Transitioning to Post-Quantum Cryptography

Modern cryptography in the midst of quantum computers

26 February 2025

Caleb "Autumn" Luzovich (they/them/theirs)

Modern Cryptography Is Under Threat

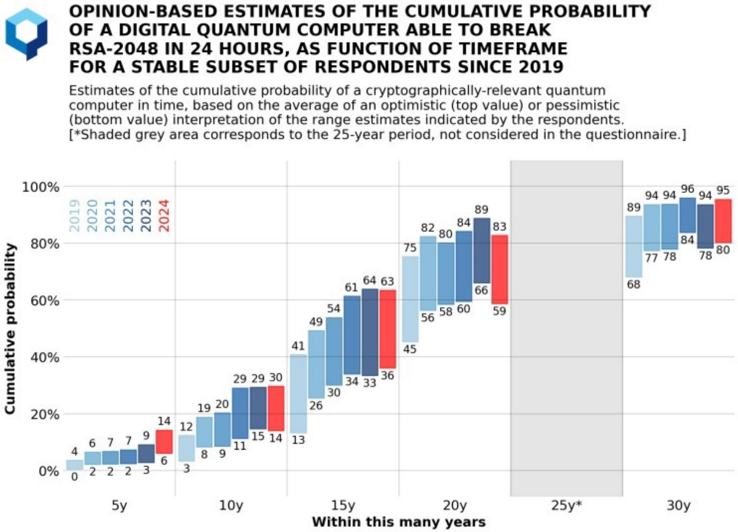

Figure 1: Respondent outlook on the power of quantum computers. (Mosca and Piani, 29)

Modern Cryptography Is Under Threat (ii)

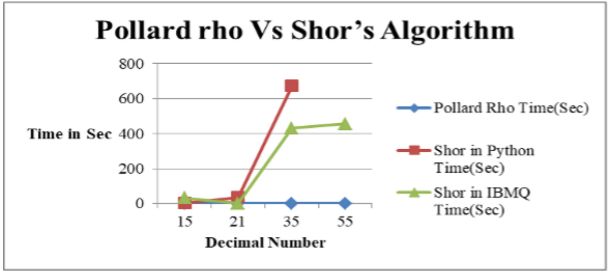

Figure 2: Factoring algorithm durations in different environments. (Kute et al., 6)

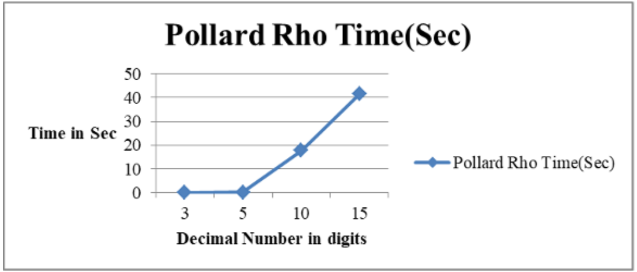

Figure 3: Pollard's rho factoring algorithm durations by digit count. (Kute et al., 6)

Cryptography Is Important

Cryptography is the practice of protecting information by doing certain things to/with it.

Most modern technology depends on cryptographic algorithms to protect information.

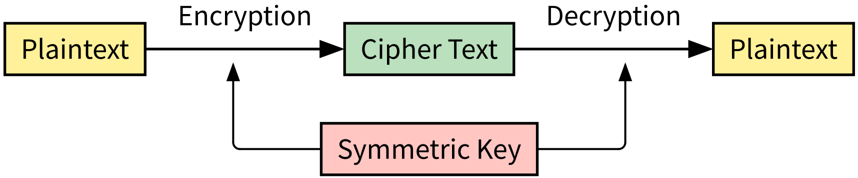

Figure 4: Symmetric encryption flow model. (Luzovich)

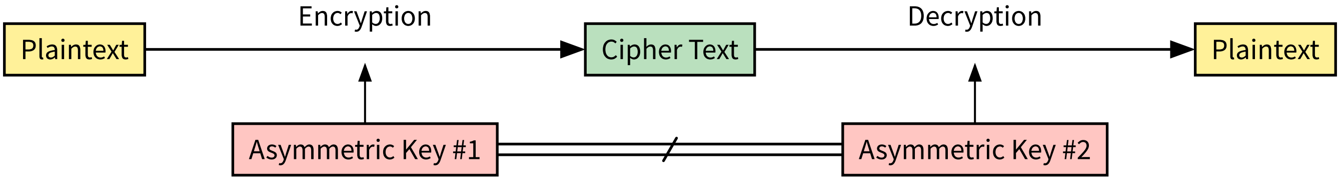

Figure 5: Asymmetric encryption flow model. (Luzovich)

What Do We Do?

20 years isn't much time to implement newer algorithms across all technology.

A disorganized transition can pose a much bigger threat.

The algorithms we do choose to transition to must be heavily vetted.

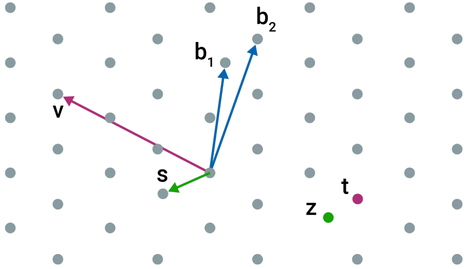

Figure 6: 2D diagram of a lattice-based cryptographic algorithm. (*What Is Lattice-Based Cryptography?*)

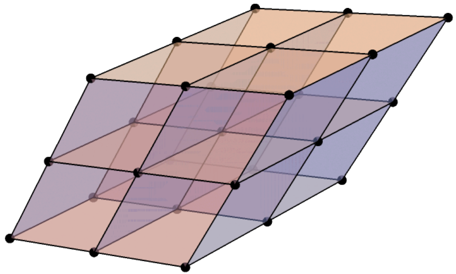

Figure 7: 3D diagram of a lattice. (*Latticeunitcellplot3d | Wolfram Function Repository*)

A Nuanced and Transparent Approach

We need to be both mindful and hasty in our transition process.

Consumers need to be made aware of this transition and need to be in the loop of current progress.

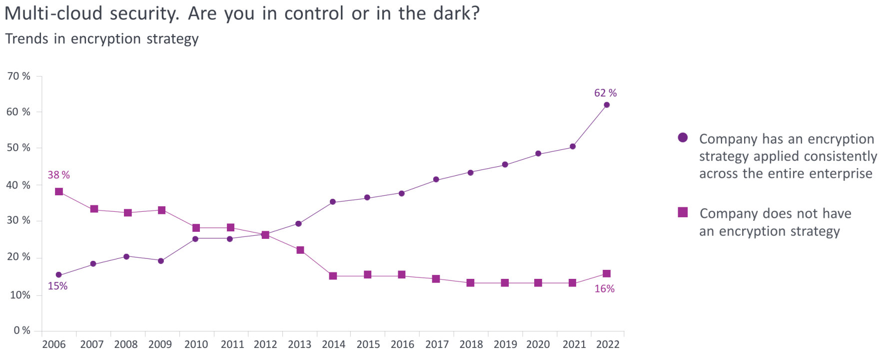

Figure 8: Company outlook towards cryptography focus and implementation. (*2022 Global Encryption Trends Study*)

Some Major Considerations

Side Channel Attacks

With 99.907% accuracy, using a neural network, the bits of the original message could be recovered even after being encrypted by CRYSTALS-Kyber. (Dubrova et al.)

Byte	Bit position in byte								avg
	0	1	2	3	4	5	6	7	
avg	0.9994	0.9991	0.9993	0.9990	0.9988	0.9985	0.9993	0.9992	**0.99907**

Table 1: Bit retrieval success with cyclic rotations. (Dubrova et al., 14)

Some Major Considerations (ii)

Depreciated and Long-Term Technology

Vehicles and other technologies can have a very long use time (over 10 years), which might be unsafe if used in a post-quantum world. Some vehicles are in the production pipeline for years, too. (Castelvecchi)

Most cryptographic algorithms are baked into these chips, making the transition difficult and unsustainable — could easily require replacement of the hardware itself.

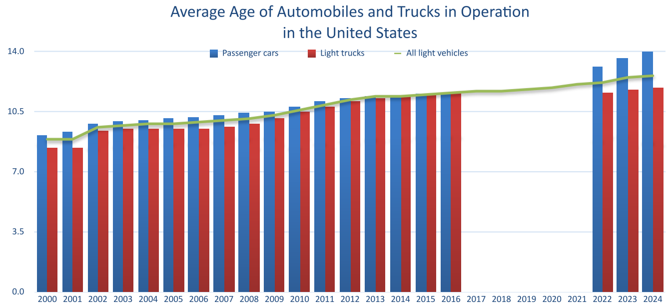

Figure 9: (U.S. Department of Transportation)

Some Major Considerations (iii)

Insecure Algorithms Are Dangerous

SIDH, the Supersingular Isogeny Diffie-Hellman protocol, had its integrity broken in 2022 despite reaching the fourth round of consideration in NIST's post-quantum algorithm standardization process.

SIKEp751, which NIST had given the maximum quantum-security level of 5, could be broken in 3 hours. (Castryck and Decru, 14)

This should be concerning!

- What does this mean for other PQC candidates?
- What lengths should we go to verifying their integrity?
- How many resources should we dedicate to that in comparison to finding more viable algorithms?

What a Transition to PQC Entails — Bitcoin

Quick Information on Bitcoin

Uses ECDSA in its key-pair technology, particularly the Secp256k1 parameterization, which is susceptible to quantum attacks.

UTXOs, or unspent transaction units, are one of the core blocks that record unspent Bitcoin which use ECDSA.

$1.39 billion average in trading volume per hour. (CoinGecko)

Figure 10: (CoinGecko)

One Potential Transition Method

1. Restrain newly created UTXOs to a post-quantum algorithm.
2. Move current-technology UTXOs to their quantum-safe form.

One Potential Transition Method (ii)

Upgrading UTXOs are itself a transition and therefore must complete with other transactions on the network. The long and short of it is that this takes time.

Bandwidth	Lower Bound on Time Taken			
	ECDSA-Based UTXOs		Schnorr-Based UTXOs	
	Hours	Days	Hours	Days
25%	7311.83	304.66	5227.18	217.80
50%	3655.92	152.33	2613.59	108.90
75%	2437.28	101.55	1742.39	72.60
100%	1827.96	76.16	1306.80	54.45

Table 2: Lower-bound downtime needed to move vulnerable UXTOs to a post-quantum algorithm. (Pont et al., 5)

Current Mainstream Quantum Chips

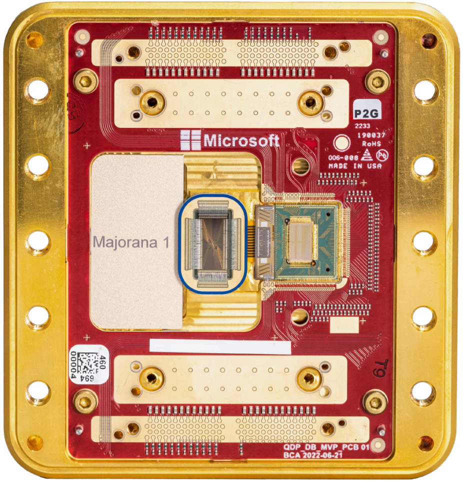

Figure 11: Majorana 1 chip (Microsoft Quantum)

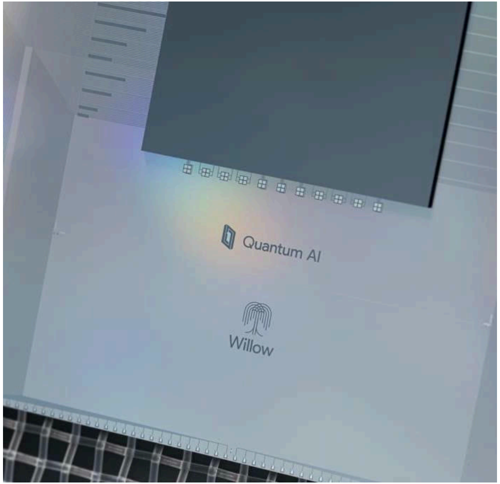

Figure 12: Willow chip (Google Quantum AI)

Works Cited

2022 Global Encryption Trends Study. Entrust, 2022, https://www.entrust.com/resources/reports/global-encryption-trends-study.

Castelvecchi, Davide. "The Race to Save the Internet from Quantum Hackers." *Nature*, vol. 602, no. 7896, Feb. 2022, pp. 198–201, https://doi.org/10.1038/d41586-022-00339-5.

Castryck, Wouter, and Thomas Decru. *An Efficient Key Recovery Attack on SIDH*. 2022, https://eprint.iacr.org/2022/975.

Dubrova, Elena, et al. *Breaking a Fifth-Order Masked Implementation of CRYSTALS-Kyber by Copy-Paste*. 2022, https://eprint.iacr.org/2022/1713.

Kute, Seema, et al. "Analysis of RSA and Shor's Algorithm for Cryptography: A Quantum Perspective." *AIP Conference Proceedings*, vol. 3222, Jan. 2024, p. 40004, https://doi.org/10.1063/5.0227773.

Latticeunitcellplot3d | Wolfram Function Repository. https://resources.wolframcloud.com/FunctionRepository/resources/LatticeUnitCellPlot3D.

Mosca, Michele, and Marco Piani. *2024 Quantum Threat Timeline Report - Global Risk Institute*. 6 Dec. 2024, https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/.

Works Cited (ii)

Pont, Jamie J., et al. *Downtime Required for Bitcoin Quantum-Safety*. 2024, https://arxiv.org/abs/2410.16965.

What Is Lattice-Based Cryptography?. 12 May 2020, https://utimaco.com/service/knowledge-base/post-quantum-cryptography/what-lattice-based-cryptography.

Additional Content

Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce. *Post-Quantum Cryptography | CSRC | CSRC*. https://csrc.nist.gov/projects/post-quantum-cryptography.

Rabbit-hole Content

Standards for Efficient Cryptography [SECG]. *SEC 2: Recommended Elliptic Curve Domain Parameters*. 27 Jan. 2010, www.secg.org/sec2-v2.pdf.