The Quest for Quantum-Safe Cryptography: Navigating the Path to Securing Our Future

Inbar Badian

Don’t Worry!
This is not a Cryptography Lecture

But if there are risks to encryption…

Encryption is the process of converting plain, readable data into a secret code to keep it secure from unauthorized access

Digital Signatures

Crypto-Currency

Secure Chatting Service

Encryption is the process of converting plain, readable data into a secret code to keep it secure from unauthorized access

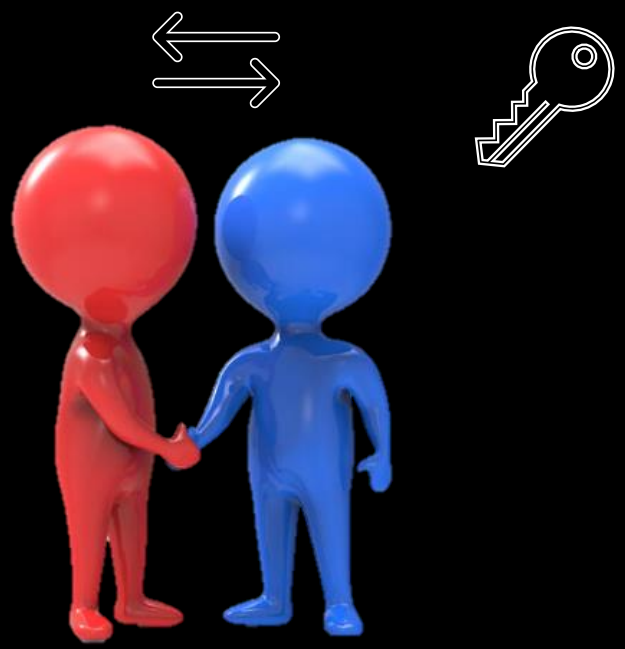
Encrypted Emails

SSL/TLS Encryption

Safe Online Banking

Symmetric vs. Asymmetric Encryption

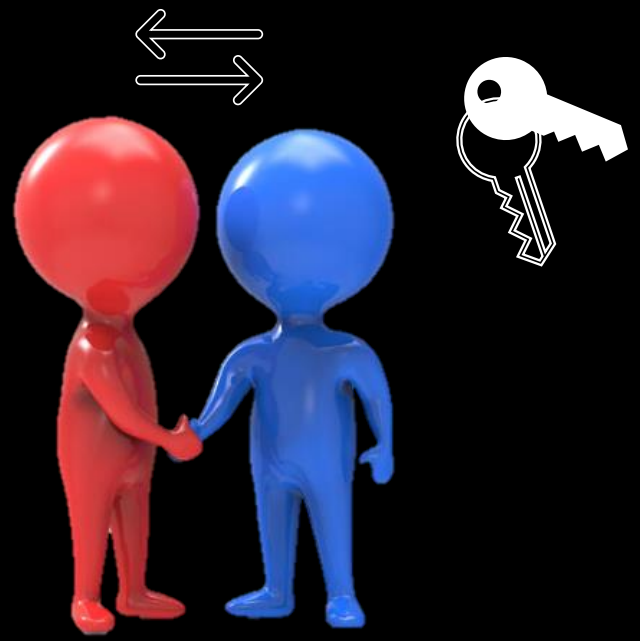
Exchange Symmetric



Symmetric Encryption

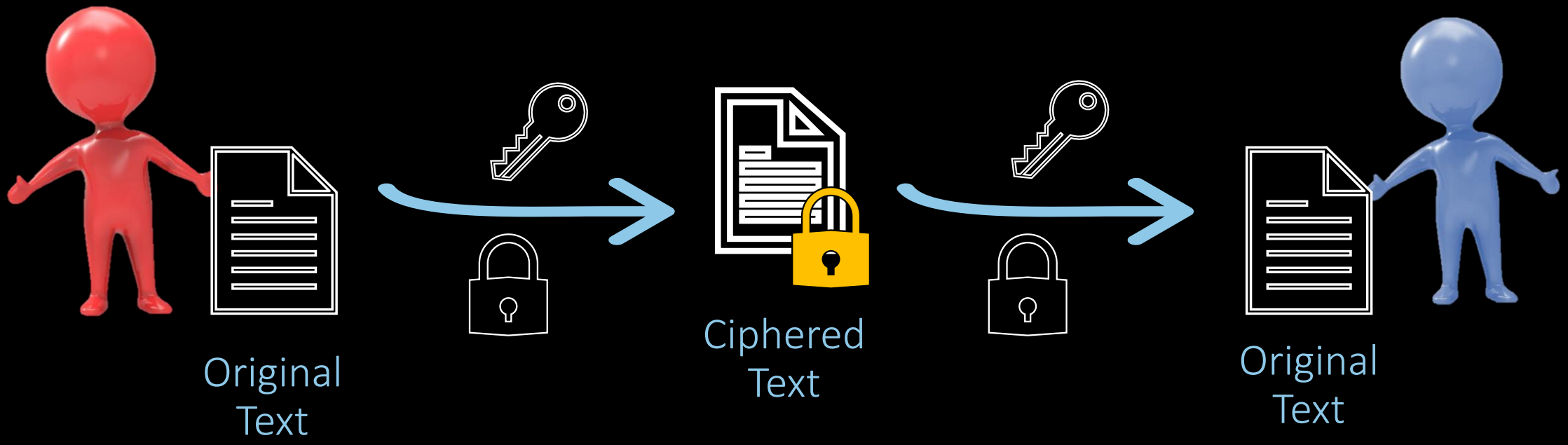
VS

Public Key Encrypts
Private Key Decrypts

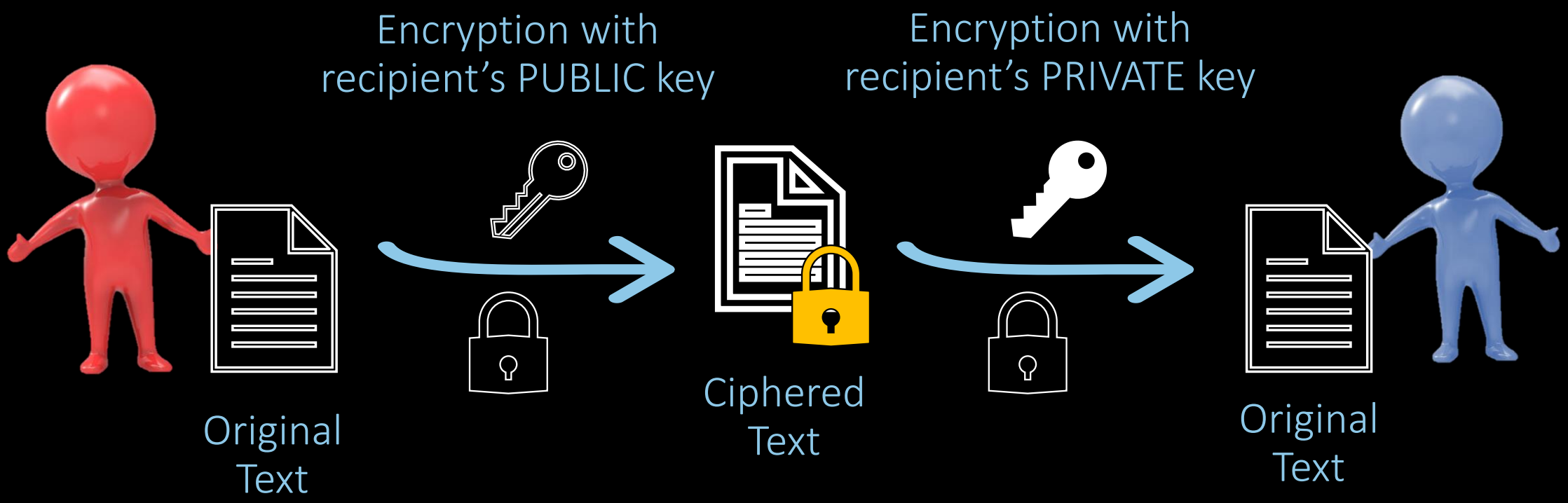


Asymmetric Encryption

Symmetric Encryption

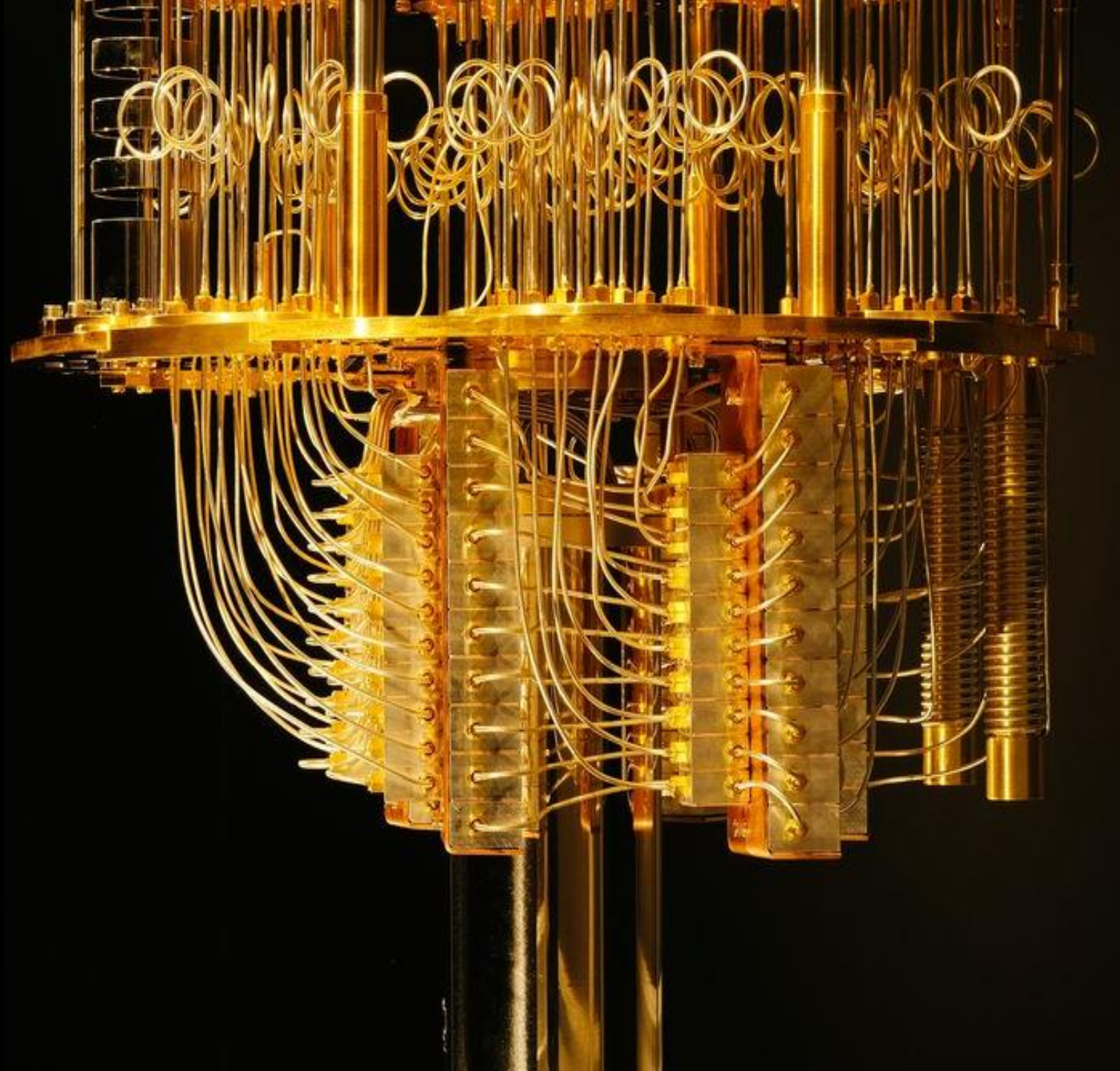


Asymmetric Encryption



? ? ?

What do quantum computers have to do with encryption?



Quantum Computing is a game changer for humanity

Quantum computers have the potential to revolutionize many fields by solving problems that are currently beyond the capabilities of classical computers

Quantum computers have the potential to revolutionize many fields by solving problems that are currently beyond the capabilities of classical computers

Simulation

Handle the complexity and ambiguity of systems that would overload classical computers.

Quantum computers have the potential to revolutionize many fields by solving problems that are currently beyond the capabilities of classical computers

Simulation

Handle the complexity and ambiguity of systems that would overload classical computers.

Optimization

Optimize the process of complex systems by finding solutions that were previously impossible.

Quantum computers have the potential to revolutionize many fields by solving problems that are currently beyond the capabilities of classical computers

Simulation

Handle the complexity and ambiguity of systems that would overload classical computers.

Optimization

Optimize the process of complex systems by finding solutions that were previously impossible.

Machine Learning

Devise and implement quantum software that enables faster machine learning.

Quantum computers have the potential to revolutionize many fields by solving problems that are currently beyond the capabilities of classical computers

Simulation

Handle the complexity and ambiguity of systems that would overload classical computers.

Optimization

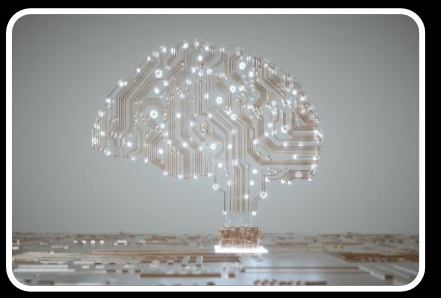
Optimize the process of complex systems by finding solutions that were previously impossible.

Machine Learning

Devise and implement quantum software that enables faster machine learning.







Quantum computers threaten asymmetric encryption

Quantum computers threaten asymmetric encryption




Quantum computers threaten asymmetric encryption

Shor's algorithm attacks the underlying mathematics of factoring (breaks RSA) and discrete logs (breaks Diffie Helman and Elliptic Curve Variants) - The basis of public-key systems

Quantum computers threaten asymmetric encryption

Shor's algorithm attacks the underlying mathematics of factoring (breaks RSA) and discrete logs (breaks Diffie Helman and Elliptic Curve Variants) - The basis of public-key systems

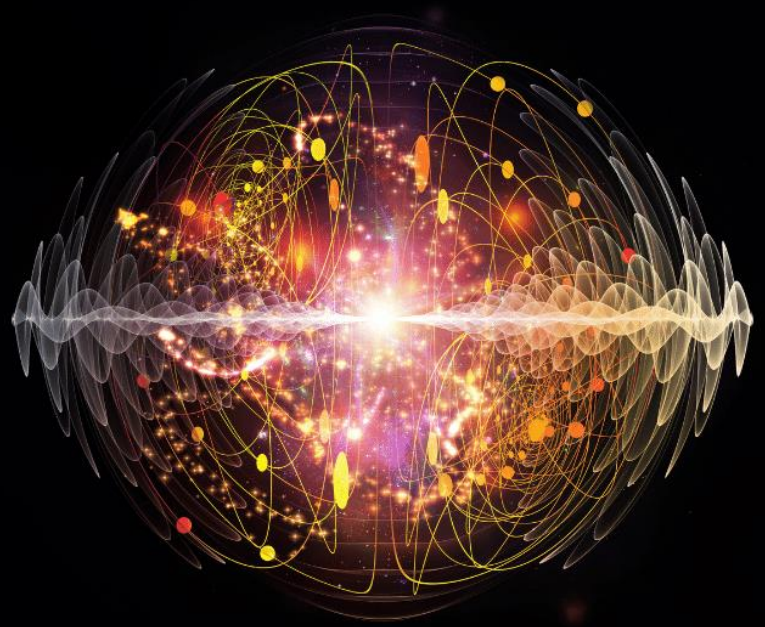
Grover algorithm improves attacks on symmetric cryptography (e.g., AES, SHA), but we have the solution: double the key/hash size

Today’s quantum systems are too small to be an immediate threat

Today’s quantum systems are too small to be an immediate threat

“When will quantum computers be usable to break encryption?” is a question being debated by many experts, speculating 5-10 years

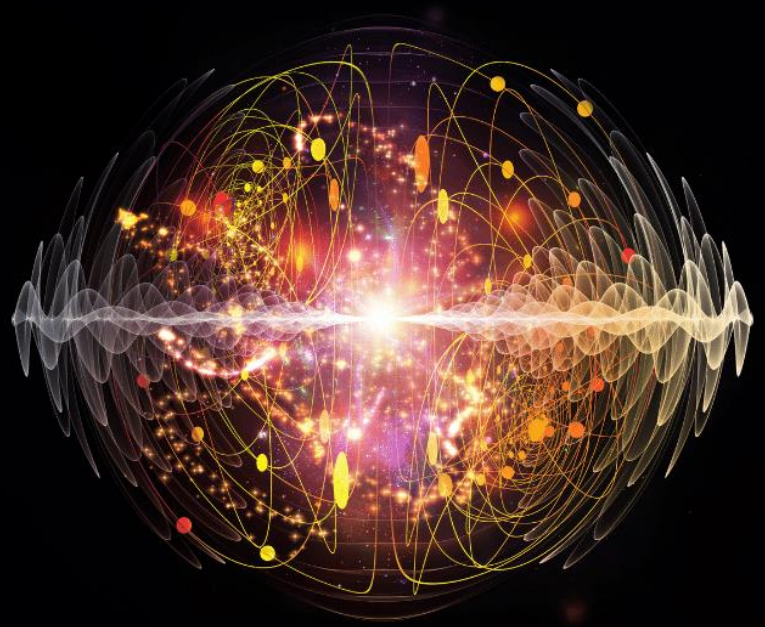
But quantum-based attack already could be occurring now



But quantum-based attack already could be occurring now

Encrypted data can be

“Harvested Now and Decrypted Later”
(HNDL)



Post Quantum Cryptography Algorithms

Post Quantum Cryptography Algorithms

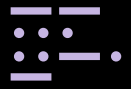
PQC are new encryption algorithms

Post Quantum Cryptography Algorithms

PQC are new encryption algorithms

PQC Algorithms Types

Key Encapsulation Mechanisms



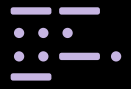
Digital Signature Algorithms

Post Quantum Cryptography Algorithms

PQC are new encryption algorithms

PQC Algorithms Types

Key Encapsulation Mechanisms



Digital Signature Algorithms

Families of Hard Problems

Lattice

Code

Isogeny

Hash

Multivariate

The Post Quantum Cryptography Standardization Process

- The NIST standardization process aims to identify and select the best PQC algorithms for securing data and communications against quantum computing threats.

The Post Quantum Cryptography Standardization Process

- The NIST standardization process aims to identify and select the best PQC algorithms for securing data and communications against quantum computing threats.
- In July, NIST announced 4 finalist for standardization after 3 rounds. Round 4 is now active. The entire process is expected to be done by end of 2024.

The Post Quantum Cryptography Standardization Process

- The NIST standardization process aims to identify and select the best PQC algorithms for securing data and communications against quantum computing threats.
- In July, NIST announced 4 finalist for standardization after 3 rounds. Round 4 is now active. The entire process is expected to be done by end of 2024.

CRYSTALS-Kyber
For encryption

CRYSTALS-Dilithium
For signatures

Falcon
For signatures

Sphincs+
For signatures

Supersingular Isogeny Key Encapsulation (SIKE) Algorithm

Supersingular Isogeny Key Encapsulation (SIKE) Algorithm

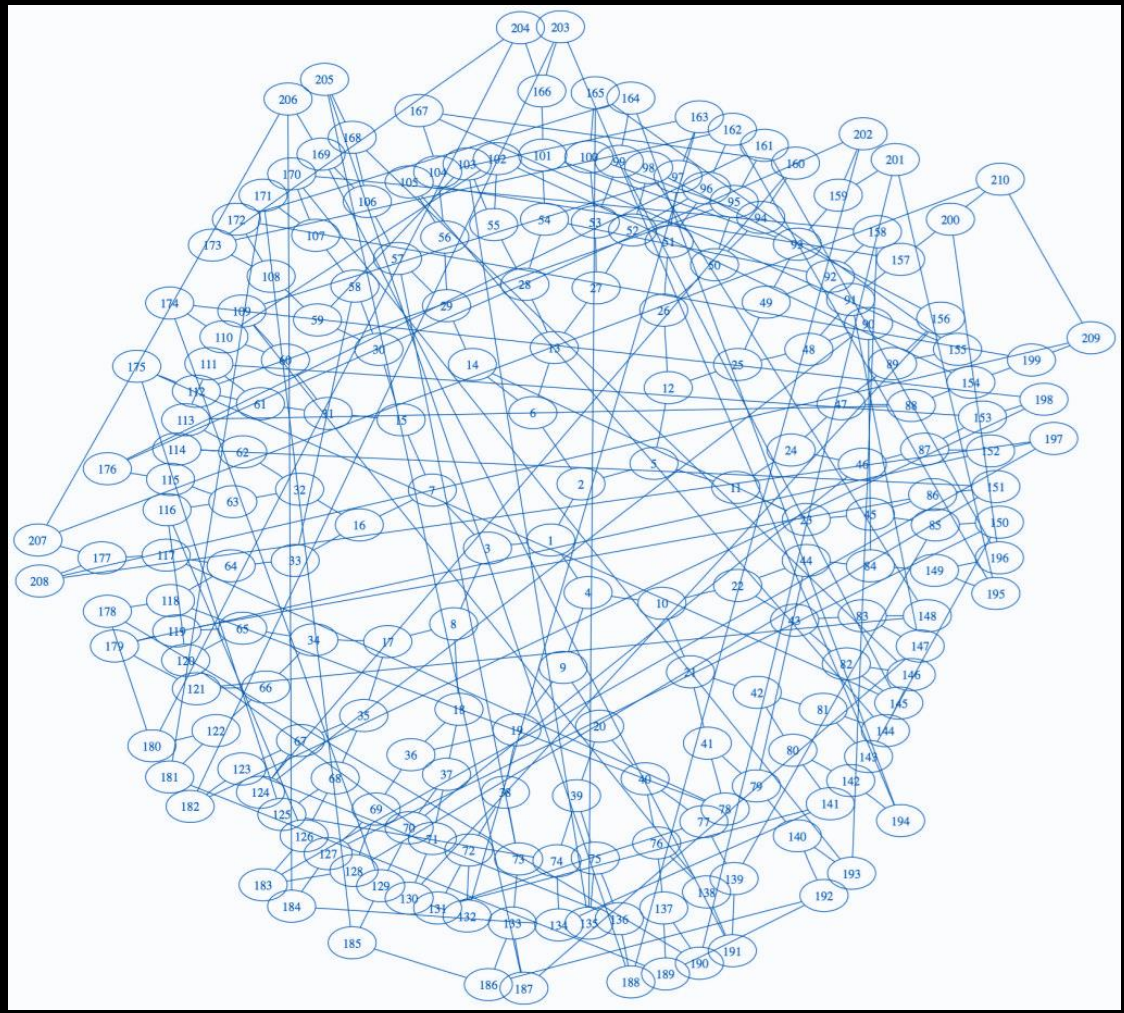
- A collaboration of researchers and engineers at Microsoft Research, Amazon, and several universities.

Supersingular Isogeny Key Encapsulation (SIKE) Algorithm

- A collaboration of researchers and engineers at Microsoft Research, Amazon, and several universities.
- Refers to a family of encryption mechanisms based on the Supersingular Isogeny Diffie-Hellman (SIDH) key exchange protocol.

Supersingular Isogeny Key Encapsulation (SIKE) Algorithm

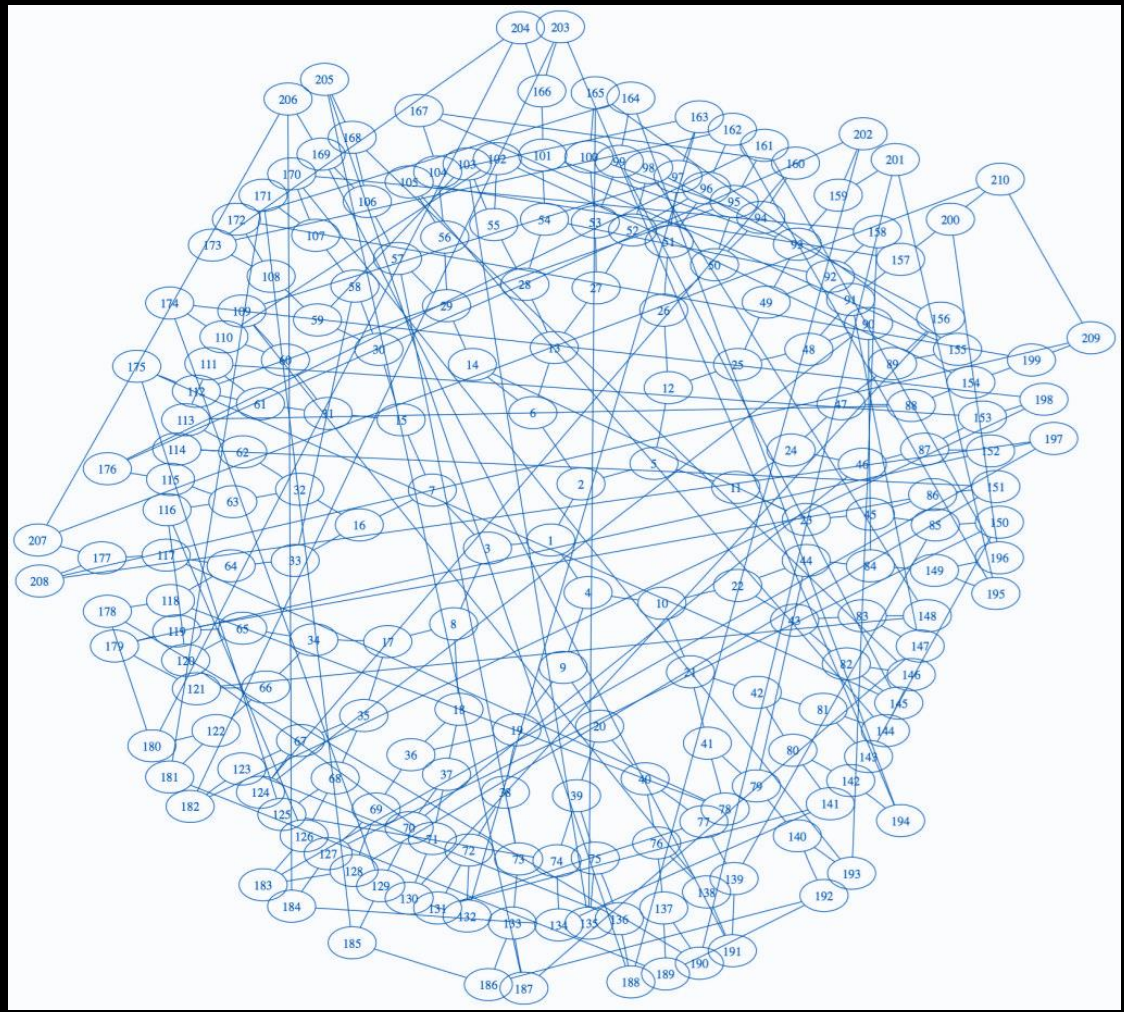
- A collaboration of researchers and engineers at Microsoft Research, Amazon, and several universities.
- Refers to a family of encryption mechanisms based on the Supersingular Isogeny Diffie-Hellman (SIDH) key exchange protocol.



A small example of a Supersingular Isogeny Graph, for the prime p=2521, graph image by Denis Charles, principal applied scientist, Microsoft Research

Supersingular Isogeny Key Encapsulation (SIKE) Algorithm

- A collaboration of researchers and engineers at Microsoft Research, Amazon, and several universities.
- Refers to a family of encryption mechanisms based on the Supersingular Isogeny Diffie-Hellman (SIDH) key exchange protocol.
- It was designed to be a PQC superhero, but it was broken in 2022



A small example of a Supersingular Isogeny Graph, for the prime p=2521, graph image by Denis Charles, principal applied scientist, Microsoft Research

Communication over an insecure Channel

Communication over an insecure Channel

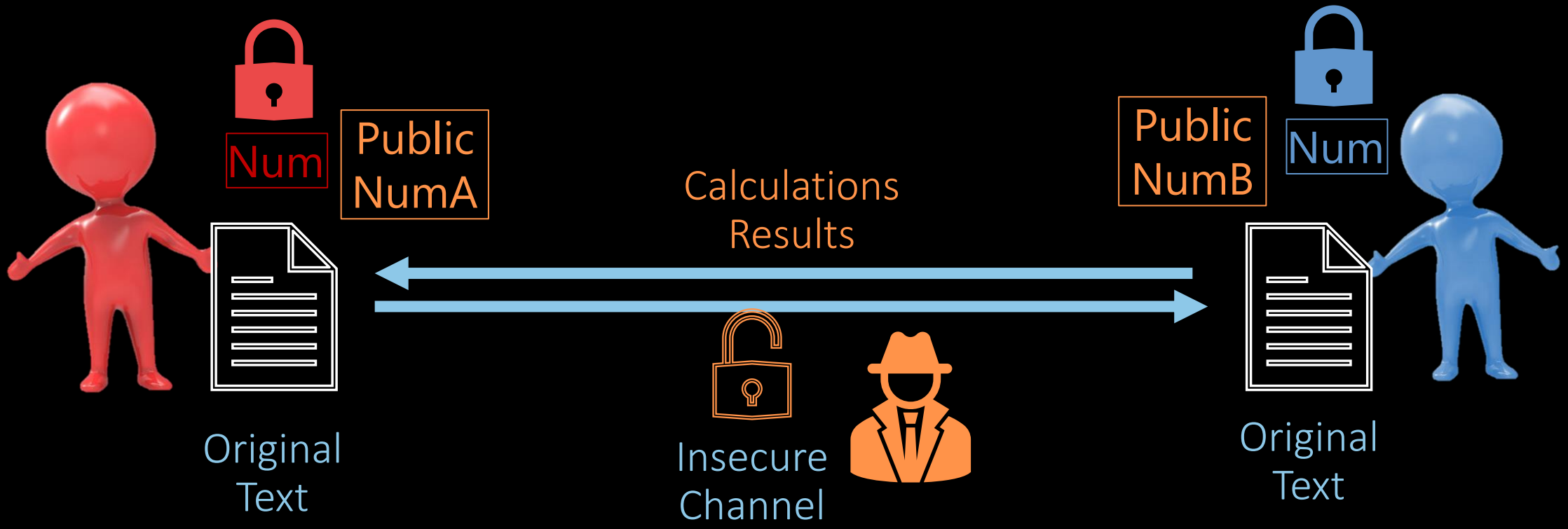
Diffie-Hellman Key Exchange Algorithm

Communication over an insecure Channel

Diffie-Hellman Key Exchange Algorithm

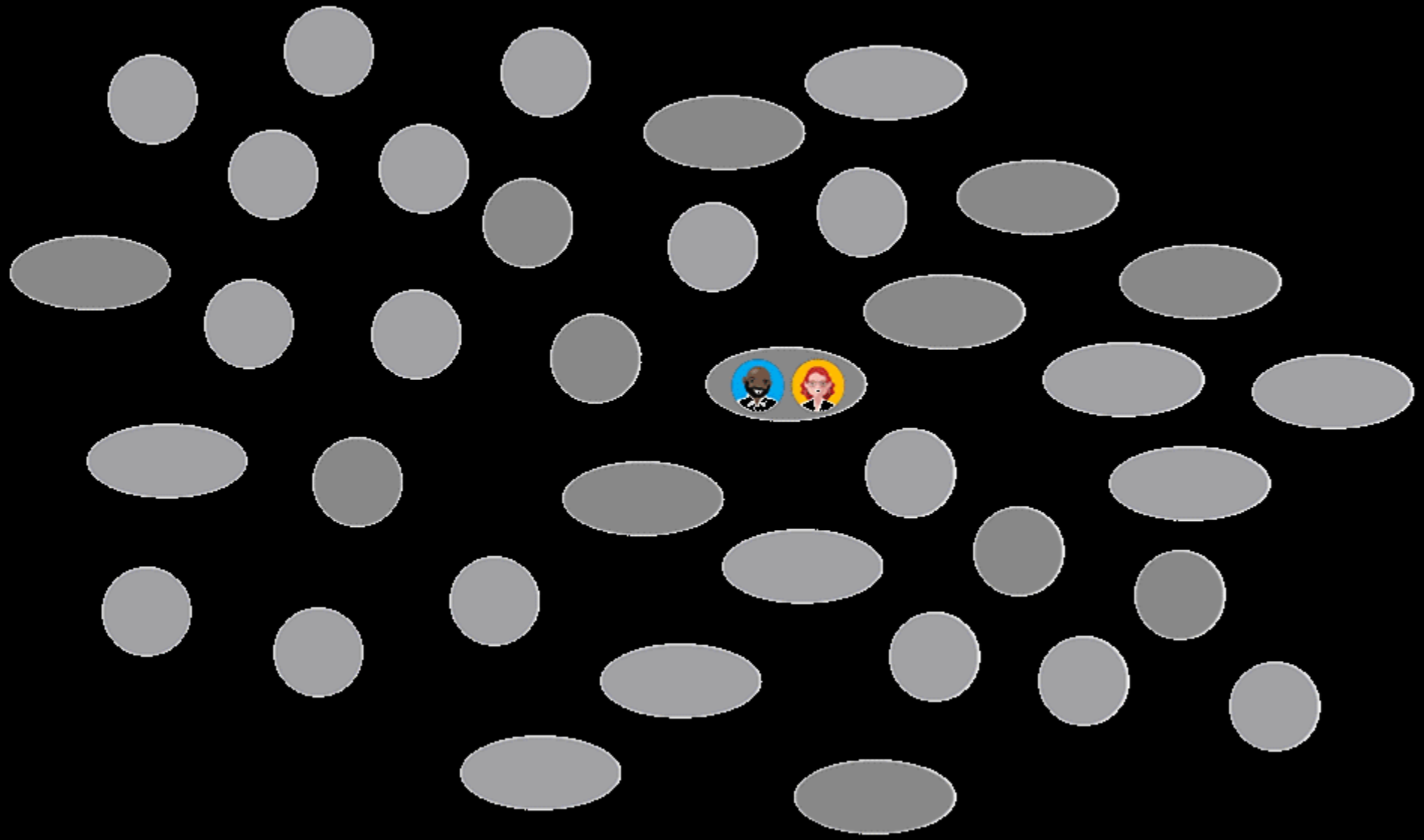
Communication over an insecure Channel

Diffie-Hellman Key Exchange Algorithm



Communication over an insecure Channel

Diffie-Hellman Key Exchange Algorithm



So… what can we do from here?

Keep in Mind and Take Action

- The field of PQC algorithms is still emerging – Explore the topic and keep up with new research and developments

Keep in Mind and Take Action

- The field of PQC algorithms is still emerging – Explore the topic and keep up with new research and developments
- Crypto protocols have security proofs that reduce the problem of complex systems to understanding simpler mathematical problems

Keep in Mind and Take Action

- The field of PQC algorithms is still emerging – Explore the topic and keep up with new research and developments
- Crypto protocols have security proofs that reduce the problem of complex systems to understanding simpler mathematical problems
- But we need people and time analyzing these problems to develop confidence about their difficulty.

Keep in Mind and Take Action

- The field of PQC algorithms is still emerging – Explore the topic and keep up with new research and developments
- Crypto protocols have security proofs that reduce the problem of complex systems to understanding simpler mathematical problems
- But we need people and time analyzing these problems to develop confidence about their difficulty.
- Prioritize hybrid cryptography and crypto agility as the preferred solution to ensure security in the present.

For more resources

- Microsoft Research Post Quantum Cryptography
- Microsoft Azure Quantum
- Microsoft Azure Quantum Resource Estimator
- Quantum Magazine
- NIST Post-Quantum Cryptography Standardization Process
- NIST Migration to Post-Quantum Cryptography Project

Thank you!