Digital Whisper
Technologic Papers

אמרנו לחכות. ההמתנה נגמרה.

על קריפטוגרפיה פוסט-קוונטית: למה ה-Harvest Now, Decrypt Later הוא כבר לא מדע בדיוני אלא בעיה תפעולית

מאת גיא ברנהרט-מגן (Profero, CTO)

רקע

בינתיים המתמטיקה התקדמה. שני מאמרים שפורסמו במרץ 2026 הראו ששבירת הצפנה מבוססת עקומים אליפטיים דורשת היום הרבה פחות ממה שחשבנו, וזה מספיק קרוב כדי שזו תהיה בעיה הנדסית קצרת-טווח ולא שאלה רחוקה בפיזיקה. תקני ההצפנה אושרו, סופיים ומוכנים לפריסה. אם אתם מאחסנים או מעבירים מידע רגיש שמוגן בהצפנה א-סימטרית חלשה, תוכנית המעבר שלכם כבר צריכה להיות קיימת. אם חוויתם אירוע ומידע מוצפן נגנב, ייתכן שהוא כבר בתור לפענוח עתידי. בדקו את ה-HSM שלכם, תתחילו עכשיו.

הקדמה

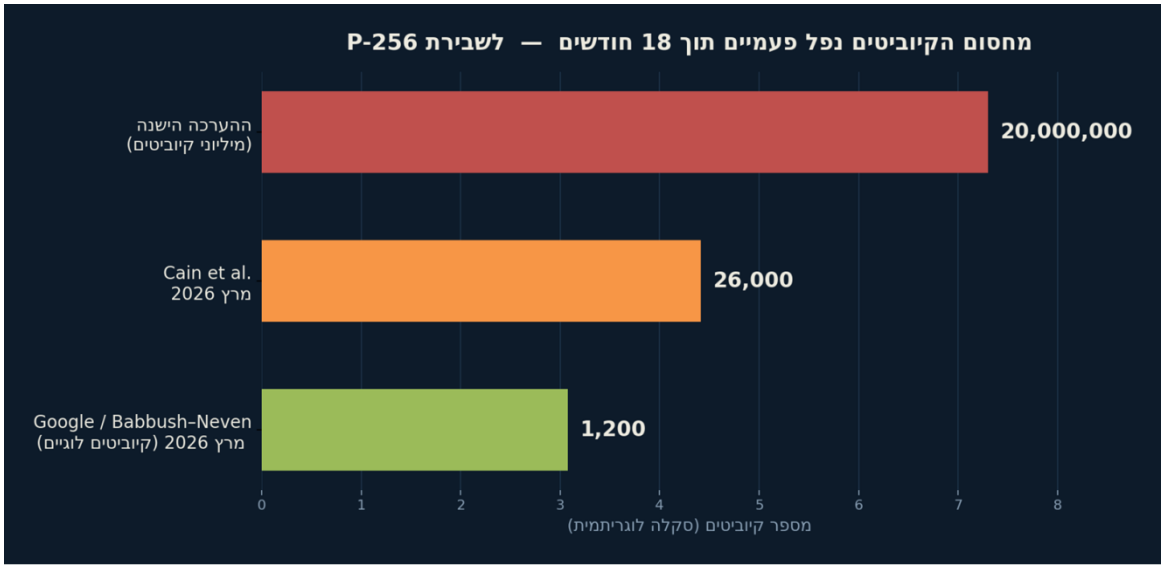
לפני כשנה כתבתי פוסט בשם "להבין קריפטוגרפיה קוונטית: להפריד בין עובדות לדמיון". הטענה הייתה פשוטה: ההייפ סביב מחשבים קוונטיים ששוברים הצפנה מודרנית התקדם הרבה יותר מהר מהמציאות (אני לא מאמין גדול ב-FUD). מחשבים קוונטיים חזקים היו רחוקים, תקני PQC עוד היו בגיבוש, והעצה הייתה ברורה: תישארו מעודכנים, אל תיכנסו לפאניקה, וחכו שהתקנים יתייצבו לפני שאתם מהמרים על תשתית.

זו הייתה ההחלטה הנכונה לאותו הזמן. אני כותב את המאמר הזה כי המציאות השתנתה, וכדאי שתבינו איך. בהמשך נעבור על מה שזז מבחינה טכנית, על האיום המעשי שכבר קיים גם בלי מחשב קוונטי בהווה, ועל מה שאפשר לעשות כבר עכשיו.

מה השתנה?

שני המניעים המרכזיים טכניים, לא פוליטיים.

דרישת הקיוביטים צנחה. כשכתבתי את הפוסט המקורי, שבירת הצפנת עקומים אליפטיים ב-256 ביט דרשה מחשב קוונטי ענק עם תיקון שגיאות: מיליוני קיוביטים פיזיים לפי רוב ההערכות. ב-31 במרץ 2026 פרסמו ראיין באבוש והרטמוט נוון מ-Google מחקר שמראה שאלגוריתם Shor נגד P-256 דורש היום פחות מ-1,200 קיוביטים לוגיים ו-90 מיליון שערי Toffoli. זו הפחתה של פי 20 במספר הקיוביטים הפיזיים. כמה ימים אחר כך הראו Cain ושותפיו שעם ארכיטקטורת אטומים ניטרליים וקישוריות לא-מקומית אפשר לפתור את בעיית הלוגריתם הבדיד של P-256 בתוך כמה ימים, על מערכת עם כ-26,000 קיוביטים פיזיים. זה כבר נראה כמו הנדסה קצרת-טווח, לא פיזיקה ספקולטיבית.



[(Cain et al. (2026 ו-Neven & Babbush תרשים להמחשה - סקלה לוגריתמית, על בסיס]

קונצנזוס המומחים השתנה. פיליפו ולסורדה, מהנדס קריפטוגרפיה שאני מכבד את שיקול הדעת שלו, שינה את עמדתו לגבי לוחות הזמנים של CRQC. ההערכה החדשה שלו מצביעה על הסתברות משמעותית למחשב קוונטי רלוונטי-קריפטוגרפית (CRQC - Cryptographically Relevant Quantum Computer) עד 2029. הוא אומר במפורש שהנטל עכשיו על הספקנים להוכיח הסתברות אפסית, לא על מחנה הדחיפות להוכיח ודאות.

הערה למי שרוצה לדייק: קיוביט לוגי הוא קיוביט "מתוקן-שגיאות" שמורכב מהרבה קיוביטים פיזיים רועשים. לכן פחות מ-1,200 הקיוביטים הלוגיים אצל Google מתורגמים למספר פיזי גדול בהרבה, והעבודה של Cain ושותפיו, שמדברת על כ-26,000 קיוביטים פיזיים, היא הערכה בארכיטקטורה אחרת לגמרי. שתי התוצאות מצביעות לאותו כיוון: המספרים מצטמצמים, וכל אחת מהן לבדה כבר מקרבת את הסף לטווח שאפשר לדמיין אותו כפרויקט הנדסי.

PQC כבר פרוס, לא רק מתוקנן. NIST סיימו את התקנים FIP, 203, 204 ו-205 באוגוסט 2024. אבל מה שאני מצביע עליו הוא מה שקרה אחרי: Chrome שלח את ML-KEM ב-TLS כברירת מחדל באמצע 2024, ו-

OpenSSL ו-BoringSSL הצטרפו. עד 2025 החלפת מפתחות היברידית פוסט-קוונטית כבר הייתה זמינה ב-stack שרוב הארגונים מריצים ממילא. הטענה שטענתי בפוסט המקורי, לחכות שהתקנים יתייצבו לפני שמהמרים על תשתית, כבר לא תקפה. התקנים התייצבו, הספריות מעודכנות, והפער בפריסה נסגר. לא נשאר חסם טכני.

רגע, מה הם ML-KEM ו-ML-DSM? ML-KEM (לשעבר Kyber, מתוקנן כ-FIPS 203)? אלו מנגנוני אנקפסולציית מפתחות מבוסס סריגים, מחליף להחלפת מפתחות כמו ECDH. ML-DSM (לשעבר Dilithium, FIPS 204) הוא סכמת חתימה דיגיטלית מקבילה, מחליף ל-ECDSA ו-RSA. SLH-DSA (FIPS 205) הוא חתימה מבוססת hash, גיבוי שמרני יותר. כל השלושה תוכננו כך שגם מחשב קוונטי לא ישבור אותם ביעילות. OpenSSL ו-BoringSSL, אגב, הן ספריות ה-TLS שמריצות חלק גדול מהאינטרנט, ולכן הרגע שבו הן מוסיפות תמיכה הוא הרגע שבו האלגוריתם נעשה זמין בפועל לכולם.

האיום שלא צריך את 2029 כדי להתחיל

לאנשי Incident Response יש כאן חשיפה ספציפית. יריבים מדינתיים (וכמה קבוצות פשע ממומנות היטב) לא צריכים מחשב קוונטי היום כדי להרוויח מאחד ב-2029. הם צריכים שהמידע עדיין יהיה שווה כשהחישוב יגיע. זה המודל של "אסוף עכשיו, פענח אחר כך" (Harvest Now, Decrypt Later): אוספים תעבורה מוצפנת היום, שומרים אותה, ומפענחים כש-CRQC נעשה זמין.

[תרשים להמחשה]

אם הארגון שלכם חווה אירוע (מידע שנפרץ, אירוע שרשרת אספקה, חדירה מדינתית), יש הסתברות סבירה שמידע מוצפן הוצא יחד עם plaintext. מפתחות הסשן של TLS, לחיצות היד של VPN, ארכיוני מייל מוצפנים, פעולות חתימת קוד: כל זה יכול לשבת באחסון קר על תשתית של מישהו אחר, ולחכות.

לא כל מידע נולד שווה כאן. רשומה רפואית, סוד מסחרי, מפתח חתימה ארוך-טווח או מידע מסווג עדיין יהיו רגישים בעוד חמש או עשר שנים, ולכן הם המטרה האטרקטיבית ל-Harvest Now, Decrypt Later. לעומת זאת, תעבורה שהערך שלה פג אחרי שעה הרבה פחות מעניינת ליריב סבלני. כשאתם מתעדפים, השאלה הראשונה היא כמה זמן המידע צריך להישאר חסוי, ולא רק כמה הוא רגיש היום. תגובה לאירוע ממוסגרת בדרך כלל סביב מה שתוקפים יכולים לעשות היום. האיום הזה ממסגר מחדש את השאלה: מה המידע שכבר יש להם יכול לעשות לכם בעוד שלוש שנים?

הצפנה סימטרית ו-HSM

אלגוריתם Grover חוצה את אורך המפתח האפקטיבי תחת מתקפה קוונטית, הסיכון האמיתי מרוכז בהצפנה א-סימטרית: החלפת מפתחות (ECDH, RSA), חתימות דיגיטליות (ECDSA, RSA-PSS), וכל מה שבנוי על הקושי של לוגריתמים בדידים או פירוק לגורמים. אלה האלגוריתמים ש-Shor שובר ביעילות.

שיקול חומרה אחד ספציפי: אם הארגון משתמש ב-HSM (Hardware Security Modules), לאחסון מפתחות, חתימת קוד או פעולות CA, בדקו אם ה-Fireware ותמיכת האלגוריתמים מכסים את ML-KEM ו-ML-DSM. הרבה HSM בייצור היום לא תומכים. מחזורי השדרוג של HSM ארוכים ולפעמים דורשים החלפה פיזית. אם CRQC יגיע לפני שה-HSM שלכם תומך באלגוריתמים פוסט-קוונטיים, שכבת הגנת המפתחות הופכת לצוואר הבקבוק. הוסיפו סקירת HSM לתכנית העבודה שלכם.

מה לעשות עכשיו?

זו בעיה של תכנון, ואין צורך בפאניקה. אבל היא חייבת להתחיל עכשיו, כי לוח הזמנים של מעבר ההצפנה הא-סימטרית ארוך.

1. **רשימת מצאי קריפטוגרפית.** מפו איפה הצפנה א-סימטרית נמצאת בשימוש: נקודות סיום TLS, קצות VPN, תהליכי חתימת קוד, שורשי אטסטציה של חומרה, טוקני אימות API, רשויות אישורים. אי אפשר להעביר את מה שאתם לא רואים, ורוב הארגונים מגלים שיש להם הרבה יותר חשיפה ממה שציפו ברגע שהם מסתכלים.
2. **תעדפו החלפת מפתחות.** ML-KEM זמין, מתוקנן ופריס ב-TLS 1.3 דרך מצבים היברידיים כבר היום. זו העדיפות הגבוהה ביותר, כי היא מנטרלת ישירות את איום ה-Harvest Now, Decrypt Later עבור תעבורה עתידית. תעבורה שמוגנת ב-ML-KEM היום בטוחה גם אם CRQC יגיע ב-2029.

3. **תכננו מעבר חתימות.** ML-DSM הוא המחליף של ECDSA ו-RSA-PSS. מחזורי החיים של אישורים אומרים שזה לוקח יותר זמן: קחו בחשבון שדרוגי CA, תמיכת HSM ותאימות לקוחות. תתחילו את מחזור התכנון עכשיו כדי שהביצוע לא ייכפה עליכם תחת לחץ.
4. **הוציאו משירות שורשים קלאסיים.** מערכות אטסטציה של חומרה ושורשי אישורים ארוכי-חיים הם הכי קשים לרוטציה. הם דורשים את זמן ההיערכות הארוך ביותר ואת הגיבוי הארגוני הגדול ביותר. שימו אותם על מפת הדרכים היום.

המספרים האלה לא נועדו להפחיד אלא לתעדף. ארגון שמתחיל היום באינוונטר ובמפת דרכים ייכנס לחלון של 2029 עם בחירה, לא עם חירום. זה ההבדל היחיד, והוא כל ההבדל.

הזווית של תגובה לאירוע

אם חוויתם חדירה מאומתת (במיוחד כזו עם חשד למעורבות מדינתית), היקף האירוע יכול להיות גדול יותר ממה שהערכת נקודת-הזמן הראתה. מידע מוצפן שהוצא ב-2023, ב-2024 או ב-2025 נמצא עכשיו בתחום של פענוח קוונטי עתידי. זה לא משנה את המיטיגציה שכבר השלמתם, אבל זה משנה את חישוב הסיכון ארוך-הטווח למידע רגיש שנחשף.

תגובה לאירוע תמיד כללה הערכה של איזה מידע נלקח. מכאן והלאה היא צריכה לכלול גם את השאלה: מה הייתה ההגנה הקריפטוגרפית על המידע הזה, וכמה זמן ההגנה הזו תחזיק מעמד?

סדר עדיפויות מעשי

סדר העדיפויות פשוט: קודם החלפת מפתחות, אחר כך חתימות, ובסוף שורשים ארוכי-חיים. החלפת מפתחות עוצרת את הדימום של Harvest Now, Decrypt Later כאן ועכשיו; חתימות ושורשים הם עבודת תשתית ארוכה שצריך בעיקר להתחיל בזמן.

ה-ZKP - מה שסופר ומה שקרה

הוכחת אפס-ידע (ZKP - Zero-Knowledge Proof) היא פרוטוקול שבו צד אחד משכנע צד אחר שטענה נכונה, בלי לחשוף שום מידע מעבר לעצם נכונותה. גוגל ייעלה את אלגוריתם Shor (זה ששובר הצפנה א-סימטרית כמו RSA ועקומים אליפטיים ברגע שיש מחשב קוונטי עם מספיק קיוביטים), אבל במקום לפרסם את המעגל המיטבי עצמו היא פרסמה הוכחת אפס-ידע על העלות שלו: הנה התוצאה, בלי לחשוף איך. זו דרך מעניינת לחשוף יכולת בלי למסור את השיטה, וזה החלק הבאמת מעניין בכל הסיפור.

הסיפור כפי שהתגלגל ב X

ב X-זה התגלגל כ-thread דרמטי (של Charles Guillemet, _P3b7@) - גוגל ייעלה את Shor, ממשל ארה"ב חסם את פרסום המאמר המלא, אז גוגל פרסמה הוכחת אפס-ידע במקום. ואז מישהו פתח תחרות לשחזר את התוצאה בעזרת AI. מודל שפה סורק מרחב עצום של מעגלים קוונטיים, כל אחד מועמד לאופטימיזציה של שור ובודק אם הוא מנצח את השיא הקודם. החלק החכם: השתמשו במאמת ה-ZKP של Google כפונקציית התגמול. אין תוצאות שווא, ומסתבר שזה אות יעיל מאוד. לפי ה-thread, תוך פחות מיומיים הקהילה שחזרה את התוצאה של גוגל וחמישה-עשר ימים אחר כך המודלים כבר 44% מעבר לה.

סיפור מצוין. הוא גם דוחס שני אירועים שונים מאוד לקשת אחת חלקה. נפריד אותם.

מה Trail of Bits באמת עשו

החלק שתפס כותרות הוא ש-Trail of Bits "ניצחו" את ההוכחה של גוגל. רק שזה לא היה הישג קוונטי, הם מצאו באגים של בטיחות-זיכרון ולוגיקה בקוד המאמת של גוגל שכתוב ב-Rust, רץ כ-guest בתוך zkVM מסוג SP1 , וזייפו הוכחה שמדווחת מספרים טובים יותר משל גוגל כולל אפס שערי Toffoli. הניצול לא נגע במעגלים קוונטיים בכלל: הוא נשען על deserialization עם access_unchecked ועל באג של register aliasing. גוגל תיקנה את המאמת (גרסה v2 של המאמר), והטענות המדעיות שלה לא נפגעו.

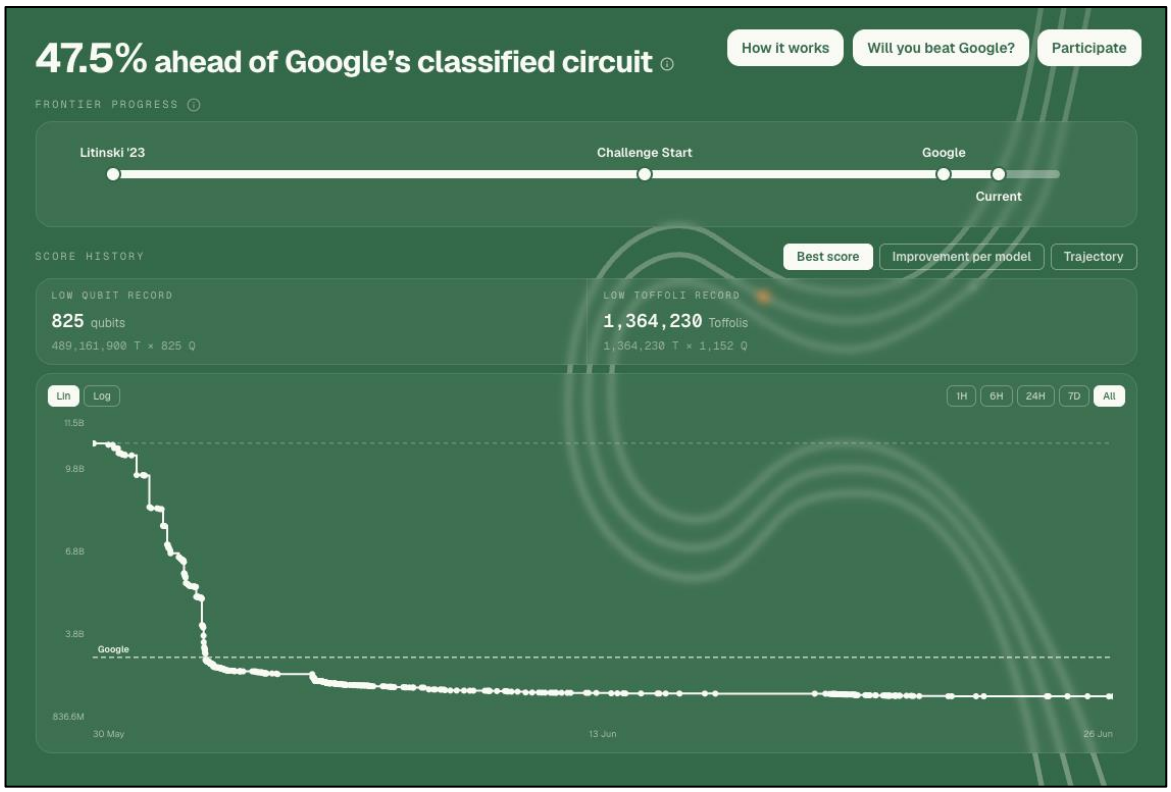
המסקנה כמו ש-Trail of Bits מנסחים: ZKP לא מבטל אמון, הוא מעביר אותו. במקום לסמוך על "האם המומחים מאמינים לזה", אתם עכשיו סומכים על המימוש של המאמת, על הקומפיילר ועל מערכת ההוכחה. זה משטח תקיפה של אבטחת יישומים, לא ערובה מתמטית.

מה הקהילה שחזרה מתוך ידע קיים

במקביל, חוקרים עצמאיים שחזרו את האופטימיזציה האמיתית מתוך ספרות פומבית, תוך מספר ימים. העבודה של André Schrottenloher על חיבור נקודות, ו-preprint על היפוך מודולרי חסכוני בזיכרון של Luo ואחרים, נשענים על תוצאות בנות עשורים: שיתוף רגיסטרים של Proos-Zalka מ-2003, והשיטה של Kaliski להיפוך. ה"סוד" של גוגל התברר כניתן לשחזור מתוך ה-prior art. תחרות בסגנון Shor-at-home המשיכה לגזום את המעגל הלאה.

לכן כשאתם רואים "הקהילה כבר X אחוז מעבר לגוגל", שווה לזכור שהמספר מערבב הוכחה מזויפת עם קריפטאנליזה אמיתית, ושהאחוז זז ותלוי באיזו מטריקה בוחרים. תתייחסו למספרים המדויקים כלא-רשמיים.

ומה זה אומר בפועל? שום דבר כאן לא שובר את ה-TLS שלכם השנה. עדיין צריך מחשב קוונטי רלוונטי-קריפטוגרפית עם מספר קיוביטים גדול, והוא לא קיים. מה שהשתנה הוא בדיוק מה שטענו בפוסט המקורי: הערכות המשאבים ממשיכות לרדת, ועכשיו אנחנו גם יודעים שהן קלות לשחזור וקשות לשמירה בסוד. תכננו לפי המגמה, לא לפי המספר של היום:



[מקור: ecdsa.fail]

סיכום

לפני שנה, "אל תיכנסו לפאניקה" הייתה העצה הנכונה: התקנים לא היו מוכנים והחישוב לא היה שם. זה השתנה. התקנים נחתו באוגוסט 2024, מחסום הקיוביטים נפל פעמיים ב-18 חודשים, והחלון לתכנון בדחיפות נמוכה נסגר. תתחילו את האינוונטר הקריפטוגרפי. תעדפו את ML-KEM להחלפת מפתחות. שימו מעבר חתימות על מפת הדרכים. ואם חוויתם אירוע עם הוצאת מידע מוצפן, הכניסו את הקוונטים למודל הסיכון ארוך-הטווח שלכם. היריבים שלכם כבר עושים את זה.

על המחבר

גיא ברנהרט-מגן הוא סמנכ"ל הטכנולוגיות של Profero וחוקר אבטחה עם רקע במתמטיקה, קריפטוגרפיה ובינה מלאכותית. הוא כותב על הנקודות שבהן קריפטוגרפיה, תגובה לאירועים ומחשוב קוונטי נפגשים. פרופרו היא חברה המתמחה בסיוע לחברות בהכנה לאירועי סייבר ותגובה לאירועים. ניתן לצור קשר דרך guy@profero.io.

מקורות מידע

- Babbush & Neven, Google Research - Safeguarding cryptocurrency by disclosing quantum vulnerabilities responsibly (https://research.google/blog/safeguarding-cryptocurrency-by-disclosing-quantum-vulnerabilities-responsibly/)
- Cain et al. - Shor's algorithm is possible with as few as 10,000 reconfigurable atomic qubits, arXiv:2603.28627 (https://arxiv.org/abs/2603.28627)
- NIST Post-Quantum Cryptography - FIPS 203 / 204 / 205 (https://csrc.nist.gov/projects/post-quantum-cryptography)
- Babbush et al. - Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities, arXiv:2603.28846 (https://arxiv.org/abs/2603.28846)
- Trail of Bits - We beat Google's zero-knowledge proof of quantum cryptanalysis (https://blog.trailofbits.com/2026/04/17/we-beat-googles-zero-knowledge-proof-of-quantum-cryptanalysis/)
- Schrottenloher - Optimized Point Addition Circuits for Elliptic Curve Discrete Logarithms, arXiv:2606.02235 (https://arxiv.org/abs/2606.02235)
- Luo et al. - Space-Efficient Quantum Algorithm for Elliptic Curve Discrete Logarithms, arXiv:2604.02311 (https://arxiv.org/abs/2604.02311)
- Proos & Zalka - Shor's discrete logarithm quantum algorithm for elliptic curves, arXiv:quant-ph/0301141 (https://arxiv.org/abs/quant-ph/0301141)
- Roetteler et al. - Quantum resource estimates for computing elliptic curve discrete logarithms (Kaliski inversion), arXiv:1706.06752 (https://arxiv.org/abs/1706.06752)
- Shor-at-home challenge - ecdsa.fail (https://ecdsa.fail)
- אלגוריתם Shor - ויקיפדיה (https://he.wikipedia.org/wiki/)
- Harvest Now, Decrypt Later - ויקיפדיה (https://en.wikipedia.org/wiki/Harvest_now,_decrypt_later)
- הפוסט המקורי Understanding Quantum Cryptography: Separating Fact from Fiction (Profero) (https://profero.io/blog/understanding-quantum-cryptography-separating-fact-from-fiction/)
- עדכון עמדה על PQC Filippo Valsorda (https://words.filippo.io/crqc-timeline/)
- הדיון ב-X (https://x.com/P3b7_/status/2066540230442692805) (@P3b7_)