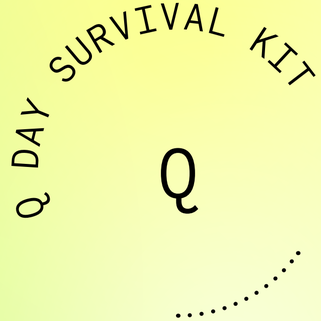
QUANTUM
CYBERSECURITY



KALYANA, LOGAN, & MATTIE

SURVIVING Q DAY

GROUP NO.#A12

Are you prepared for **Q DAY???**

THE DAY QUANTUM BECOMES A REALITY

THE SAFE HOLDS THE ANSWER TO SAVING THE DA(Y)TA...

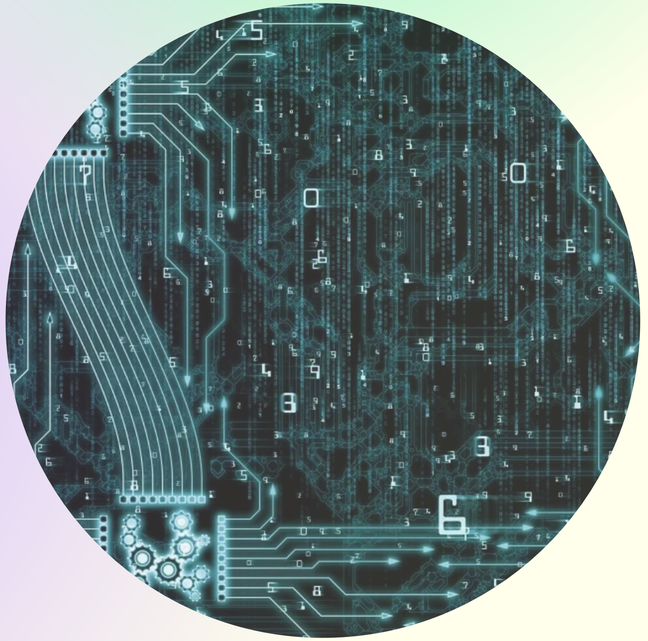
THE KEY WILL BE DEVELOPED

AFTER WE DISCUSS...

- FOUNDATIONS OF ENCRYPTION & QUANTUM
- THE QUANTUM THREAT
- POST-QUANTUM ENCRYPTION

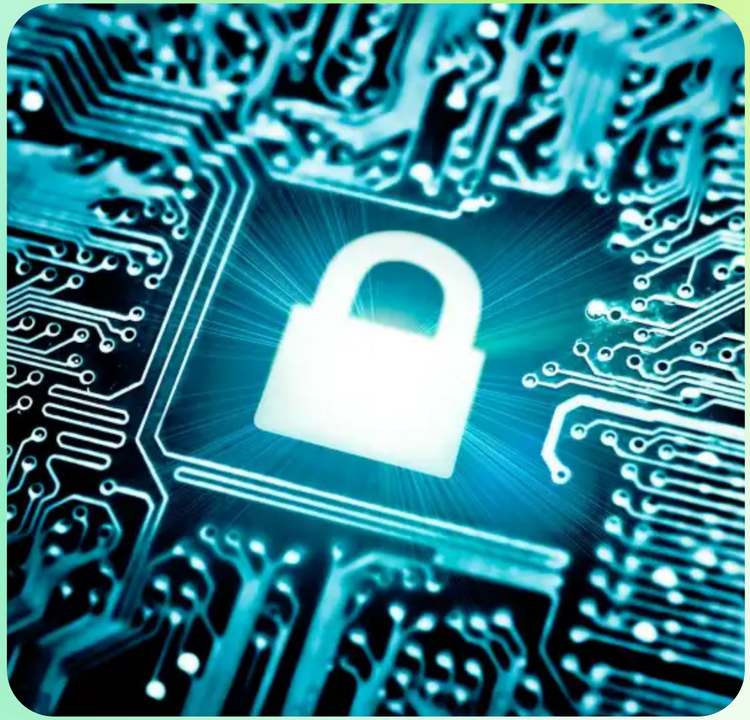
ACT I
THE WORLD BEFORE Q DAY

TODAY!



BASIC METHODS OF ENCRYPTION &
INTRODUCTION TO QUANTUM COMPUTING

THE FUNDAMENTALS OF ENCRYPTION



PLAIN TEXT TO CIPHERTEXT

CIPHERTEXT: ILLEGIBLE TRANSFORMATION OF PLAINTEXT

ENCRYPTION ALGORITHM CONVERTS PLAINTEXT TO CIPHERTEXT

KEY CONVERTS CIPHERTEXT TO PLAINTEXT

PUBLIC KEY

THE KEY!

(ASYMMETRIC) ENCRYPTION

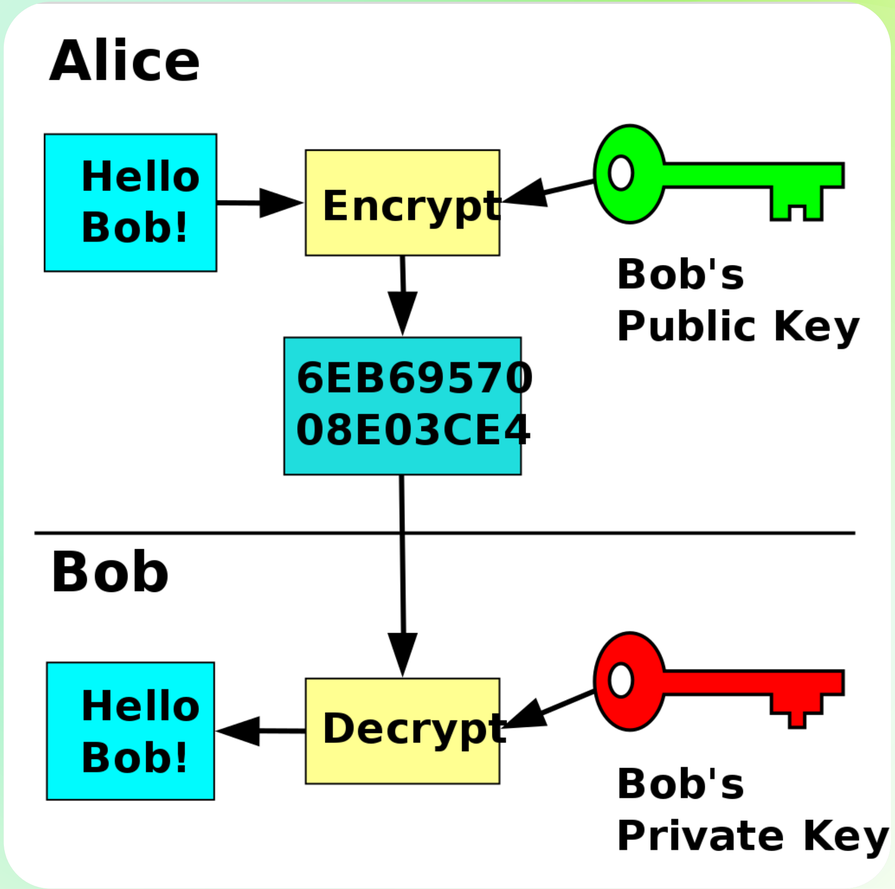
EVERYONE HAS A PUBLIC AND A PRIVATE KEY

PUBLIC KEY: EVERYBODY CAN SEE

PRIVATE KEY: ONLY THE OWNER CAN SEE

DATA ENCRYPTED WITH ONE’S PUBLIC KEY CAN ONLY BE DECRYPTED WITH THEIR PRIVATE KEY

HOW ASYMMETRIC ENCRYPTION **WORKS** —



RSA

CONVENTIONAL COMPUTERS CAN’T CRACK THIS!

PUBLIC-KEY ENCRYPTION ALGORITHM

OLD AND WIDELY USED

PRIVATE KEY IS VERY HARD TO DERIVE FROM THE PUBLIC KEY

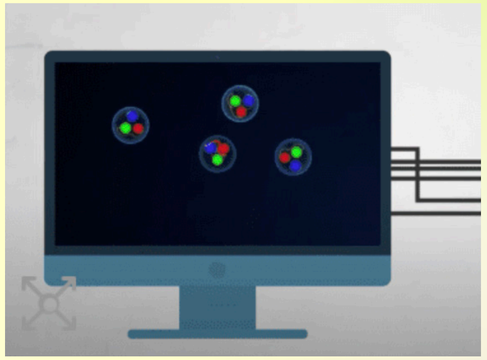
TAKES ADVANTAGE OF DIFFICULT FINDING FACTORS OF LARGE PRIME NUMBERS

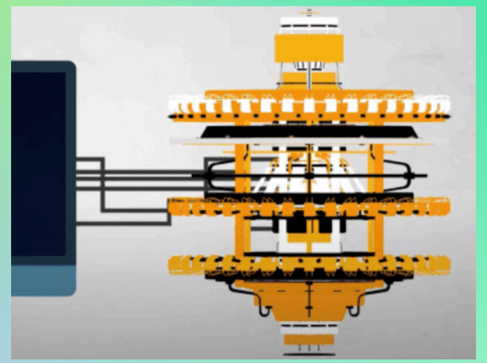
TAKES CONVENTIONAL COMPUTERS TOO LONG TO CRACK

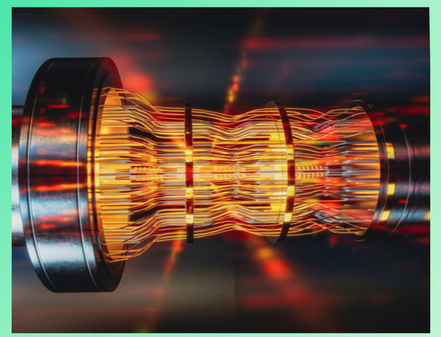
QUANTUM COMPUTING

FUNDAMENTALS

QUANTUM PARTICLES ARE WEIRD!!







CLASSICAL COMPUTERS USE TRANSITORS

- TINY SWITCHES
- ON OR OFF

QUANTUM COMPUTERS USE QUBITS

- QUANTUM PARTICLES
- AMBIGUOUS STATES OF BOTH AND NEITHER ON OR OFF

SUPERPOSITION

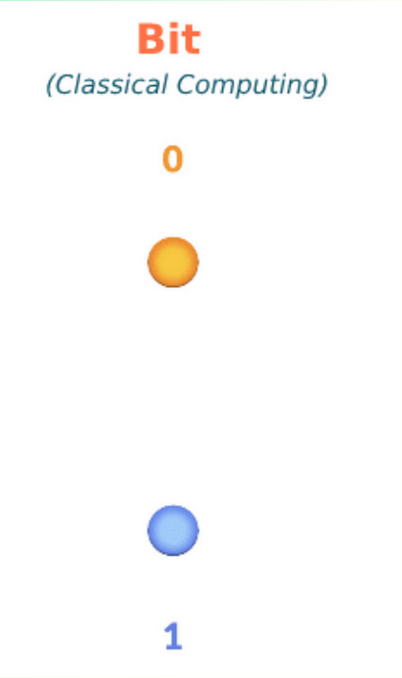
ALLOWS FOR RAPID PARALLELISM OF PROCESSING DATA

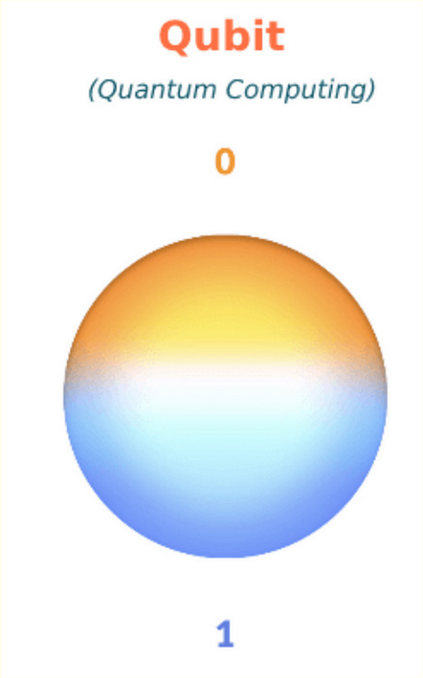
QUANTUM PARTICLES EXIST IN A COMBINATION BETWEEN STATES

DETERMINES A STATE UPON MEASUREMENT

HEAVILY UTILIZED IN QUANTUM COMPUTING FOR PARALLELISM

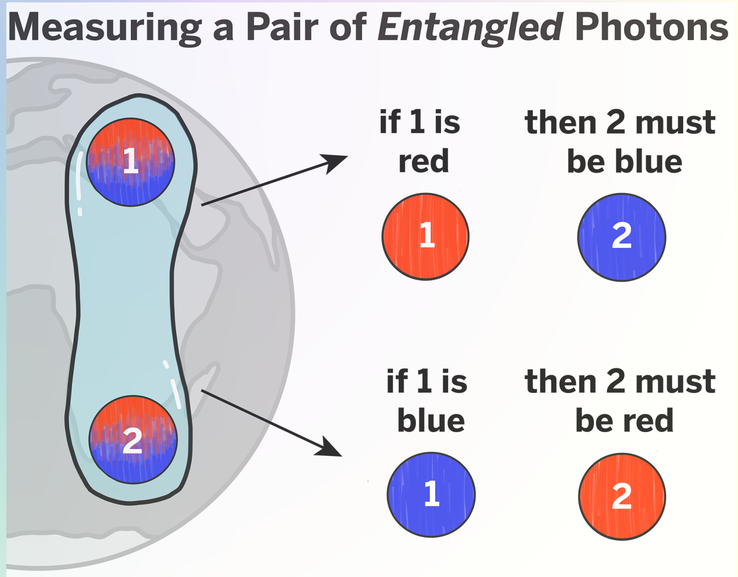
ALLOWS FOR MULTIPLE CALCULATIONS TO BE PERFORMED SIMULTANEOUSLY





ENTANGLEMENT

FASTER THAN LIGHT INFORMATION TRAVEL?



QUANTUM PARTICLES CAN BECOME ENTANGLED (BOUND) WITH OTHERS

KNOWING THE STATE OF ONE TELLS YOU SOMETHING ABOUT THE OTHER

ALLOWS YOU TO INSTANTLY GAIN INFORMATION ABOUT ANOTHER PARTICLE!

NOT ACTUALLY FASTER THAN LIGHT :(

ACT II THE ARRIVAL OF Q-DAY

QUANTUM LEAP!

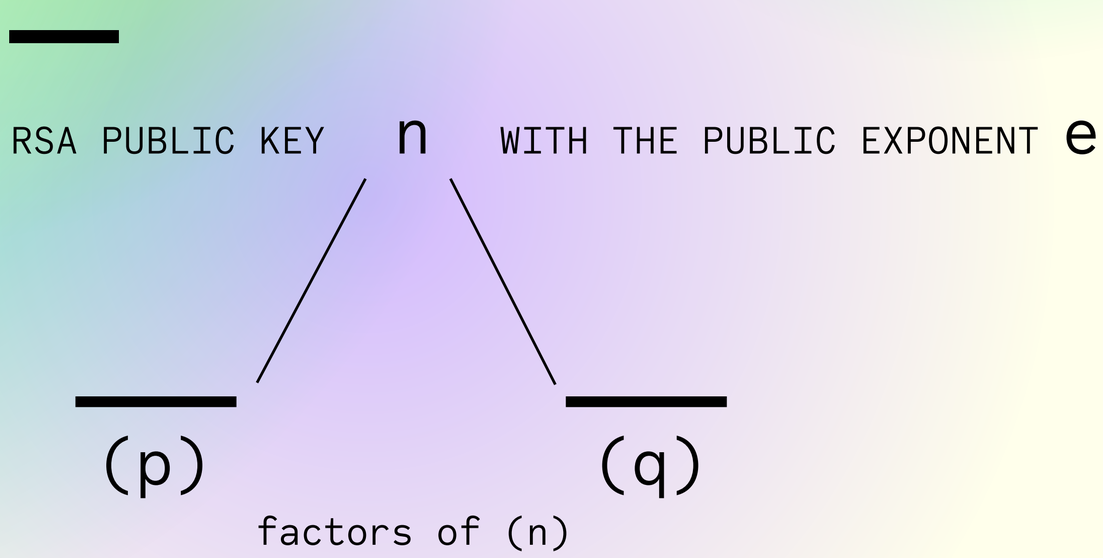
WHEN QUANTUM COMPUTING MEETS ENCRYPTION

HOW ONE WOULD HYPOTHETICALLY GO ABOUT HACKING THE RSA AND INITIATING Q DAY?

STEP ONE

OPEN SOURCE

OBTAIN THE RSA's PUBLIC KEY



Now, The RSA relies on the **DIFFICULTY and TIME it takes** to factor large semi-primes to keep its security.

Now, The RSA relies on the

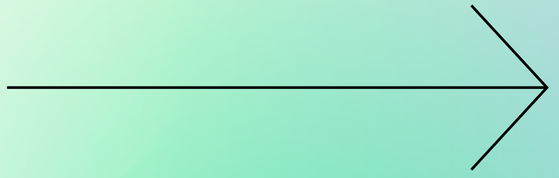
~~**DIFFICULTY and TIME it takes**~~

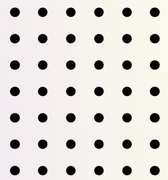
to factor large semi-primes to keep its security.

QUANTUM ELIMINATES BOTH ISSUES

HOW?

WELL IN THIS QUANTUM PROCESS...





SUPERPOSITION ALLOWS FOR THE PARALLEL CONSIDERATION OF MANY POSSIBILITIES

ENTANGLEMENT ENSURES THAT THE OUTCOMES ARE INTERCONNECTED IN A WAY THAT CAN INFLUENCE EACHOTHER

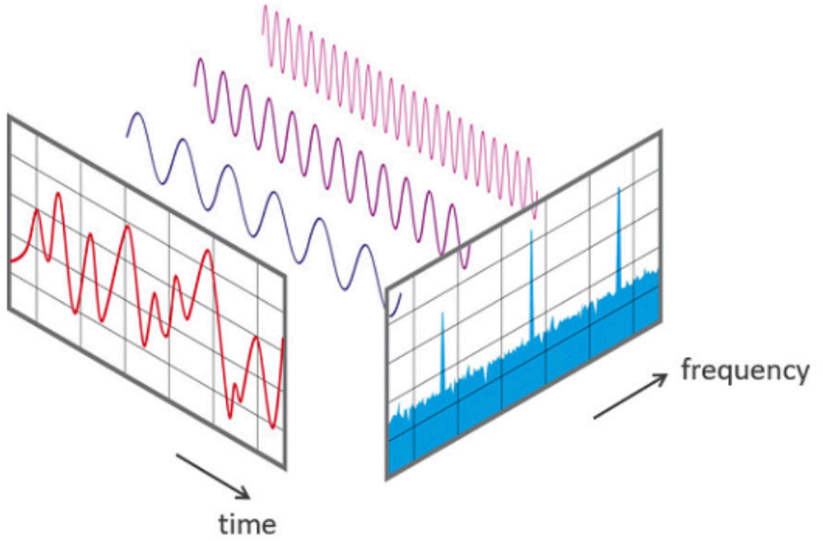
AND QUANTUM INTERFERENCE HELPS TO ELIMINATE INCORRECT PATHS, HONING IN ON THE CORRECT SOLUTION.

QUANTUM FOURIER TRANSFORM

SUPERPOSITION: QFT TAKES ADVANTAGE OF SUPERPOSITION BY PROCESSING A QUANTUM STATE THAT REPRESENTS A COMBINATION OF ALL POSSIBLE INPUTS SIMULTANEOUSLY

PARALLELISM: BECAUSE OF SUPERPOSITION, THE QFT CAN ANALYZE THE ENTIRE SPECTRUM OF POSSIBILITIES AT ONCE.

EFFICIENCY: THE EFFICIENCY OF QFT IS CRUCIAL FOR ALGORITHMS LIKE SHOR'S IN A REASONABLE TIMEFRAME.



View of a signal in the time and frequency domain

FOURIER TRANSFORM TO MEASURE SOUNDWAVES

IMAGINE YOU HAVE A MUSICAL NOTE; THE FOURIER TRANSFORM CAN TELL YOU WHAT PITCHES (FREQUENCIES) ARE PRESENT AND HOW LOUD EACH PITCH IS.

ONCE WE OBTAIN

(P) AND (Q) …

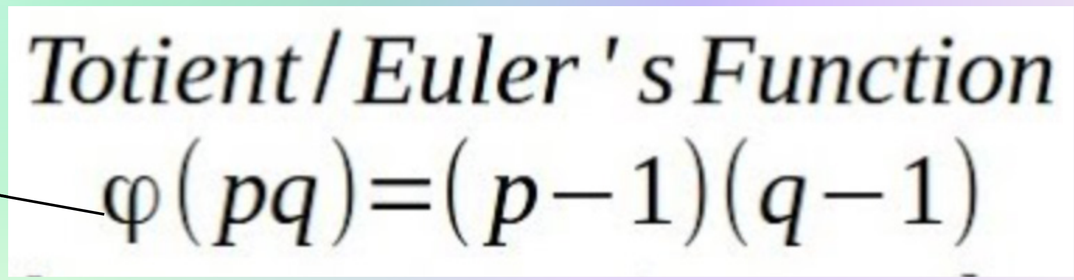
THE FACTORS OF (N)

FACTORS OF N

PUBLIC KEY

PLUG N CHUG

STEP 3:
GET THIS VALUE



FINAL STEP

W**FIND** (d) ...

NOW THAT WE HAVE

e **AND** $\phi(n)$

PRIVATE KEY!

THE MODULAR MULTIPLICATIVE INVERSE OF e modulo $\phi(n)$

WHICH MEANS SOLVING FOR (d)
IN THE EQUATION:

$$ed \equiv 1 \mod \phi(n).$$

CROSSROADS OF CYBERSECURITY

QUANTUM LEAP!

SHIFT TO QUANTUM-RESISTANT ALGORITHMS IS IMMINENT

INTEROPERABILITY AND SECURITY DURING TRANSITION ARE CRITICAL

TYPES OF QUANTUM RESISTANT ALGORITHMS BEING DEVELOPED

CHALLENGES INVOLVED IN TRANSITIONING FROM CURRENT SUSTEMS TO QUANTUM-SAFE SYSTEMS

ACT III
SURVIVING Q-DAY

QUANTUM-SAFE ENCRYPTION

PRACTICAL STEPS FOR PREPAREDNESS

ONGOING EFFORTS IN CYBERSECURITY

SO WHAT NOW?

QUANTUM KEY DISTRIBUTION —

BASICS OF QKD

- GENERATION OF A CRYPTOGRAPHIC KEY BY UTILIZING QUANTUM
- UTILIZES THE UNIQUE PROPERTIES OF PHOTONS
- THE KEY IS GENERATED AND TRANSMITTED USING A PHOTON’S GIVEN POLARITY

DRAWBACKS OF QKD

- NO WAY OF VERIFYING KEY AUTHENTICITY
- KEY GENERATION RATE DECREASES OVER DISTANCE
- REQUIRES EXPENSIVE EQUIPTMENT

POST-QUANTUM

CRYPTOGRAPHY STANDARIZATION

PROJECT

MANAGED BY THE NATIONAL INSTITUE OF STANDARD TECHNOLOGY (NIST)

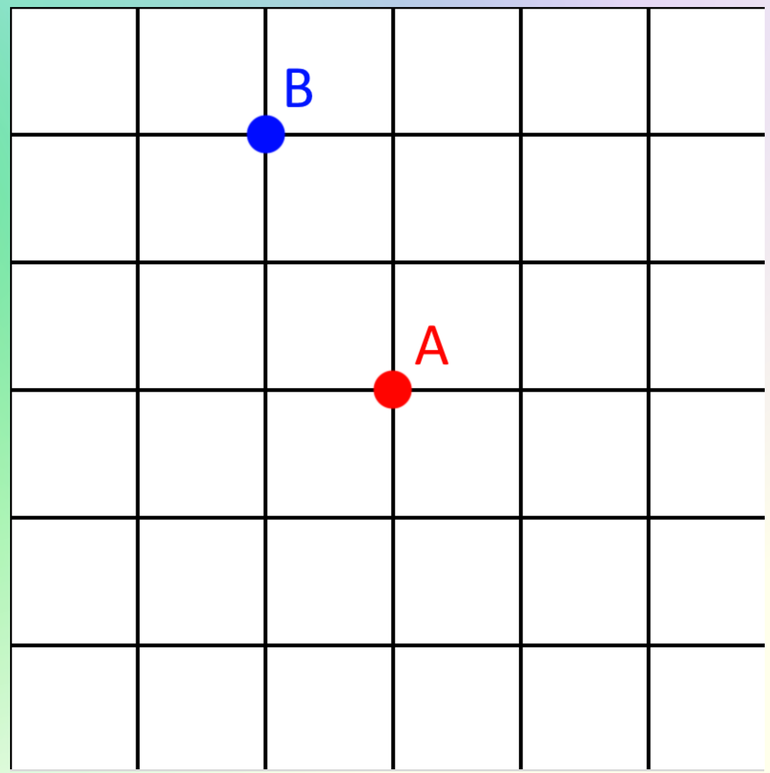
COMPETITION TO DEVELOP QUANTUM RESISTANT ALGORITHMS

69 ALGORITHMS ENTERED!

4 WINNERS SELECTED!!

- CRYSTALS-Kyber
- CRYSTALS-Dilithium
- FALCON
- SPHINCS+

HOW MANY VECTORS DOES IT TAKE TO GET FROM POINT A TO POINT B?



STRUCTURED LATTICES

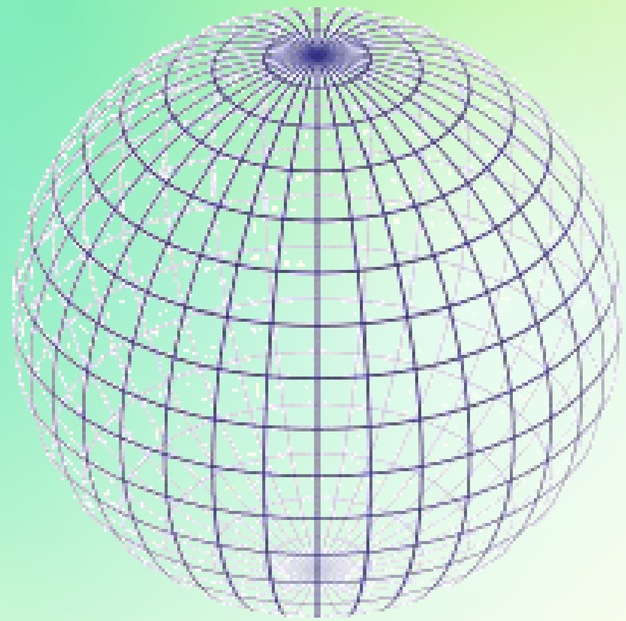
HOW DOES IT BEAT QUANTUM COMPUTERS?

BASICS OF CRYSTALS-Kyber, CRYSTALS-Dilithium, and FALCON

A STRUCTURED LATTICE CAN THEORETICALLY HAVE AS MANY DIMENSIONS AS NECESSARY

THE LOCATION OF ENCRYPTED DATA DOES NOT HAVE TO BE DIRECTLY ON A LATTICE POINT.

IN THIS CASE, THE COMPUTER ONLY HAS TO FIND THE NEAREST POINT



THE **BACKUP**

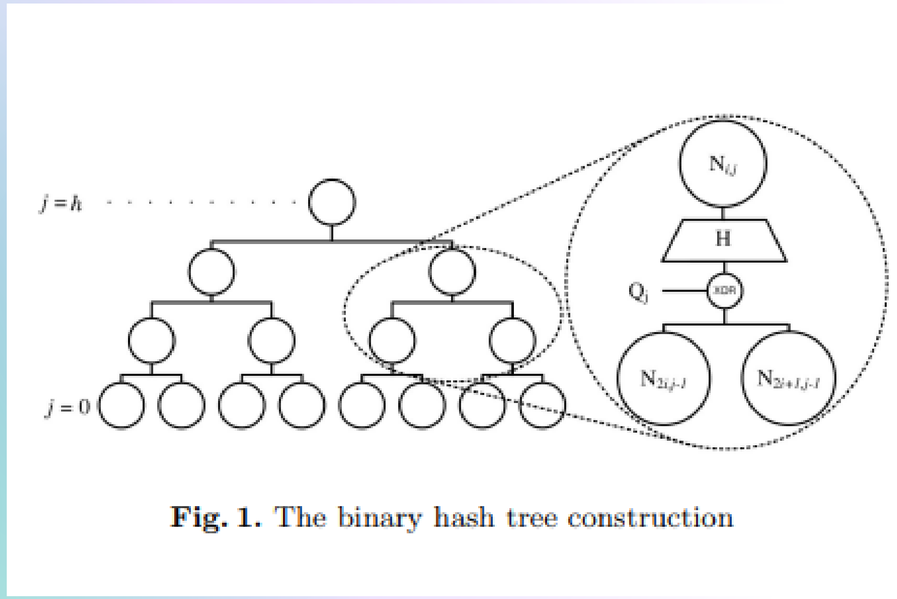


Fig. 1. The binary hash tree construction

SPHINCS+ WAS SELECTED
BY THE NIST AS A BACKUP

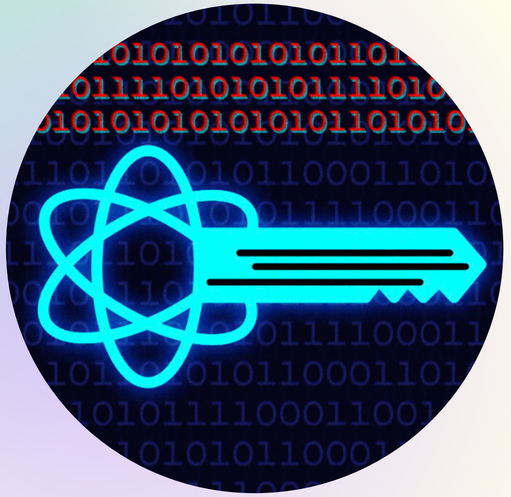
- BUILT UP OF BINARY HASH TREES
- BULKY AND SLOWER THAN LATTICE

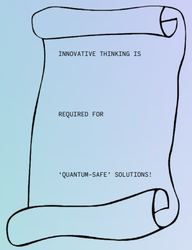
PART OF SELECTION DUE TO
NOT BEING LATTICE-BASED

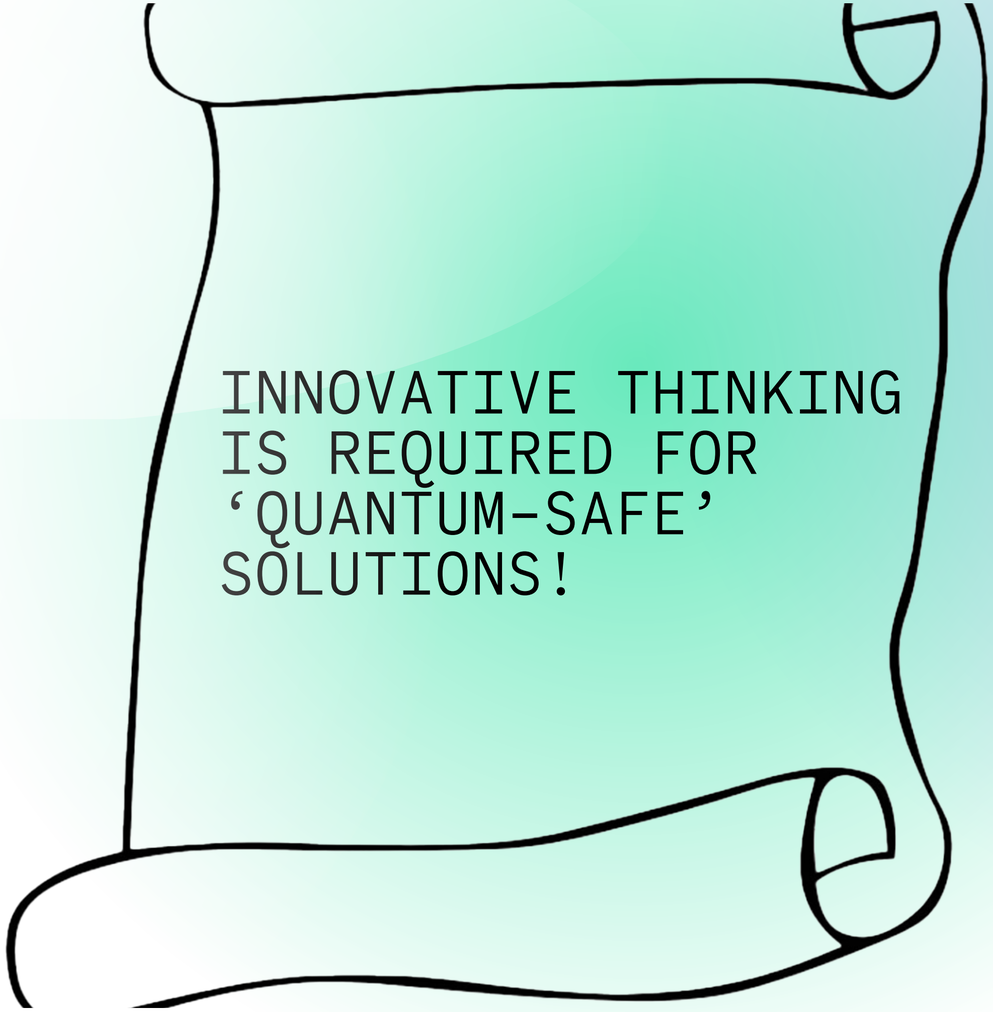
YOU SURVIVED Q-DAY!

HERE'S THE KEY

—




INNOVATIVE THINKING IS
REQUIRED FOR
'QUANTUM-SAFE' SOLUTIONS!



QUANTUM ALGORITHMS COULD ‘UNLOCK’ THE SAFE AND PROTECT US FROM QUANTUM THREATS

MAKING THE FUTURE ‘QUANTUM-SAFE’

- DEVELOPMENT OF QUANTUM-RESISTANT ALGORITHMS
- GLOBAL EFFORTS IN STANDARDIZING POST-QUANTUM CRYPTOGRAPHY
- ONGOING RESEARCH IS KEY TO STAYING AHEAD OF QUANTUM THREATS

CITATIONS —

Q DAY SURVIVAL PACK

CRYSTALS. (2020, December 23). Kyber. CRYSTALS: Cryptographic Suite for Algebraic Lattices. Retrieved from https://pq-crystals.org/kyber/index.shtml

CRYSTALS. (2021, February 16). Dilithium. CRYSTALS: Cryptographic Suite for Algebraic Lattices. Retrieved from https://pq-crystals.org/dilithium/index.shtml

Fouque, P. A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Prest, T., Ricosset, T., Seiler, G., Whyte, W., & Zhang, Z. (n.d.). FALCON. Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU. Retrieved from https://falcon-sign.info/

Hülsing, A., Aumasson, J. P., Bernstein, D. J., Beullens, W., Dobraunig, C., Eichlseder, M., Fluhrer, S., Gazdag, S. L., Kampanakis, P., Kölbl, S., Kudinov, M., Lange, T., Lauridsen, M. M., Mendel, F., Niederhagen, R., Rechberger, C., Rijneveld, J., Schwabe, P., & Westerbaan, B. (2023, August 02). SPHINCS+: Stateless hash-based signatures. Retrieved from https://sphincs.org/index.html

National Institute of Standards and Technology. (2022, July 05). NIST Announces First Four Quantum-Resistant Cryptographic Algorithms. Retrieved from https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

National Security Agency. (n.d.). Quantum Key Distribution (QKD) and Quantum Cryptography (QC). Retrieved from https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

Magaña, E. M. (2022). Kyber Crystal [Photograph]. Retrieved from https://www.artstation.com/artwork/RnLwAv

Veritasium. (2023, March 20). How Quantum Computers Break The Internet… Starting Now [Video]. Retrieved from https://www.youtube.com/watch?v=-UrdExQW0cs

TüftelLab. (2022, May 03). Quantum Key Distribution, BB84 - simply explained | Quantum 1x1 [Video]. Retrieved from https://www.youtube.com/watch?v=8hNQyTdNil4

Takeoka, M., Guha, S., & Wilde, M. (2014). Fundamental rate-loss tradeoff for optical quantum key distribution. Nature Communications, 5(5235). https://doi.org/10.1038/ncomms6235

Bernstein, D. J., Hopwood, D., Hülsing, A., Lange, T., Niederhagen, R., Papachristodoulou, L., Schneider, M., Schwabe, P., & Wilcox-O'Hearn, Z. (2015). SPHINCS: Practical Stateless Hash-Based Signatures. Department of Computer Science, University of Illinois at Chicago.

Caltech. (n.d.). What is quantum computing?. Caltech Science Exchange. Retrieved from https://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-computing-computers

Cobb, M. (2021, November 4). What is the RSA algorithm? TechTarget. Retrieved from https://www.techtarget.com/searchsecurity/definition/RSA

OpenText. (n.d.). What is encryption and how does it work? Retrieved from https://www.opentext.com/what-is/encryption

Quantum Xchange. (2022, December 15). Quantum Entanglement Communication: Quantum Xchange. Retrieved from https://quantumxc.com/blog/is-quantum-communication-faster-than-the-speed-of-light/

MIT OpenCourseWare. (2014, June 18). Lecture 1: Introduction to Superposition [Video]. Retrieved from https://www.youtube.com/watch?v=lZ3bPUKo5zc

Veritasium. (2023, March 20). How Quantum Computers Break The Internet… Starting Now [Video]. Retrieved from https://www.youtube.com/watch?v=-UrdExQW0cs

Shor, P. W. (1994). Algorithms for Quantum Computation: Discrete Logarithms and Factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 124-134. IEEE. https://doi.org/10.1109/SFCS.1994.365700

3Blue1Brown. (2017, December 17). Quantum Computing for Computer Scientists [Video]. Retrieved from https://www.youtube.com/watch?v=lvTqbM5Dq4Q&t=6s

PBS Space Time. (2018, November 14). How the Quantum Eraser Rewrites the Past [Video]. Retrieved from https://www.youtube.com/watch?v=46owkTBnFx8

Caltech. (n.d.). What is quantum computing?. Caltech Science Exchange. Retrieved from https://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-computing-computers

Cobb, M. (2021, November 4). What is the RSA algorithm? TechTarget. Retrieved from https://www.techtarget.com/searchsecurity/definition/RSA

OpenText. (n.d.). What is encryption and how does it work? Retrieved from https://www.opentext.com/what-is/encryption

Quantum Xchange. (2022, December 15). Quantum Entanglement Communication: Quantum Xchange. Retrieved from https://quantumxc.com/blog/is-quantum-communication-faster-than-the-speed-of-light/

MIT OpenCourseWare. (2014, June 18). Lecture 1: Introduction to Superposition [Video]. Retrieved from https://www.youtube.com/watch?v=lZ3bPUKo5zc

Fermilab. (2020, February 12). Quantum Entanglement: Spooky Action at a Distance [Video]. Retrieved from https://www.youtube.com/watch?v=JFozGfxmi8A

THANK YOU!
QUESTIONS?