

מחשוב קוונטי

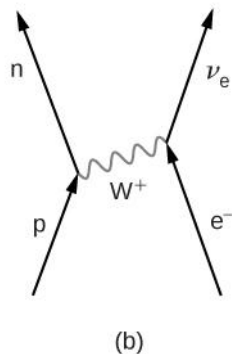
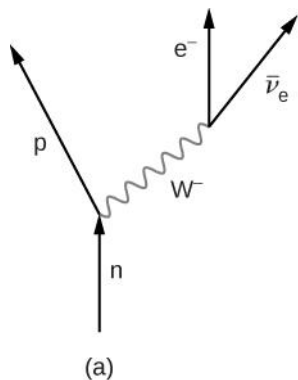
הבטחה ואיום



- איך נראה מחשב קוונטי?
- הבטחה ואיום על תקשורת מאובטחת
- מה מיוחד במחשב קוונטי?
- מה אפשר לעשות עם מחשבים קוונטים היום?
- מי מעוניין במחשוב קוונטי?



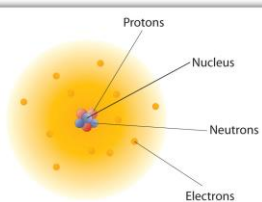
לידת המחשב הקוונטי (~1980)



ריצ'רד פיינמן
נובל 1965

- מחשב קלאסי נכשל בהתמודדות עם בעיות במכניקה קוונטית
- אלקטרון, פוטון, ושאר החלקיקים הקוונטים מתמודדים!!
- הפתרון: מחשב קוונטי

פיזיקה קלאסית מול קוונטית



- פיזיקה קלאסית: תיאור של העולם המאקרוסקופי
- פיסיקה קוונטית: תיאור של העולם המיקרוסקופי



- התיאור המיקרוסקופי עשיר יותר
- לעולם הקוונטי חוקים משלו: זר ומוזר



- קרן אור מתפצלת לשתי קרניים
- לאן ילך פוטון יחיד?
- היתור על דטרמיניזם (=חורצניות)



בעיות חישוב קשות מול בעיות חישוב קלות



מספר בן 20 ספרות $\approx 2^{64}$
גידול מעריכי (אכספוננציאלי)



$64^2 = 4096$
גידול פולינומי

יש יתרון מעריכי למחשב קוונטי
בבעיות קשות **מסוימות**

בעיות חישוב קשות טובות לשמירת סוד

מספרים ראשונים: 2,3,5,7,11,13,17

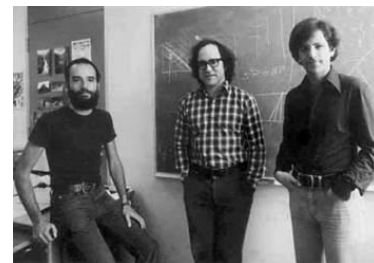
$$(p_1, p_2) \rightarrow p_1 \times p_2 \rightarrow p_1$$

קל

קשה

- מיליונית שניה להכפיל שני מספרים בני 100 ספרות כל אחד
- שבוע למצוא את p_1 עבור $p_1 \times p_2$ בעל 100 ספרות

הצפנת RSA מבוססת על הקושי למצוא את p_1



Shamir Rivest Adelman
1977

האיום על תקשורת מאובטחת

למחשב קוונטי יש יתרון מעריכי בפיצוח RSA

נתונה מכפלה של שני ראשונים בעלת 100 ספרות:

- מחשב קוונטי ימצא את הראשונים אחרי כ- 10,000 צעדים
- מחשב קלאסי צריך כ- 10,000,000,000 צעדים



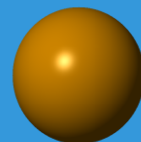
פיטר שור
1994

אלגוריתם שור: פוטנציאל למשבר תנכי באבטחת מידע
מחשב קוונטי שיכול להתמודד עם RSA הוא נשק שובר שוויון
מחשב קוונטי שיכול לשבור את RSA עדיין לא קיים

סיבית קוונטית מול קלאסית



סיבית קלאסית: מטבע, סיבית קוונטית (קיוביט) כדור



$|1\rangle$ —

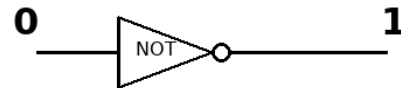
$|0\rangle$ —

סיבית קוונטית: שתי רמות אנרגיה באטום

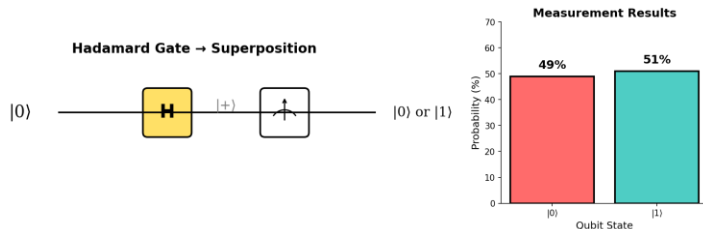
$$\alpha|0\rangle + \beta|1\rangle$$

- סיבית קוונטית מחזיקה יותר מידע מסיבית קלאסית
- אבל חושפת מידע קלאסי

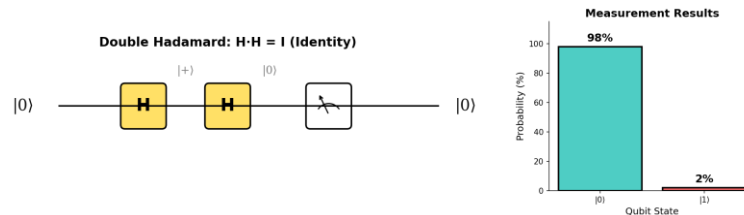
חישוב קלאסי מול חישוב קוונטי



- סופרפוזיציה מאפשרת ביזור (=חישוב מקבילי)
- ומאפשרת לכנס את הביזור



ביזור

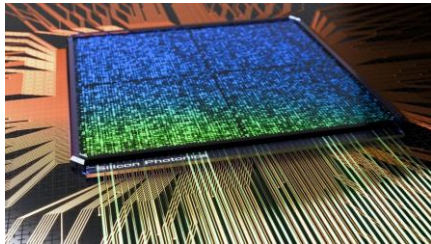


כינוס

המחשבים הקוונטים של היום

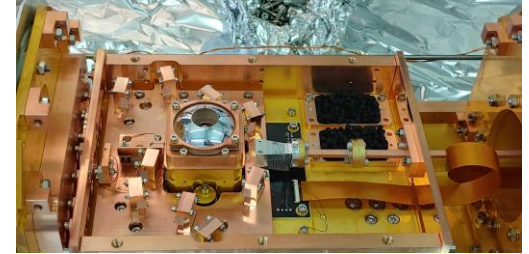


על מוליכים

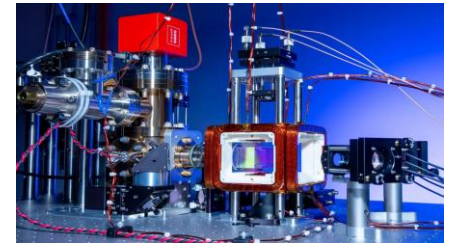


חישוב קוונטי מבוסס אור

- קטנים: 10-100 קיוביטים מול מיליארדי ביטים במחשב קלאסי
- רועשים: יותר מפי מיליארד
- איטיים: פי 10-1000
- יקרים: פי 1000
- עתירי טכנולוגיה



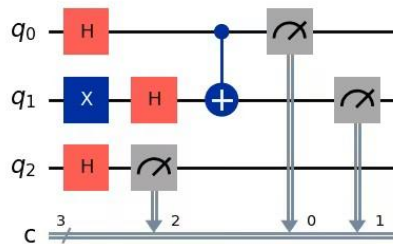
יונים במלכודת



אטומים אדישים וקרים

מה אפשר לעשות עם מחשבים קוונטים היום

+1	+1	+1
+1	-1	-1
-1	+1	?

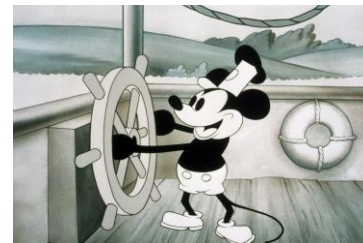


- לשחק
- לחנך
- להדגים יתרונות של מחשב קוונטי מול מחשב קלאסי
- לחקור
- לאתגר





מי מעוניין במחשוב קוונטי?



- אבטחת מידע
- פיזיקאים וכימאים קוונטים
- פרמה, כימיה, ביולוגיה
- מעבדי נתונים גדולים