזכרים לעיל בא לידי ביטוי ביכולתו לבצע תהליכי סימולציה מורכבים הדורשים זמן וזיכרון, שאינם נמצאים במחשבים הקלאסיים. מדובר גם בחיסכון משמעותי בזמן ובמשאבי מעבדה וכן בכוח אדם מקצועי, עקב היכולת לבצע חישוביים ניסיוניים כדי לפתח אמצעים, כולל אמצעי לחימה, באופן יעיל ונסתר.

## סטטוס הפיתוח של מערכות קוונטיות בישראל

לטכנולוגיה הקוונטית חשיבות במספר היבטים החשובים למדינת ישראל – אזרחיים וביטחוניים כאחד. יודגש שהיישומים האזרחיים והצבאיים שזורים זה בזה, וכל פיתוח במגזר האזרחי הינו בעל פוטנציאל יישומי בהיבטים הביטחוניים. היישומים הרלבנטיים לישראל בכלל ולמערכת הביטחון בפרט הם:

- תקשורת קוונטית חסינה מהאזנה
- פיתוח שיטת ההצפנה, בנוסף לשיטה המקובלת כיום (פרוטוקול RSA)
- פיתוח ויישום טכנולוגיות הקשורות במיחשוב קוונטי ,
- פענוח מהיר ויעיל של שיטת ההצפנה המקובלת כיום - צופן RSA
- אופטימיזציה וסימולציה של תהליכים מרובי משתנים.
- ניתוב של מידע במסדי נתונים ענקיים - **data centers** – ושליטה בו.
- פיתוח תרכובות כימיות חדשות – פיתוח יכולות ואמצעי לחימה (חומרי נפץ חדשים, למשל) וכן אמצעי הגנה נגד לוחמה כימית או ביולוגית, מבוססים על תרכובות כימיות חדשניות או סימולציה של מנגנוני ביולוגיה מולקולרית.

הפעילות בנושא באה לידי ביטוי במספר רב של מיזמים לאומיים.

במסגרת התכנית הלאומית למדע וטכנולוגיה הושקה בשנת 2020 התכנית הלאומית למדע וטכנולוגית קוונטים [בתקציב של 1.5 מיליארד שקל](#), במימון רשות החדשנות, המרכז לפיתוח אמצעי לחימה במשרד הביטחון (מפא"ת), ות"ת ומספר משרדי ממשלה. בנוסף, בשנת 2022,



רשות החדשנות והמנהל למחקר פיתוח אמצעי לחימה ותשתית טכנולוגית - מפא"ת - הקציבו 200 מיליון ש"ח להקמת מחשב קוונטי בהשתתפות חברות ישראליות, חברות מחו"ל וחוקרים מהאקדמיה בישראל.

על מנת לקדם את הטכנולוגיות הקוונטיות לרמת מיחשב קוונטי בן עשרות קיוביטים, אישרה לאחרונה רשות החדשנות [הקמת מאגד לפיתוח טכנולוגיות מיחשוב קוונטי](#) בהיקף של 115 מיליון ש"ח - [מאגד כולל חברות מובילות ואקדמיות](#). לפיתוח טכנולוגיות של חמרה ותכנה של מחשב קוונטי "כחול לבן". סך ההשקעות במיחשוב קוונטי בשנים 2018 - 2023 הוא כ- 480 מיליון \$.

ההשקעות ברחבי העולם בפיתוח טכנולוגיות של חמרה ותכנה עבור מחשבים קוונטים, כולל פיתוח טכנולוגיות קוונטיות, הן גבוהות ביותר. הפעילות המדעית היא רב תחומית ומצריכה כוח אדם מקצועי ברמה מדעית גבוהה ביותר. בכל פעילות הכרוכה בפיתוח טכנולוגיות של מיחשוב קוונטי בישראל יש להביא בחשבון את המשאבים הזמינים מבחינת כוח אדם מקצועי, את היתרון הטכנולוגי-מדעי של ישראל מבחינת תשתית תעשייתית, ותשתיות רלבנטיות לנושא באקדמיה. העלויות הכרוכות בפיתוח טכנולוגיות קוונטיות מבחינת ההשקעה בציוד ייעודי ובכוח אדם מיומן הן גבוהות ביותר ויעידו על כך הסכומים הגדולים שמקציבה הממשלה בישראל לפעילות משולבת של תעשייה, אקדמיה ומערכת הביטחון. יצויין [שלבד מסין, ישראל](#) היא המדינה שמשקיעה במוצא את האחוז הגדול ביותר מתוך התוצר המקומי הגלמי - **GDP** (0.082%) בנושאי מיחשוב קוונטי. בנוסף להשקעה זו יש להביא בחשבון את התרומה המשמעותית של ההון האנושי והתשתית האקדמית המפותחת בישראל, שמתאימה לסוג זה של פעילות. טבלה מס' 1 מציגה את [ההשקעות ב-\\$ אמריקאי](#) במדינות שונות בנושא מיחשוב קוונטי

טבלה מס' 1: השקעות ב-\$ אמריקאי במדינות שונות בנושא מיחשוב קוונטי (מקור: <https://thequantuminsider.com/2021/04/29/leading-quantum-computing-countries>)

מדינה	השקעות \$ (BILLION) US	משך תקופת ההשקעה
ישראל	0.480	2018-2023
סין	10	2018-2023
גרמניה	3.1	2018-2023
צרפת	1.8	אין נתון
ארה"ב	1.275	2018-2023
הודו	1.0	2020-2024
אנגליה	1.013	2014-2024
רוסיה	0.663	2019-2023
יפן	0.470	2020-2023
האיחוד האירופאי	0.230	2018-2021
אוסטרליה	0.094	2017-2024

## **היבטים ביטחוניים והרלבנטיות לישראל:**

היישומים שנסקרו לעיל דרבנו מדינות שונות וישראל בכללן למרוץ לפיתוח טכנולוגיות קוונטיות] הדורש תשתית מדעית וטכנולוגית רב תחומית הכרוכה בהשקעות מרובות.

בדומה לסין, על ישראל לשאוף ולהוביל במרוץ ל"עליונות קוונטית" בהיבטים של פענוח צפנים, שיטות הצפנה ותקשורת חסינות מהאזנה, וסימולציות מורכבות בשילוב יכולות חישוב ויכולות של בינה מלאכותית -AI. השגת עליונות בטכנולוגיות AI קשורה ישירות ליכולות אדירות של חישוב ועיבוד נתונים סטיטסטיים ומכאן נגזרת חשיבות נוספת לפיתוח יכולות מיחשוב קוונטי.

כיום, סין מובילה במרוץ [לעליונות קוונטית](#) ולהצפנת מידע מבוסס על תכונות פיזיקליות בסיסיות, שמקורן בתורת הקוונטים. ההובלה הסינית עוררת דאגה במדינות המערב וכמובן בישראל עקב שדרוג היכולות של סין בפיצוח קודים, בשימוש שוטף ורציף בתקשורת המוצפנת באופן מוחלט ובאופטימיזציה מרובת משתנים. היתרון היחסי של הסינים בהצפנה קוונטית ביבשה ובחלל גרם לכך שמדינות נוספות, ביניהן ארצות הברית, בריטניה, יפן ומספר מדינות באירופה, משקיעות כ-79 מיליון \$ בהקמת מערך לוויינים [Federated Quantum Systems \(FQS\)](#) שינהלו תקשורת בהצפנה קוונטית. מערך דומה של רשת לוויינים בהובלת האיחוד האירופי - [EuroQCI](#) - נמצא בהקמה אף הוא. המרוץ לעליונות קוונטית מצריך השקעות רבות בתשתיות ובהכשרת כוח אדם מדעי מיומן. המשמעות של הופעת הטכנולוגיות הקוונטיות במערכות הביטחוניות ובשדה הקרב העתידי בהיבטים הרלבנטיים לישראל פרושה שינוי בפרדיגמות הקיימות- מה שמחייב [השקעות בישראל](#) בתחומים שונים כמפורט להלן:

1. פיצוח מנגנוני הצפנה: היכולת של מחשב קוונטי לפצח את מנגנוני ההצפנה הנוכחיים בשניות ספורות הופך למעשה את הממד הדיגיטלי של שדה הקרב העתידי למיושן, שכן, הרכיבים הבסיסיים של הממד הדיגיטלי, כגון התקשורת הצבאית, מערכות השליטה והבקרה של התשתיות הצבאיות והאזרחיות ומערך האינטרנט, הופכים חדירים ופגיעים ולכן מחייבים פיתוח שיטות אבטחה ייחודיות. המשמעות היא שינוי אופי לוחמת הסייבר, המתבססת כיום על התמודדות עם מערכים דיגיטליים ובעתיד תתחייב התמודדות עם טכנולוגיות קוונטיות.

2. תקשורת חסינה מהאזנה: היכולות לקיים תקשורת תלת ממדית (יבשה-חלל) חסינה מהאזנה מהווה מהפכה של ממש מבחינה צבאית בהיבטים אסטרטגיים וטקטיים, שכן הן מאפשרות הפעלה של נחילי כלים בלתי-מאוישים ומאוישים בערוצים חסינים, ללא חשש משיבוש התקשורת או האזנה לה, ושליטה בהם. כיום, הממד הספקטראלי מכיל תדרי שידור לתקשורת ורוחב הפס קובע את מספר התדרים הזמינים. בתקשורת הקוונטית אין משמעות לרוחב הפס, שכן מדובר בתקשורת המתבצעת תוך יישום התכונות [הקוונטיות של האור](#).

3. עליונות בממד הספקטראלי: בנוסף לתקשורת חסינה מהאזנה, הטכנולוגיה הקוונטית מאפשרת שליטה אופטימלית במיתוג העברת נתונים מתוך מאגרי מידע אדירים בשרתי ענן. כך מתאפשרת תקשורת מהירה, יעילה וחסינה מהאזנה.

4. אופטימיזציה וסימולציה של תהליכים עם משתנים מרובים: כאמור, למחשב הקוונטי יכולות לבצע סימולציות מורכבות תוך שימוש בכלים סטטיסטיים לניתוח מאגרי נתונים רלבנטיים ובאלמנטים מתורת המשחקים. נושא זה נקרא גם "לימוד מכונה קוונטי, או **quantum machine learning** - השילוב של יכולות חישוב קוונטי בלתי מוגבלות ויכולות של **AI**. נושא זה כולל בין היתר ניתוח סטטיסטי, פיתוח מודלים של שפה ולימוד איטרטיבי של המערכות השונות, עשויים לשנות את הסטטוס הנוכחי של הבינה המלאכותית לעבר מערכות משוכללות של ממשק אדם-מכונה. כך תתאפשר התמודדות אופטימלית עם תרחישי קיצון בשדה הקרב העתידי, דוגמת התמודדות רב ממדית עם מספר רב של נחילי תקיפה, תוך שילוב והטמעה של טכנולוגיות ספקטראליות ואלקטרו-אופטיות חדשניות על מנת להשיג הכרעה בשדה הקרב.

5. פיתוח תרכובות כימיות חדשות – פיתוח יכולות ואמצעי לחימה (חמרי נפץ חדשים, למשל) וכן אמצעי הגנה נגד לוחמה כימית או ביולוגית, אמצעים המבוססים על תרכובות כימיות חדשניות, על אמצעי נגד/תרופות ביולוגיות, כולל תרופות, ואמצעי נגד מותאמים אישית. מדובר בתהליכים סבוכים הכרוכים בסימולציה של מנגנוני ביולוגיה מולקולרית, ואשר למחשב דיגיטלי קלאסי אין משאבי זיכרון לביצועם ובוודאי לא בזמן סביר.

6. נגישות: יש לצפות כי הטכנולוגיה הקוונטית, על כל הסיבוכים ההנדסיים הכרוכים בהפעלתה, תהיה זמינה יותר מאשר מחשבי העל הקיימים כיום בידי מעצמות בלבד, ומעניקים להן יתרון טכנולוגי משמעותי. המחשב קוונטי עשוי לבטל יתרון יחסי זה. כך תתאפשר גישה קלה יותר למחשבים קוונטים וגמישות בהפעלת מערכות מבוססות על טכנולוגיה קוונטית. מסיבה זו יש לצפות כי מחשבי על יהפכו להתקנים חסרי משמעות. הסכנה היא, כי כך גם תתאפשר תפוצה רחבה של יכולת כשל מעצמת על למדינות קטנות, ואולי בעתיד לארגונים סמי-צבאיים. כך עלול גם להישחק יתרון יחסי של ישראל.

יישומי המיחשוב הקוונטי ויתרונותיו על פני המחשבים הדיגיטליים הנוכחיים מסוכמים בטבלה הבאה:

**טבלה מס' 2: יישומי המיחשוב הקוונטי ויתרונותיו על פני מחשבים דיגיטליים נוכחיים**

נושא	מצב נוכחי	יתרון המחשב הקוונטי	מצב עתידי
תיקשורת	אפשרות להאזנה מיגבלות רחב פס	חסינות מוחלטת מהאזנה, אין מיגבלות רחב פס	מהפכה טקטית *ואסטרטגית בשו"ב
הצפנה	הצפנת מידע בשיטת RSA, בלתי אפשרי לפיצוח.	פיצוח המנגנונים הנוכחיים של הצפנה בשניות ספורות Shor ע"י אלגוריתם	מערכות שליטה ובקרה (שו"ב) ואינטרנט הופכות לחדירות, נידרש שינוי דרמטי באופי לוחמת, סייבר
מסדי נתונים ענקיים	זמן ממוצע לחיפוש הוא לא מעשי, נדרש זמן בלתי סביר	שניות או דקות ספורות Grover ע"י אלגוריתם	שיפור משמעותי ביעילות הצפנת מידע ובחיפוש מפתחות מתאימים
AI, בינה מלאכותית data centers ניהול	כוח חישוב מוגבל	יכולת עיבוד עצומה של נתונים סטטיסטיים, פיתוח מודלים של שפה	פיתוח מימשק אדם מכונה, התמודדות עם תרחישים מרובי מישתנים
סימולציה ואופטימיזציה של תהליכים מורכבים	דורש משאבי זמן ומשאבי חישוב ניכרים תוצאות לא אופטימליות	ביצוע מהיר ומדויק של סימולציות מורכבות חישוב אופטימלי של מסלולים	AI שילוב עם התמודדות יעילה עם נחילי תקיפה
זמינות של כוח חישוב	מחשבי על-טכנולוגיה מוגבלת למעצמות	זמינות למדינה בעלת יכולת טכנולוגית-מדעית	תפוצה רחבה לגורמים עוינים או סמי צבאיים
הנדסת חמרים	כוח חישוב מוגבל לסימולציות של תהליכים כימיים	יכולות חישוב וסימולציה של תהליכים מורכבים לשם יצירת חומרים מיוחדים	פיתוח חמרים בעלי יישום צבאי (חמרי נפץ מיוחדים למשל), או אמצעים כנגד לוחמה כימית או ביולוגית

**סיכום**

המחשב הקוונטי מבוסס על יישום העקרונות העיוניים של תורת הקוונטים והוא מהווה חלק מהמהפכה הקוונטית השנייה. המחשב הקוונטי יכול לבצע מספר רב של פעולות חישוב

במקביל, בניגוד למחשב הקלאסי הפועל בטור ולכן הוא בעל יכולות חישוב אדירה של בעיות ספציפיות ואשר המחשב הקלאסי לא יכול להתמודד עימן.

אשר לישראל, ליכולת הטכנולוגית לפתח תכנה וחמרה של מחשב קוונטי יש משמעויות אסטרטגיות בעיקר בנושאי הצפנה, פיצוח קודים, סימולציה של תהליכים שונים, השגת עליונות בממד הספקטראלי ואופטימיזציה מרובת משתנים. על כן יש למקד מאמצים מרובים בנושא זה כחלק מתפיסת הביטחון, הגורסת שילוב ושליטה ביכולות טכנולוגיות קריטיות. יתר על כן, השליטה בטכנולוגיות של המיחשוב הקוונטי מהווה מנוע צמיחה להתפתחות של החברה האנושית, התפתחותה מתבססת על יכולות חישוב הולכות וגדלות והמחשב הקוונטי מגלם ביכולותיו האדירות את הטכנולוגיה העתידית אשר תגשר על הפער שנוצר עקב היכולות המוגבלות האובייקטיביות של המחשבים הקלאסיים.

אין ספק, שעל מדינת ישראל לשאוף ולהאיץ את המחקר והפיתוח העיוני והיישומי בנושא ולהגיע ל"עליונות קוונטית", שכן יישומי הטכנולוגיה הקוונטית מציינים עידן טכנולוגי חדש: אין מדובר ב"טכנולוגיה משבשת", המשבשת עידן ישן, אלא במהפכה טכנולוגית המשלימה את הטכנולוגיות הקלאסיות הישנות ומתגברת על מגבלות מובנות שלהן באמצעות יישום על עקרונות פיזיקליים יסודיים. ל"עליונות קוונטית" יש משמעות בהיבט הכולל של החוסן הלאומי: בהיבטים כלכליים, ביישומים והגנה על תשתיות קריטיות, ובהיבטים ביטחוניים.

העתיד של הטכנולוגיות הקוונטיות בשילוב מחשבים קוונטים צופן בחובו הפתעות ואי-ודאויות, בדומה למה שארע עם פיתוח המחשב הקלאסי. באנלוגיה להתפתחות המדהימה ולעיתים הבלתי-צפויה של יכולות החישוב והיישומים של המחשב הדיגיטלי, וכשם שאיש לא ידע לצפות את כוונת ההתפתחות, גם במקרה המיחשוב הקוונטי הדמיון אינו יכול לצפות את המציאות וההשלכות העתידיות.

---

עורכי הסדרה: ענת קורץ ואלדד שביט