QUANTUM CRYPTOGRAPHY

Alex Kish and Erik Danielson

OVERVIEW

- Standard Encryption Methods
- Quantum Computing
- Post Quantum Encryption Methods

"…nobody really understands quantum mechanics." – Richard Feynman

STANDARD ENCRYPTION

Symmetric and Asymmetric

TYPICAL PROCESS

QUANTUM CURVEBALL

QUANTUM DECRYPTION PROCESS

1. Make a crappy guess, g
2. Classical Part
    1. Euclidean Algorithm
    2. Shor's Algorithm
3. Quantum Part

EUCLIDEAN ALGORITHM

- Algorithm for finding the greatest common divisor of two numbers. GCD(N,g)

Rules:

1. If N = 0, then GCD(N,g) = GCD(0,g) = g
2. If g = 0, then GCD(N,g) = GCD(N,0) = N
3. Uses the quotient remainder form:

$$N = g*Q + r \rightarrow N \bmod g$$

EUCLIDEAN ALGORITHM

Example:

GCD(544, 119)

→ 544 = 119*4 + 68

GCD(119, 68)

→ 119 = 68*1 + 51

GCD(68,51)

→ 68 = 51*1 + 17

GCD(51,17)

→ 51 = 17*3 + 0

GCD(17, 0)

→ GCD(544,119) = 17

SHOR'S ALGORITHM

$$A, B \Rightarrow \quad A^P = m \cdot B + 1$$

No common factors

SHOR’S ALGORITHM

$$g^P = m \cdot N + 1 \Rightarrow g^{P/2} \pm 1 = m \cdot N$$

$$\left(g^{P/2} + 1\right)\left(g^{P/2} - 1\right) = m \cdot N$$

THE QUANTUM PART

- Quantum Superposition: a linear combination of quantum states (this linear combination is itself a quantum state)

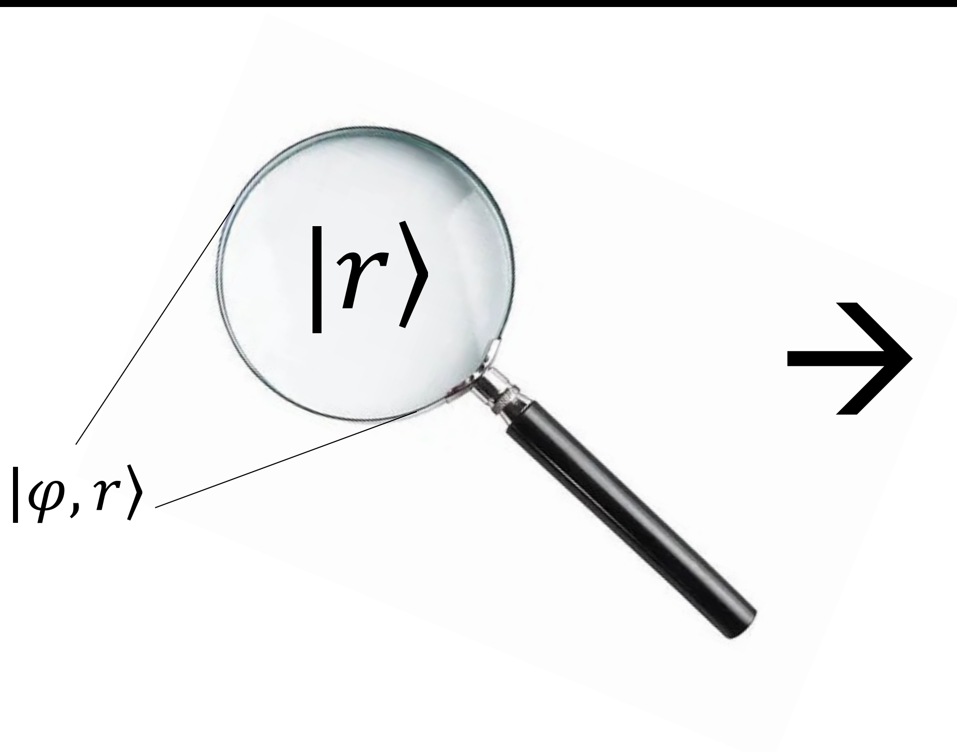
$$|\varphi\rangle = |1\rangle + |2\rangle + |3\rangle + |4\rangle + \cdots + |N-1\rangle$$

THE QUANTUM PART

$$|\varphi\rangle \rightarrow f(\varphi) = g^{\varphi} \rightarrow |\varphi, g^{\varphi}\rangle \rightarrow f(g^{\varphi}) = m \cdot N \; - g^{\varphi} \rightarrow |\varphi, r\rangle$$

$$|\varphi, r\rangle = |1, 32\rangle \; + |2, 6\rangle + |3, 17\rangle + \cdots$$

THE QUANTUM PART



→

$$g^{\varphi} = m_1 \cdot N + r$$

$$\vdots$$

$$g^{\varphi+p} = m_2 \cdot N + r$$

$$\vdots$$

$$g^{\varphi+2p} = m_3 \cdot N + r$$

QUANTUM FOURIER TRANSFORM

"The Fourier transform is a mathematical formula that transforms a signal sampled in time or space to the same signal sampled in temporal or spatial frequency. In signal processing, the Fourier transform can reveal important characteristics of a signal, namely, its frequency components."

– Mathworks.com

$$|r\rangle = |\varphi_1, r\rangle + |\varphi_2, r\rangle + |\varphi_3, r\rangle + \cdots$$

$$|\varphi_1\rangle + |\varphi_2\rangle + |\varphi_3\rangle + \cdots \rightarrow QFT \rightarrow |\, \frac{1}{P}\, \rangle$$

QUANTUM CURVEBALL

$$g \xrightarrow{QC+Shor's} P \rightarrow g^* \xrightarrow{Euclidean\ Alg.} r = 0? \xrightarrow{No} Repeat\ with\ g^*$$

Yes ↓

Access Information

QUANTUM CRYPTOGRAPHY

Using the principles of quantum mechanics to utilize encryption and secure the transmission and storage of data

- Quantum Key Distribution (QKD)
- Quantum coin-flipping
- Position-based
- Device-independent
- Kek protocol
- Y-00 protocol

QUANTUM KEY DISTRIBUTION

Not for encrypting data, but to establish a secure key exchange by two parties

- Photon light particles are sent across fiber optic cables as a qubit (either 1 or 0, based on the spin)
- The sender uses polarized filters to fixate the orientation of each photon to a certain position
- The receiver uses two beam splitters to read the position of each photon
- Compare the received orientations and the sent orientations to make sure they match and were not tampered with

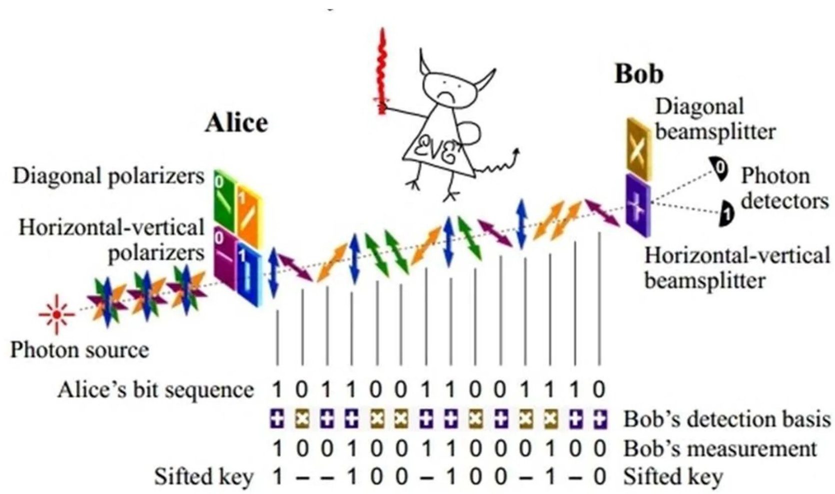


Image: https://wpo-altertechnology.com/quantum-key-distribution-qkd/

THE GOOD AND THE BAD

BENEFIT

Quantum Mechanic: a particle cannot be observed without tampering with the particle, in some way

- Eavesdropping is theoretically impossible
- Observation is detectable
- “Unbreakable”

VULNERABILITIES

- Requires special equipment
- $$$$
- Increased risk to insiders
- Denial of Service Attacks

CURRENT PROBLEM

- Powerful quantum computers make current cryptographic standards obsolete
- Harvest now, decrypt later
- Need to prepare

Image: https://www.citypng.com/photo/8370/hd-among-us-orange-crewmate-character-with-sus-sticky-note-hat-png

POST-QUANTUM CRYPTOGRAPHY

Post-Quantum Cryptography (PQC) are algorithms deemed secure enough to withstand an attack from a quantum computer

NIST hosted a competition

- Cryptography experts submitted 82 algorithms
- 69 were analyzed and evaluated
- Found 15 of the top candidates
- Released standards for 4 of these algorithms*

*Only 3 have been officially released

NIST PQC STANDARDS

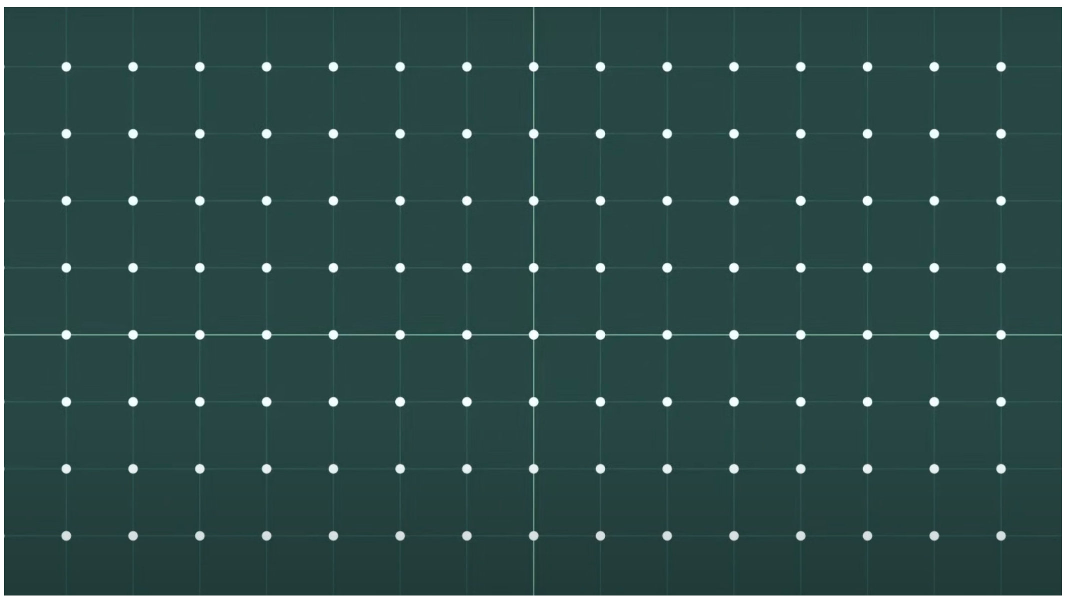
ML-KEM
(Kyber)
Key encapsulation mechanism for general encryption

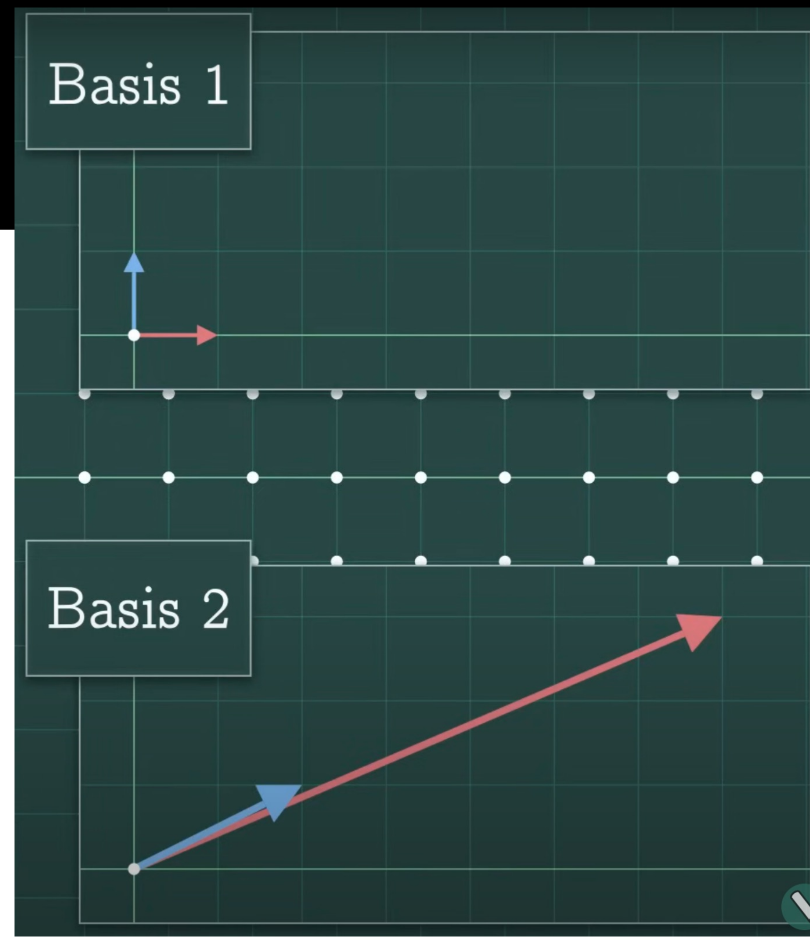
ML-DSA
(Dilithium)
Lattice-based for digital signatures (module vector spaces)

NL-DSA
(Falcon)
Lattice-based for digital signatures (NTRU lattices)

SLH-DSA
(SPHINCS+)
Stateless hash-based digital signature scheme

LATTICE-BASED





Closest Vector Problem and Shortest Vector Problem

LEARNING WITH ERRORS

$$
\begin{aligned}
77x + 7y + 28z + 23w &= 2859 + -3 \\
21x + 19y + 30z + 48w &= 3508 + 2 \\
4x + 24y + 33z + 38w &= 3848 + -1 \\
8x + 20y + 84z + 61w &= 6225 + 0 \\
6x + 53y + 1z + 86w &= 4886 + 4 \\
42x + 86y + 31z + 8w &= 9062 + -1 \\
5x + 24y + 79z + 27w &= 6103 + -2 \\
16x + 7y + 35z + 21w &= 2589 + 2 \\
56x + 18y + 25z + 58w &= 3576 + 0
\end{aligned}
$$

$$
\begin{aligned}
77x + 7y + 28z + 23w &= 2856 \\
21x + 19y + 30z + 48w &= 3510 \\
4x + 24y + 33z + 38w &= 3847 \\
8x + 20y + 84z + 61w &= 6225 \\
6x + 53y + 1z + 86w &= 4890 \\
42x + 86y + 31z + 8w &= 9061 \\
5x + 24y + 79z + 27w &= 6101 \\
16x + 7y + 35z + 21w &= 2591 \\
56x + 18y + 25z + 58w &= 3576
\end{aligned}
$$

Images from ChalkTalk youtube video:
https://youtu.be/K026C5YaB3A?si=yFmMreh2ikb3amno

TAKEAWAYS

- Quantum computers are on the horizon
- Really good at making guesses
- Be proactive - integrate PQC algorithms
- But, quantum is confusing
- And does anyone really understand it?

SOURCES

- National Institute of Standards and Technology. "FIPS 203 Module-Lattice-Based Key Encapsulation Mechanism Standard." *Federal Information Processing Standards Publication*, Computer Security, U.S. Department of Commerce, 13 Aug. 2024, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf.

- National Institute of Standards and Technology. "FIPS 204 Module-Lattice-Based Digital Signature Standard." *Federal Information Processing Standards Publication*, Computer Security, U.S. Department of Commerce, 13 Aug. 2024, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf.

- National Institute of Standards and Technology. "FIPS 205 Stateless Hash-Based Digital Signature Standard." *Federal Information Processing Standards Publication*, Computer Security, U.S. Department of Commerce, 13 Aug. 2024, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.pdf.

- Chalk Talk. "Lattice-based Cryptography: The Tricky Math of Dots." *YouTube*, 4 Jan. 2023, https://youtube.com/watch?v=QDdOoYdb748.

- Chalk Talk. "Learning With Errors: Encrypting With Unsolvable Equations." *YouTube*, 5 Jan. 2023, https://youtube.com/watch?v=K026C5YaB3A.

- Schneider, Josh and Smalley Ian. "What is Quantum Cryptography?." *IBM*, 1 Dec. 2023, https://ibm.com/think/topics/quantum-cryptography.

- "What Is Post-Quantum Cryptography?." *NIST*, 10 Apr. 2025, https://nist.gov/cybersecurity/what-post-quantum-cryptography.

- "Dilithium Vs. Falcon." 5 July 2024, https://wolfssl.com/dilithium-vs-falcon.

- "A Brief Guide to Quantum Encryption vs. Post-Quantum Cryptography [INFOGRAPHIC]." *QuantumXchange*, 19 Nov. 2018, https://quantumxc.com/blog/quantum-encryption-vs-post-quantum-cryptography-infographic.

- National Security Agency. "Quantum Key Distribution (QKD) and Quantum Cryptography (QC)." *National Security Agency*, https://nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC.

SOURCES

- “Fourier Transforms.” *MathWorks,* https://mathworks.com/help/matlab/math/fourier-transforms.html.
- “Difference Between Symmetric and Asymmetric Key Encryption.” *GeeksforGeeks*, 5 Feb. 2025, https://geeksforgeeks.org/difference-between-symmetric-and-asymmetric-key-encryption.
- “Shor’s Factorization Algorithm.” *GeeksforGeeks*, 16 Jan. 2024, https://geeksforgeeks.org/shors-factorization-algorithm.
- “The Euclidean Algorithm.” *Khan Academy*. https://khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/the-euclidean-algorithm.
- Mental Outlaw. “How RSA Encryption Works.” *YouTube*, 10 Feb. 2021, https://youtube.com/watch?v=ZPXVSJnDA_A.
- MinutePhysics. “How Quantum Computers Break Encryption | Shor’s Algorithm Explained.” *YouTube*, 1 May 2019, https://youtube.com/watch?v=lvTqbM5Dq4Q.