01 יולי 2025

ה' תמוז תשפ"ה

דוח מודיעין – מחשבים קוונטיים והשפעתם על אבטחת המידע

שלום רב,

בדו"ח מודיעין זה נציג את השפעת המחשוב הקוונטי על אבטחת המידע, נציג את המחשבים הקוונטיים ואת יכולותיהם השונות וביצד הם מסוגלים לפצח חלק מהאלגוריתמים שמשמשים להצפנה א-סימטרית.

בנוסף נציג את הסיכונים השונים של מחשוב קוונטי וכן דרכי ההתמודדות נגדם.

פרטים:

בעשורים האחרונים פותחו מחשבים קוונטיים אשר מבוססים על עקרונות מכניקת הקוונטיים ומסוגלים לבצע חישובים מהירים ויעילים בהרבה ממחשבים קלאסיים.

מחשבים קוונטיים מסוגלים לפצח חלק מאלגוריתמי ההצפנה הנפוצים שמשתמשים בהם כיום לצורך הצפנה א-סימטרית כגון RSA, Diffie-Hellman ו-ECC.

לאור התחזקות המחשבים הקוונטיים בשנים האחרונות ואף כי טרם זוהתה יכולת פומבית לבצע באופן אפקטיבי את פיצוח אלגוריתמי ההצפנה, מומלץ להתחיל להיערך כבר כעת להטמעת פתרונות אבטחה חסינים ליכולות המחשוב הקוונטי בארגון.

מחשבים קוונטיים:

מחשב אשר מבוסס על עקרונות מכניקת הקוונטים אשר מאפשרים לו לבצע חישובים באופן שונה, מהיר ויעיל יותר ממחשבים קלאסיים, לדוגמא:

- "קיוביט" ו-"סופרפוזיציה" - במחשבים קלאסיים יחידת המידע הבסיסית היא "סיבית" (bit) אשר מוצגת כ-0 או 1 בלבד. במחשבים קוונטיים, יחידת המידע הבסיסית היא "קיוביט" (Qubit) אשר מוצגת כ-1,0 או במצב של "סופרפוזיציה" (מצב בו קיימות הסתברויות להיות 0 או 1).

עקרון הסופרפוזיציה מאפשר למחשב קוונטי לייצג ולעבד מספר מצבים בו-זמנית, דבר שיכול להפוך חישובים מסוימים ליעילים יותר. זאת לעומת מחשב קלאסי שמייצג ומעבד כל אפשרות בנפרד.

- "שזירה קוונטית"- קשר קוונטי שנוצר בין שני קיוביטים, כך שהמצב של הראשון תלוי בשני גם אם הם רחוקים זה מזה. כאשר "מודדים" קיוביט אחד, הקיוביט השני מיד מקבל את ערכו בהתאם למצב השזירה שלהם (סוג הקשר הקוונטי שקיים ביניהם).

- "מדידה" - כאשר יוצרים קיוביט לצורך שימוש בהצפנה קוונטית, יש לבחור בעבורו "בסיס מדידה" מסוים כאשר ישנן שתי אפשרויות – בסיס מדידה [+] ובסיס מדידה [x] (בדומה לקידוד).
הבסיס הנ"ל קובע את האופן שבו הקיוביט יוצג וישפיע על התוצאה של פעולת "המדידה" בהמשך.
כאשר מבצעים "מדידה" על קיוביט (מנסים לגלות את הערך שלו) הוא "קורס" למצב יחיד (0 או 1).
לאחר פעולת המדידה, הקיוביט נשאר בערך שהתקבל בעבורו ולא יכול לחזור למצבו הקודם ללא פעולה חיצונית כלשהי.

הצפנה קוונטית:

שיטת הצפנה אשר מאפשרת יצירת מפתח הצפנה סודי משותף בצורה מאובטחת כך שלא ניתן "לעקוב" אחר המפתח ולנסות להשיגו לצורך האזנה מבלי להיחשף.
אחד הפרוטוקולים הנפוצים בהם משתמשים לצורך יצירת מפתח ההצפנה בהצפנה קוונטית הוא BB84.
להלן דוגמא לתהליך יצירת המפתח תוך שימוש בפרוטוקול BB84, כאשר ממשים בו את עקרון המדידה:

1. שליחת קיוביטים בין השולח למקבל - אליס (השולחת) רוצה לשלוח מפתח הצפנה סודי לבוב (המקבל). במקום לשלוח את מפתח ההצפנה בביטים רגילים (לדוגמא "10101100"), השולח יוצר קיוביטים שערכיהם מייצגים 0 או 1, תוך שימוש ב"בסיסי מדידה" אקראיים עבור כל קיוביט.
לאחר יצירתם, אליס (השולחת) שולחת את הקיוביטים אל בוב (המקבל).
2. ביצוע פעולת ה"מדידה" על ידי המקבל - בוב (המקבל) קיבל את הקיוביטים מאליס (השולחת) ולאחר מכן מבצע עליהם את פעולת ה"מדידה" תוך שימוש ב"בסיסי מדידה" אקראיים, מבלי לדעת באילו "בסיסי מדידה" אליס (השולחת) השתמשה עבור היצירה של כל קיוביט וקיוביט. נדגיש כי אם פעולת "המדידה" מתבצעת באותו "בסיס המדידה" שבו הקיוביט נוצר – התוצאה תהיה זהה לערך המקורי שנוצר אך אם פעולת "המדידה" מתבצעת ב"בסיס מדידה" שונה מזה שבו הקיוביט נוצר התוצאה תהיה ערך אקראי - הסתברות של 50% שיתקבל 0 והסתברות של 50% שיתקבל 1.
כך, לאחר ביצוע פעולת ה"מדידה", חלק מערכי הקיוביטים שבוב קיבל, יהיו לא תואמים לערכי הקיוביטים שאליס יצרה.
3. השוואת בסיסי המדידה - אליס ובוב משווים את בסיסי המדידה שבהם הם השתמשו עבור כל קיוביט. ערכי הקיוביטים עצמם לא נחשפים בעת ההשוואה אלא שאך ורק בסיסי המדידה ששימשו לצורך יצירתם ומדידתם. לאחר ההשוואה, אליס ובוב "זורקים" את כל הקיוביטים שפעולת המדידה עליהם התבצעה בבסיסים לא תואמים (כך שערכיהם יצאו שונים).
הקיוביטים שנשארו הם קיוביטים בעלי אותו הערך ואלו משמשים ליצירת מפתח ההצפנה הסודי והמאובטח.

במידה והתוקף מאזין ומודד את הקיוביטים, פעולת ה"מדידה" מקריסה את הערכים כך שהתוקף מקבל קיוביטים במצב 0 או 1. כשהתוקף שולח את הקיוביטים שקיבל לפעולת "מדידה" שתתבצע על ידי בוב (המקבל), חלק מהקיוביטים יהיו שונים מהמצב המקורי שבו אליס שלחה אותם. לבן אם תוקף ינסה להאזין להעברת הקיוביטים זה יוביל לשיבוש תהליך יצירת מפתח ההצפנה וחשיפת פעולת ההאזנה של התוקף.

פיצוח הצפנות על ידי מחשבים קוונטיים:

מחשבים קוונטיים הינם בעלי יכולת לפצח הצפנה של מספר אלגוריתמים בעיקר אלו העוסקים בהצפנה א-סימטרית, כגון RSA(Factorization), Diffie-Hellman(Discrete Logarithms), ECC(Elliptic Curve Discrete Logarithms).

המחשבים הקוונטים מפצחים את ההצפנה על ידי אלגוריתם שור (Shor's Algorithm).

אלגוריתם זה מסוגל לבצע חישובים מסובכים בצורה יעילה ומהירה בעזרת שימוש בעקרון הסופרפוזיציה ובעקרון השזירה הקוונטית.

נזכיר - הצפנה א-סימטרית הינה הצפנה אשר משתמשת בשני מפתחות הצפנה שונים:

מפתח ציבורי אשר משמש בדר"כ לצורך ביצוע ההצפנה ומפתח פרטי לצורך הפענוח.

ההתאמה בין המפתחות היא חד-חד ערכית ולכן משמעות של פיצוח ההצפנה היא מציאת המפתח הפרטי שמפענח את ההצפנה שהתבצעה על ידי המפתח הציבורי התואם.

כל אחד מאלגוריתמי ההצפנה הא-סימטרית מבוסס על בעיה מתמטית קשה לפתרון על ידי מחשבים קלאסיים לעומת מחשבים קוונטיים.

ישנם מספר אלגוריתמי הצפנה א-סימטרית אשר אלגוריתם שור מסוגל לפצח, לדוגמא:

- RSA – מבוסס על בעיה מתמטית של פירוק מספר גדול לגורמים הראשוניים שלו (Factorization).
- Diffie-Hellman – מבוסס על בעיה מתמטית של פתרון Discrete Logarithm.
- ECC (Elliptic Curve Cryptography) – מבוסס על בעיה מתמטית של פתרון "לוגריתם דיסקרטי בעקומים אליפטיים" (Elliptic Curve Discrete Logarithms).

יש לציין כי אלגוריתם "שור" מסוגל לפתור בעיות מתמטיות מסוימות כך שקיימים אלגוריתמי הצפנה א-סימטריים שעמידים בפני מחשוב קוונטי (נכון להיום).

עדיין לא זוהתה יכולת פומבית לבצע באופן אפקטיבי את פיצוח ההצפנה של אלגוריתמים אלו, אך התשתית התאורטית קיימת והמחשוב הקוונטי מתחזק ביכולותיו באופן מובהק לאורך זמן.

פרוטוקולים מאובטחים כמו TLS, SSL VPN, ו- API Secure Communication משתמשים באלגוריתמי הצפנה א-סימטרית כחלק מהתהליך של "יצירת" מפתח הצפנה סודי משותף.

לאחר שהמפתח הסודי המשותף נוצר, המשך התקשורת והעברת המידע נעשית בעזרת הצפנה סימטרית.

לכן, אם מחשב קוונטי יהיה מסוגל לשבור את אלגוריתם ההצפנה הא-סימטרי ששימש כחלק מהתהליך של "יצירת" מפתח הצפנה סודי משותף יהיה ניתן להשיג את מפתח ההצפנה הסודי המשותף להשיג גישה לכל הנתונים המוצפנים שיועברו בתקשורת.

נציין כי לעומת היכולת של המחשבים הקוונטיים לפצח הצפנה א-סימטרית הם אינם מסוגלים לשבור בקלות הצפנה סימטרית באותה הצורה אך כן יכולים להשתמש באלגוריתם "גרובר" (Grover's Algorithm) כדי להאיץ את החיפוש אחר המפתח הסודי שיפענח את ההצפנה.

לא ניתן להעריך במדויק מתי יושגו יכולות אלו וייתכנו פריצות דרך שיאיצו את התהליך בצורה משמעותית.

יש לשים לב לכך שאלגוריתמי ההצפנה הא-סימטריים שציינו משמשים במספר רב של מערכות אבטחה.

סיכונים במחשוב קוונטי:

- זיוף חתימות דיגיטליות בקבצים ורכיבי תוכנה - חתימות דיגיטליות משמשות לווידוא שקובץ, תוכנה, או גרסאות קושחה (Firmware) לא שונו או זויפו על ידי גורם זדוני ושהוא אכן מהימן ומקורי.
חתימות דיגיטליות מבוססות על הצפנה א-סימטרית והן עושות שימוש במפתח פרטי על מנת להצפין את החתימה ובמפתח ציבורי כדי לאמת שמדובר בחתימה המקורית.
מחשב קוונטי יכול לשחזר את המפתח הפרטי מתוך המפתח הציבורי באמצעות אלגוריתם "שור" וכך לזייף וליצור חתימות אמינות ולגרום למערכות השונות להאמין שהן לגיטימיות.
- זיוף חתימות דיגיטליות במסמכים פיננסיים - מסמכים פיננסיים שניתנים להמרה מידית לכסף עושים שימוש בחתימות דיגיטליות לצורך בדיקת מהימנות של המסמך.
אם מחשב קוונטי יכול לזייף חתימה דיגיטלית, הוא יוכל לזייף את אותם המסמכים וכך לשנות את הנתונים של הבעלות על הנכסים או לבצע העברות נכסים באופן בלתי חוקי ולא לגיטימי.
לדוגמא מטבעות קריפטוגרפים משתמשים בחתימות דיגיטליות כדי להבטיח שהעברות שמתבצעות מארנק מסוים הן לגיטימיות. ארנק של מטבעות קריפטוגרפים משתמש במפתח פרטי כדי לחתום על עסקאות באשר המפתח הציבורי מאפשר למערכת לוודא שהחתימה מקורית.
אם מחשב קוונטי יפצח את אלגוריתמי ההצפנה הא-סימטרית, תוקף יכול להשיג את המפתח הפרטי שאיתו חותמים על העסקאות וכך לזייף עסקאות של העברה מארנק מסוים ולגנוב ממנו מטבעות קריפטוגרפים.
- מערכות קריטיות שלא ניתן לעדכן בקלות - מערכות תעשייתיות קריטיות (ICS/SCADA) ומכשירים רפואיים חכמים (IoMT) משתמשים בחתימות דיגיטליות כדי לוודא שעדכוני הקושחה (firmware) מקוריים. במערכות אלו לא תמיד ניתן לשדרג את אלגוריתמי ההצפנה שמשמשים לאימות החתימה הדיגיטלית שכן החומרה לא בנויה לכך. בנוסף, רכישה של מוצרים חדשים כאלה שמשתמשים באלגוריתמים מתקדמים יותר מתבצעת בתדירות נמוכה של פעם בכמה שנים.
- הקלטת תעבורה מוצפנת ופענוח שלה בעתיד (Harvest Now, Decrypt Later) - תוקפים יכולים להקליט תעבורה מוצפנת בהצפנה שאינה חסינה לפיצוח קוונטי ולשמור אותה ובעתיד לפצחה.
לכן ייתכן שהקלטת התעבורה היא סיכון אקטואלי כבר בעת.

חסרונות:

- מורכבות טכנולוגית – בניית מחשב קוונטי יציב היא אתגר אדיר מכיוון שהקיוביטים (יחידות המידע במחשב קוונטי) רגישים מאוד להפרעות סביבתיות כמו רעשים אלקטרומגנטיים וטמפרטורה לא מתאימה. כדי לשמור על יציבות המצב של הקיוביטים, מחשבים קוונטיים חייבים לפעול בטמפרטורות נמוכות מאוד (קרוב לאפס המוחלט) ולכן כל מחשב קוונטי דורש בין היתר מערכות קירור מתוחכמות במיוחד דבר שמגביל את השימוש בו.
  כל מחשב קוונטי דורש הפעלה בסביבה מבוקרת שבהם הקיוביטים יוכלו להיות יציבים.
- יישום מוגבל – חשוב לציין כי מחשב קוונטי לא בהכרח מחליף מחשב קלאסי אלא טוב רק לפתרון של בעיות מסוימות. בעיות רבות נפתרות בצורה מיטבית במחשבים רגילים ואין צורך במחשוב קוונטי עבורן. לדוגמא מעבדי GPU (כרטיסי מסך) יכולים לפתור בעיות של "למידת מכונה" בצורה יעילה יותר ממחשבים קוונטיים.
- איום על אבטחת המידע הקיימת – כמו שציינו מעלה, מחשוב קוונטי מסוגל לפצח את ההצפנה של אלגוריתמי הצפנה א-סימטריים כמו RSA. באמצעות אלגוריתם "שור" מחשוב קוונטי מסוגל ליצור את המפתח הפרטי מתוך המפתח הציבורי של אותה ההצפנה הא-סימטרית וכך לפענח את כל המידע שהוצפן עם אותו המפתח הציבורי.

דרכי התמודדות:

- נמליץ לבצע מיפוי מידע קריטי של הארגון בהתאם לסוגי ההצפנות.
- מעבר לשימוש באלגוריתמים שעמידים ליכולות הפענוח של המחשוב הקוונטי PQC Algorithms.
  בשנת 2022, NIST הכריז על ארבעה אלגוריתמים שאושרו כתקנים פדרליים (FIPS):
  ML-KEM (CRYSTALS-Kyber) - אלגוריתם להצפנה א-סימטרית
  שלושת הנוספים מיועדים לשימוש בחתימות דיגיטליות:
  ML-DSA (CRYSTALS-Dilithium) – מתאים לשימושים כלליים (ברירת המחדל של NIST).
  FN-DSA (FALCON) – מתאים למערכות אשר עושות שימוש בחתימות "קטנות" מבחינת גודלן.
  SLH-DSA (SPHINCS+) – מבוסס על פונקציית Hash ונחשב לבטוח יותר אך גם כבד חישובית.
  מומלץ מאוד להשתמש באלגוריתמים אלו (PQC Algorithms) ובאלגוריתמים נוספים שיאושרו בעתיד (אשר יהוו בסיס לפתרונות חסינים למחשוב קוונטי).
- הצפנה במערכות ענן ובשירותים חיצוניים - יש לוודא שספקים אלו פועלים לתמוך באלגוריתמי הצפנה שחסינים לפענוח על ידי מחשוב קוונטי (PQC), כדי להגן מפני הסיכון של פיצוח ההצפנה של המידע והנתונים שנמצאים באותן המערכות.
- בחינת טכנולוגיות אבטחה חלופיות - מומלץ לבחון טכנולוגיות אבטחה חלופיות המציעות חוסן מפני יכולות המחשוב הקוונטי, לדוגמא הטכנולוגיה QKD (Quantum Key Distribution). חשוב לציין כי טכנולוגיה זו דורשת תשתיות מתאימות ושזהו פתרון משלים ל-PQC.

- שימוש בהצפנה סימטרית חזקה – במערכות שעושות שימוש בהצפנה סימטרית, מומלץ להשתמש באלגוריתם AES-256, הנחשב בשלב זה כחסין ליכולות המחשוב הקוונטי.
- שימוש ב- SHA-256 או מעבר ל- SHA-384/SHA-512 - ישנם פרוטוקולים ואלגוריתמים שונים שעושים שימוש בפונקציית ה-Hash. פונקציית SHA-256 עדיין נחשבת בשלב זה כחסינה מפני יכולות המחשוב הקוונטי אך נמליץ לבחון שימוש בפונקציית-SHA-384 או בפונקציית-SHA-512. שיפור זה עשוי לשפר את החסינות כנגד יכולות המחשוב הקוונטי שילכו וישתפרו עם הזמן.
- יש לשים לב שפרוטוקולי TLS.2 ו-TLS.1 אינם הצפנה חזקה וניתנים לפריצה בקלות.

בברכה,

SOC מגזר התקשורת

קישור למסמך של מערך הדיגיטל אודות מוכנות להתמודדות עם הצפנות בעידן המחשוב הקוונטי:

https://www.gov.il/BlobFolder/policy/preparedness_to_deal_with_encryption_in_the_quantum_computing/he/meshilut_preparedness_to_deal_with_encryption_in_the_quantum_computing.pdf