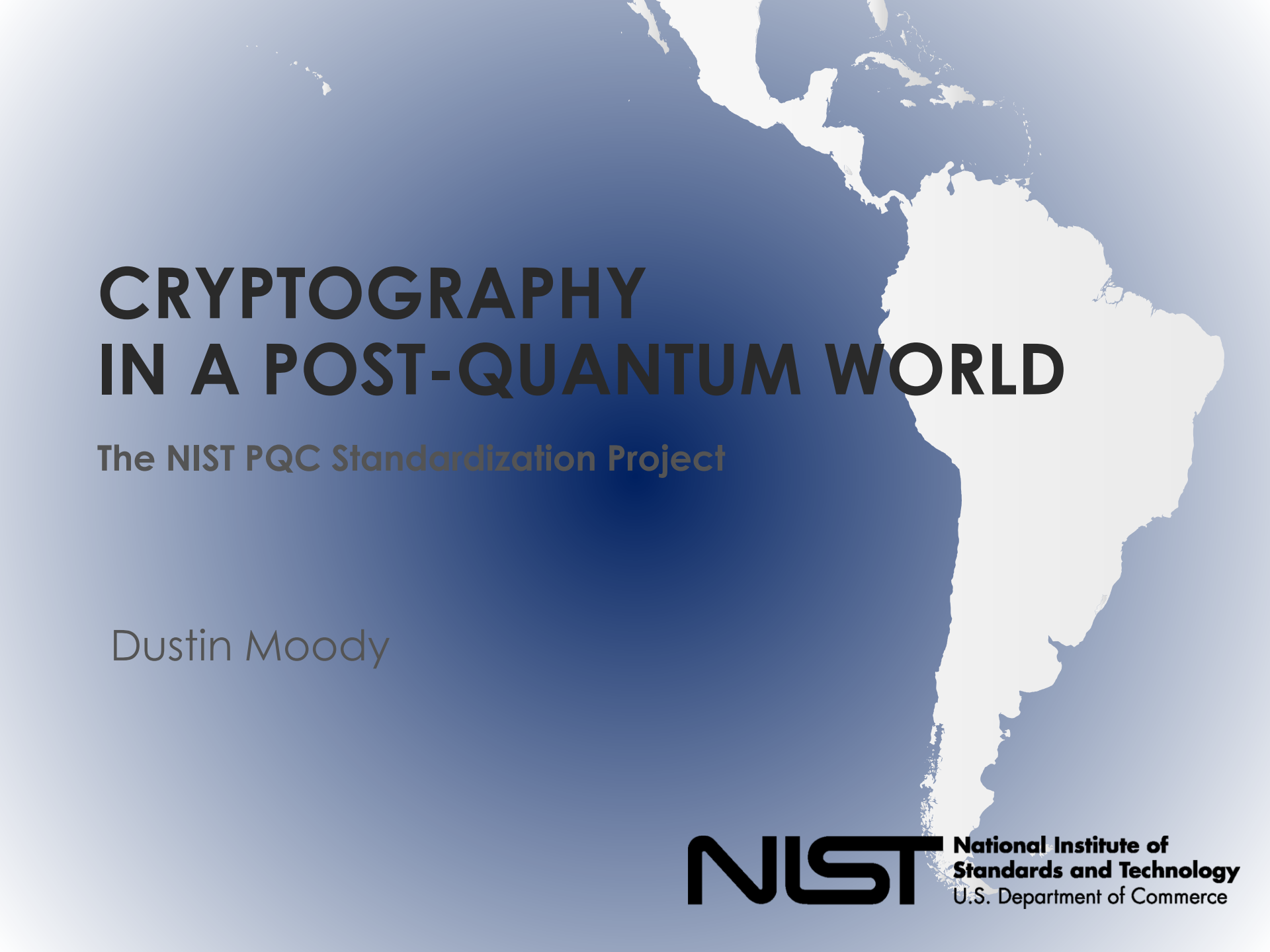


CRYPTOGRAPHY IN A POST-QUANTUM WORLD

The NIST PQC Standardization Project

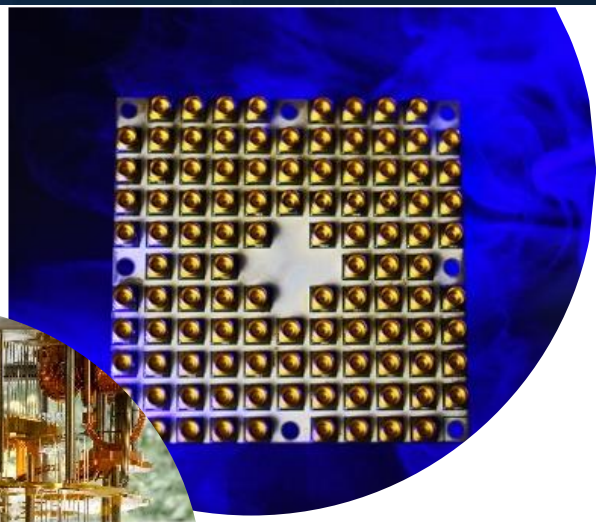
Dustin Moody

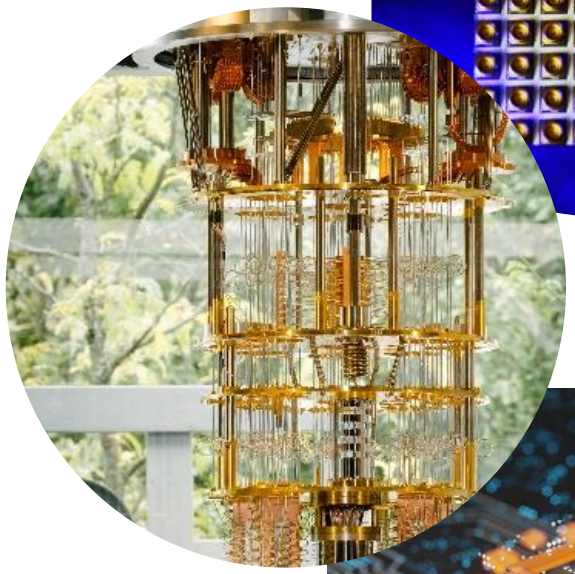
National Institute of Standards and Technology
U.S. Department of Commerce

Quantum Computers

- Exploit quantum mechanics to process information
- ”Qubits” instead of bits
- Potential to vastly increase computational power beyond classical computing limit

- Limitations:
  - When a measurement is made on quantum system, superposition collapses
  - Only good at certain problems
  - Quantum states are very fragile and must be extremely well isolated





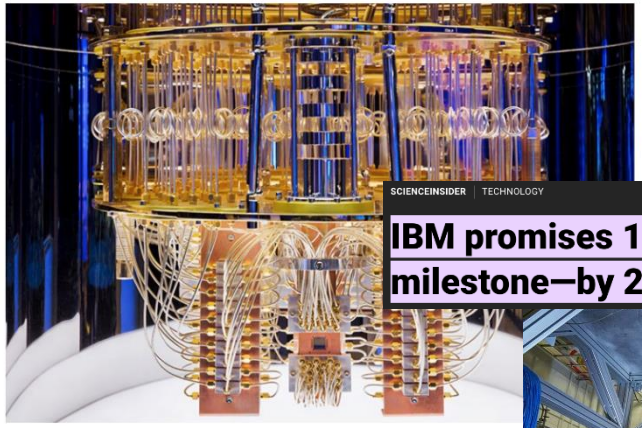
PROGRESS OF QUANTUM COMPUTING

NIST

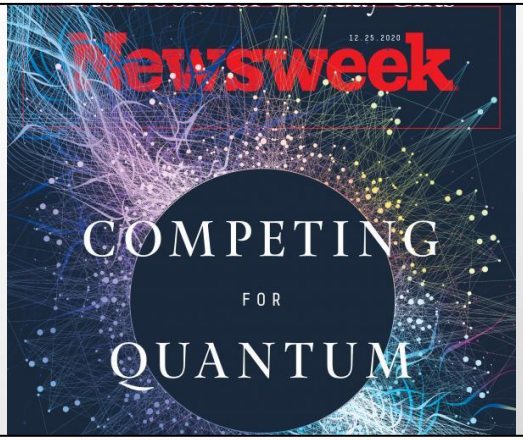
First quantum computer to pack 100 qubits enters crowded race

But IBM's latest quantum chip and its competitors face a long path towards making the machines useful.

Philip Ball



Quantum computers may be able to break Bitcoin sooner than you think

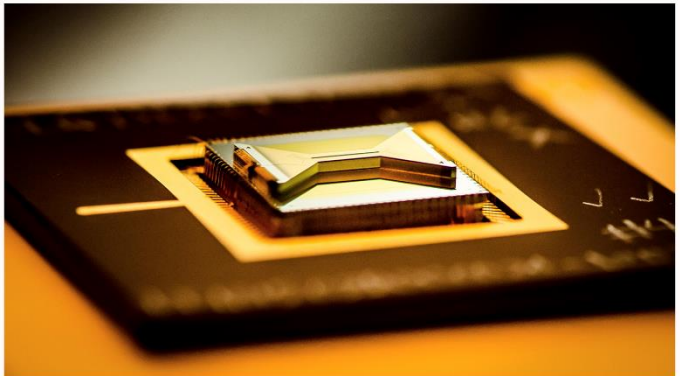


SCIENCEINSIDER | TECHNOLOGY

IBM promises 1000-qubit quantum computer—a milestone—by 2023

Scientists are one step closer to error-correcting quantum computers

Multiple quantum bits were combined into one 'logical qubit' to detect mistakes



Quantum computing venture backed by Je will leap into public trading with $1.2B valu

MOTIVATION

- 1994 – SHOR'S ALGORITHM
  - A QUANTUM ALGORITHM GIVING AN EXPONENTIAL SPEED-UP OVER CLASSICAL COMPUTERS
    - FACTORING LARGE INTEGERS
    - FINDING DISCRETE LOGARITHMS

Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974, USA

Abstract

A computer is generally considered to be a universal computational device; i.e., it is believed able to simulate any physical computational device with a cost in computation time of at most a polynomial factor. It is not clear whether this is still true when quantum mechanics is taken into consideration. Several researchers, starting with David Deutsch, have developed models for quantum mechanical computers and have investigated their computational properties. This paper gives fast algorithms for finding discrete logarithms and factoring integers on a quantum computer that take a number of steps which is polynomial in the input size, e.g., the number of digits of the integer to be factored. These two problems are generally considered hard on a classical computer and have been used as the basis of several proposed cryptosystems. (We thus give the first examples of quantum cryptanalysis.)

1 Introduction

Since the discovery of quantum mechanics, people have found the behavior of the laws of probability in quantum mechanics counterintuitive. Because of this behavior, quantum mechanical phenomena behave quite differently than the phenomena of classical physics that we are used

[1, 2]. Although he did not ask whether quantum mechanics conferred extra power to computation, he did show that a Turing machine could be simulated by the reversible unitary evolution of a quantum process, which is a necessary prerequisite for quantum computation. Deutsch [9, 10] was the first to give an explicit model of quantum computation. He defined both quantum Turing machines and quantum circuits and investigated some of their properties.

The next part of this paper discusses how quantum computation relates to classical complexity classes. We will then first give a brief intuitive discussion of complexity classes for those readers who do not have this background. There are generally two resources which limit the ability of computers to solve large problems: time and space (i.e., memory). The field of analysis of algorithms considers the asymptotic demands that algorithms make for these resources as a function of the problem size. Theoretical computer scientists generally classify algorithms as efficient when the number of steps of the algorithm grows as a polynomial in the size of the input. The class of problems which can be solved by efficient algorithms is known as P. This classification has several nice properties. For one thing, it does a reasonable job of reflecting the performance of algorithms in practice (although an algorithm whose running time is the tenth power of the input size, say, is not really efficient). For another, this classification is nice theoretically, as different reasonable machine models

- 1996 - GROVER'S ALGORITHM
  - POLYNOMIAL SPEED-UP IN UNSTRUCTURED SEARCH, FROM O(N) TO O($\sqrt{N}$)

A fast quantum mechanical algorithm for database search

Lov K. Grover
3C-404A, AT&T Bell Labs
600 Mountain Avenue
Murray Hill NJ 07974
lkg@mhcnet.att.com

Summary

An unsorted database contains N records, of which just one satisfies a particular property. The problem is to identify that one record. Any classical algorithm, deterministic or probabilistic, will clearly take $O(N)$ steps since on the average it will have to examine a large fraction of the N records. Quantum mechanical systems can do several operations simultaneously due to their wave

like properties. This paper gives an $O(\sqrt{N})$ step quantum mechanical algorithm for identifying that record. It is within a constant factor of the fastest possible quantum mechanical algorithm.

1. Introduction

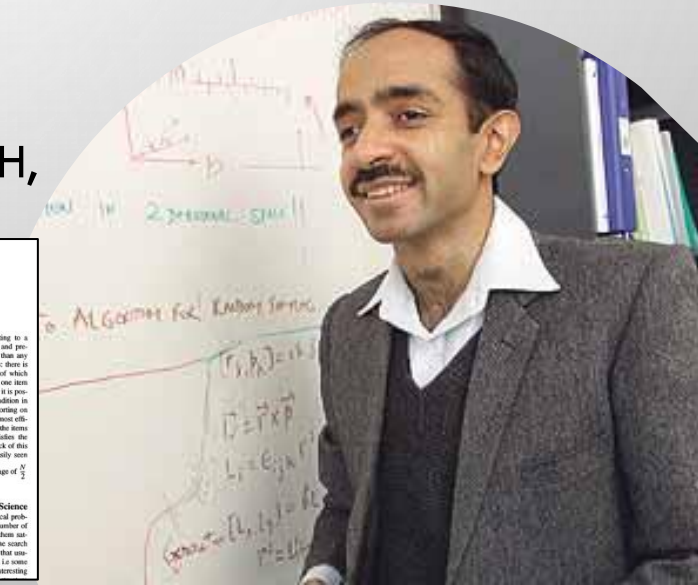
1.0 Background Quantum mechanical computers were proposed in the early 1980's [Benioff80] and shown to be at least as powerful as classical computers - an important but not surprising result, since classical computers, at the deepest level, ultimately follow the laws of quantum mechanics. The description of quantum mechanical computers was formalized in the late 80's and early 90's [Deutsch85][BB92] [BV93] [Yao93] and they were shown to be more powerful than classical computers on various specialized problems. In early

This paper applies quantum computing to a mundane problem in information processing and presents an algorithm that is significantly faster than any classical algorithm can be. The problem is this: there is an unsorted database containing N items out of which just one item satisfies a given condition - that one item has to be retrieved. Once an item is examined, it is possible to tell whether or not it satisfies the condition in one step. However, there does not exist any sorting on the database that would aid its selection. The most efficient classical algorithm for this is to examine the items in the database one by one. If an item satisfies the required condition step; if it does not, keep track of this item so that it is not examined again. It is easily seen

that this algorithm will need to look at an average of $\frac{N}{2}$

items before finding the desired one.

1.1 Search Problems in Computer Science Even in theoretical computer science, the typical problem can be looked at as that of examining a number of different possibilities to see which, if any, of them satisfy a given condition. This is analogous to the search problem stated in the summary above, except that usually there exists some structure to the problem, i.e some sorting does exist on the database. Most interesting

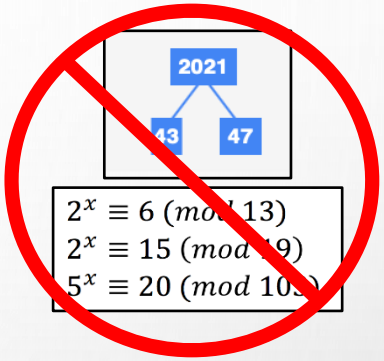


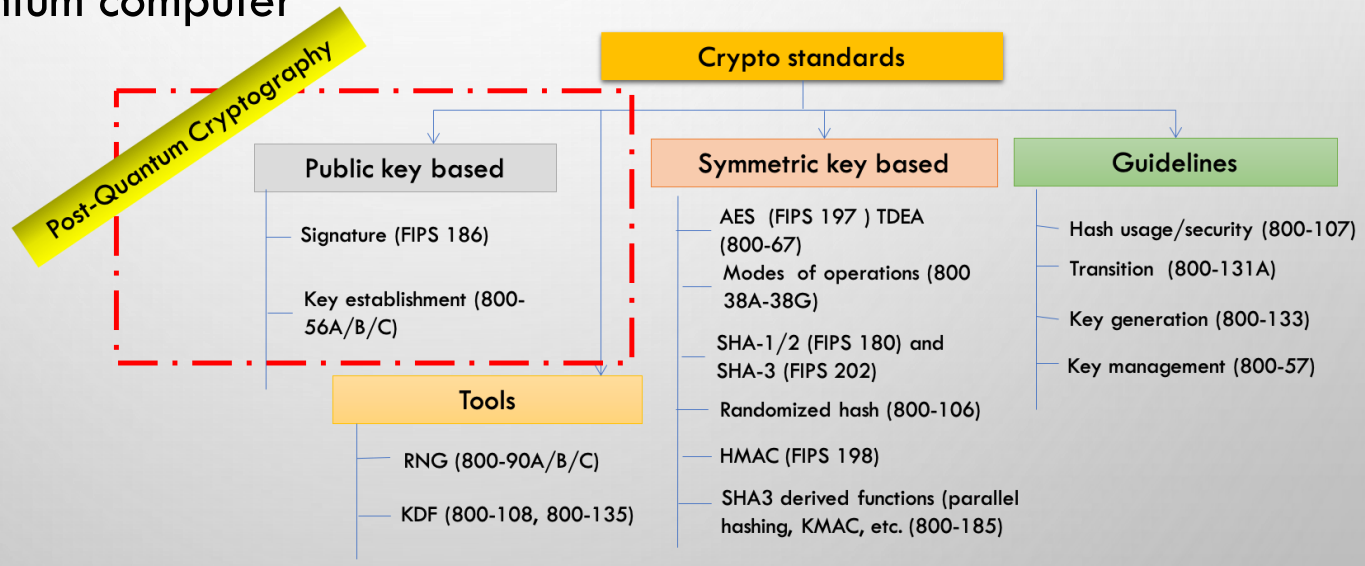
THE QUANTUM THREAT

- NIST public-key crypto standards
  - **SP 800-56A**: Diffie-Hellman, ECDH
  - **SP 800-56B**: RSA encryption
  - **FIPS 186**: RSA, DSA, and ECDSA signatures

  all vulnerable to attacks from

  a (large-scale) quantum computer



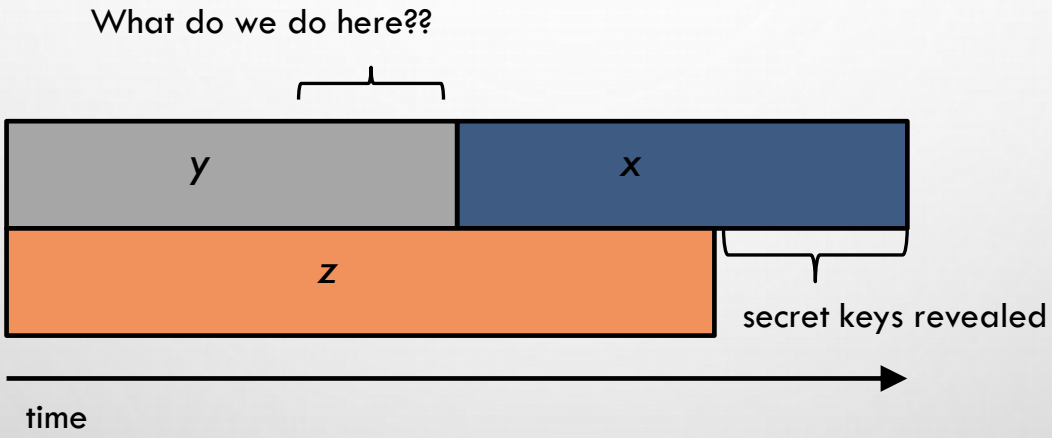


- Symmetric-key crypto (AES, SHA) would also be affected, but less dramatically

HOW SOON DO WE NEED TO WORRY?

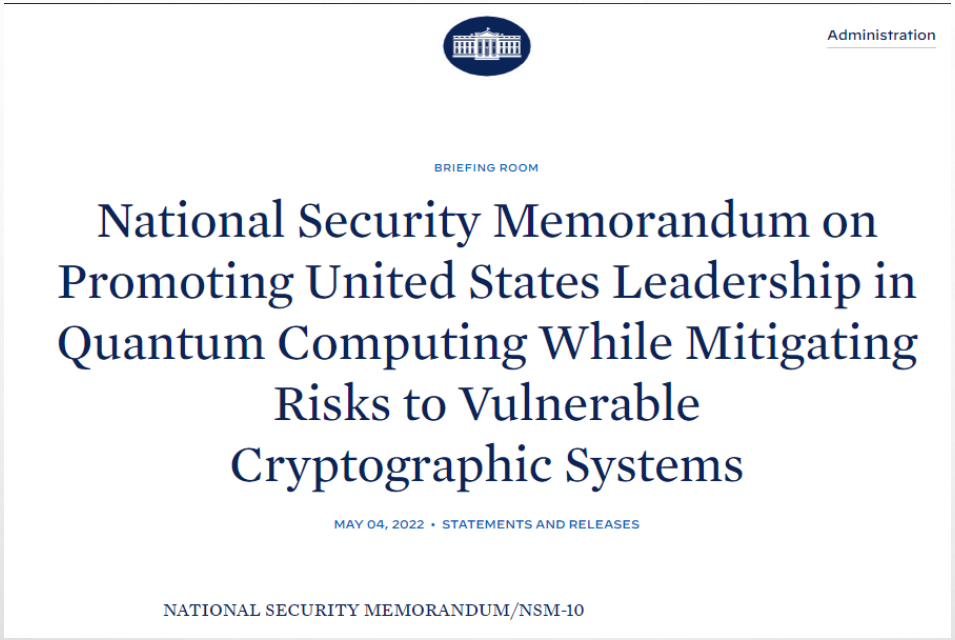
HOW SOON DO WE NEED TO WORRY?

Theorem (Mosca): If $x + y > z$, then problem ("*Harvest now, decrypt later*")



x – how long data needs to be safe
y – time for standardization and adoption
z – time until quantum computers

U.S. WHITE HOUSE NATIONAL SECURITY MEMO



Administration

BRIEFING ROOM

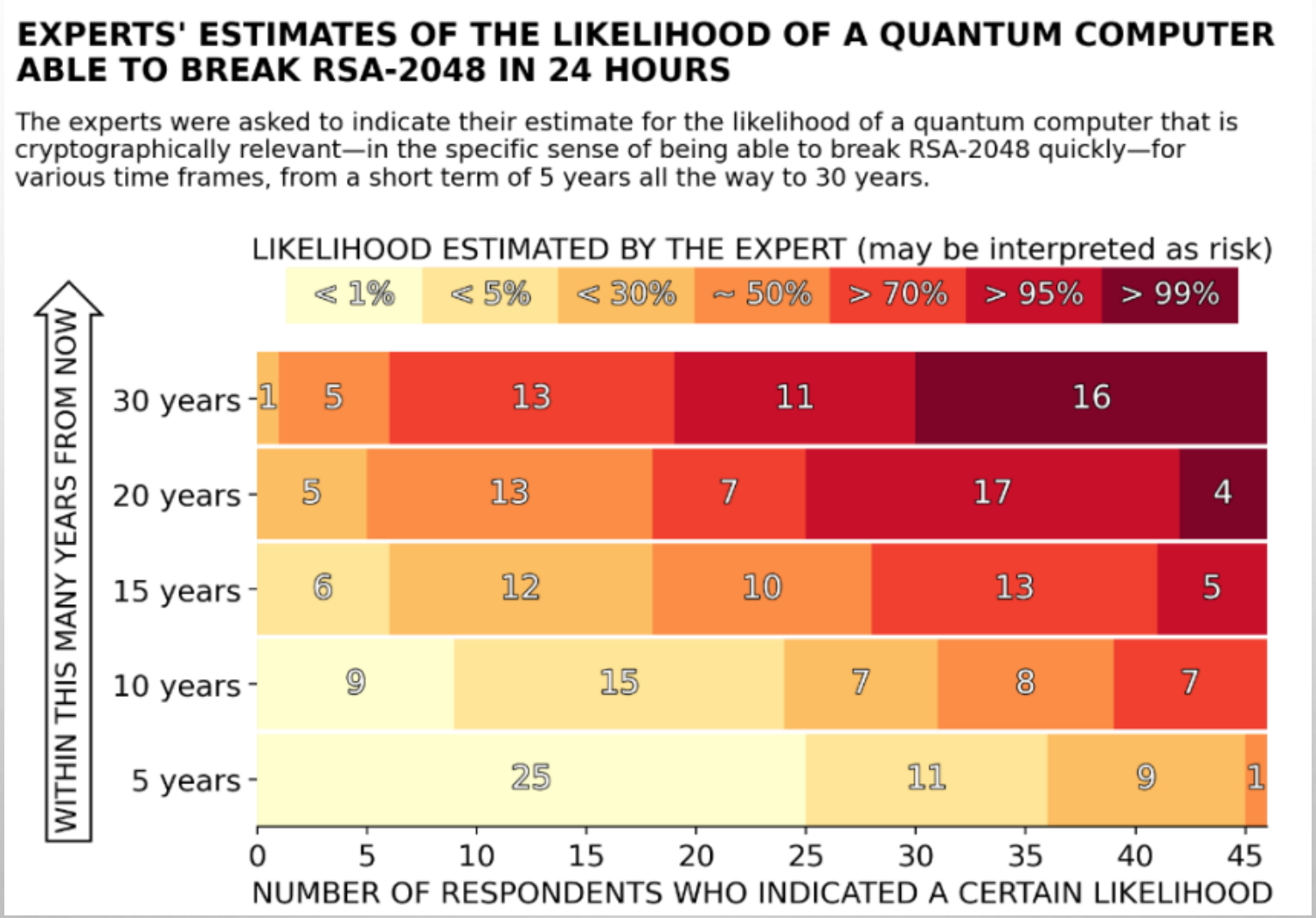
National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

MAY 04, 2022 • STATEMENTS AND RELEASES

NATIONAL SECURITY MEMORANDUM/NSM-10

"WITHIN 1 YEAR OF THE RELEASE OF THE FIRST SET OF NIST STANDARDS FOR QUANTUM-RESISTANT CRYPTOGRAPHY …, THE DIRECTOR OF OMB … SHALL ISSUE A POLICY MEMORANDUM REQUIRING FCEB AGENCIES TO DEVELOP A PLAN TO UPGRADE THEIR NON-NSS IT SYSTEMS TO QUANTUM-RESISTANT CRYPTOGRAPHY."

WHEN WILL A QUANTUM COMPUTER BE BUILT?



Source: M. Mosca, M. Piani, Quantum Threat Timeline Report, 2021
https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/

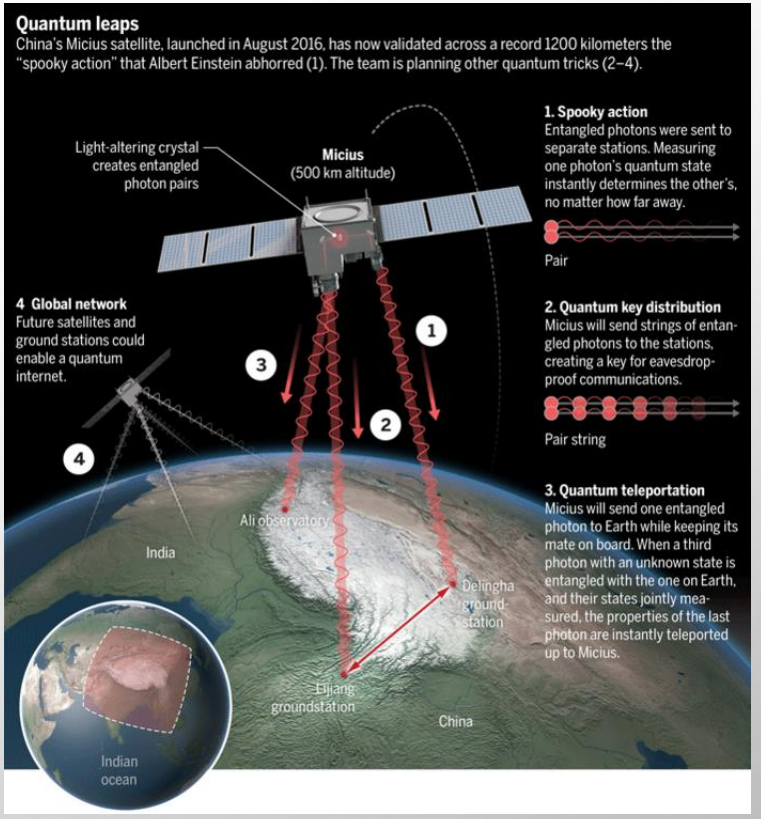
QUANTUM CRYPTOGRAPHY AKA QKD

USING QUANTUM TECHNOLOGY TO BUILD CRYPTOSYSTEMS

- THEORETICALLY UNCONDITIONAL SECURITY GUARANTEED BY THE LAWS OF PHYSICS

LIMITATIONS

- CAN DO ENCRYPTION, BUT NOT AUTHENTICATION
- QUANTUM NETWORKS NOT VERY SCALABLE
- EXPENSIVE AND NEEDS SPECIAL HARDWARE



LOTS OF MONEY BEING SPENT ON "QUANTUM"

THIS IS <u>NOT</u> OUR FOCUS

NIST PQC MILESTONES AND TIMELINES

2010-2015
NIST PQC project team builds

First PQC conference

2016

Determined criteria and requirements, published NISTIR 8105

Announced call for proposals

2017
Received 82 submissions

Announced 69 1st round candidates

2018

Held the 1st NIST PQC standardization Conference

2019
Announced 26 2nd round candidates, NISTIR 8240

Held the 2nd NIST PQC Standardization Conference

2020
Announced 3rd round 7 finalists and 8 alternate candidates. NISTIR 8309

2021
Hold the 3rd NIST PQC Standardization Conference

2022 Make 3rd round selection and draft standards

2023 Release draft standards and call for public comments

THE NIST PQC TEAM

SELECTION CRITERIA

1. **SECURE** AGAINST BOTH CLASSICAL AND QUANTUM ATTACKS

2. **PERFORMANCE** - MEASURED ON VARIOUS "CLASSICAL" PLATFORMS

3. **OTHER PROPERTIES**
   - DROP-IN REPLACEMENTS - COMPATIBILITY WITH EXISTING PROTOCOLS AND NETWORKS
   - PERFECT FORWARD SECRECY
   - RESISTANCE TO SIDE-CHANNEL ATTACKS
   - SIMPLICITY AND FLEXIBILITY
   - MISUSE RESISTANCE, AND
   - MORE

SECURITY CATEGORIES

Security – against both classical and quantum attacks

Level	Security Description
I	At least as hard to break as AES128 (exhaustive key search)
II	At least as hard to break as SHA256 (collision search)
III	At least as hard to break as AES192 (exhaustive key search)
IV	At least as hard to break as SHA384 (collision search)
V	At least as hard to break as AES256 (exhaustive key search)

- Computational resources should be measured using a variety of metrics
  - Number of classical elementary operations, quantum circuit size, etc…
  - Consider realistic limitations on circuit depth (e.g. 2^{40} to 2^{80} logical gates)
  - May also consider expected relative cost of quantum and classical gates.

A Worldwide Effort

25 Countries

16 States

6 Continents

THE FIRST THREE ROUNDS

ROUND 1 (DEC '17 – JAN '18)

- 69 CANDIDATES AND 278 DISTINCT SUBMITTERS
- SUBMITTERS FROM >25 COUNTRIES, ALL 6 CONTINENTS
- APR 2018, 1ST NIST PQC CONFERENCE
- ALMOST 25 SCHEMES BROKEN/ATTACKED
- NISTIR 8240, NIST REPORT ON THE 1ST ROUND

	Signatures	KEM/Encryption	Overall
Lattice-based	5	21	26
Code-based	2	17	19
Multi-variate	7	2	9
Symmetric based	3		3
Other	2	5	7
Total	**19**	**45**	**64**

ROUND 2 (JAN '18 – JUL '20)

- 26 CANDIDATES
- AUG 2019 – 2ND NIST PQC CONFERENCE
- 7 SCHEMES BROKEN/ATTACKED
- NISTIR 8309, NIST REPORT ON THE 2ND ROUND

	Signatures	KEMs/Encryption	Total
Lattice-based	3	9	12
Code-based	0	7	7
Multi-variate	4	0	4
Symmetric-based	2		2
Other	0	1	1
Total	**9**	**17**	**26**

ROUND 3 (JUL '20 – JUL '22)

- 7 FINALISTS AND 8 ALTERNATES
- JUNE 2021 – 3RD NIST PQC CONFERENCE
- NISTIR 8413, NIST REPORT ON THE 3RD ROUND

	Signatures	KEMs/Encryption	Total
Lattice-based	2	5	7
Code-based	0	3	3
Multi-variate	2	0	2
Symmetric-based	2	0	2
Other	0	1	1
Total	**6**	**9**	**15**

WHAT WAS SELECTED

- NIST SELECTED 4 ALGORITHMS TO BE STANDARDIZED
- THERE ARE 4 ADDITIONAL ALGORITHMS ADVANCING TO A 4TH ROUND OF EVALUATION

	Selected	4th Round
KEMs/Encryption	Kyber	BIKE Classic McEliece HQC SIKE
Signatures	Dilithium Falcon SPHINCS+	

TIMELINE

- The 3rd Round has ended!!
  - NIST is currently writing draft standards for the selected algorithms
- The 4th Round has begun
  - BIKE, Classic McEliece, HQC, and SIKE to be further studied
    - Tweaks due October 1, 2022
  - The 4th round will likely be 18-24 months
- The 4th NIST PQC Standardization Conference
  - Nov 29-Dec 1, 2022, held virtually
- Draft standards for public comment should be in 2022-2023
- The first PQC standards should be published around 2024

AN ON-RAMP FOR SIGNATURES

- After the conclusion of the 3rd Round, NIST will issue a new Call for Signatures
  - There will be a deadline for submission, likely Jan 2023
  - This will be much smaller in scope than main NIST PQC effort
  - The main reason for this call is to diversify our signature portfolio
  - These signatures will be on a different track than the candidates in the 4th round

- We are **most interested** in a general-purpose digital signature scheme which is not based on structured lattices
  - We may be interested in other signature schemes targeted for certain applications. For example, a scheme with very short signatures.
- The more mature the scheme, the better.
- NIST will decide which (if any) of the received schemes to focus attention on

GETTING READY FOR PQC

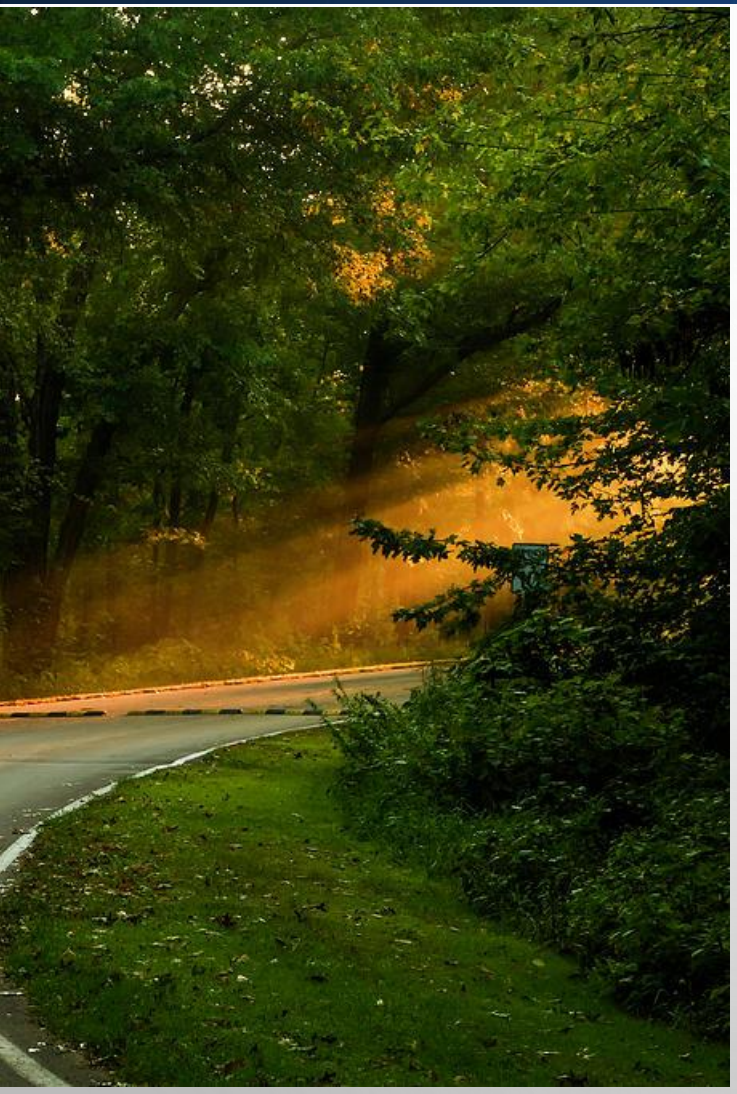
NIST

- The National Cybersecurity Center of Excellence (NCCoE) has a project for Migration to PQC . The goals:
  - Align and complement the NIST PQC standardization activities
  - Raise awareness and develop practices to ease the migration to PQC algorithms
  - Deliver white papers, playbooks, and demonstrable implementations for organizations
  - Target organizations that provide cryptographic standards and protocols and enterprises that develop, acquire, implement, and service cryptographic products
- NCCoE recently teamed up with the Dept. of Homeland Security in this effort.
- If you are interested in joining the project team as a collaborator, please review the requirements identified in the Federal Register Notice which is based on the final project description.
  - Questions and comments: applied-crypto-pqc@nist.gov

WHAT CAN ORGANIZATIONS DO NOW?

- PERFORM A QUANTUM RISK ASSESSMENT WITHIN YOUR ORGANIZATION
  - IDENTIFY INFORMATION ASSETS AND THEIR CURRENT CRYPTO PROTECTION
  - IDENTIFY WHAT 'X', 'Y', AND 'Z' MIGHT BE FOR YOU – DETERMINE YOUR QUANTUM RISK
  - PRIORITIZE ACTIVITIES REQUIRED TO MAINTAIN AWARENESS, AND TO MIGRATE TECHNOLOGY TO QUANTUM-SAFE SOLUTIONS
- EVALUATE VENDOR PRODUCTS WITH QUANTUM SAFE FEATURES
  - KNOW WHICH PRODUCTS ARE NOT QUANTUM SAFE
  - ASK VENDORS FOR QUANTUM SAFE FEATURES IN PROCUREMENT TEMPLATES
- DEVELOP AN INTERNAL KNOWLEDGE BASE AMONGST IT STAFF
- TRACK DEVELOPMENTS IN QUANTUM COMPUTING AND QUANTUM SAFE SOLUTIONS, AND TO ESTABLISH A ROADMAP TO QUANTUM READINESS FOR YOUR ORGANIZATION

- ACT NOW – IT WILL BE LESS EXPENSIVE, LESS DISRUPTIVE, AND LESS LIKELY TO HAVE MISTAKES CAUSED BY RUSHING AND SCRAMBLING



CONCLUSION

- THE BEGINNING OF THE END IS HERE!
- NIST IS GRATEFUL FOR EVERYBODY'S EFFORTS
- CHECK OUT WWW.NIST.GOV/PQCRYPTO
  - SIGN UP FOR THE PQC-FORUM FOR ANNOUNCEMENTS & DISCUSSION
  - SEND E-MAIL TO PQC-COMMENTS@NIST.GOV