****

**דרכי פעולה מומלצות**

**היערכות ארגונית לעידן**

**פוסט-קוונטי**

**(Post-Quantum Age)**

מסמך זה נכתב ע"י מערך הסייבר הלאומי לצורך קידום הגנת הסייבר במשק הישראלי. כל הזכויות שמורות למדינת ישראל – מערך הסייבר הלאומי. המסמך נכתב כשירות לציבור. העתקת המסמך או שילובו במסמכים אחרים כפוף לתנאים הבאים: מתן קרדיט למערך הסייבר הלאומי בפורמט המופיע להלן; שימוש בגרסה העדכנית של המסמך; אי הכנסת שינויים במסמך.

המסמך מכיל מידע מקצועי, אשר יישומו בארגון מצריך היכרות עם מערכות הארגון והתאמה למאפייניו בידי איש מקצוע בתחום הגנת הסייבר.

הערות והתייחסויות למסמך ניתן להעביר למייל: tora@cyber.gov.il

נובמבר 2021

**דרכי פעולה מומלצות**

**היערכות ארגונית לעידן פוסט קוונטי**

**(Post-Quantum Age)**

**תוכן עניינים**

[1. מבוא ........................................................................................................3](#_Toc85722825)

[2. מטרות ויעדים 12](#_Toc85722826)

[3. קהל היעד 12](#_Toc85722827)

[4. תיחום המסמך 13](#_Toc85722828)

[5. איומים הנגזרים מתקיפות מבוססות מחשוב קוונטי 13](#_Toc85722829)

[6. דרכי פעולה מומלצות - היערכות ארגונית לעידן פוסט-קוונטי 16](#_Toc85722830)

[7. נספחים 18](#_Toc85722831)

[8. קיצורי שמות וראשי תיבות 22](#_Toc85722832)

[9. מסמכים ישימים 24](#_Toc85722833)

היערכות ארגונית לעידן פוסט-קוונטי

# **מבוא**

* 1. **רקע**

ניתן להניח כי היקף צריכת משאבי המחשוב בעולם יגדל משמעותית בשנים הבאות, וזאת לאור העלייה ברמת המורכבות והיקף בעיות החישוב אשר יידרש לתת להם מענה. בכלל זה ניתן לראות דרישה הולכת וגוברת לשימוש בנְתוּנֵי עָתֵק (Big Data) כמקור להפקת תובנות עסקיות ואחרות, מתן מענה סימולטאני למספר אסטרונומי של פניות/בקשות מהתקנים (דוגמת IoT) ומשתמשים, ודרישה הולכת וגוברת לקבלת מענה מדויק ובזמן אמת (Real Time).

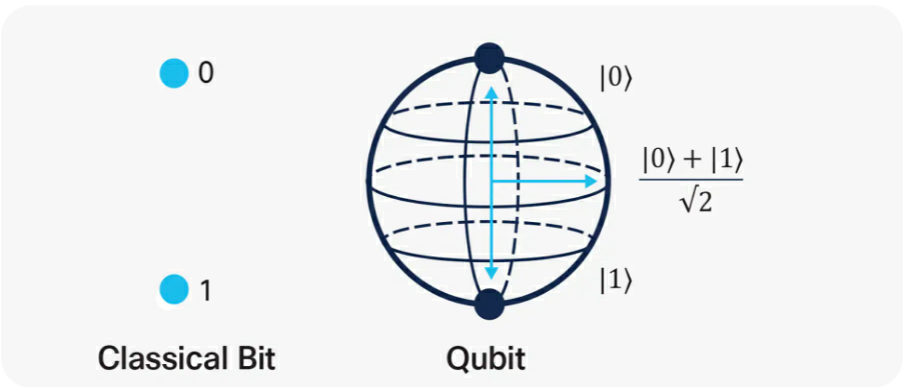
המחשוב המסורתי מבוסס על מערכת ספירה בבסיס בִּינָארִי; שימוש בסיביות[[1]](#footnote-1) לביצוע חישובים. שיטת מחשוב זו סובלת ממגרעות וממגבלות שונות, הבולטות מבניהן הן קיומו של רף פיזיקלי המגביל את צפיפות ומזעור הטרנזיסטורים על גבי שבב הסיליקון (ממנו עשוי המעבד, ובכך מוגבלת יכולת שיפור הביצועים של המחשב), ארכיטקטורת מחשב בעלת חסמי יעילות אלגוריתמיים למשפחה חשובה של בעיות (בפועל ״אינן פתירות״ במדויק ע"י המחשבים הנוכחיים), ואלגוריתמיקה המוגבלת ביעילות בשל הסיבוכיות שלה וזמן הריצה הארוך שלה. מחשוב קוונטי (Quantum Computing) מתעלה ככל הנראה על מגבלות אלו, מאפשר שיפור משמעותי בזיכרון ובכוח החישוב, ומהווה פתרון יעיל של בעיות חישוביות, תוך שימוש בארכיטקטורת מחשב המתבססת על תורת הקוונטים. העקרונות המרכזיים של תורת הקוונטים המאפשרים חישוב מתקדם הם ה״סופרפוזיציה״ המאפשרת חישוב מקבילי על מספר רב של קלטים ו״שזירה״ המשמרת קשר קורלטיבי. עקרונות אלו והשלכתם על אפשרויות המחשוב יוסברו בפירוט בהמשך המסמך. בזכות עקרונות הסופרפוזיציה הקוונטית המתארת הסתברות של מצבים שונים בו-זמנית, השזירות הקוונטית היוצרת קורלציות שאינן אפשריות בסיביות מסורתיות, וההתאבכות הקוונטית המתארת את המבנה הגלי של החומר – תופעות שיוצגו בהמשך – המחשוב הקוונטי עתיד לשנות באופן מהותי את מגמת ההתקדמות של עוצמת המחשוב במחשבים הקיימים היום בשוק, עבור חלק מהמימושים, ולתת יכולות שוברות שוויון מובהקות ביחס ליכולת החישוב המוכרת כיום. שילוב כוחות בין המחשבים הקיימים (״קלאסיים״) לבין מחשבים קוונטיים עשוי לאפשר את ההתכנות שגם המחשבים הקוונטים ישמשו כיחידת חישוב נפרדת להאצת תהליכים במחשבים שאנו מכירים היום בשוק ובכך יאפשרו פריצות דרך רבות משמעותיות.

לפיכך, מדינות וארגונים שונים משקיעים משאבים נכבדים במחקר לכיוון זה, במטרה להשיג עליונות טכנולוגית, שתאפשר עליונות במחקר ובמדע, דוגמת שימוש ביכולות המתקדמות[[2]](#footnote-2) לצורך בעיה מתמטית של ״פירוק לגורמים״ ופתרון של בעיות דיפרנציאליות לטובת ביצוע סימולציות של קיפול חלבונים במסגרת מחקר רפואי, או לצורך בניית מנוע מהיר לחיפוש מידע[[3]](#footnote-3). כל אלו הינם תחומים בהם הוכחה יעילות זמן הריצה של מחשב קוונטי על פני המחשבים והאלגוריתמים הקיימים כיום.

השוני המהותי בין המחשוב המסורתי לבין המחשוב הקוונטי הינו ההסתמכות של הקוונטי על מודל פיזיקלי ייחודי ברמה האטומית, המבוסס על מכניקת הקוונטים (QM - Quantum Mechanics) .

בניגוד למחשוב המסורתי, שבו נעשה שימוש ביחידת העיבוד הבסיסית ״ביט״ (Bit) המאפשרת שני מצבים בלבד– 0 או 1, יחידת העיבוד הבסיסית במחשוב הקוונטי הינה קיוביט[[4]](#footnote-4) (Qubit) (סיבית קוונטית). הקיוביט[[5]](#footnote-5) מתאר יחידת מידע של מידע, אך בנוסף ליכולתו לייצג 1 או 0 לוגים, הוא יכול להיות במצב של סופרפוזיציה קוונטית – אשר משמעותה היא שהקיוביט (חלקיק) נמצא בו-זמנית בשני מצבים. הקיוביט ״בוחר״ את אחד משני המצבים (0 או 1) רק כאשר מבצעים מדידה שלו. עד המדידה, ניתן לשנות את ההסתברויות של הקיוביט להיות במצב ״0״ או במצב ״1״. כלומר, אם מודדים את מצב הקיוביט, יתכן שהוא יהיה בערך 0 בהסתברות מסוימת ובערך 1 בהסתברות המשלימה. בנוסף, הקיוביט עשוי להיות שזור עם קיוביטים אחרים, כפי שיוצג בהמשך. סופרפוזיציה הינה התופעה הבסיסית שביסוד תורת הקוונטים, אשר משלבת למעשה כל מצב בין המצבים 0 ו-1 ומאפשרת לבצע מניפולציות מורכבות, ביניהן היכולת לבצע התאבכות קוונטית של מצבים לקבלת פתרון בזמן ריצה מהיר יותר וזאת לצד היכולת ״לאפס״ הסתברויות לא מעניינות. היכולת לבצע מניפולציה של הסתברויות המצבים של הקיוביט הינה בבסיס יכולת החישוב הקוונטי. הפעלה של סדרת מניפולציית (=אלגוריתם קוונטי) מגדילה את הסיכוי למדידה של התוצאות הרצויות ומורידה (ואף מאפסת) את הסיכוי למדוד את יתר התוצאות האפשריות. בניגוד לביט הקלאסי שמייצג מידע בצורה דיסקרטית ('0' או '1'), קיוביט מייצג את המידע ברצף מצבים הסתברותי. בצורתו הכללית ביותר, מיוצג קיוביט באמצעות קומבינציה לינארית של הערכים '0' ו-'1':

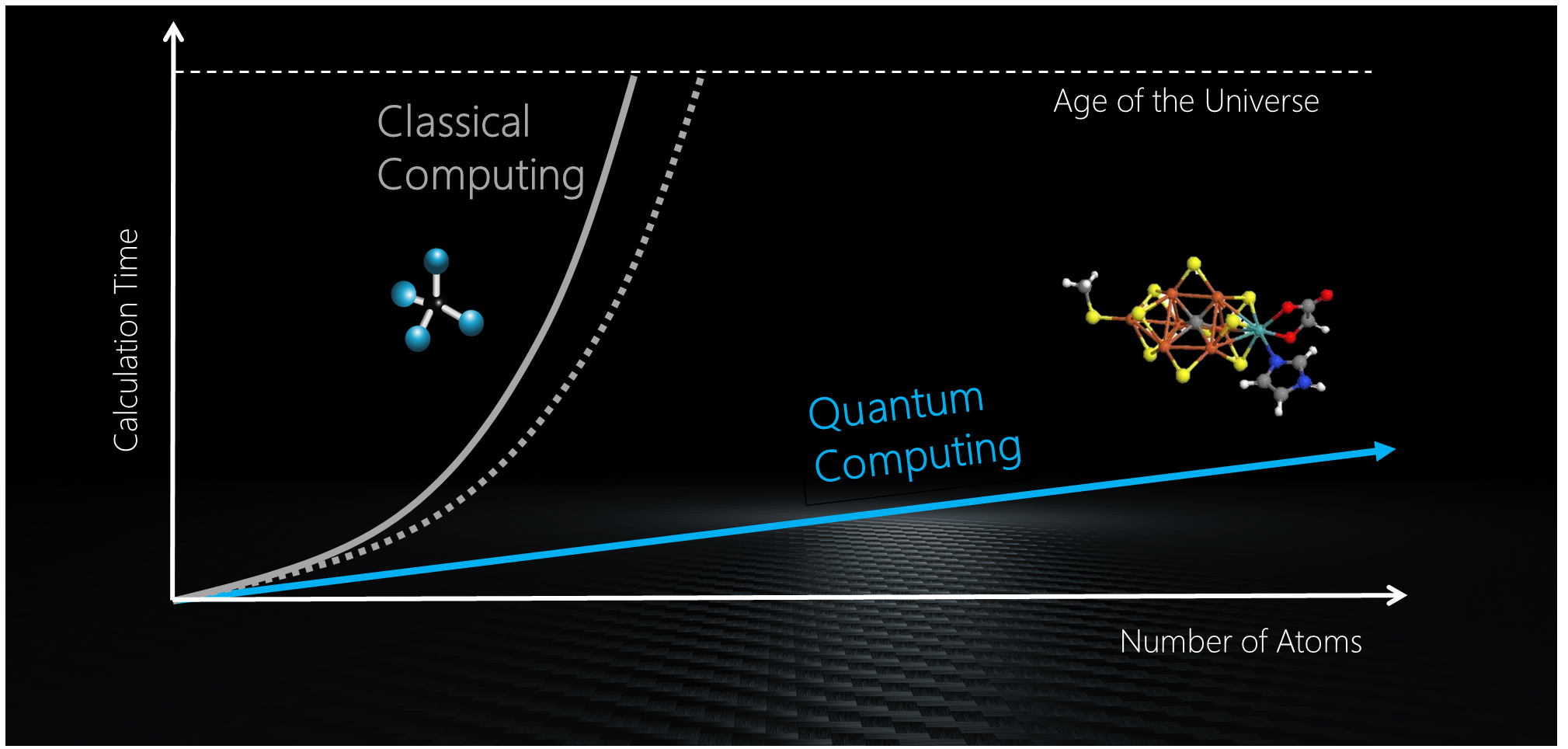
כאשר ו- הם מספרים מרוכבים שמקיימים .

 **תרשים 1:**[[6]](#footnote-6) **קיוביט ביחס לביט המסורתי. בעוד ביט מסורתי מאפשר שני מצבים - 0,1, הקיוביט הקוונטי הפשוט ביותר מאפשר שני מצבים - 0,1 וסופרפוזיציה הסתברותית.**

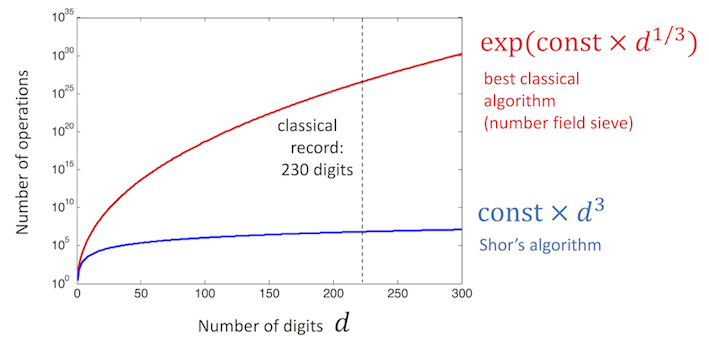
בנוסף, מחשוב קוונטי עושה שימוש בשזירה קוונטית (Quantum Entanglement), המאפשרת יצירת קשר קוונטי חזק גם בין קיוביטים שונים. כלומר, הפעלת פעולה על אחד משני הקיוביטים תשנה את מצבו של הקיוביט האחר באופן המשמר את הקשר הקורלטיבי ביניהם. שני עקרונות יסוד אלו של מכניקת הקוונטים מאפשרים מיקבול רב של תהליך החישוב, כאשר הסופרפוזיציה מאפשר חישוב על מספר מצבים במקביל והשזירה מאפשר חישוב בו זמני על מספר קיוביטים. ראוי לציין כי פעילות מחשוב קוונטי נסמכת על עקרונות פיזיקליים נוספים דוגמת תופעת התאבכות גלים, אך קצרה היריעה מלדון בהם במסמך זה.

כתוצאה משיטת הפעולה הייחודית של מחשוב קוונטי, ישנן בעיות חישוב מסוימות (דוגמת בעיות סיבוכיות/אופטימיזציה) שייתכן שיהיו ניתנות לפתרון על מחשב קוונטי אך אינן ניתנות לפתרון על כל מחשב מסורתי.

תרשים 2 סוקר את ההבדלים בזמני החישוב הנדרשים לשם ביצוע סימולציות דינמיקה של מולקולות גדולות, כאשר ניתן להבחין כי ככל שמספר האטומים במולקולה גדול יותר המחשוב הקוונטי יעיל יותר בזמן החישוב ביחס למחשוב מסורתי (שמגיע לחסם עליון בזמן קצר מאוד):

 **תרשים 2:**[[7]](#footnote-7) **זמני החישוב** **הנדרשים לשם ביצוע סימולציות דינמיקה של מולקולות גדולות. התרשים מלמד כי המחשוב הקוונטי מצליח להתמודד באופן אפקטיבי עם הגדילה במספר האטומים בסימולציה.**

תרשים 3 סוקר את ההבדלים בזמני החישוב הנדרשים לשם ביצוע פירוק לגורמים (Factoring), כאשר ניתן לראות כי זמן החישוב על גבי מחשב מסורתי גבוה משמעותית מזה שעל גבי מחשב קוונטי העושה שימוש באלגוריתם שור (Shor).

 **תרשים 3:**[[8]](#footnote-8) **זמני החישוב הנדרשים לשם ביצוע פירוק לגורמים (Factoring), כאשר ניתן לראות כי זמן החישוב על גבי מחשב מסורתי גבוה משמעותית מזה שעל גבי מחשב קוונטי העושה שימוש באלגוריתם שור (Shor).**

עולם הקריפטוגרפיה (Cryptography) נשען על פתרון בעיות מתמטיות ״מסובכות״ כבסיס לביצוע פעולות אבטחה כדוגמת הצפנת מידע או ביצוע חתימות דיגיטליות. המחשוב הקוונטי עשוי להוות איום ממשי על ארגונים העושים שימוש באלגוריתמים/פרוטוקולים קיימים אשר אינם חסינים בפני מחשוב מסוג זה. יתר על כן, מידע רגיש נאסף כבר כיום לקראת המועד בו ניתן יהיה לפרוץ ולפענח אותו, ועל כן ארגונים ברחבי העולם דורשים שיפור ביכולות ההגנה על המידע שלהם כבר כיום.

להלן מספר דוגמאות הממחישות את האיום מסוג זה:

* ארגונים העושים שימוש בתשתית מפתח ציבורי-פרטי (PKI), המסתמכת על הגנה באמצעות אלגוריתמים כדוגמת RSA או ECC, עשויים להיות חשופים לתקיפות זיוף שדר או פענוח תוכן מוצפן.[[9]](#footnote-9)
* המחשוב הקוונטי עשוי לאפשר פגיעה בסודיות המידע בעת עבודה עם פרוטוקול דיפי-הלמן   
  (Diffie-Hellman), המשמש לשיתוף מפתחות על גבי רשת לא בטוחה.
* השימוש במחשוב הקוונטי חושף גם פגיעויות של אלגוריתם DSA, המשמש בתהליכי חתימה דיגיטלית ובבדיקת תקינותה, אשר עשוי לאפשר לתוקף פוטנציאלי לזייף שדר.
* לבסוף, ישנה אפשרות לקיצור הזמן לפיצוח הצפנה מסוג AES[[10]](#footnote-10), בהתחשב בכך שמספר הצעדים הנדרשים לביצוע הפיצוח במחשב המסורתי הינו 2128 , בעוד שמספר הצעדים הנדרש במחשב קוונטי קטן ל-264. במאמר מוסגר יצוין כי במקרה של AES, שימוש במפתח ארוך יותר (דוגמת bit 256 AESבאופן הפעלה GCM) עשוי במקרים מסוימים לספק מענה אבטחתי הולם בהיבט של עלות מול תועלת לזמן הקרוב.
* מחשב קוונטי יוכל גם לכרות מטבעות וירטואליים בקצב מהיר לעומת קצב הכרייה של מחשב מסורתי, תוך פיצוח אלגוריתם SHA-256 (1282 לעומת 2562), ובכך פוטנציאלית יוכל להפיל את שוק המטבעות הווירטואליים ונתחי השוק שנסמכים על ידיהם.[[11]](#footnote-11)
* עולם המחשוב הקוונטי עושה היום צעדים ראשונים לשבירת פונקציות גיבוב חד-כיווני   
  (OWHF – One-Way Hash Function) על ידי סימולטורים קוונטיים המאפשרים מציאת מינימום מקומי לפונקציה (פתרון מתמטי לפונקציה) בזמן ריצה מהיר[[12]](#footnote-12).

ראוי לציין, כי תיאורטית אין הוכחה לכך שלא ניתן לבצע פעולות אלה גם על מחשב מסורתי, אך לעת הזו לא ידוע אלגוריתם שיכול לעשות זאת בזמן סביר. בנוסף, כפי שיתואר בהמשך, ניתן להשתמש בטכנולוגיות הנסמכות על עקרונות פיזיקליות-קוונטיות לשם החלפת מפתחות קוונטים (למשל QKD/BB84), דבר המעלה את רמת הביטחון בתהליך התקשורת על-גבי תווך שאינו מאובטח. ראוי לציין כי לעיתים התהליך מכונה בציבור בשם ״הצפנה קוונטית״, למרות שמעשית לא נעשה שימוש ביכולות הצפנה לשם אבטחת תהליך החלפת המפתחות.

סביר להניח כי המחשוב הקוונטי לא ייתר את הצורך במחשוב המסורתי, וכי תצורת העבודה העתידית עשויה להיות היברידית (קרי, מחשב אשר כולל מעבד מסורתי לצד מעבד קוונטי).



|  |
| --- |
| אחד האתגרים המהותיים לצד המגן הינה העובדה כי תוקף עשוי לפתח יכולות מחשוב קוונטי מבצעיות ולהפעילן בסתר. לפיכך ארגונים ויחידים עשויים להיות חשופים תקופה ארוכה לאיומים (דוגמת דלף מידע) וזאת ללא ידיעתם.  כמו כן, ניתן ללמוד כי בשנים האחרונות היקף ההשקעות בתחום זה עולה וגובר[[13]](#footnote-13), דבר המעיד כי גורמי מקצוע רבים מניחים כי קיימת סבירות גבוהה לפריצת דרך משמעותית בטווח של פחות מ 10-15 שנה. |

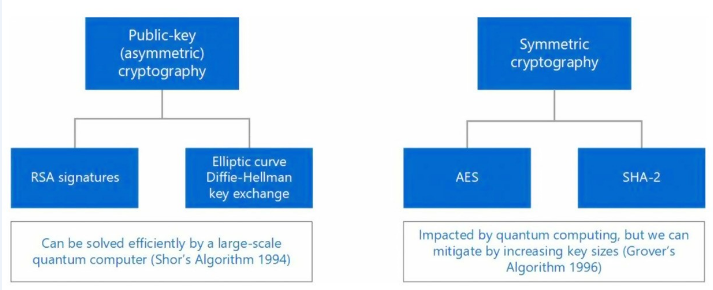
תרשים 4 מציג הערכה כללית אודות לוח הזמנים למעבר ארגונים בעולם לשימוש ביכולות פוסט-קוונטיות. ראוי לציין כי לוח הזמנים עשוי להשתנות בפועל עקב חידושים בתחום או סיבות אחרות.



**תרשים 4:**[[14]](#footnote-14) **הערכה כללית אודות לוח הזמנים למעבר לשימוש ביכולות פוסט-קוונטיות.**

* 1. **אסטרטגיות ההתמודדות עם תקיפות מבוססות מחשוב קוונטי**

ניתן לחלק את אסטרטגית ההתמודדות עם מתקפות מבוססות מחשוב קוונטי הפועלות נגד אלגוריתמים קריפטוגרפים לשני כיוונים עיקריים: האחד, בטווח הקצר - שיפור רמת החסינות של אלגוריתמי/פרוטוקולי קריפטוגרפיה מוכרים, וזאת ע"י הגדלת אורך המפתח, קיצור אורך החיים של המפתח, או אימוץ שיטה אחרת. השני, בראיה רחבה ולטווח הארוך, נדרש להחליף את אלגוריתמי/פרוטוקולי הקריפטוגרפיה   
(PQC – Post-Quantum Cryptography) ולשקול אימוץ טכנולוגיות מתקדמות יותר. יצוין כי ביצוע צעד מסוג זה מחייב תכנון ובחינה מקדימה, וזאת לאור העובדה כי תחום ידע זה חדש, ולפיכך אין ודאות שאימוץ טכנולוגיות חדשות יספק באופן ודאי את רמת החסינות הרצויה.



**תרשים 5: אסטרטגית ההתמודדות עם תקיפות מבוססות מחשוב קוונטי.**

נקדים את המאוחר ונציין כי החלפת/שדרוג תשתית ומערכות עשויה לחייב השקעת משאבים וזמן, ולפיכך מומלץ כי ארגונים שעשויים להיות חשופים משמעותית למתאר איום זה ייערכו בהתאם.

אחד המאמצים הגדולים ביותר לפתרונות בתחום ההצפנה בעידן הפוסט-קוונטי מתבצע על ידי NIST (National Institute of Standards and Technology) , התהליך ארוך במטרה לחפש אחר אלגוריתם שיענה לכלל הצרכים של העידן החדש. החלפת שיטת הצפנה אינה דבר טריוויאלי וזהו תהליך ארוך שייקח מספר שנים שרק בסופם יבחר האלגוריתם המתאים. לאורך הדרך ניתן לראות כיצד אלגוריתמים שנחשבו כחסינים מוכחים כבעלי חולשות, וכי תהליך זה איטי כאשר במקביל הטכנולוגיה והאלגוריתמיקה הקוונטית רק הולכת ומשתפרת. עם זאת, חשוב לזכור שלמרות שכרגע לא ידוע על אלגוריתם קוונטי היכול לפרוץ ביעילות הצפנות סימטריות, או להתמודד עם האלגוריתמים הפוסט-קוונטיים שנשקלים ב-NIST, אין הבטחה שאלגוריתם כזה לא יתגלה בהמשך.

* 1. **הזדמנויות של טכנולוגיות קוונטים בתחום**

האיום המוצג במסמך זה מעלה צורך בשיטת הגנה למניעת דלף מידע אף בעידן שלפני המחשבים הקוונטים, זאת על מנת למנוע האזנה והקלטה של מידע שישמר עד לתקופה בה ניתן יהיה לפענח אותו על בסיס כוח המחשוב העתידי. על אף האיום הגדול שההתפתחות בתחום הקוונטים מציבה בפני היכולת לשמור על מידע מוצפן ומאובטח, קיימת טכנולוגיה מובילה (QKD) בתחום ההגנתי שמדינות רבות החלו לאמץ על מנת לשמור על מתקני תשתיות קריטיות בשטחם.

החלפת מפתחות קוונטית היא טכנולוגיה אשר משתמשת בעקרונות יסוד מתחום הפיסיקה הקוונטית על מנת לאבטח את פרוטוקול החלפת המפתחות הסימטריים. בספרות שיטה זו נקראת QKD – Quantum Key Distribution. קיימים כיום מספר פרוטוקולי QKD שעושים שימוש בתכונות הקוונטיות של האור (לדוגמא) על מנת לאבטח את ערוץ התקשורת מפני האזנה של גורם שלישי לא רצוי. QKD מאפשרת לשני צדדים לחלוק מפתח סימטרי מאובטח, ללא צורך בהחלפת מידע קודם. הטכנולוגיה הקיימת היום בשוק מתבצעת ברובה על בסיס סיבים אופטיים, אך יש התקדמות מהירה ופורצת דרך בתחום לתקשורת בתווך חופשי (Free-Space). מדינות רבות משקיעות היום מאמצים רבים בבניית רשתות מתאימות בין תשתיות קריטיות עליהן הן רוצות להגן.

אחד העקרונות הקוונטיים עליו מבוססים פרוטוקולי ה-QKD השונים הוא שמדידה של מצב קוונטי משנה אותו, ולכן ניתן לזהות את ביצוע המדידה על הקיוביט. בשילוב עם עקרונות קוונטיים נוספים (דוגמת עקרון   
״אי-השכפול״, אשר לא נרחיב עליו במסמך זה) ההצפנה הקוונטית מאפשרת לזהות מאזינים בערוץ, ולשערך את כמות המידע שדלף. באמצעות שיטות שונות מתורת האינפורמציה, ניתן לצמצם מידע שדלף למאזין, או לבחור לנטוש את הפרוטוקול במקרה ודלף מידע בהיקף חריג. מאחר והמידע שעובר בערוץ הקוונטי משמש להחלפת מפתחות הצפנה בלבד, אין נזק ממשי בדליפת מידע למאזין, שכן למפתח אין ערך עד שנבחר להשתמש בו, וכפי שצוין, אם דלף מידע בהיקף חריג, ניתן לבחור לזרוק את המפתח.

בשלב זה, עקב קצב התקשורת האיטי של מערכות QKD, נעשה בהן שימוש לטובת סנכרון מפתחות סימטריים (דוגמת AES). שימוש ב-QKD חוסך את הצורך להסתמך על מפתחות מבוססי קריפטוגרפיה א-סימטרית (דוגמת RSA), אשר נחשבים כפגיעים למחשוב קוונטי. יחד עם זאת, קצב התקשורת גדל משמעותית בשנים האחרונות, וניתן לצפות לפריצה בתחום[[15]](#footnote-15).

חשוב לציין שהחלפת מפתחות קוונטית מספקת חסינות תאורטית מלאה מפני מתקפה, אך רק בתנאי שהמימוש שלה מושלם. מאחר וכל מימוש הנדסי יכיל פגמים ואי-יעילויות, מתאפשרות מתקפות שונות על מערכות החלפת מפתחות קוונטית[[16]](#footnote-16). עם זאת, חלק גדול מהמתקפות דורשות מהמאזין גישה פיזית למערכות הקצה או למגברי אותות בדרך (בניגוד להתקפה על מערכת קלאסית, בה גישה לערוץ התקשורת מספקת), ולכן מימושן של מתקפות מסוג זה קשה משמעותית. בשל עובדה זו, רצוי לבחון שילוב מערכות החלפת מפתחות קוונטית (״הצפנה קוונטית״) עם מערכות הצפנה קלאסיות, ולא להסתמך על ההגנה התיאורטית שמספקת ההצפנה הקוונטית בלבד.

ראוי לציין כי ארגונים שיחלו כיום לבחון אימוץ של שיטות עבודה הכוללות שימוש במחשוב קוונטי עשויים להשיג יתרון בעתיד ביחס למתחרים עסקיים שלא עשו כן, דוגמת פיתוח מוצרים ושירותים חדשים או שיפור היעילות של מוצרים ושירותים קיימים.

# **מטרות ויעדים**

מסמך זה מציג דרכי פעולה מומלצות להיערכות ארגונית לעידן פוסט-קוונטי.

# **קהל היעד**

מסמך זה נכתב עבור מנהל הגנת הסייבר בארגון (CISO), מוסמך מתודולוגיות הגנת סייבר, מוסמך מיישם הגנת סייבר, מוסמך טכנולוגיות הגנת סייבר (ארכיטקט הגנה בסייבר), ואנשי תקשורת נתונים/תקשוב/IT SYSTEM.

גורמים נוספים אשר עשויים להפיק תועלת ממסמך זה הם מנהלי מערכות המידע (CIO – Chief Information Officer), מהנדסי מערכת, מנהלי פיתוח ומחקר (R&D), מנהלי טכנולוגיות ראשיים (CTO), וגורמים עסקיים הנדרשים לאשר את הערכת הסיכונים של נכס הסייבר/התהליך העסקי.

# **תיחום המסמך**

מסמך זה מתמקד בדרכי פעולה מומלצות לשיפור היערכות ארגונית לעידן פוסט-קוונטי.

ראוי לציין כי המסמך אינו מרחיב בנושאים שלגביהם מערך הסייבר הלאומי כתב ופרסם מסמכים ייעודיים. דוגמה לנושא מסוג זה הינה הגנה פרטנית על מערכת ותשתית, דבר הזוכה למענה במסגרת מסמך *תורת ההגנה בסייבר לארגון* אשר נכתב ופורסם על-ידי מערך הסייבר הלאומי.

# **איומים הנגזרים מתקיפות מבוססות מחשוב קוונטי**

פרק זה סוקר את האיומים העיקריים הנגזרים מתקיפות מבוססות מחשוב קוונטי, כמפורט להלן:

|  | שם האיום |  | תיאור | |
| --- | --- | --- | --- | --- |
|  | דלף מידע  (Data Leakage) | | | 1. תוקף עשוי לבצע הקלטה של תעבורה מוצפנת, ולפענח אותה בעת זמינות מחשוב קוונטי. 2. תוקף עשוי לגשת למידע מוצפן (דוגמת גניבת מחשב נייד אשר הדיסק שלו מוצפן), ולפענח את ההצפנה בעת זמינות מחשוב קוונטי. 3. תוקף אשר יש ברשותו כיום יכולות מבצעיות של מחשוב קוונטי עשוי לממש את התקיפות לעיל כבר כיום. |
|  | זיוף חתימה דיגיטלית/אלקטרונית | | | 1. תוקף עשוי לזייף חתימות דיגיטלית/אלקטרונית, ובכך לפגוע במהימנות רשומות דיגיטליות רגישות/חסויות קיימות. 2. תוקף עשוי ״לשבור״ בלוקצ׳יין (Blockchain) ולשנות רשומות קיימות ללא ידיעת המשתמשים, או ליצור הסתעפות לא מתוכננת בשרשרת קיימת (New Fork). במקרה זה הדבר עשוי להשפיע על תוקף/קבילות חוזים דיגיטליים, ושירותים נוספים אשר מסתמכים על טכנולוגיה זו. 3. תוקף עשוי לזייף חתימה דיגיטלית/אלקטרונית ולחתום על מסמך בשמו של אדם אחר, ללא ידיעתו והסכמתו. 4. תוקף עשוי לזייף חתימה דיגיטלית/אלקטרונית ולחתום על רכיב תוכנה זדוני, וזאת תוך יצירת מצג שווא למגן כי מדובר ברכיב אותנטי (Authenticity). סוגיה זו מהותית בעת שימוש ב- FOTA\SOFA או ממשק אחר לקבלת עדכונים מרחוק (Remote Update). |
|  | תקיפת אדם מתווך (MiTM) | | | בתווך מידע ״קלאסי״, תוקף עשוי לנצל נגישות לתעבורת נתונים בין שני צדדים ויכולת לפענח אותה לשם הזרקת קוד זדוני לתוכה או לשנותה. לאור העובדה כי ביכולת התוקף לחתום על שדרים, הצד המגן עשוי להתקשות בגילוי ובזיהוי של התקיפה, ולפיכך לא יוכל לסכלה לפני שתגרום נזק לארגון. |
|  | התכחשות לפעולה (Repudiation) | | | משתמש אשר ביצע פעולה (דוגמת העברת כסף) עשוי לטעון בדיעבד כי לא ניתן לסמוך על האמצעים הקריפטוגרפיים המשמשים לאימות הפעולה. |
|  | מימוש לקוי של שיטת קריפטוגרפיה | | | תוקף עשוי לנצל לרעה מימוש לקוי של שיטת קריפטוגרפיה חדשה בנכס סייבר של הארגון, ובכך לפגוע בסודיות, במהימנות, בשלמות, ויתכן שאף בזמינות של המידע הארגוני. |
|  | שבירת פונקציות גיבוב חד-כיוונית (OWHF) | | | 1. התקפת התנגשות (Collision Attack) – תוקף עשוי ליצור שני פרטי מידע (דוגמת קבצים) בעלי ערך פונקציית גיבוב חד-כיווני זהה. ראוי לציין כי שכיח לראות נוזקות מתקדמות עושות שימוש בטכניקה זו לשם התחמקות מגילוי וזיהוי (Anti-Evasion Technique). 2. התקפה לפני תמונה (Preimage Attack) – תוקף עשוי למצוא את הקלט המקורי שאפשר הפקה של ערך פונקציית גיבוב חד-כיווני. כלומר, התקפה זו עשויה במקרים מסוימים לגרום לדלף מידע רגיש/חסוי. 3. התקפה לפני תמונה שנייה (Second-Preimage Attack) - תוקף עשוי למצוא את הקלט הספציפי שמייצר את אותו ערך פונקציית גיבוב חד-כיווני של קלט אחר, שאותו הוא כבר מכיר. כלומר, התקפה זו עשויה במקרים מסוימים לגרום לדלף מידע רגיש/חסוי. |
|  | כרייה ״לא הוגנת״ של מטבע וירטואלי | | | תוקף עשוי לכרות מטבע וירטואלי ביכולת עולה לעין שיעור על עמיתים ללא יכולת קוונטית, ובכך להטות באופן זדוני את הכף לטובתו. |
|  | מימוש לקוי של פרוטוקול QKD | | | תוקף עשוי לנצל לרעה מימוש לקוי של החלפת המפתחות על ידי פרוטוקול QKD בנכס סייבר של הארגון, ובכך לחשוף מפתחות הצפנה שבשימוש של הארגון מבלי להתגלות. |

**טבלה 1: איומים עיקריים הנגזרים מתקיפות מבוססות מחשוב קוונטי**

להלן דוגמאות של תחומים אשר עשויים להיות חשופים באופן מהותי לאיומים ממחשוב קוונטי:

• Public Key Infrastructure (PKI)

• Key Management Systems

• Authenticated Web Communication (TLS)

• Secure Point-to-Point (SSH)

• Transport Security (Osc)

• Key Agreement

• Identification and Authentication

• Password-Authenticated Key Exchange (PAKE)

• PGP/GPG

• Secure/Multipurpose Internet Mail Extensions (S/MIME)

• Over-the-Air Rekeying (OTAR)

• Domain Name System Security Extensions (DNSSEC)

• Encrypted File System

• Internet Key Exchange (IKE)

• ZRTP (Secure VoIP Protocol D1)[[17]](#footnote-17)

# **דרכי פעולה מומלצות - היערכות ארגונית לעידן פוסט-קוונטי**

פרק זה מציג רשימה של דרכי פעולה מומלצות, שמימוש נכון שלהן יסייע בהיערכות ארגונית לעידן פוסט-קוונטי, כמפורט להלן:

| מס' | ההמלצה | סטאטוס (בוצע/לא בוצע) |
| --- | --- | --- |
| פעולות מומלצות לביצוע על ידי הארגון בטווח זמן קצר | | |
| 1 | מיפוי נכסי הסייבר הארגוניים. **נספח 2** מכיל דוגמא למיפוי בסיסי. |  |
| 2 | סקירת סיכונים וניתוח המשמעויות הנגזרות מקיום תקיפות באמצעות מחשוב קוונטי. |  |
| 3 | ניתוח המשמעויות הנגזרות משינוי תצורת העבודה לתמיכה באלגוריתמים/ פרוטוקולים חסינים מפני מחשוב קוונטי. **נספח 3** מכיל דוגמא לשאלות מנחות. |  |
| 4 | מעקב אחר פרסומים אודות ההתפתחויות בתחום המחשוב הקוונטי, לשם שיפור איכות תהליך ניהול הסיכונים וניתוח משמעויות נגזרות. בכלל זה, מומלץ לבחון באופן עתי את תקני ארגון NIST בתחום הקריפטוגרפיה. |  |
| 5 | עיגון משפטי מול ספקי מיקור חוץ/יצרניות תוכנה של הדרישה כי המוצרים יכילו יכולת מובנית לשדרוג יכולות קריפטוגרפיות מתקדמות, וזאת ללא ביצוע שינויים מהותיים (Crypto Agility). |  |
| 6 | במקרה שהארגון עוסק בפיתוח של תשתית ומערכות - ווידוא תמיכה מובנית במוצר המתבטאת ביכולת לבצע שדרוג יכולות קריפטוגרפיות מתקדמות, וזאת ללא ביצוע שינויים מהותיים (Crypto Agility). יש לתת את הדעת שבמקרים מסוימים זמן הפיתוח והבדיקות עשוי להיות ארוך מהמקובל בארגון. |  |
| 7 | בחינת שימוש ביכולות מובנות בתשתית ובמערכות הקיימות לשם צמצום החשיפה האפשרית לאיומים של מחשוב קוונטי.  להלן דוגמאות ליישום:   1. שימוש במפתחות ארוכים יותר (דוגמת AES 256 Bit, SHA 512 Bit בתצורת עבודה GCM). 2. קיצור אורך החיים של מפתח (לרבות Session Key). 3. שימוש במנגנון סודיות מושלמת קָדימה (PFS - Perfect Forward Secrecy). 4. קביעת זמן המתנה בין איטרציות במהלך גישה לנכסי סייבר. 5. שימוש באמצעים מקובלים לגילוי וזיהוי האזנה (Eavesdropping Attack), לרבות שימוש באמצעים פיזיים לאבטחת התווך. 6. הוספת ״רעש לבן״ לתעבורה המשונעת בתווך, דוגמת שינוע במקביל של מידע רגיש/חסוי ומידע פומבי או שימוש ברִפּוּד תַּעֲבוּרָה (Padding) אקראי לחבילות מידע רגיש/חסוי. 7. ניתוק פיזי/לוגי מהרשת של נכסי סייבר אשר לא ניתן לשפר את חוסן הפרוטוקולים/האלגוריתמים שלהם. 8. שימוש ב״הצפנה מאומתת״ (Authenticated Encryption). |  |
| 8 | בחינת עירוב טכנולוגיות ואלגוריתמים נוספים וזאת במטרה להעלות את מספר שכבות ההגנה האפשריות ולהוריד את סיכויי הכשל / ההצלחה של תקיפה.  דוגמא ליישום: שימוש בשתי שכבות הצפנה בלתי תלויות, כאשר כל שכבה תעשה שימוש באלגוריתם הצפנה שונה, ומפתח ייעודי; (IEEE 802.1AE) MACsec  ו-TLS. |  |
| 9 | הנחיית צוות הפיתוח לדאוג לכך שהמוצרים המפותחים יעשו שימוש לפי הצורך בפרוטוקולים/אלגוריתמים החסינים בפני מחשוב קוונטי (PQC), על פי המלצות  ה- NISTהרלוונטיות באותו הזמן ולפי העניין. |  |
| פעולות מומלצות לביצוע בטווח זמן ארוך יותר | | |
| 1 | עיגון משפטי מול ספקי מיקור חוץ/יצרניות תוכנה של הדרישה כי המוצרים מטעמם יעשו שימוש בפרוטוקולים/אלגוריתמים החסינים בפני מחשוב קוונטי. |  |
| 2 | בחינת אמצעי אבטחה העושים שימוש בטכנולוגיות קוונטיות. בפרט שימוש בפרוטוקול (QKD) על בסיס תקשורת קוונטית **להחלפת מפתחות**. תוך כדי יש לתת את הדעת לערוצי צד קלאסיים הקיימים גם בהחלפת מפתחות קוונטית הפגיעים להתקפות (וזאת תוך הכרה כי לא ניתן להגיע לשלמות ברמת הביטחון).  ניתן לשפר את רמת הביטחון באמצעות מספר שיטות, דוגמת:   1. אימוץ סכמות מתקדמות דוגמת Decoy States. 2. שימוש ב- Qudit(יחידה חישובית מרובת מימדים כחלופה לקיוביט דו-ממדי).[[18]](#footnote-18) |  |
| 3 | קידום יכולות מחקר ופיתוח (R&D – Research and Development) רלוונטיות בארגון. |  |
| 4 | בחינת שימוש ב- Quantum Fingerprints'’ לשם אימות חד-ערכי של זהות נכס סייבר או לשם גילוי וזיהוי הטמנות (Implant/Hardware Trojan) או רכיבים אלקטרונים מזויפים (Counterfeit).[[19]](#footnote-19) |  |
| 5 | מעבר לשימוש במחוללי מספרים רנדומאליים מסוג QRNG (Quantum Random Number Generators). יש לתת את הדעת כי מפתחות אשר מבוססים על אלגוריתמים חסינים בפני מחשוב קוונטי עשויים להתבסס על מספר רב יחסית של מספרים רנדומאליים או שיעלה הצורך להבטיח רמת אנטרופיה גבוהה של כל מספר רנדומאלי. |  |

**טבלה 2: דרכי פעולה מומלצות - היערכות ארגונית לעידן פוסט-קוונטי**



|  |
| --- |
| יש לתת את הדעת על כך שבארגונים רבים אורך החיים של מידע רגיש/חסוי עשוי לנוע בין שנים בודדות לעשרות שנים, אם לא מאות. לאור זאת, גם אם אין לתוקף יכולת תקיפה אפקטיבית כיום, הוא יוכל בעתיד לפענח מידע מוצפן או לזייף חתימה, ובכך התוקף יוכל להגיע להישג משמעותי. |



|  |
| --- |
| ניתן לראות כי כבר כיום מחשוב קוונטי ברמת אב-טיפוס (פרוטוטיפ) מוצע כמודל שירות בענן QCaaS (Quantum Computing as a Service), כך שתוקפים פוטנציאליים אינם חייבים לפתח יכולות עצמאיות, והם עשויים לרכוש שירות כחלופה. ראוי לציין שאב הטיפוס המוצע כיום רחוק מיכולות הביצוע המוזכרות במסמך זה. |

# **נספחים**

**נספח 1 – היערכות ארגונית לעידן פוסט-קוונטי**

**מטרת הנספח**

לשקף לקורא את אופן פיתוח המסמך, לציין את הגורמים המעורבים בתהליך כתיבתו, ובהעברת משוב על התכנים שלו, לצורך הבטחת שקיפות התהליך וגילוי נאות של הגורמים המעורבים בביצועו.

1. **כיצד גובש המסמך - סקר שוק/סילבוס/השוואה בעולם**
   * + 1. בחינה של תיעוד/תקינה מהעולם כגון NIST ו-ISO (דוגמאות עיקריות מוצגות במסמך בפרק ״מסמכים ישימים״).
       2. בחינה של פרסומים מקובלים בתחום (דוגמאות עיקריות מוצגות במסמך בפרק ״מסמכים ישימים״).
       3. קבלת משוב מהציבור לטיוטות המסמך אשר פורסמו:
2. Triarii Research Ltd
3. Check Point Software Technologies Ltd.
4. IBM
5. Classiq Technologies
6. Cisco Systems
7. Nvidia (Mellanox Technologies)
8. D-Wave Systems
9. הטכניון - מכון טכנולוגי לישראל
10. אוניברסיטת תל-אביב
11. אוניברסיטת בר-אילן
12. אוניברסיטת בן גוריון
13. אוניברסיטת חיפה
14. ד״ר שי הרשקוביץ, עמית מחקר בכיר במכון לחקר המודיעין
15. עו"ד חגי מטלון (CISO)

**נספח 2 – דוגמא למיפוי נכסי סייבר**

**מטרת הנספח**

עזר לביצוע מיפוי מצב קיים של נכסי הסייבר בארגון.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| מס' | שם נכס הסייבר | אורך חיים של מידע שהוצפן במנוחה | אורך חיים של מידע שהוצפן בעת שינוע | אורך חיים של מידע שהוצפן בעת עיבוד | תדירות החלפת מפתח | סוג וגרסת פרוטוקול/ אלגוריתם הצפנה | סוג וגרסת פרוטוקול/ אלגוריתם גיבוב חד-כיווני (Hash) |
| 1 | שרת Web | n/a | שעה | n/a | מפתח פעילות פעם בשעה  מפתח פרטי של תעודה דיגיטלית פעם בשנתיים | פרוטוקול TLS גרסה 1.2 + 1.3  אלגוריתם הצפנה אסימטרית – RSA 2,048  אלגוריתם הצפנה סימטרית – AES 256 Bit | SHA 256 Bit |
| 2 | שרת DB | 20 שנה | שעה | שעה | מפתח פעילות פעם בשעה  מפתח פרטי של תעודה דיגיטלית פעם בשנתיים | פרוטוקול הצפנה ייעודי של היצרן  אלגוריתם הצפנה אסימטרית – RSA 2,048  אלגוריתם הצפנה סימטרית – AES 256 Bit | SHA 256 Bit |
| 3 | שרת VPN | n/a | שעה | n/a | מפתח פעילות פעם בשעה  מפתח פרטי של תעודה דיגיטלית פעם בשנתיים | פרוטוקול הצפנה ייעודי של היצרן  אלגוריתם הצפנה אסימטרית – RSA 2,048 Bit  אלגוריתם הצפנה סימטרית – AES 256 Bit | SHA 256 Bit |
| 4 | מחשב נייד | 10 שנים  אמצעי אחסון ניידים: 100 שנה  רכיבי IoT: 100-  1000 שנה | שעה | n/a | מפתח פעילות פעם בשעה  מפתח פרטי של תעודה דיגיטלית פעם בשנתיים | פרוטוקול הצפנה ייעודי של היצרן  אלגוריתם הצפנה אסימטרית – RSA 2,048 Bit  אלגוריתם הצפנה סימטרית – AES 256 Bit | SHA 256 Bit |

**טבלה 3: דוגמא למיפוי נכסי סייבר**

**נספח 3 – דוגמא לשאלות מנחות**

**מטרת הנספח**

עזר לביצוע תשאול אודות משמעות המעבר לתצורת עבודה התומכת באלגוריתמים/פרוטוקולים החסינים בפני מחשוב קוונטי.

|  |  |  |
| --- | --- | --- |
| מס' | השאלה | התשובה |
| 1 | מתי יצרן/ספק נכס הסייבר מתחייב לספק תמיכה באלגוריתמים/פרוטוקולים החסינים בפני מחשוב קוונטי?  מהו המימוש שנבחר על ידי היצרן/הספק? |  |
| 2 | האם בעקבות השינוי בתצורת העבודה תהיה פגיעה בביצועים או בקיבולת נכסי הסייבר של הארגון? |  |
| 3 | האם ברשות הארגון את הידע המקצועי למתן מענה לסוגיות בתחום הקריפטוגרפיה?  אם לא, האם לארגון קיימת התקשרות עם גורם חיצוני אשר יוכל לספק מענה בנושא? |  |
| 4 | מהי רמת התאימות של נכסי הסייבר של הארגון לעבודה בתצורה החדשה (דפדפנים, מערכות הפעלה, וכד')? |  |
| 5 | האם הארגון עושה שימוש בספריות קוד פתוח (Open Source) המתמחות בקריפטוגרפיה? אם כן, האם ומתי הספרייה תכיל מענה לאלגוריתמים התומכים בתצורת העבודה החדשה? |  |
| 6 | מהי רמת התאימות של נכסי הסייבר של לקוחות הארגון לעבודה בתצורה החדשה (דפדפנים, מערכות הפעלה, וכד')? |  |
| 7 | האם נדרשת תאימות לאחור בעבודה? אם כן, לאיזו תקופה? |  |
| 8 | האם ישנו צורך לפענח מידע מוצפן הקיים בארגון, ולאחר מכן להצפינו מחדש ע"י אלגוריתם החסין בפני מחשוב קוונטי? אם כן, מהי משמעות ביצוע התהליך? |  |
| 9 | כיצד ניתן לשלב פרוטוקול QKD בתשתית הקיימת כשכבת הגנה נוספת או מחליפה? |  |

**טבלה 4: דוגמא למיפוי נכסי סייבר**

# **קיצורי שמות וראשי תיבות**

הפרק מציג את קיצורי השמות וראשי התיבות בהם נעשה שימוש במסמך זה.

| שם המונח | ביאור |
| --- | --- |
| דוא"ל | דואר אלקטרוני |
| ACID | Atomicity, Consistency, Isolation, Durability |
| ACL | Access Control List |
| AES | Advanced Encryption Standard |
| API | Application Programming Interface |
| CTO | Chief Technology Officer |
| DLP | Discrete Logarithm Problem |
| DNSSEC | Domain Name System Security Extensions |
| DSA | Digital Signature Algorithm |
| EAL | Evaluation Assurance Level |
| ECC | Elliptical Curve Cryptography |
| ECDH | Elliptic-curve Diffie–Hellman |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| FOTA | Firmware Over-The-Air |
| GCM | Galois/Counter Mode |
| GPG | GNU Privacy Guard |
| HSM | Hardware Security Module |
| HTTP | Hypertext Transfer Protocol |
| IEEE | Institute of Electrical and Electronics Engineers |
| IFP | Integer Factorization Problem |
| IKE | Internet Key Exchange |
| IoT | Internet of Things |
| KMS | Key Management Server |
| MACsec | Media Access Control security |
| MiTM | Man-in-the-Middle Attack |
| NIST | (US) National Institute of Standards and Technology |
| OTAR | Over-the-Air Rekeying |
| OWHF | One way hash function |
| PAKE | Password-Authenticated Key Exchange |
| PFS | Perfect forward secrecy |
| PGP | Pretty Good Privacy |
| PKI | Public Key Infrastructure |
| PQC | Post-Quantum Cryptography |
| QCaaS | Quantum Computing as a Service |
| QKD | Quantum Key Distribution |
| QM | Quantum Mechanics |
| QoS | Quality of Services |
| QRNG | Quantum Random Number Generators (QRNG) |
| R&D | Research and Development |
| RSA | Ron Rivest, Adi Shamir, and Leonard Adleman |
| S/MIME | Secure / Multipurpose Internet Mail Extensions |
| SHA | Secure Hash Algorithm |
| SLA | Service Level Agreement |
| SOD | Segregation of Duties |
| SOTA | Software Over-The-Air |
| SSH | Secure Shell \ Secure Point-to-Point |
| SSL | Transport Layer Security |
| TLS | Secure Sockets Layer |
| TTL | Time to Live |
| VPN | Virtual Private Network |

**טבלה 5: קיצורי השמות וראשי התיבות בהם נעשה שימוש במסמך זה**

# **מסמכים ישימים**

פרק זה מכיל את מקורות המידע עליהם הסתמכו הכותבים בעת כתיבת המסמך.

**מקורות מידע בעברית:**

**מערך הסייבר הלאומי**

אונא, יגאל. (2019). הגנת מרחב הסייבר הלאומי. *סייבר, מודיעין וביטחון*, *3*(1), 147–152. https://www.inss.org.il/he/wp-content/uploads/sites/2/2019/06/Cyber3.1HEB\_e-1.pdf.

*חיזוק זיהוי משתמשים במערכות ותשתיות של ארגונים ע"י שימוש באימות רב-גורמי (MFA).* מערך הסייבר הלאומי (מאי 2020).  
 https://www.gov.il/he/departments/general/mfa

*תורת ההגנה בסייבר לארגון*. מערך הסייבר הלאומי (אפריל 2018).  
https://www.gov.il/he/departments/policies/cyber\_security\_methodology\_for\_organizations

*תפיסה לאומית בסייבר להיערכות ולניהול מצבי משבר*. (נובמבר 2018).  
https://www.gov.il/he/Departments/news/cybercrisispreparedness

*שאלון ספקים לחיזוק שרשרת האספקה*. (מאי 2020).  
https://www.gov.il/he/departments/news/querysupply

מדיניות לאומית להזדהות בטוחה. (מאי 2018).  
https://www.gov.il/he/departments/news/bio\_safeidpolicy

**כללי**

קירזנר, אופק. 2021. *מחשוב קוונטי: ים של הזדמנויות, ים של קשיים*. גיקטיים.  
<https://www.geektime.co.il/quantum-computing-software-development/amp/>

אלכסנדרוביץ׳, גדי. 2019. *אז מה זה מחשב קוונטי?* לא מדויק.  
<https://gadial.net/2019/02/11/what_is_quantum_computer/>

הרשקוביץ, שי (ד״ר). *כיצד מחשבים קוונטיים יעצבו את הבטחון הלאומי?.* המכון לחקר המתודולוגיה של המודיעין   
<https://www.intelligence-research.org.il/userfiles/banners/Zarkor%20-%2025.pdf>

שורש, דוד. ״אסטרטגיה בעידן הבינה המלאכותית, תהליך תכנון אסטרטגי למגמות טכנולוגיות משבשות״. *בין הקטבים* 18(דיגיטל 2.0).  
https://www.idf.il/media/44662/%D7%90%D7%A1%D7%98%D7%A8%D7%98%D7%92%D7%99%D7%94-%D7%91%D7%A2%D7%99%D7%93%D7%9F-%D7%94%D7%91%D7%99%D7%A0%D7%94-%D7%94%D7%9E%D7%9C%D7%90%D7%9B%D7%95%D7%AA%D7%99%D7%AA-%D7%93%D7%95%D7%93-%D7%A9%D7%95%D7%A8%D7%A9.pdf

**חקיקה**

תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017

חוק הגנת הפרטיות, תשמ"א-1981

חוק חתימה אלקטרונית תשס"א-2001

חוק הארכיונים, תשט"ו-1955

General Data Protection Regulation (GDPR)

PCI Standard

**מקורות מידע באנגלית:**

**General**

Batraski, E. (2018, October 5). *A radical new paradigm in quantum computing, Venrock's investment into Atom Computing.* Venrock. Retrieved from https://www.venrock.com/radical-new-paradigm-quantum-computing-venrocks-investment-atom-computing/

Bernhardt, C. (2020). *Quantum computing for everyone*. The MIT Press.

Carlson, J., Dean, D. J., Hjorth-Jensen, M., Kaplan, D., Preskill, J., Roche, K., Savage, M. J., & Troyer, M. (n.d.). *Institute For Nuclear Theory Report*, 18(008). Retrieved from https://www.int.washington.edu/PROGRAMS/17-66W/QuantumComputing\_NUCLEARPHYSICS\_FINAL\_pdf.pdf.

CB Insights. (2021, September 3). *What is Quantum Computing? Definition, Industry Trends & Benefits Explained.* CB Insights Research. Retrieved from https://www.cbinsights.com/research/report/quantum-computing/

Engdahl, S. (2008). *Exploring quantum error mitigation with Mitiq and Amazon Braket.* Amazon. Retrieved from https://aws.amazon.com/blogs/quantum-computing/exploring-quantum-error-mitigation-with-mitiq-and-amazon-braket/

Engdahl, S. (2008). *Post-quantum TLS now supported in AWS KMS*. Amazon. Retrieved from https://aws.amazon.com/blogs/security/post-quantum-tls-now-supported-in-aws-kms/

Engdahl, S. (2008). *Round 2 post-quantum TLS is now supported in AWS KMS*. Amazon. Retrieved from https://aws.amazon.com/blogs/security/round-2-post-quantum-tls-is-now-supported-in-aws-kms/

Gallagher, R. (2021, February 7). *A Swiss Company Says It Found Weakness That Imperils Encryption.* Bloomberg.com. Retrieved from https://www.bloomberg.com/news/articles/2021-02-07/a-swiss-company-says-it-found-weakness-that-imperils-encryption

Gerhardt, I., Liu, Q., Lamas-Linares, A., Skaar, J., Kurtsiefer, C., & Makarov, V. (2012, March 18). *Full-Field Implementation of a Perfect Eeavesdropper on a Quantum Cryptography System*. arXiv.org. Retrieved from https://arxiv.org/abs/1011.0105

Gibney, E. (2019, October 2). *Quantum Gold Rush: The Private Funding Pouring into Quantum Start-Ups.* Nature News. Retrieved from https://www.nature.com/articles/d41586-019-02935-4

Goled, S. (2021, May 23). *Top Countries Pumping Money into Quantum Computing Technology*. Analytics India Magazine. Retrieved from https://analyticsindiamag.com/top-countries-pumping-money-into-quantum-computing-technology

Grumbling, E., & Horowitz, M. (Eds.). (2019). *Quantum Computing: Progress and Prospects.* The National Academies Press. Retrieved from https://www.nap.edu/download/25196

ISARA Corporation. (n.d.). *Managing cryptographic and Quantum Risk*. ISARA Corporation. Retrieved from https://www.isara.com/resource-center/managing-cryptographic-and-quantum-risk.html

Krelina, M. (2021, November 2). *Quantum technology for military applications*. arXiv.org. Retrieved from https://arxiv.org/abs/2103.12548

Mashatan, A., & Heintzman, D. (2021, May 17). *The complex path to Quantum Resistance*. ACM Queue, 19(2). Retrieved from https://queue.acm.org/detail.cfm?id=3466779

Palmer, M. (2021, May 19). *The Big Idea: Computer Chips with Quantum 'Fingerprints'.* Sifted. Retrieved from https://sifted.eu/articles/computer-chips-quantum-fingerprints/

*Quantum computing is coming to your business*. IBM. (n.d.). Retrieved from https://www.ibm.com/thought-leadership/institute-business-value/report/quantumstrategy

*The quantum computing revolution*. Klecha & Co. (2021, June 14). Retrieved from https://www.klecha-co.com/last-research/the-quantum-computing-revolution/

*Quantum Computing: D-wave.* D. (n.d.). Retrieved from https://www.dwavesys.com/quantum-computing

Reding, D. F., & Eaton, J. (2020, March). *Science & Technology Trends 2020-2040.* NATO Science & Technology Organization. Retrieved from https://www.nato.int/nato\_static\_fl2014/assets/pdf/2020/4/pdf/190422-ST\_Tech\_Trends\_Report\_2020-2040.pdf

*Rethinking cybersecurity in a Quantum World*. PwC. (2021, July). Retrieved from https://www.pwccn.com/en/issues/cybersecurity-and-privacy/rethinking-cybersecurity-in-a-quantum-world-jul2021.html

Shore, P. W. (1994). *Algorithms for quantum computation: Discrete logarithms and factoring*. Proceedings 35th Annual Symposium on Foundations of Computer Science. Retrieved from https://ieeexplore.ieee.org/document/365700/

Sutor, R. (2019). *Dancing with qubits: How quantum computing works and how it can change the world.* Packt Publishing Ltd.

Tasnim News Agency. (2021, January 26). *Iran Runs Quantum Cryptographic Test.* Tasnim News Agency. Retrieved from https://www.tasnimnews.com/en/news/2021/01/26/2440187/iran-runs-quantum-cryptographic-test

Tessler, L., & Byrnes, T. (2018, January 9). *Bitcoin and Quantum Computing*. arXiv.org. Retrieved from https://arxiv.org/abs/1711.04235

U.S. Government Accountability Office. (2021, October 20). *Quantum Computing and Communications: Status and prospects.* U.S. GAO. Retrieved from https://www.gao.gov/products/gao-22-104422

Wang, Y., Hu, Z., Sanders, B. C., & Kais, S. (2020, November 10). *Qudits and High-Dimensional Quantum Computing.* Frontiers. Retrieved from https://www.frontiersin.org/articles/10.3389/fphy.2020.589504/full

Yuan, Z. L., Plews, A., Takahashi, R., Doi, K., Tam, W., Sharpe, A. W., Dixon, A. R., Lavelle, E., Dynes, J. F., Murakami, A., Kujiraoka, M., Lucamarini, M., Tanizawa, Y., Sato, H., & Shields, A. J. (n.d.). *10~MB/s quantum key distribution.* arXiv Vanity. Retrieved from https://www.arxiv-vanity.com/papers/1807.04484/

**Cisco Systems**

Cisco. (2020, July 16). *Post Quantum Security Brief*. Cisco. Retrieved from https://www.cisco.com/c/en/us/products/collateral/optical-networking/solution-overview-c22-743948.html

Kampanakis, P. (2020, April 17). *Post-quantum MACsec in Cisco switches.* Cisco Blogs. Retrieved from https://blogs.cisco.com/security/post-quantum-macsec-in-cisco-switches

**Cloud Security Alliance (CSA)**

Cloud Security Alliance. (n.d.). Retrieved from https://cloudsecurityalliance.org/online-resources/

Faux, R. (2018, April 23). *The State of Post-Quantum Cryptography*. Cloud Security Alliance. Retrieved from https://cloudsecurityalliance.org/artifacts/the-state-of-post-quantum-cryptography/

Faux, R. (2021, February 25). *Confidence in Post Quantum Algorithms*. Cloud Security Alliance. Retrieved from https://cloudsecurityalliance.org/artifacts/confidence-in-post-quantum-algorithms/

Grimes, R. (2021, October 19). *Practical Preparations for the Post-Quantum World*. Cloud Security Alliance. Retrieved from https://cloudsecurityalliance.org/artifacts/practical-preparations-for-the-post-quantum-world/

Huttner, B. (2021, May 2). *Blockchains in the Quantum Era*. Cloud Security Alliance. Retrieved from https://cloudsecurityalliance.org/artifacts/blockchains-in-the-quantum-era/

**ENISA**

Beullens, W., D’Anvers, J.-P., Hülsing, A., Lange, T., Panny, L., de Saint Guilhem, C., & Smart, N. P. (2021, May 3). *Post-Quantum Cryptography: Current State and Quantum Mitigation.* European Union Agency for Cybersecurity (ENISA). Retrieved from https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

Smart, N. (2021, February 9). *Crypto assets: Introduction to Digital Currencies and Distributed Ledger Technologies.* European Union Agency for Cybersecurity (ENISA). Retrieved from https://www.enisa.europa.eu/publications/crypto-assets-introduction-to-digital-currencies-and-distributed-ledger-technologies

**NCSC**

*Quantum Security Technologies*. National Cyber Security Center (NCSC). (2020, March 24). Retrieved from https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies

*Quantum-Safe Cryptography*. National Cyber Security Center (NCSC). (2016, November 30). Retrieved from https://www.ncsc.gov.uk/whitepaper/quantum-safe-cryptography

**NIST**

Barker, W., Polk, W., & Souppaya, M. (2021, April 28). *Getting Ready for Post-Quantum Cryptography.* National Institute of Standards and Technology (NIST). Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf

National Institute of Standards and Technology (NIST). (n.d.). *Migration to Post-Quantum Cryptography.* National Cybersecurity Center of Excellence. Retrieved from https://www.nccoe.nist.gov/projects/building-blocks/post-quantum-cryptography

*Post-Quantum Cryptography.* National Institute of Standards and Technology (NIST). (n.d.). Retrieved from https://csrc.nist.gov/projects/post-quantum-cryptography

**\*\*\* סוף מסמך \*\*\***

1. בִּיטים בלעז, כאשר סיבית יכולה להכיל ערך 0 או 1 בלבד, והיא מהווה את יחידת הנתונים הקטנה ביותר שבה משתמש המחשב. [↑](#footnote-ref-1)
2. נכון לזמן זה, מרבית החוקרים בתחום סבורים כי מחשב קוונטי יפגין עליונות ביחס למחשב מסורתי בפתירת הבעיות המתמטיות הבאות:

   1. פירוק לגורמים (Factoring) - מציאת שני מספרים אשר המכפלה שלהם תפיק מספר נתון.
   2. היפוך (Inverting) - מציאת קלט של פונקציה אשר יפיק פלט נתון.

   סימולציה (דימוי) של מערכות קוונטיות (Quantum Systems). [↑](#footnote-ref-2)
3. דוגמת אלגוריתם החיפוש של גרובר (Grover). [↑](#footnote-ref-3)
4. מכונה גם - ביט קוונטי. [↑](#footnote-ref-4)
5. ישנם מספר סוגי קיוביטים (Qubits) בהם ניתן לעשות שימוש במסגרת מחשוב קוונטי. [↑](#footnote-ref-5)
6. Copyright Notification:

   © Cisco Systems. All rights reserved.

   Post Quantum Security Brief

   https://www.cisco.com/c/en/us/products/collateral/optical-networking/solution-overview-c22-743948.html [↑](#footnote-ref-6)
7. Copyright Notification:

   © 2017 Microsoft. All rights reserved. [↑](#footnote-ref-7)
8. Reprint Courtesy of IBM Corporation ©  
   Shor’s algorithm https://quantum-computing.ibm.com/composer/docs/iqx/guide/shors-algorithm [↑](#footnote-ref-8)
9. P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," Proceedings 35th Annual Symposium on Foundations of Computer Science, 1994, pp. 124-134, doi: 10.1109/SFCS.1994.365700  
   https://ieeexplore.ieee.org/document/365700 [↑](#footnote-ref-9)
10. למרות שישנם מחקרים שאומרים שנכון שאלגוריתם Groover אכן מקצר את זמן החיפוש הממצה, יש לתת את הדעת כי הדבר דורש לממש את AES כמעגל קוואנטי, ולפיכך זמן החיפוש הוא גבוה יותר. [↑](#footnote-ref-10)
11. Bitcoin and quantum computing, Louis Tessler, Tim Byrnes, [Submitted on 12 Nov 2017 (v1), last revised 9 Jan 2018 (this version, v2)]  
    https://arxiv.org/abs/1711.04235 [↑](#footnote-ref-11)
12. A Swiss Company Says It Found Weakness That Imperils Encryption  
    https://www.bloomberg.com/news/articles/2021-02-07/a-swiss-company-says-it-found-weakness-that-imperils-encryption [↑](#footnote-ref-12)
13. Quantum gold rush: the private funding pouring into quantum start-ups

    https://www.nature.com/articles/d41586-019-02935-4

    Top Countries Pumping Money Into Quantum Computing Technology

    https://analyticsindiamag.com/top-countries-pumping-money-into-quantum-computing-technology [↑](#footnote-ref-13)
14. Copyright Notification:

    © Cisco Systems. All rights reserved.

    Post Quantum Security Brief

    https://www.cisco.com/c/en/us/products/collateral/optical-networking/solution-overview-c22-743948.html [↑](#footnote-ref-14)
15. 10 Mb/s quantum key distribution

    https://arxiv.org/abs/1807.04484 [↑](#footnote-ref-15)
16. Full-field implementation of a perfect eavesdropper on a quantum cryptography system  
    Ilja Gerhardt, Qin Liu, Antia Lamas-Linares, Johannes Skaar, Christian Kurtsiefer, Vadim Makarov, Merch 2012  
    https://arxiv.org/abs/1011.0105

    Hacking Quantum Key Distribution via Injection Locking, February 2019

    Xiao-Ling Pang, Ai-Lin Yang, Chao-Ni Zhang, Jian-Peng. Dou, Hang Li, Jun Gao, Xian-Min Jin

    https://arxiv.org/abs/1011.0105 [↑](#footnote-ref-16)
17. Confidence-in-Post-Quantum-Algorithms

    https://cloudsecurityalliance.org/artifacts/confidence-in-post-quantum-algorithms/ [↑](#footnote-ref-17)
18. Qudits and High-Dimensional Quantum Computing  
    https://www.frontiersin.org/articles/10.3389/fphy.2020.589504/full [↑](#footnote-ref-18)
19. The big idea: computer chips with quantum ‘fingerprints’  
    https://sifted.eu/articles/computer-chips-quantum-fingerprints/ [↑](#footnote-ref-19)