CHARTING EDUCATION AND WORKFORCE PATHWAYS TO DEVELOP QUANTUM PROFICIENT CYBER SECURITY EXPERTS

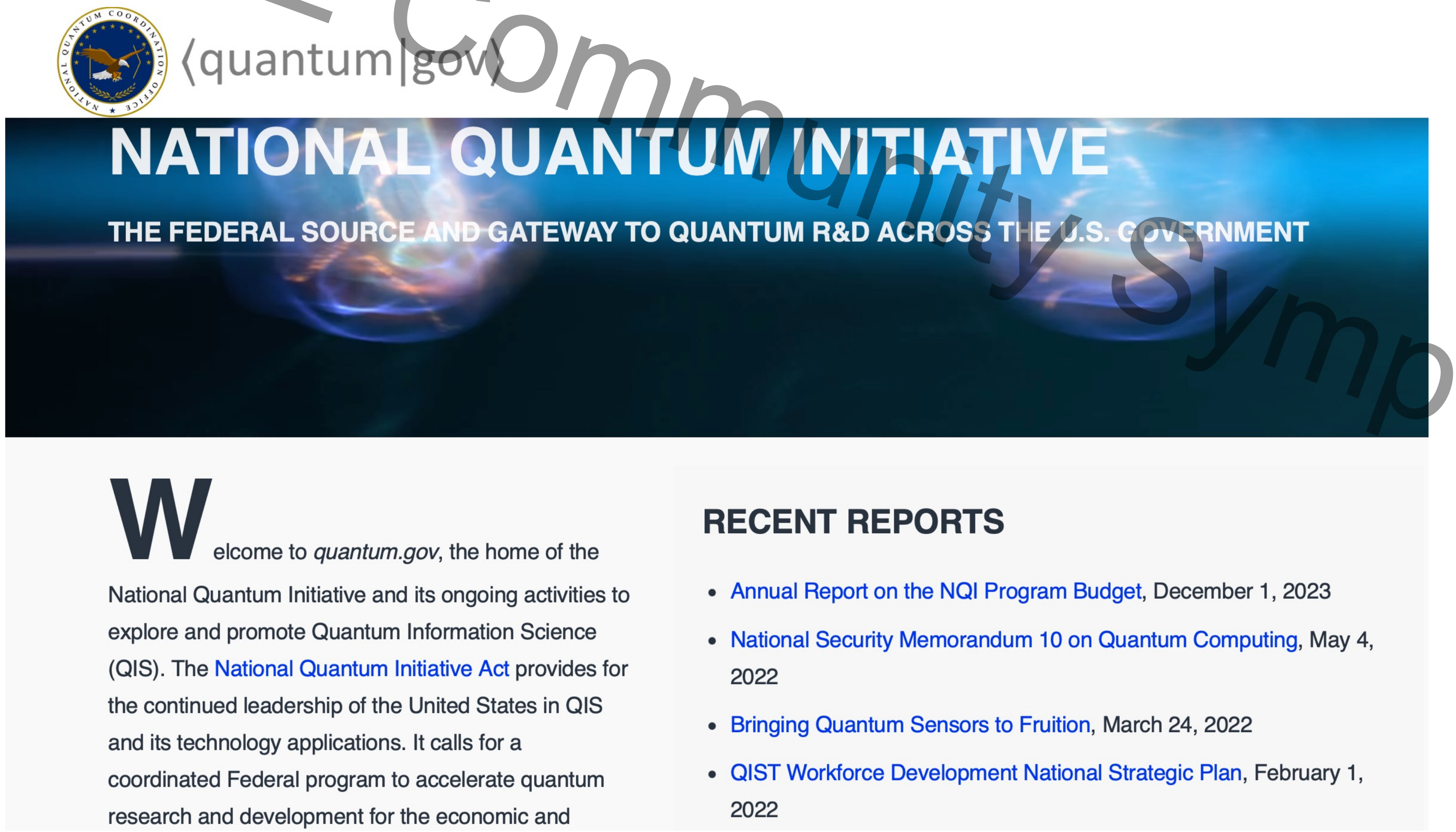
Xiuwen Liu, Mike Burmester, and Weikuan Yu

Department of Computer Science

Florida State University

BACKGROUND

- National Quantum Initiative and its ongoing activities to explore and promote Quantum Information Science (QIS)
  - The National Quantum Initiative Act provides for the continued leadership of the United States in QIS and its technology applications



⟨quantum|gov⟩

NATIONAL QUANTUM INITIATIVE

THE FEDERAL SOURCE AND GATEWAY TO QUANTUM R&D ACROSS THE U.S. GOVERNMENT

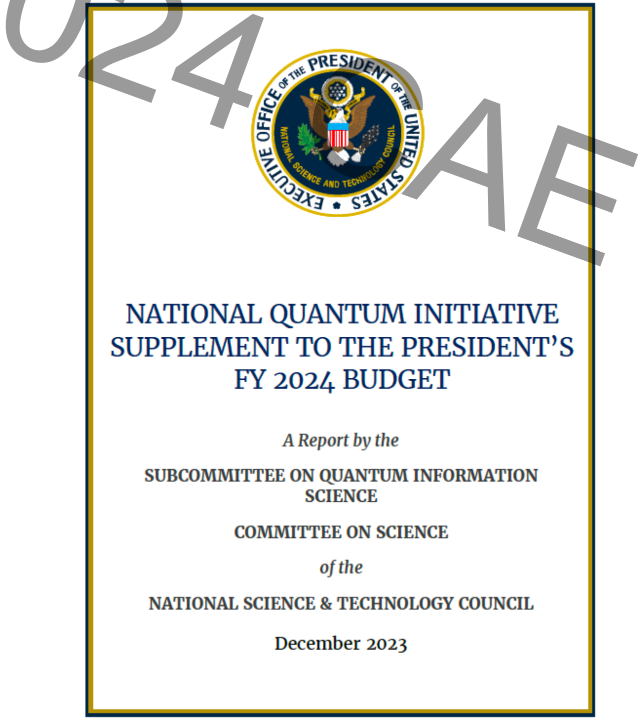
Welcome to *quantum.gov*, the home of the National Quantum Initiative and its ongoing activities to explore and promote Quantum Information Science (QIS). The National Quantum Initiative Act provides for the continued leadership of the United States in QIS and its technology applications. It calls for a coordinated Federal program to accelerate quantum research and development for the economic and

RECENT REPORTS

- Annual Report on the NQI Program Budget, December 1, 2023
- National Security Memorandum 10 on Quantum Computing, May 4, 2022
- Bringing Quantum Sensors to Fruition, March 24, 2022
- QIST Workforce Development National Strategic Plan, February 1, 2022

BACKGROUND – CONT.

- In the most recent report, the Initiative emphasizes the importance of creating a quantum-proficient workforce



NATIONAL QUANTUM INITIATIVE SUPPLEMENT TO THE PRESIDENT'S FY 2024 BUDGET

A Report by the

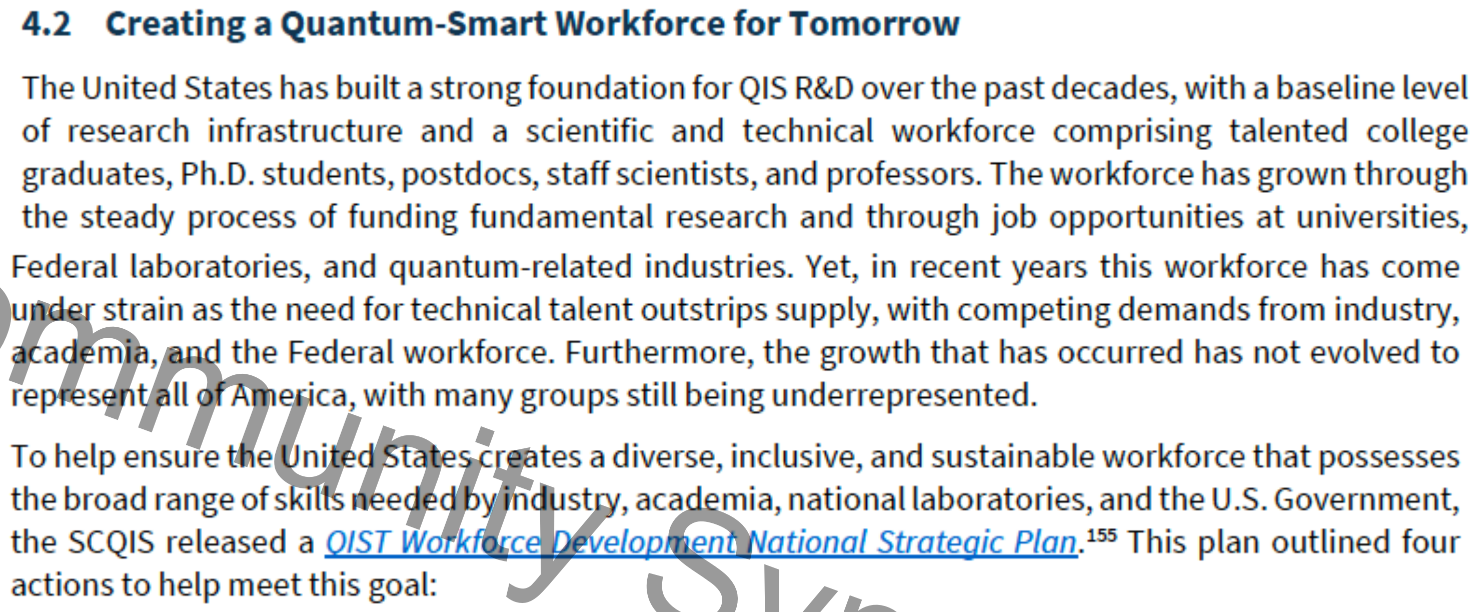
SUBCOMMITTEE ON QUANTUM INFORMATION SCIENCE

COMMITTEE ON SCIENCE

of the

NATIONAL SCIENCE & TECHNOLOGY COUNCIL

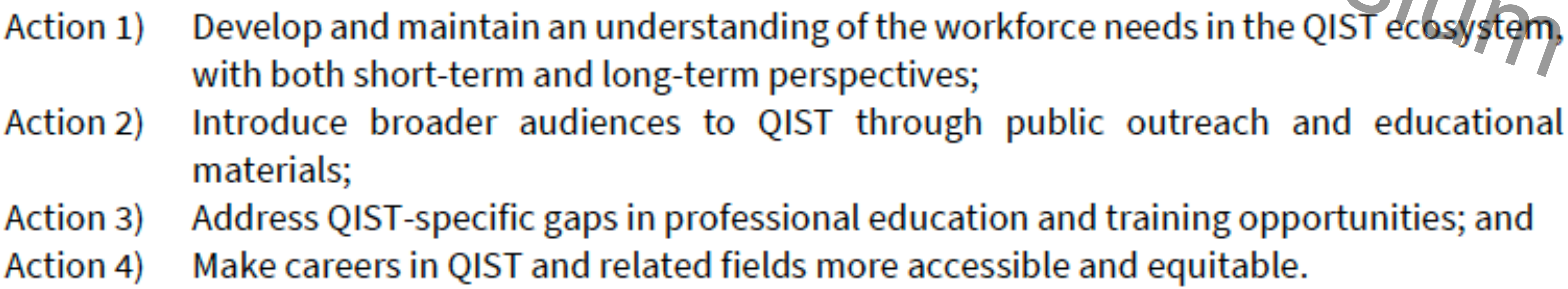
December 2023



4.2 Creating a Quantum-Smart Workforce for Tomorrow

The United States has built a strong foundation for QIS R&D over the past decades, with a baseline level of research infrastructure and a scientific and technical workforce comprising talented college graduates, Ph.D. students, postdocs, staff scientists, and professors. The workforce has grown through the steady process of funding fundamental research and through job opportunities at universities, Federal laboratories, and quantum-related industries. Yet, in recent years this workforce has come under strain as the need for technical talent outstrips supply, with competing demands from industry, academia, and the Federal workforce. Furthermore, the growth that has occurred has not evolved to represent all of America, with many groups still being underrepresented.

To help ensure the United States creates a diverse, inclusive, and sustainable workforce that possesses the broad range of skills needed by industry, academia, national laboratories, and the U.S. Government, the SCQIS released a *QIST Workforce Development National Strategic Plan*.[155] This plan outlined four actions to help meet this goal:



Action 1) Develop and maintain an understanding of the workforce needs in the QIST ecosystem, with both short-term and long-term perspectives;

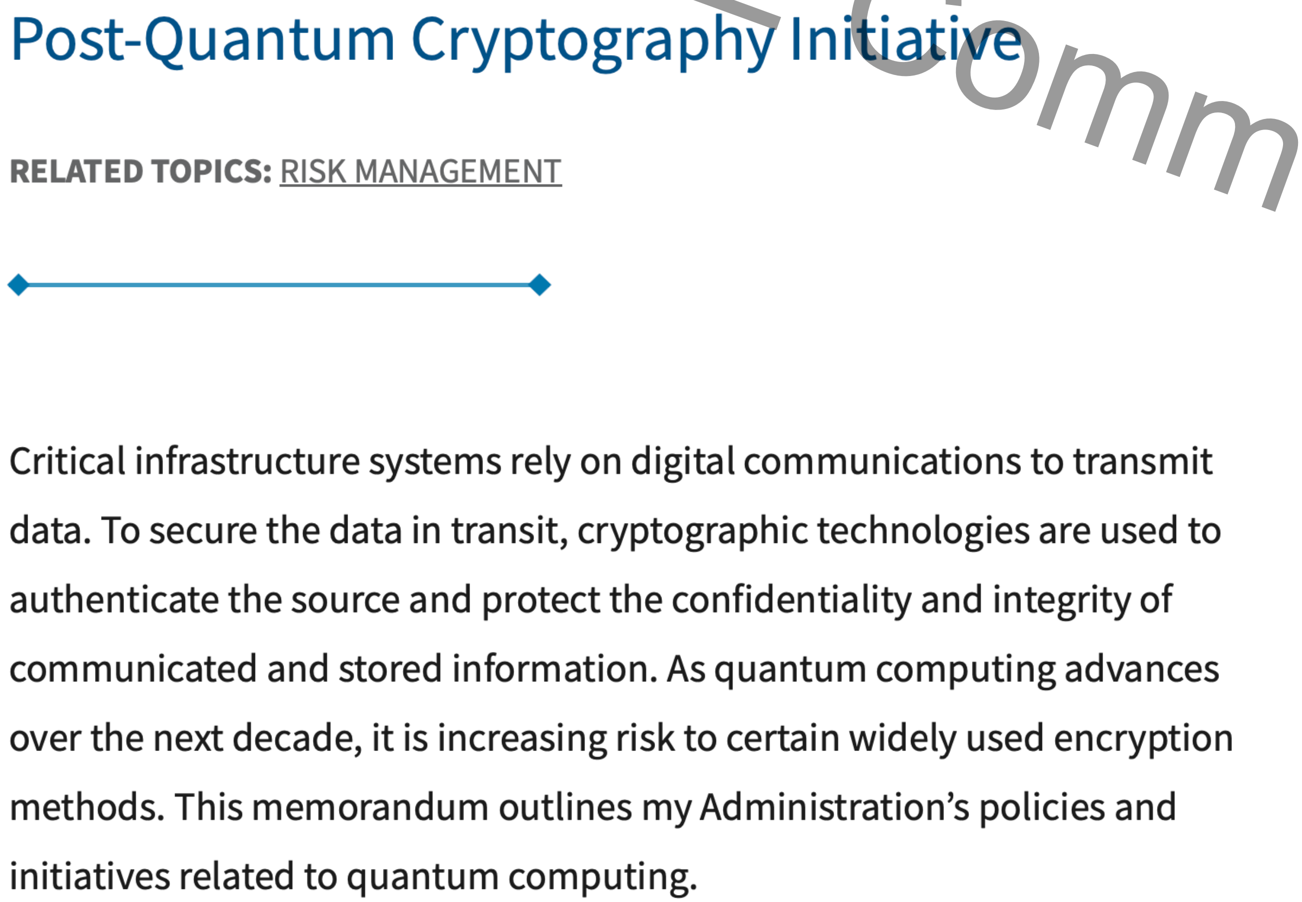
Action 2) Introduce broader audiences to QIST through public outreach and educational materials;

Action 3) Address QIST-specific gaps in professional education and training opportunities; and

Action 4) Make careers in QIST and related fields more accessible and equitable.

BACKGROUND – CONT.

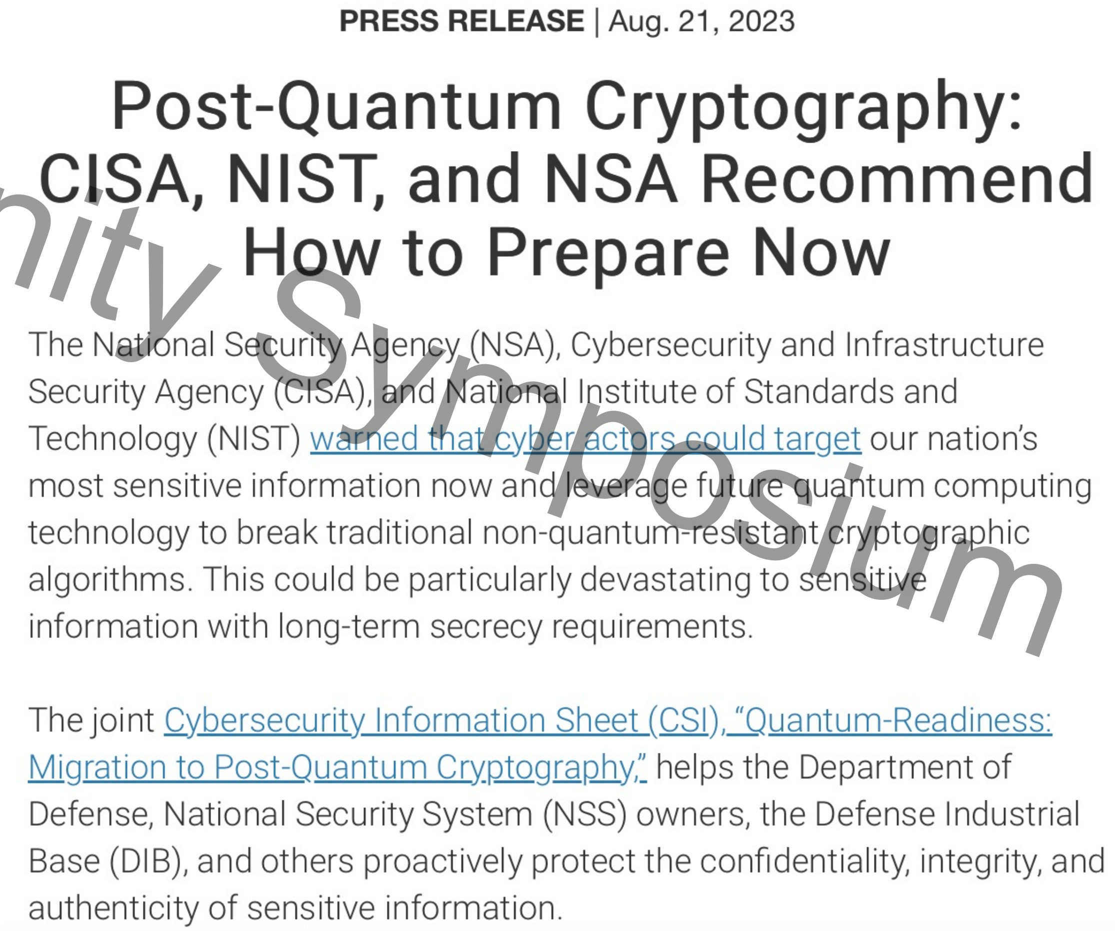
- Due to the potential threats posted by quantum algorithms that could break otherwise secure public cryptographic protocols that are widely used, CISA, NIST, and NSA have asked the agencies and others to mitigate to the current protocols to quantum-resistant ones



Post-Quantum Cryptography Initiative

RELATED TOPICS: RISK MANAGEMENT

Critical infrastructure systems rely on digital communications to transmit data. To secure the data in transit, cryptographic technologies are used to authenticate the source and protect the confidentiality and integrity of communicated and stored information. As quantum computing advances over the next decade, it is increasing risk to certain widely used encryption methods. This memorandum outlines my Administration's policies and initiatives related to quantum computing.



PRESS RELEASE | Aug. 21, 2023

Post-Quantum Cryptography: CISA, NIST, and NSA Recommend How to Prepare Now

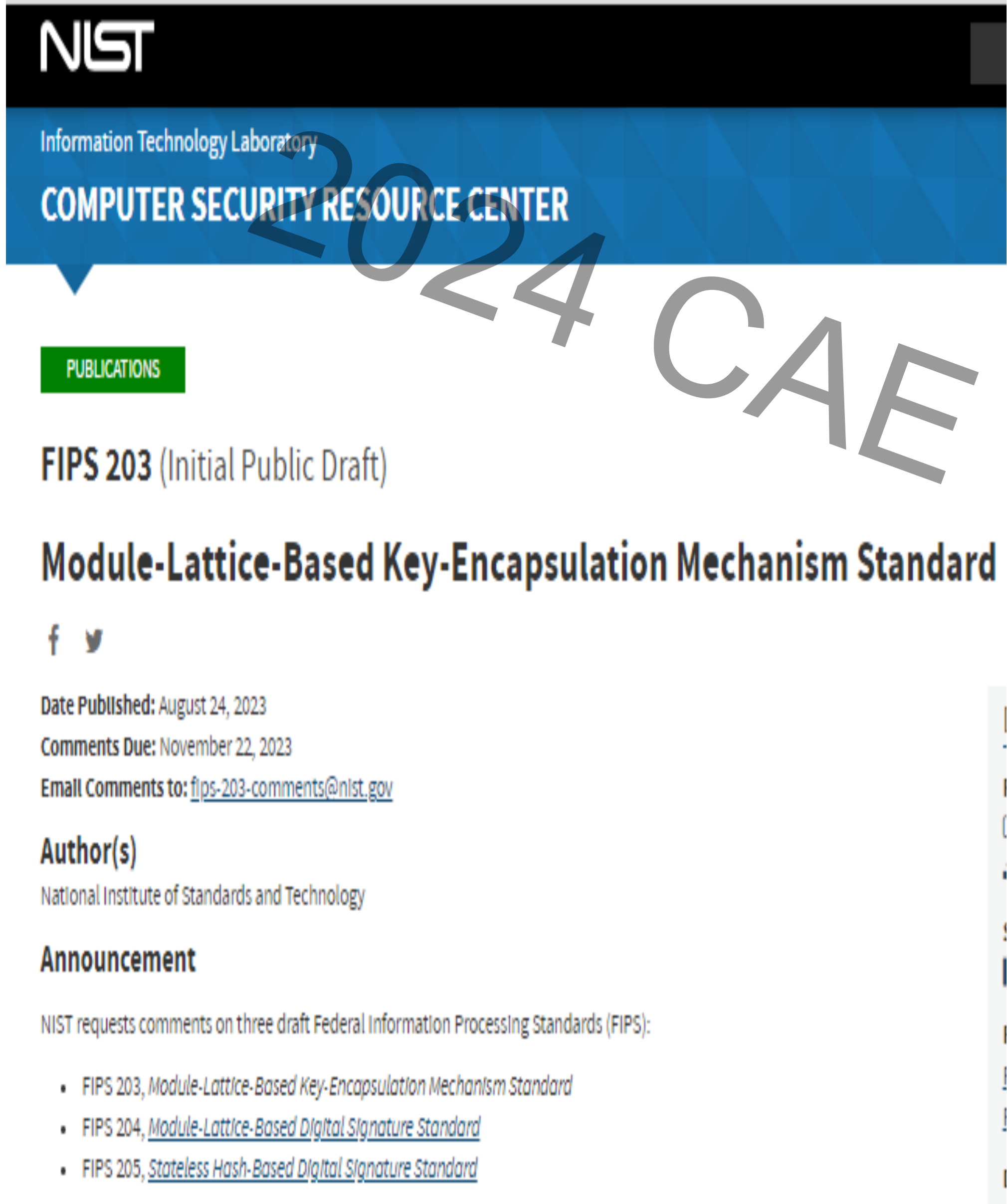
The National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), and National Institute of Standards and Technology (NIST) warned that cyber actors could target our nation's most sensitive information now and leverage future quantum computing technology to break traditional non-quantum-resistant cryptographic algorithms. This could be particularly devastating to sensitive information with long-term secrecy requirements.

The joint Cybersecurity Information Sheet (CSI), "Quantum-Readiness: Migration to Post-Quantum Cryptography," helps the Department of Defense, National Security System (NSS) owners, the Defense Industrial Base (DIB), and others proactively protect the confidentiality, integrity, and authenticity of sensitive information.

BACKGROUND – CONT.

- Note that while quantum computers that can break RSA in a few hours are not feasible yet, they can be relevant today through the failure of the perfect forward secrecy requirement
  - If the parties establish keys using the RSA algorithms without perfect forward secrecy, one can store the packets related to a session
  - Years later, the malicious parties could use quantum computers to break the RSA and therefore the secrecy of the session
  - Such risks can not be justified for some top secrets

BACKGROUND – CONT.



NIST

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PUBLICATIONS

FIPS 203 (Initial Public Draft)

Module-Lattice-Based Key-Encapsulation Mechanism Standard

Date Published: August 24, 2023
Comments Due: November 22, 2023
Email Comments to: fips-203-comments@nist.gov

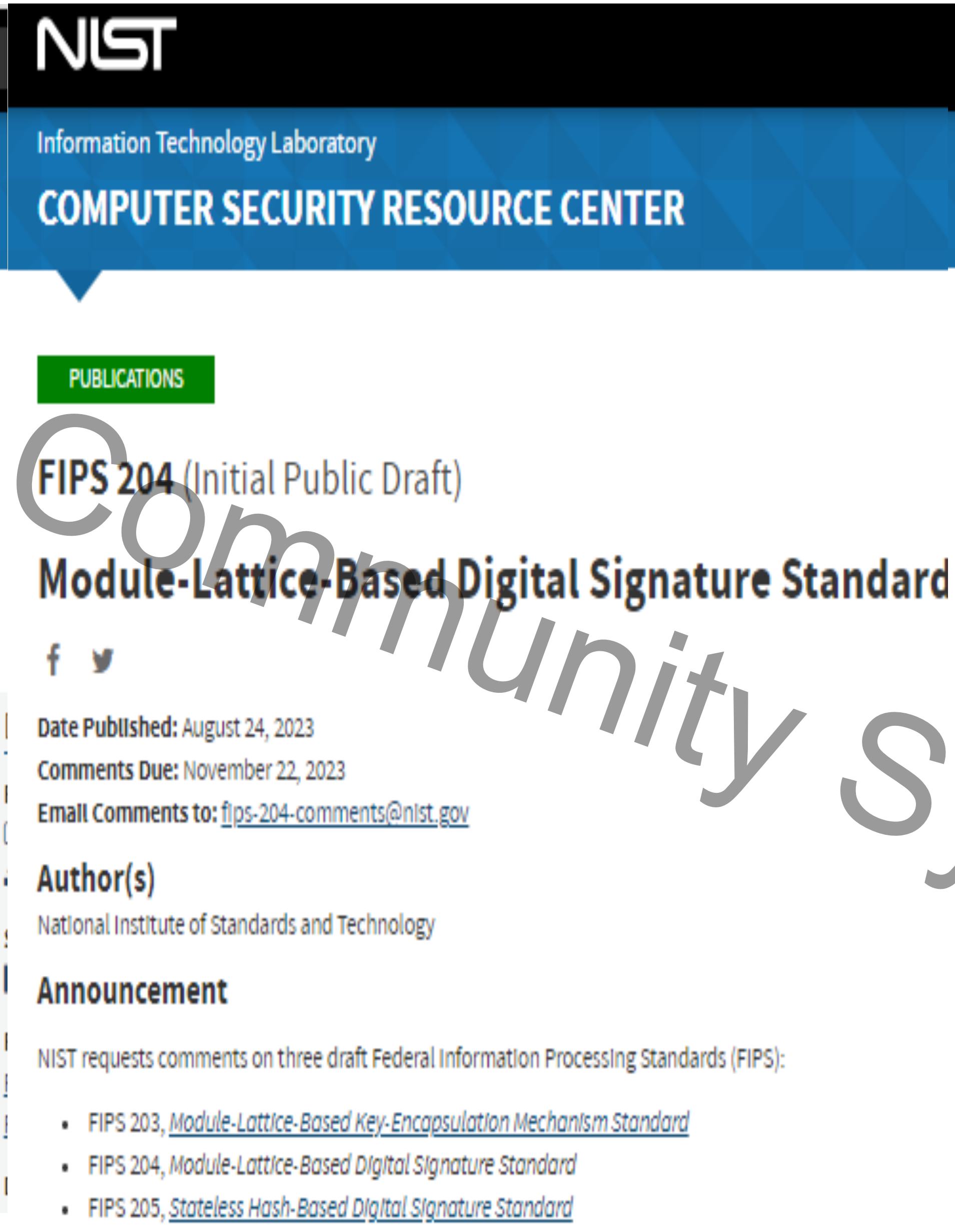
Author(s)

National Institute of Standards and Technology

Announcement

NIST requests comments on three draft Federal Information Processing Standards (FIPS):

- FIPS 203, *Module-Lattice-Based Key-Encapsulation Mechanism Standard*
- FIPS 204, *Module-Lattice-Based Digital Signature Standard*
- FIPS 205, *Stateless Hash-Based Digital Signature Standard*



NIST

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PUBLICATIONS

FIPS 204 (Initial Public Draft)

Module-Lattice-Based Digital Signature Standard

Date Published: August 24, 2023
Comments Due: November 22, 2023
Email Comments to: fips-204-comments@nist.gov

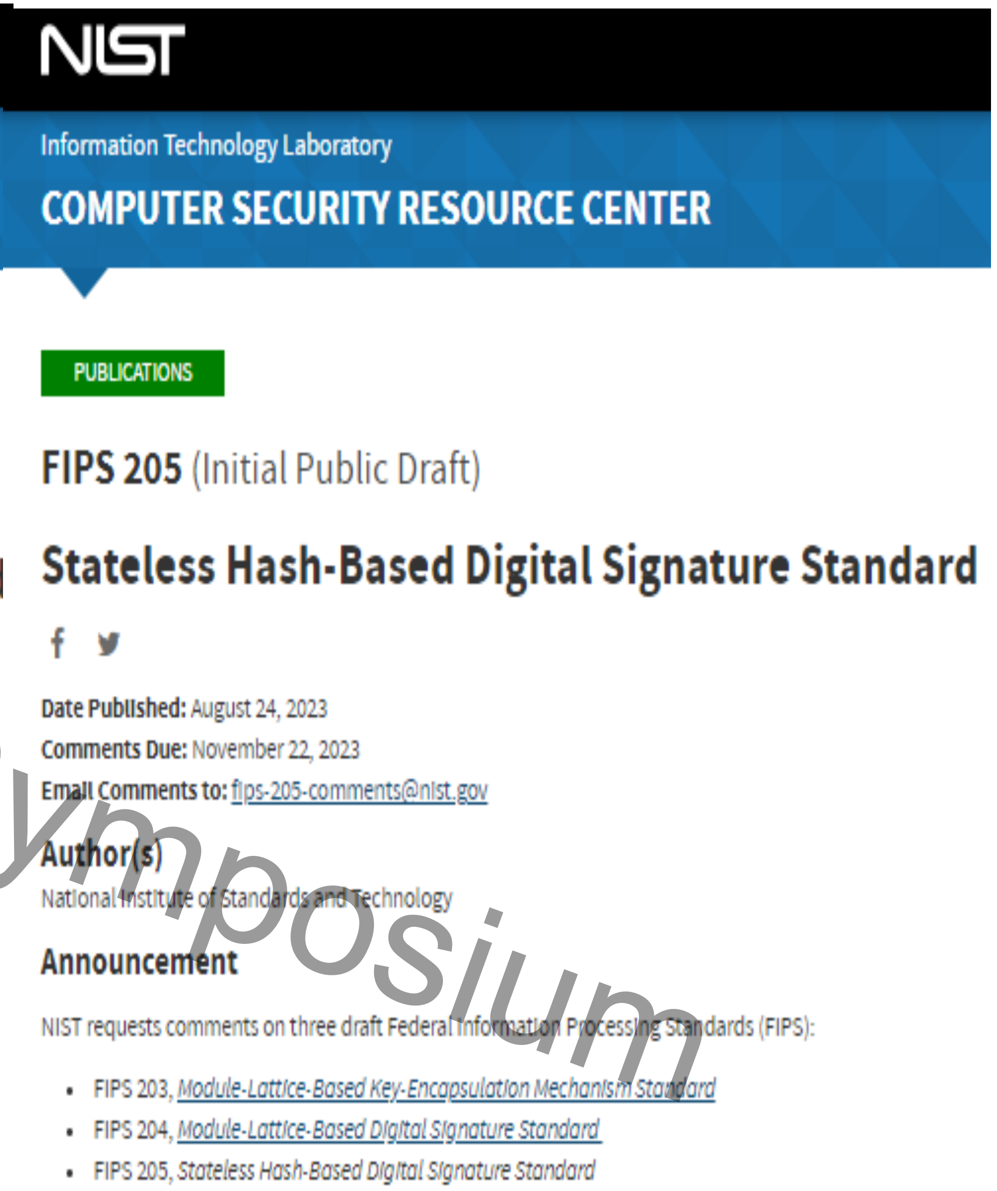
Author(s)

National Institute of Standards and Technology

Announcement

NIST requests comments on three draft Federal Information Processing Standards (FIPS):

- FIPS 203, *Module-Lattice-Based Key-Encapsulation Mechanism Standard*
- FIPS 204, *Module-Lattice-Based Digital Signature Standard*
- FIPS 205, *Stateless Hash-Based Digital Signature Standard*



NIST

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PUBLICATIONS

FIPS 205 (Initial Public Draft)

Stateless Hash-Based Digital Signature Standard

Date Published: August 24, 2023
Comments Due: November 22, 2023
Email Comments to: fips-205-comments@nist.gov

Author(s)

National Institute of Standards and Technology

Announcement

NIST requests comments on three draft Federal Information Processing Standards (FIPS):

- FIPS 203, *Module-Lattice-Based Key-Encapsulation Mechanism Standard*
- FIPS 204, *Module-Lattice-Based Digital Signature Standard*
- FIPS 205, *Stateless Hash-Based Digital Signature Standard*

BACKGROUND – CONT.

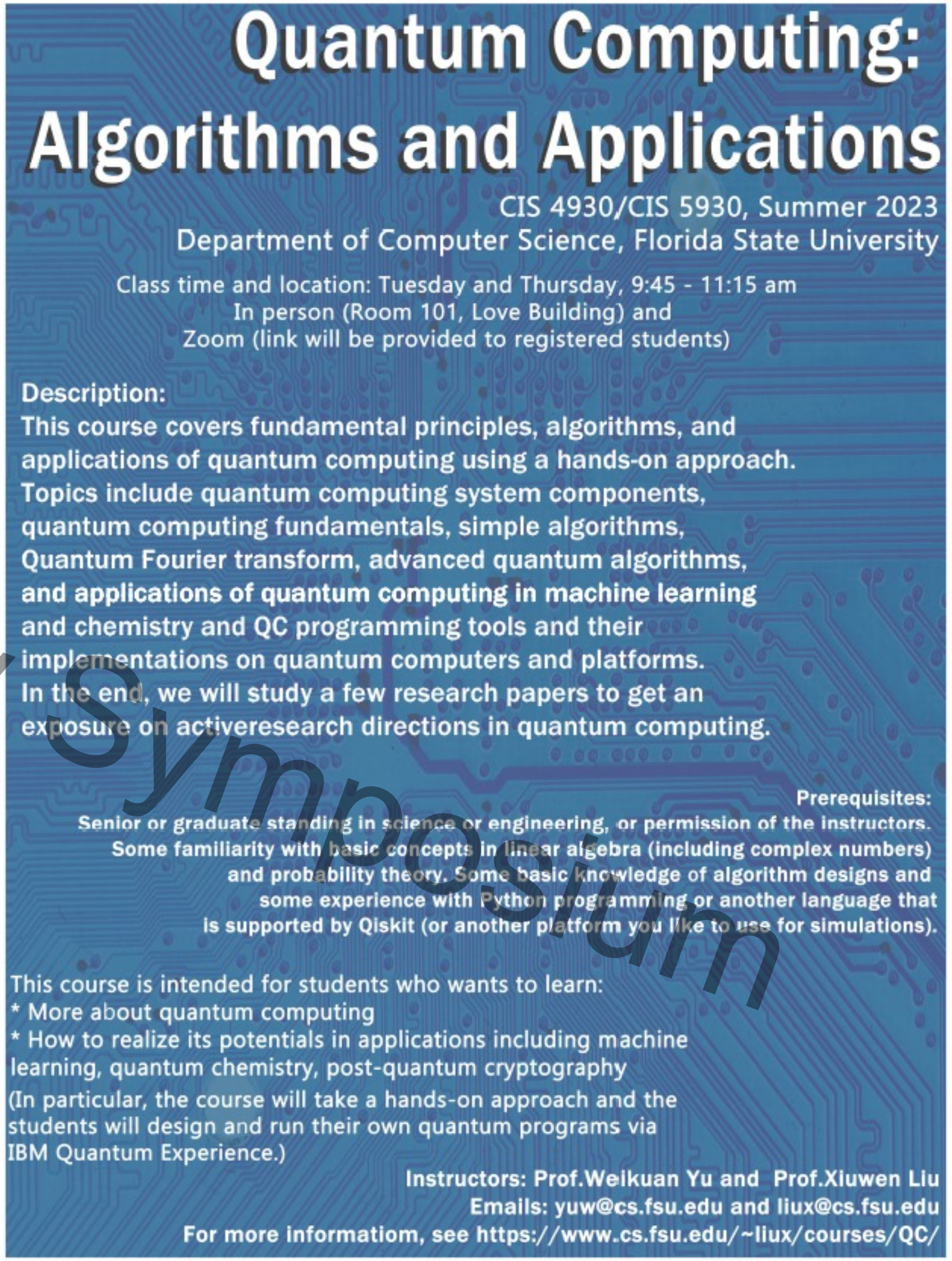
- While the needs of a quantum-proficient workforce is well recognized when quantum technologies become an important component of the economy, the challenge is how to produce a workforce NOW
  - Quantum information and computing techniques are new to most computer science programs
    - They are not part of the existing curricular in most universities
    - Most of computer science and cyber security faculty do not know the subject
    - They are very different from typical computer science courses
  - While quantum technologies could become very important, they are in the very early stages and **face many technical challenges and uncertainties**
    - We cannot educate a workforce to be potentially employed after 10 or 20 years

PROPOSED SOLUTION

- The core component of our proposed solution is to enhance cyber security majors to be quantum proficient
  - Built on the strong problem solving and programming foundations of cyber security majors
- There are several reasons that we believe this is the best solution
  - As post-quantum cryptographic protocols are required in the next two or three years, there would be a great need to redesign and test web sites and web services
    - As we all know, there are many challenges to secure the current web applications and servers
  - Teaching quantum information and computing to cyber security majors can be achieved if this is done effectively

PROPOSED SOLUTION – CONT.

- We are pioneering a QIS program at our department
  - We have developed and taught a class in summer 2023 on quantum computing
  - We will teach this course again in summer 2024
- We design the course on top of the computer science courses our students have already taken
  - Computer circuits in computer architecture
  - Programming platforms and Python libraries
  - Making use of the IBM Quantum Platform



Quantum Computing: Algorithms and Applications

CIS 4930/CIS 5930, Summer 2023
Department of Computer Science, Florida State University

Class time and location: Tuesday and Thursday, 9:45 - 11:15 am
In person (Room 101, Love Building) and
Zoom (link will be provided to registered students)

Description:
This course covers fundamental principles, algorithms, and applications of quantum computing using a hands-on approach. Topics include quantum computing system components, quantum computing fundamentals, simple algorithms, Quantum Fourier transform, advanced quantum algorithms, and applications of quantum computing in machine learning and chemistry and QC programming tools and their implementations on quantum computers and platforms. In the end, we will study a few research papers to get an exposure on activeresearch directions in quantum computing.

Prerequisites:
Senior or graduate standing in science or engineering, or permission of the instructors. Some familiarity with basic concepts in linear algebra (including complex numbers) and probability theory. Some basic knowledge of algorithm designs and some experience with Python programming or another language that is supported by Qiskit (or another platform you like to use for simulations).

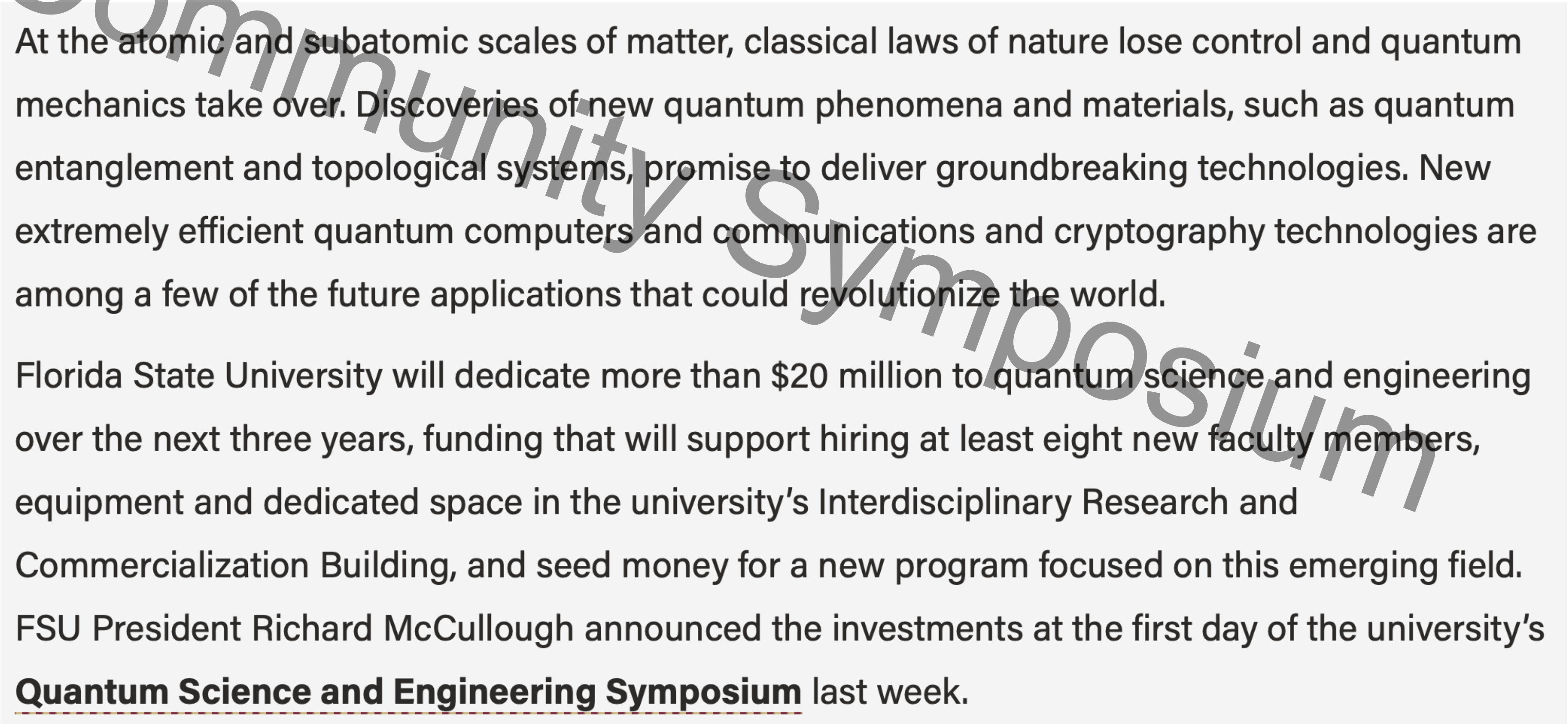
This course is intended for students who wants to learn:
* More about quantum computing
* How to realize its potentials in applications including machine learning, quantum chemistry, post-quantum cryptography
(In particular, the course will take a hands-on approach and the students will design and run their own quantum programs via IBM Quantum Experience.)

Instructors: Prof.Weikuan Yu and Prof.Xiuwen Liu
Emails: yuw@cs.fsu.edu and liux@cs.fsu.edu
For more informatiom, see https://www.cs.fsu.edu/~liux/courses/QC/

BACKGROUND – CONT.

- Florida State University has invested significantly in quantum science and engineering
  - With more than $20 million dedicated to the area, FSU is positioned to be a hub for research and education in quantum science

FSU ANNOUNCES BOLD INVESTMENTS IN QUANTUM SCIENCE AND ENGINEERING
FLORIDA STATE UNIVERSITY
VIRES ARTES MORES
1851



At the atomic and subatomic scales of matter, classical laws of nature lose control and quantum mechanics take over. Discoveries of new quantum phenomena and materials, such as quantum entanglement and topological systems, promise to deliver groundbreaking technologies. New extremely efficient quantum computers and communications and cryptography technologies are among a few of the future applications that could revolutionize the world.

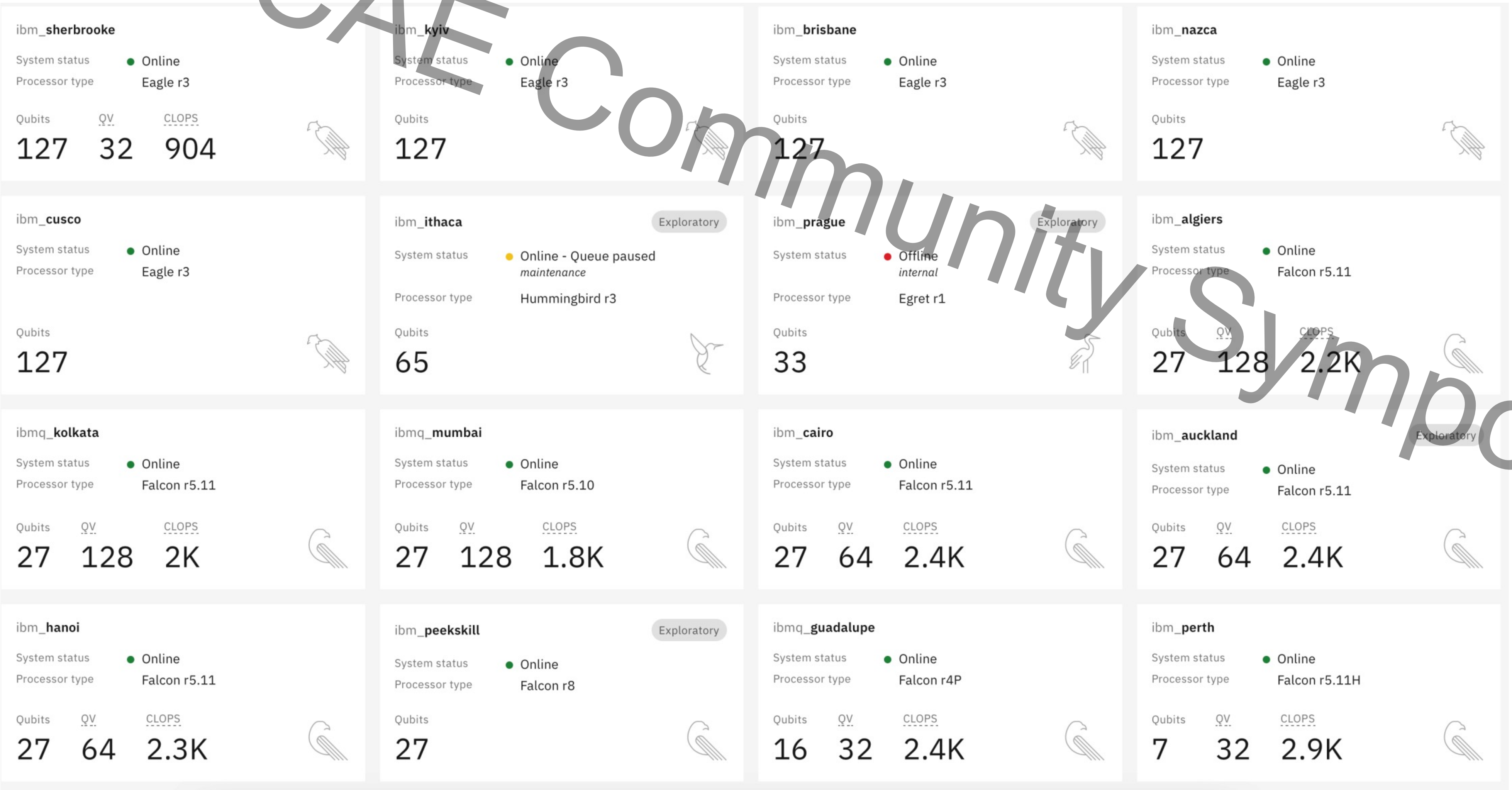
Florida State University will dedicate more than $20 million to quantum science and engineering over the next three years, funding that will support hiring at least eight new faculty members, equipment and dedicated space in the university's Interdisciplinary Research and Commercialization Building, and seed money for a new program focused on this emerging field. FSU President Richard McCullough announced the investments at the first day of the university's **Quantum Science and Engineering Symposium** last week.

PROPOSED SOLUTION – CONT.

- In the next few slides, we will introduce the quantum algorithms and the ways we have covered them so that you can see that they are not as difficult as they appear
- One of the common misconceptions is that quantum computing requires a good understanding of quantum mechanism
  - While building and designing new quantum bits would require advanced degrees in quantum mechanism, physics, chemistry, and materials sciences, quantum information and computing builds on quantum bits
    - The situation is very similar to what we do in computer science today with respect to gates and semi-conductance materials
      - Actually, computer architectures would require a good understanding of quantum mechanism as the quantum effects are relevant

STATE OF QUANTUM COMPUTING

- There are very active and large investments from governments and companies, trying to leverage the unique properties of quantum states
  - An easy way to experiment with real quantum computers is via IBM Quantum



ibm_**sherbrooke**
System status ● Online
Processor type Eagle r3
Qubits 127 | QV 32 | CLOPS 904

ibm_**kyiv**
System status ● Online
Processor type Eagle r3
Qubits 127

ibm_**brisbane**
System status ● Online
Processor type Eagle r3
Qubits 127

ibm_**nazca**
System status ● Online
Processor type Eagle r3
Qubits 127

ibm_**cusco**
System status ● Online
Processor type Eagle r3
Qubits 127

ibm_**ithaca** Exploratory
System status ● Online - Queue paused *maintenance*
Processor type Hummingbird r3
Qubits 65

ibm_**prague** Exploratory
System status ● Offline *internal*
Processor type Egret r1
Qubits 33

ibm_**algiers**
System status ● Online
Processor type Falcon r5.11
Qubits 27 | QV 128 | CLOPS 2.2K

ibmq_**kolkata**
System status ● Online
Processor type Falcon r5.11
Qubits 27 | QV 128 | CLOPS 2K

ibmq_**mumbai**
System status ● Online
Processor type Falcon r5.10
Qubits 27 | QV 128 | CLOPS 1.8K

ibm_**cairo**
System status ● Online
Processor type Falcon r5.11
Qubits 27 | QV 64 | CLOPS 2.4K

ibm_**auckland** Exploratory
System status ● Online
Processor type Falcon r5.11
Qubits 27 | QV 64 | CLOPS 2.4K

ibm_**hanoi**
System status ● Online
Processor type Falcon r5.11
Qubits 27 | QV 64 | CLOPS 2.3K

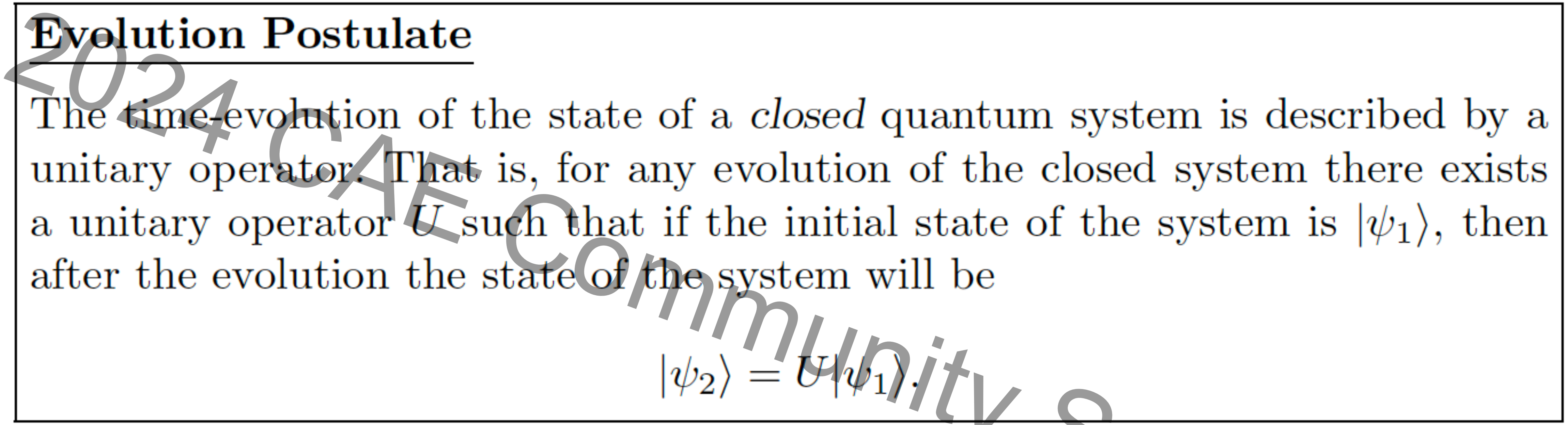
ibm_**peekskill** Exploratory
System status ● Online
Processor type Falcon r8
Qubits 27

ibmq_**guadalupe**
System status ● Online
Processor type Falcon r4P
Qubits 16 | QV 32 | CLOPS 2.4K

ibm_**perth**
System status ● Online
Processor type Falcon r5.11H
Qubits 7 | QV 32 | CLOPS 2.9K

QUANTUM MECHANIC SYSTEM MODEL

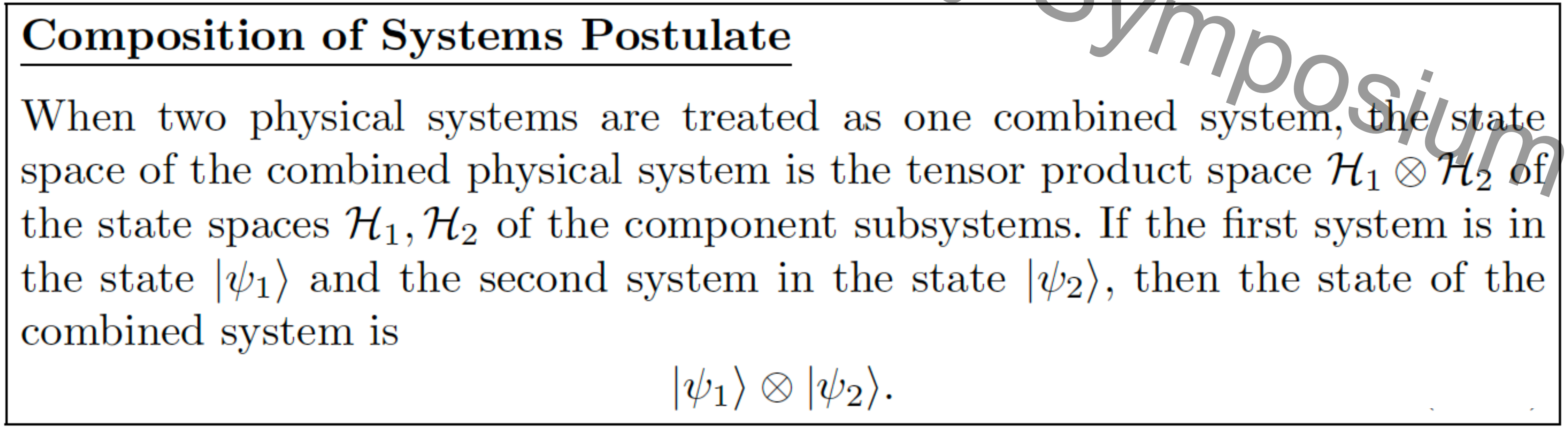
- Key properties



Evolution Postulate

The time-evolution of the state of a *closed* quantum system is described by a unitary operator. That is, for any evolution of the closed system there exists a unitary operator U such that if the initial state of the system is $|\psi_1\rangle$, then after the evolution the state of the system will be

$$|\psi_2\rangle = U|\psi_1\rangle.$$



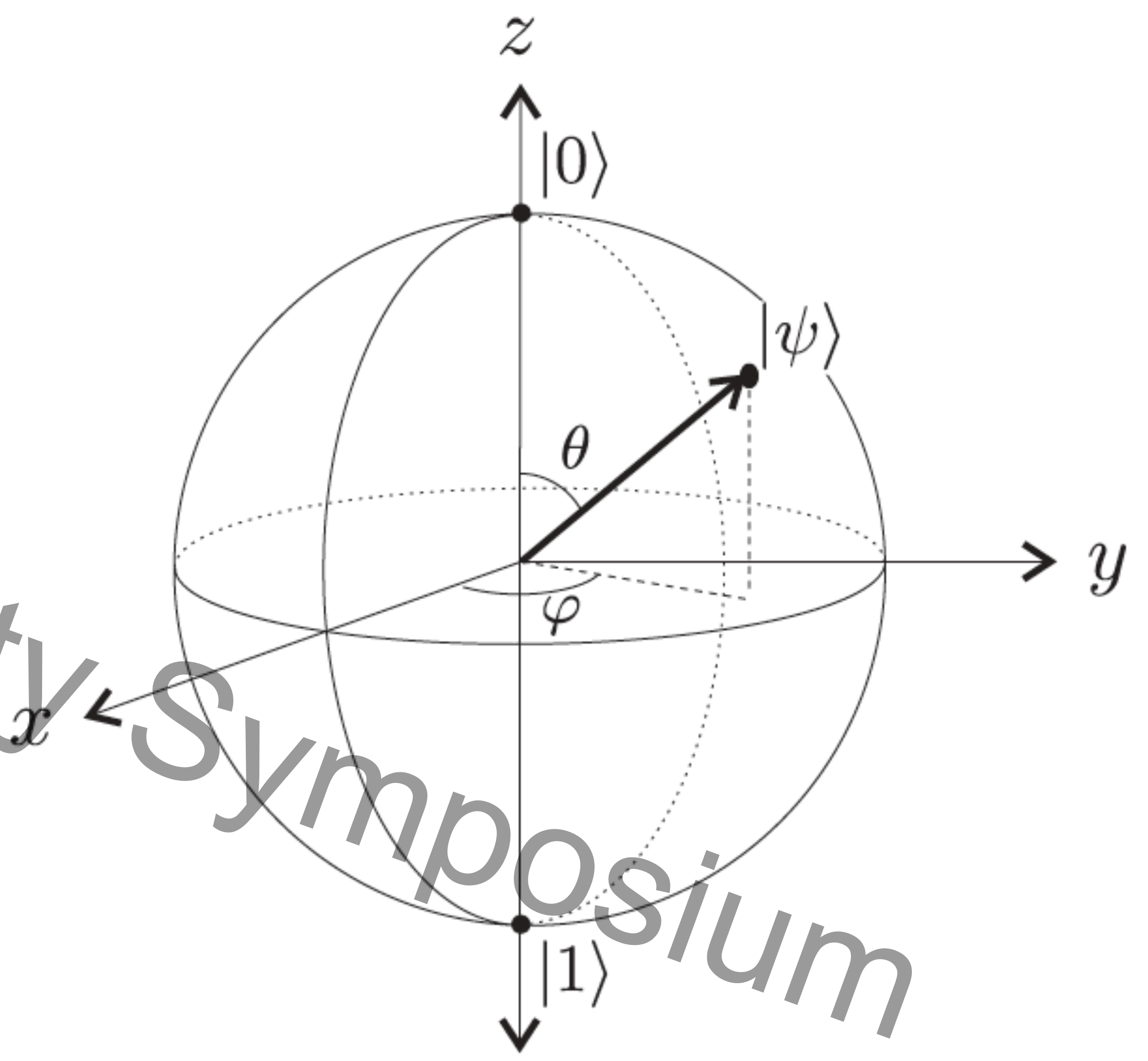
Composition of Systems Postulate

When two physical systems are treated as one combined system, the state space of the combined physical system is the tensor product space $\mathcal{H}_1 \otimes \mathcal{H}_2$ of the state spaces $\mathcal{H}_1, \mathcal{H}_2$ of the component subsystems. If the first system is in the state $|\psi_1\rangle$ and the second system in the state $|\psi_2\rangle$, then the state of the combined system is

$$|\psi_1\rangle \otimes |\psi_2\rangle.$$

PROBLEM SOLVING USING QUANTUM COMPUTING

- Quantum Superposition
  - A quantum bit represents 0 and 1 at the same time probabilistically
  - The Block sphere is a good and common way to visualize quantum bits
  - Keep in mind that one can only measure 0 or 1 each time, creating a bottleneck
- Quantum Entanglement
  - Typically, a system with more quantum bits is obtained by composing systems with fewer qubits
- Quantum Parallelism

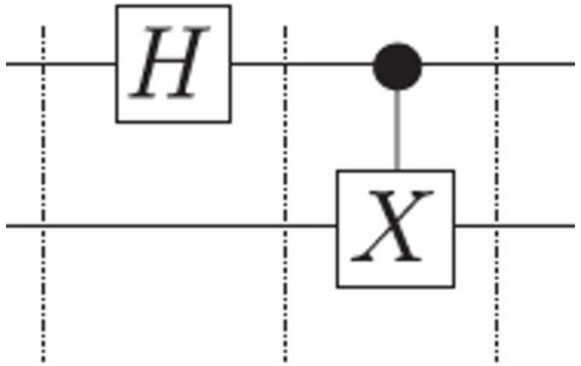


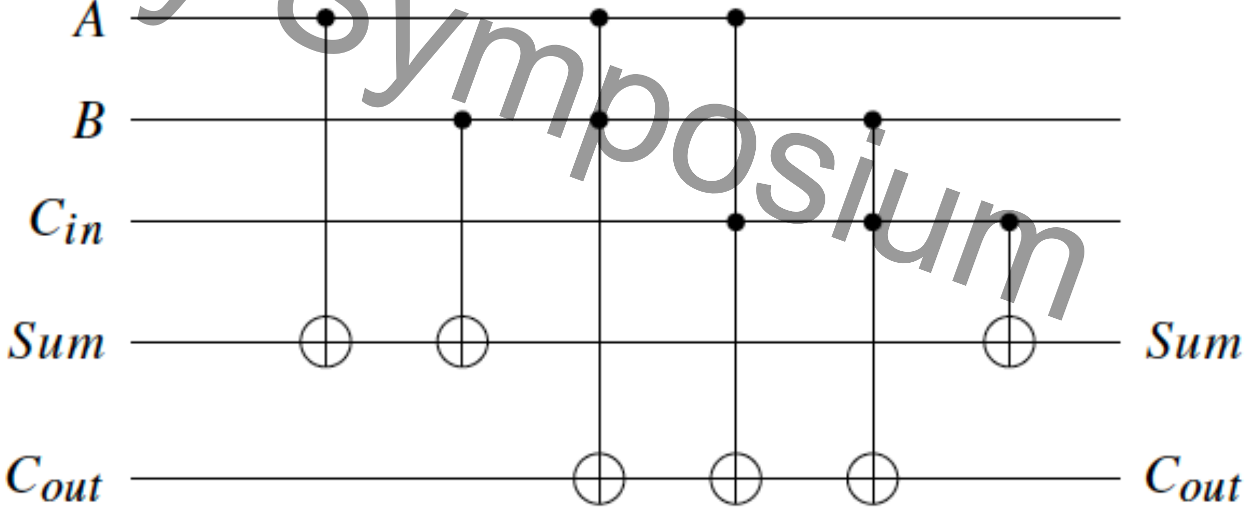
PROBLEM SOLVING USING QUANTUM COMPUTING

- Quantum Algorithms
  - Fundamentally, quantum algorithms are quantum circuits, consisting of quantum gates
  - By utilizing some key properties of the gates, one can solve certain problems more efficiently than any classical algorithms
  - Quantum circuits can be modeled as matrix multiplications, very similar to reversible computing

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

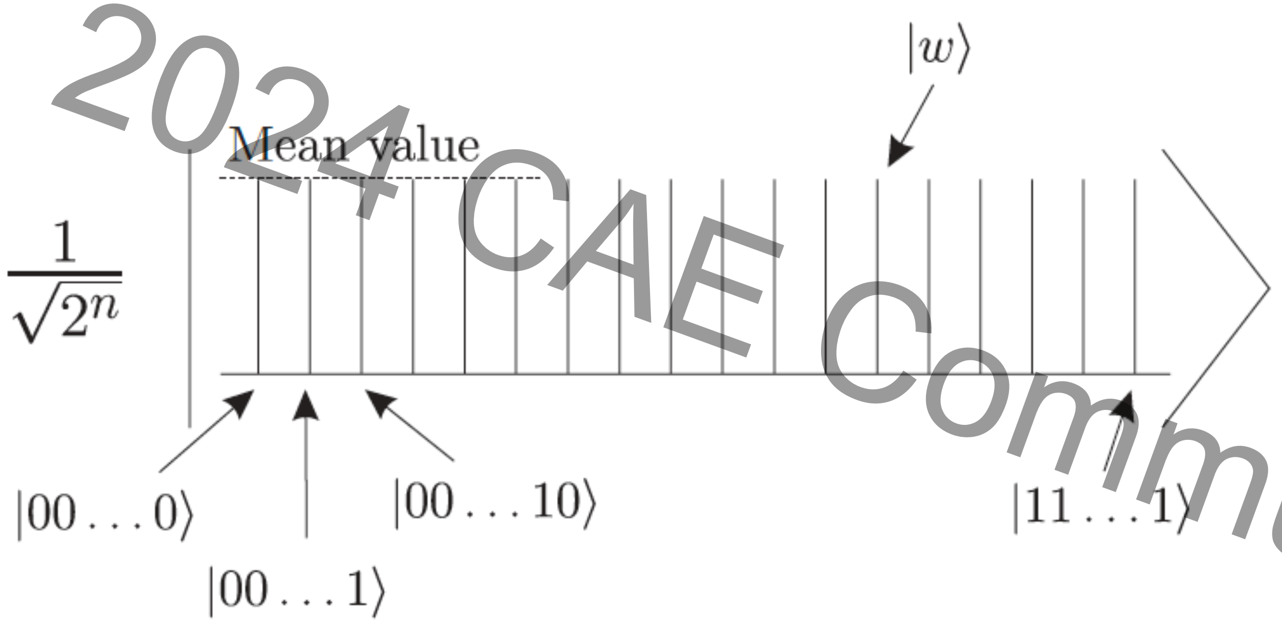
$$H|0\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$H|1\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

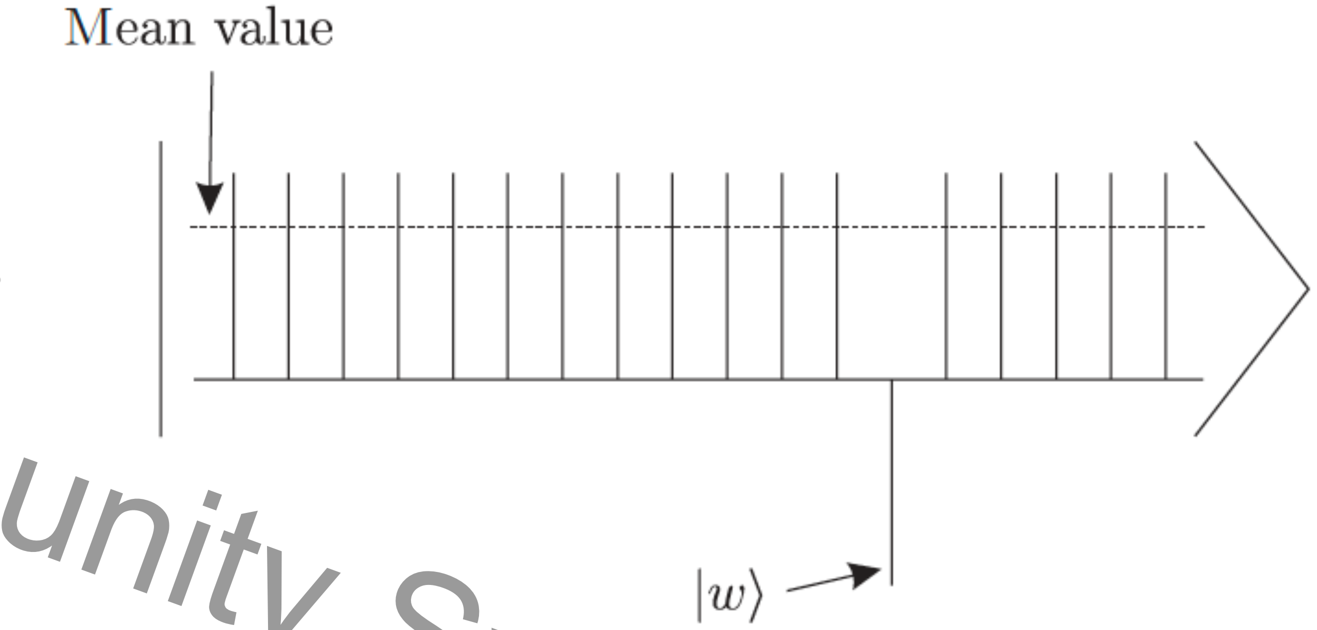


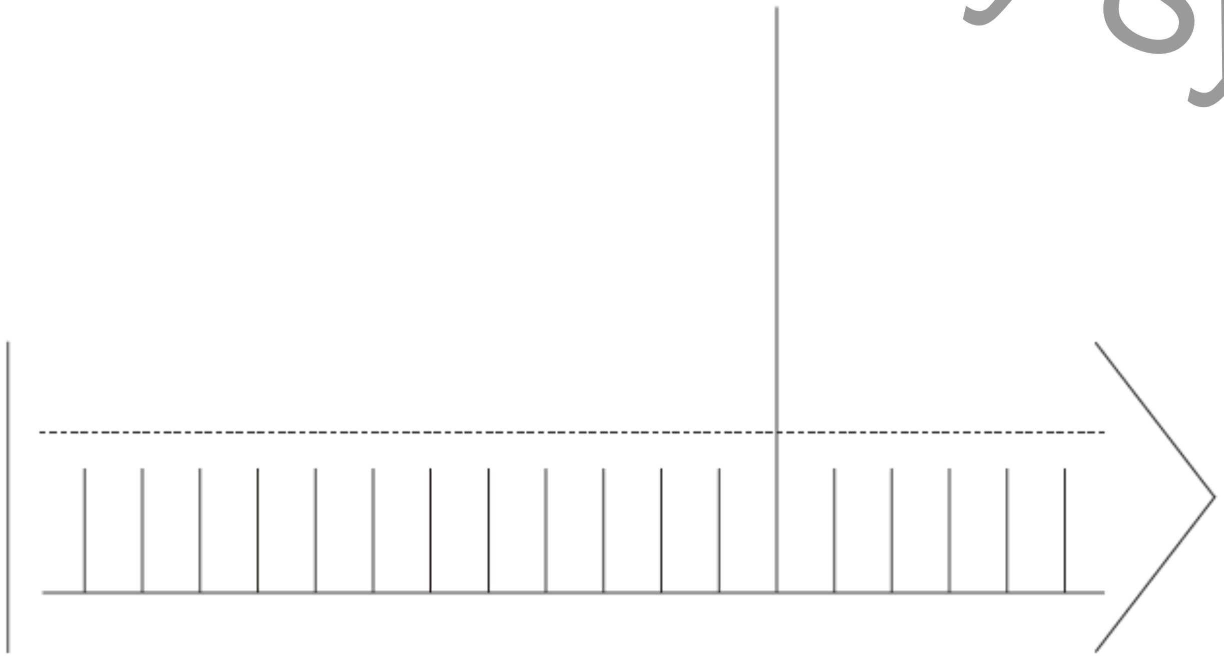


PROBLEM SOLVING USING QUANTUM COMPUTING

- Quantum Algorithms – Flipping About the Mean Operator and Grover’s Algorithm

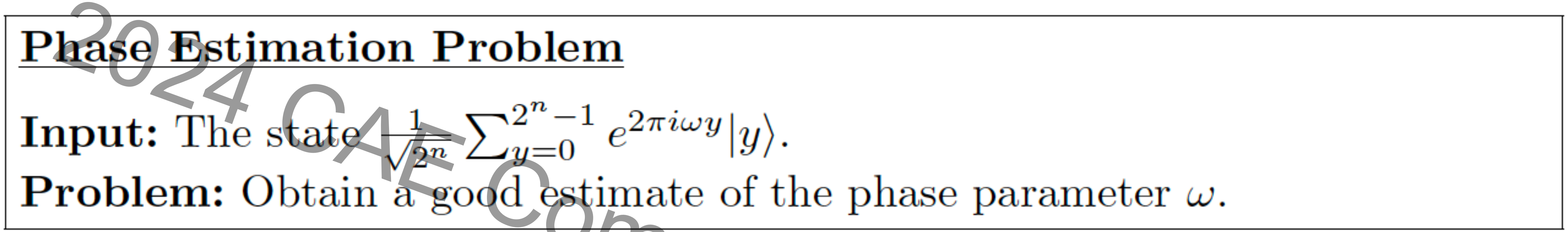






QUANTUM PHASE ESTIMATION – CONT.

- Here is the quantum phase estimation problem



Phase Estimation Problem

Input: The state $\frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1} e^{2\pi i \omega y}|y\rangle$.

Problem: Obtain a good estimate of the phase parameter ω.

- – An efficient solution to this problem is almost the same as the quantum Fourier transform and is also a key component to the eigenvalue estimation problem
- – We use a binary encoding for ω,

$$\omega = 0.x_1x_2x_3\cdots$$

  - This is a binary number representation for fraction numbers
  - The value is given by $x_1 \cdot 2^{-1} + x_2 \cdot 2^{-2} + x_3 \cdot 2^{-3} + \cdots$

QUANTUM PHASE ESTIMATION – CONT.

- A key property of

$$\frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1} e^{2\pi i\omega y}|y\rangle$$

  - It can be written as the tensor product of n terms

$$\frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1} e^{2\pi i\omega y}|y\rangle = \left(\frac{|0\rangle + e^{2\pi i(2^{n-1}\omega)}|1\rangle}{\sqrt{2}}\right)\otimes\left(\frac{|0\rangle + e^{2\pi i(2^{n-2}\omega)}|1\rangle}{\sqrt{2}}\right)\otimes\cdots$$

$$\cdots\otimes\left(\frac{|0\rangle + e^{2\pi i(\omega)}|1\rangle}{\sqrt{2}}\right)$$

$$= \left(\frac{|0\rangle + e^{2\pi i(0.x_n x_{n+1}\cdots)}|1\rangle}{\sqrt{2}}\right)\otimes\left(\frac{|0\rangle + e^{2\pi i(0.x_{n-1}x_n x_{n+1}\cdots)}|1\rangle}{\sqrt{2}}\right)\otimes\cdots$$

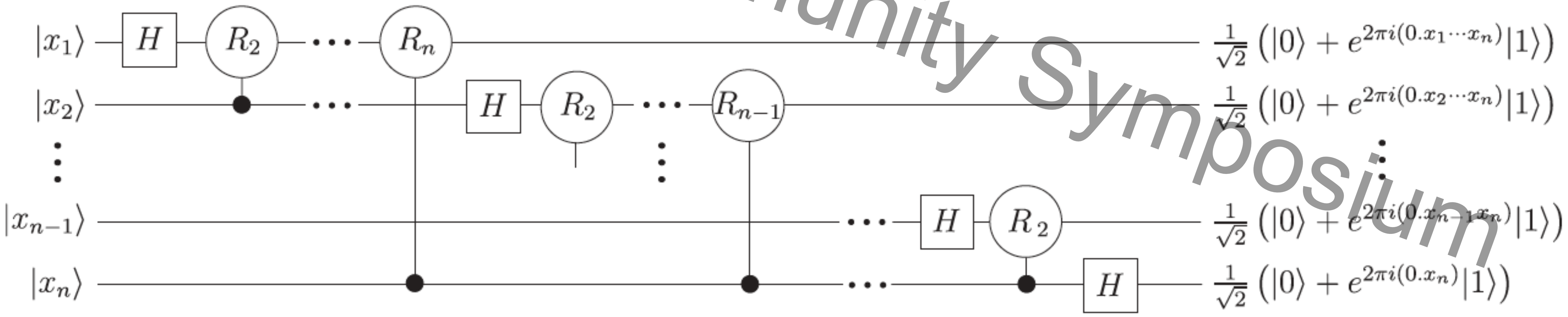
$$\cdots\otimes\left(\frac{|0\rangle + e^{2\pi i(0.x_1 x_2\cdots)}|1\rangle}{\sqrt{2}}\right).$$

QUANTUM PHASE ESTIMATION – CONT.

- The inverse of quantum phase estimation is the quantum Fourier transform

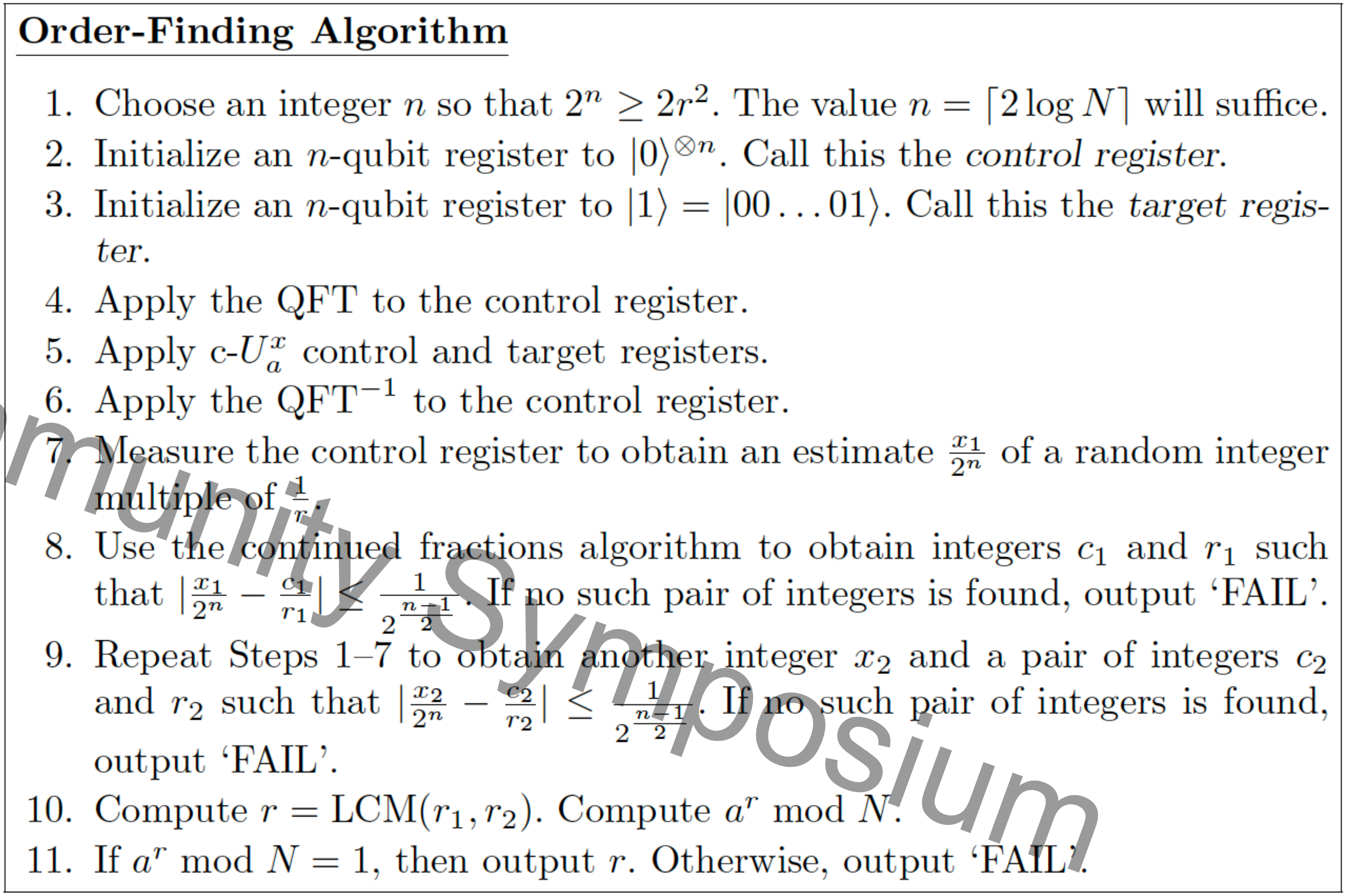
$$|x\rangle \longmapsto \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{x}{2^n} y} |y\rangle$$

  - The algorithm is simply running the quantum phase estimation backward


$|x_1\rangle$
$|x_2\rangle$
$|x_{n-1}\rangle$
$|x_n\rangle$
H
R_2
R_n
R_{n-1}
$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i (0.x_1 \cdots x_n)}|1\rangle\right)$
$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i (0.x_2 \cdots x_n)}|1\rangle\right)$
$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i (0.x_{n-1} x_n)}|1\rangle\right)$
$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i (0.x_n)}|1\rangle\right)$

QUANTUM PHASE ESTIMATION – CONT.

- The circuits for quantum phase estimation and for quantum Fourier transform are the key for exponential speedup for a number of quantum algorithms
  - Including Shor’s factorization algorithm and solution to the discrete logarithmic problem
  - Harrow-Hassidim-Lloyd algorithm
    - It does not have an exponential speedup as an end-to-end solution to solving linear equations



Order-Finding Algorithm

1. Choose an integer n so that $2^n \geq 2r^2$. The value $n = \lceil 2 \log N \rceil$ will suffice.
2. Initialize an n-qubit register to $|0\rangle^{\otimes n}$. Call this the *control register*.
3. Initialize an n-qubit register to $|1\rangle = |00\ldots01\rangle$. Call this the *target register*.
4. Apply the QFT to the control register.
5. Apply c-U_a^x control and target registers.
6. Apply the QFT^{-1} to the control register.
7. Measure the control register to obtain an estimate $\frac{x_1}{2^n}$ of a random integer multiple of $\frac{1}{r}$.
8. Use the continued fractions algorithm to obtain integers c_1 and r_1 such that $|\frac{x_1}{2^n} - \frac{c_1}{r_1}| \leq \frac{1}{2^{\frac{n-1}{2}}}$. If no such pair of integers is found, output ‘FAIL’.
9. Repeat Steps 1–7 to obtain another integer x_2 and a pair of integers c_2 and r_2 such that $|\frac{x_2}{2^n} - \frac{c_2}{r_2}| \leq \frac{1}{2^{\frac{n-1}{2}}}$. If no such pair of integers is found, output ‘FAIL’.
10. Compute $r = \mathrm{LCM}(r_1, r_2)$. Compute $a^r \bmod N$.
11. If $a^r \bmod N = 1$, then output r. Otherwise, output ‘FAIL’.

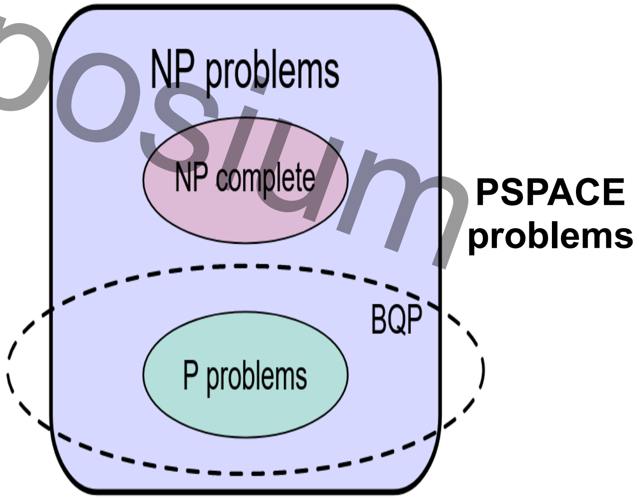
SUMMARY – PART I

- Quantum bits and gates provide unique advantages with no counter parts in classical computing
  - Utilizing these properties has resulted in algorithms with exponential speedup, including factorization
    - This renders the current public key cryptography systems insufficient
  - Problem solving using quantum computing has been being explored actively
    - Considering the algorithms as end-to-end solutions elucidates the advantages and limitations of quantum algorithms
- Post-quantum cryptographic systems will be a reality in the next one or two years

POST QUANTUM CRYPTOGRAPHY
QUANTUM COMPUTERS (QC): THE GOOD, THE BAD, AND UGLY

- QC are much more powerful than conventional computers: on storage size n they can compute as if they were operating on 2^n values in parallel.
- QC are very expensive to build and operate at temperatures close to absolute zero. Qubits are fragile and susceptible to noise, to errors, and have a very short lifespan of $\sim 2ms$.
- If you read the state of a QC you *see only one value*: the *others disappear*.
- Bounded error Quantum Polynomial time (BQP): decision problems that can be solved by a QC in polynomial time.

  It is widely believed that QC cannot solve NP hard problems
- Average-case hardness vs worst-case hardness.



THREATS TO CURRENT SYMMETRIC AND ASYMMETRIC PROTOCOLS

- *Grover's Quantum Algorithm*: Brute-force search for the n-bit secret key k of a symmetric-key algorithm that encrypts a message m to a ciphertext c requires only $\sqrt{2^n} = 2^{n/2}$ tries. Same for MACs.

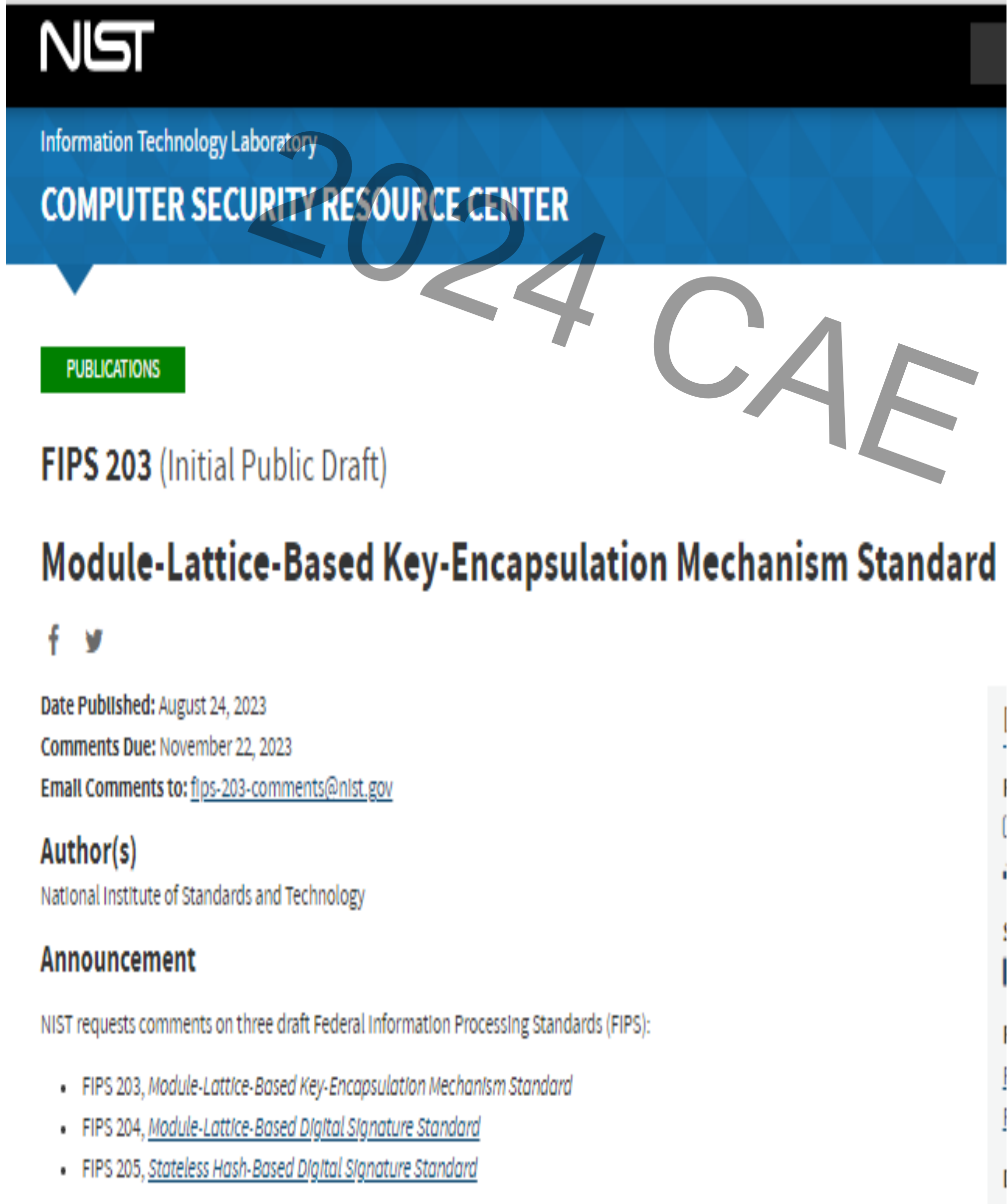
This means that AES-128 offers only 64-bit protection. *Must use AES-256*

- *Shor's Algorithm*: Solves the factoring, discrete logarithm, and period finding problems efficiently.

This means that a sufficiently large QC will *break all current* public-key algorithms: RSA, Diffie-Hellman, ElGamal, elliptic curve crypto.

- *What is needed*: a few thousand logical qubits and a program that applies a few billion logical gates (not yet feasible)

NIST: THREE NEW ALGORITHMS FOR 2024.



NIST

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PUBLICATIONS

FIPS 203 (Initial Public Draft)

Module-Lattice-Based Key-Encapsulation Mechanism Standard

Date Published: August 24, 2023
Comments Due: November 22, 2023
Email Comments to: fips-203-comments@nist.gov

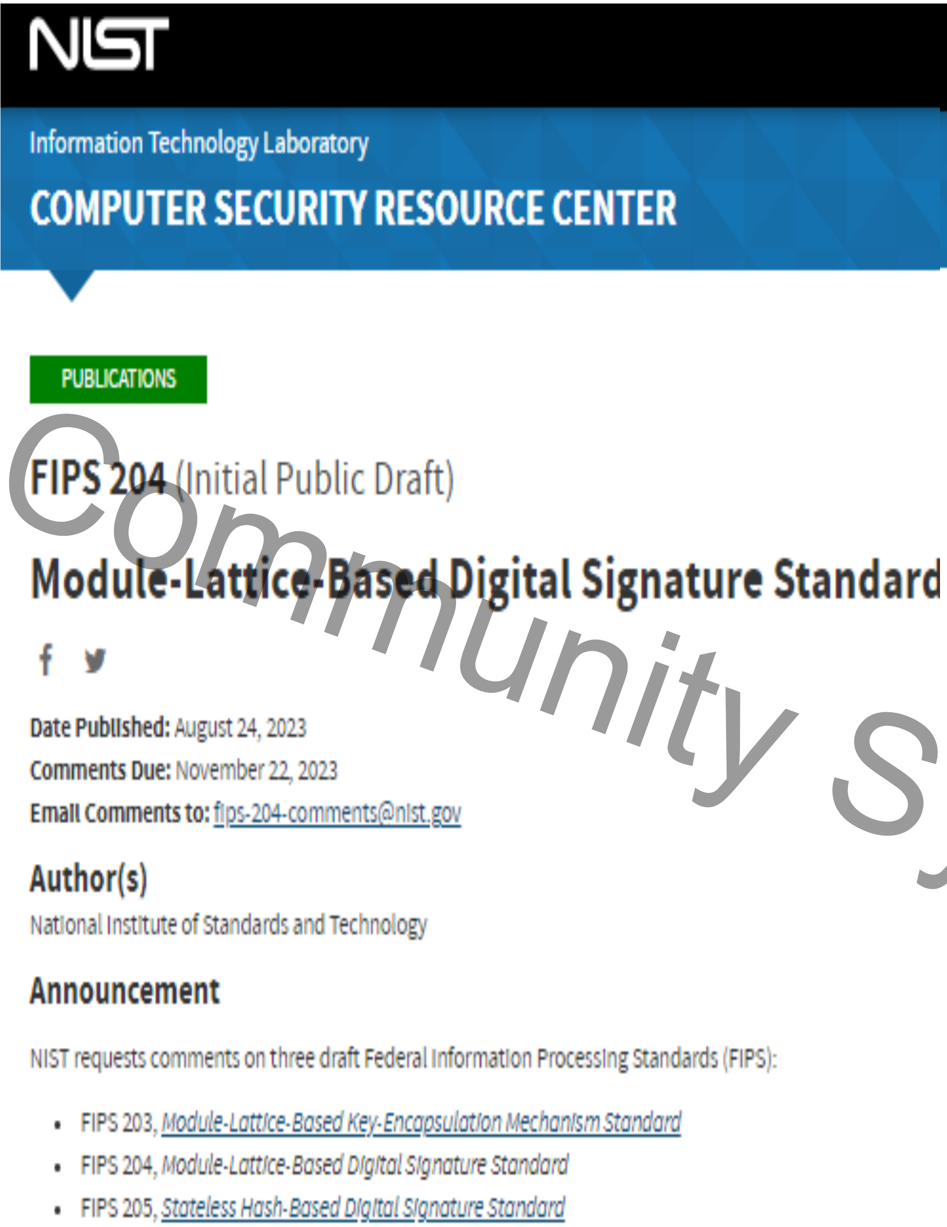
Author(s)

National Institute of Standards and Technology

Announcement

NIST requests comments on three draft Federal Information Processing Standards (FIPS):

- FIPS 203, *Module-Lattice-Based Key-Encapsulation Mechanism Standard*
- FIPS 204, *Module-Lattice-Based Digital Signature Standard*
- FIPS 205, *Stateless Hash-Based Digital Signature Standard*



NIST

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PUBLICATIONS

FIPS 204 (Initial Public Draft)

Module-Lattice-Based Digital Signature Standard

Date Published: August 24, 2023
Comments Due: November 22, 2023
Email Comments to: fips-204-comments@nist.gov

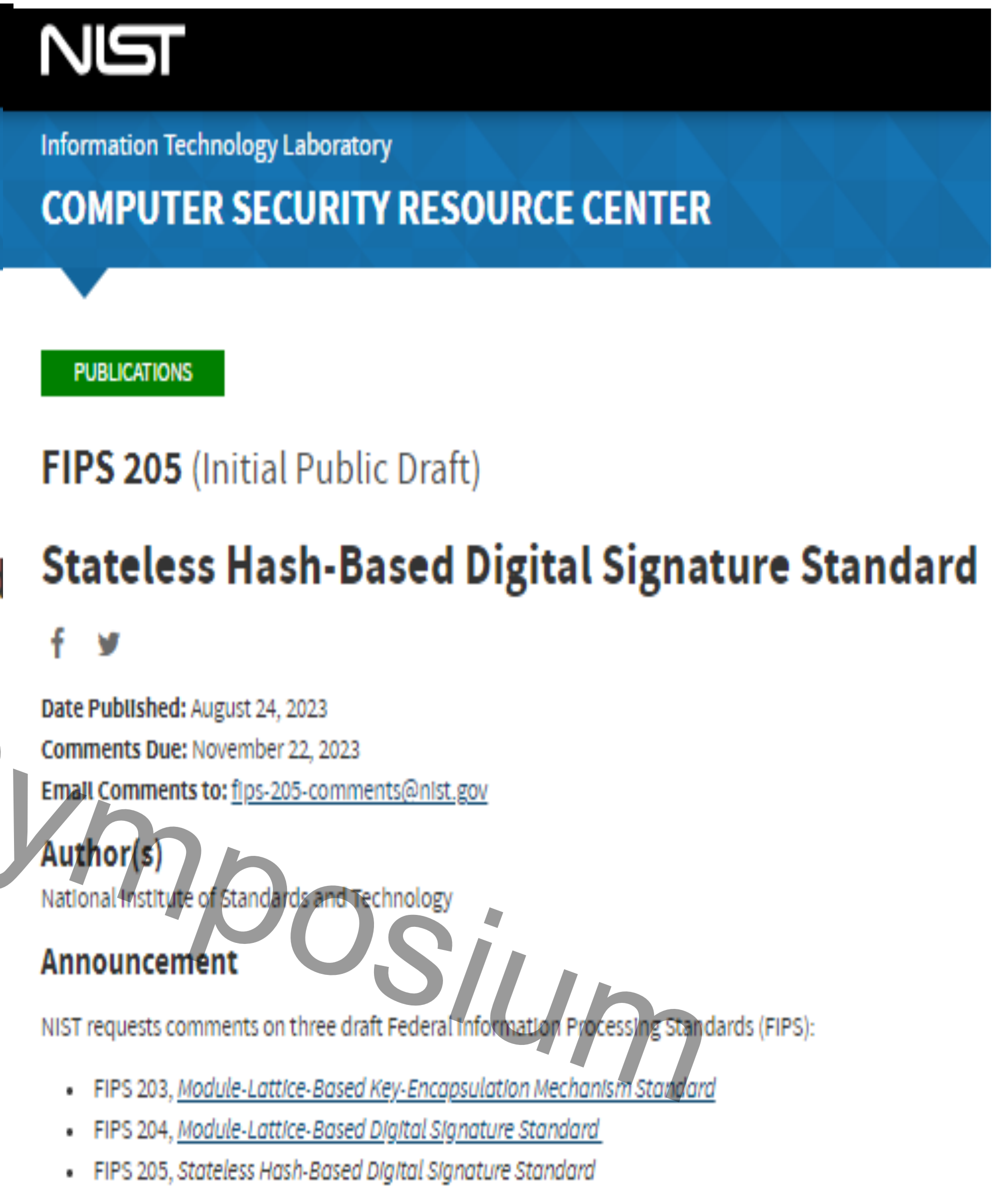
Author(s)

National Institute of Standards and Technology

Announcement

NIST requests comments on three draft Federal Information Processing Standards (FIPS):

- FIPS 203, *Module-Lattice-Based Key-Encapsulation Mechanism Standard*
- FIPS 204, *Module-Lattice-Based Digital Signature Standard*
- FIPS 205, *Stateless Hash-Based Digital Signature Standard*



NIST

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PUBLICATIONS

FIPS 205 (Initial Public Draft)

Stateless Hash-Based Digital Signature Standard

Date Published: August 24, 2023
Comments Due: November 22, 2023
Email Comments to: fips-205-comments@nist.gov

Author(s)

National Institute of Standards and Technology

Announcement

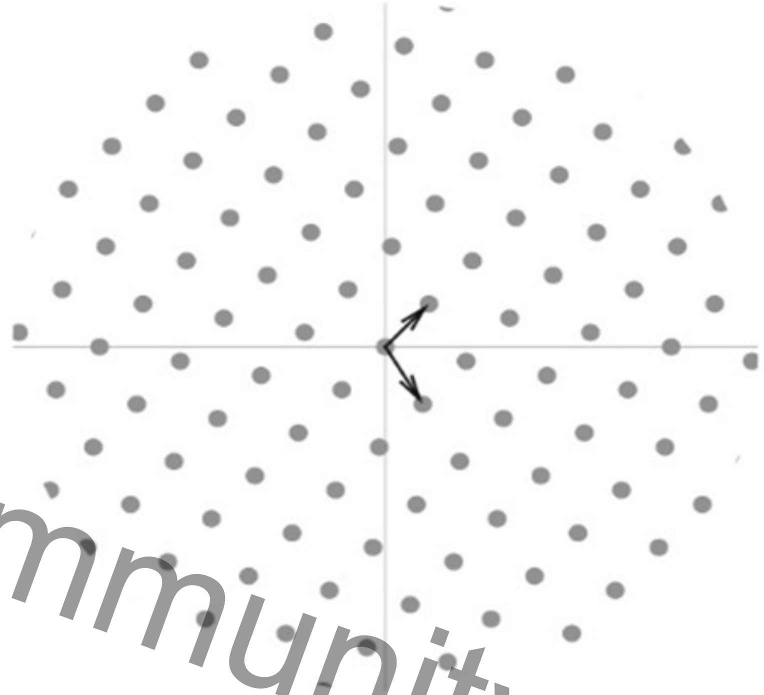
NIST requests comments on three draft Federal Information Processing Standards (FIPS):

- FIPS 203, *Module-Lattice-Based Key-Encapsulation Mechanism Standard*
- FIPS 204, *Module-Lattice-Based Digital Signature Standard*
- FIPS 205, *Stateless Hash-Based Digital Signature Standard*

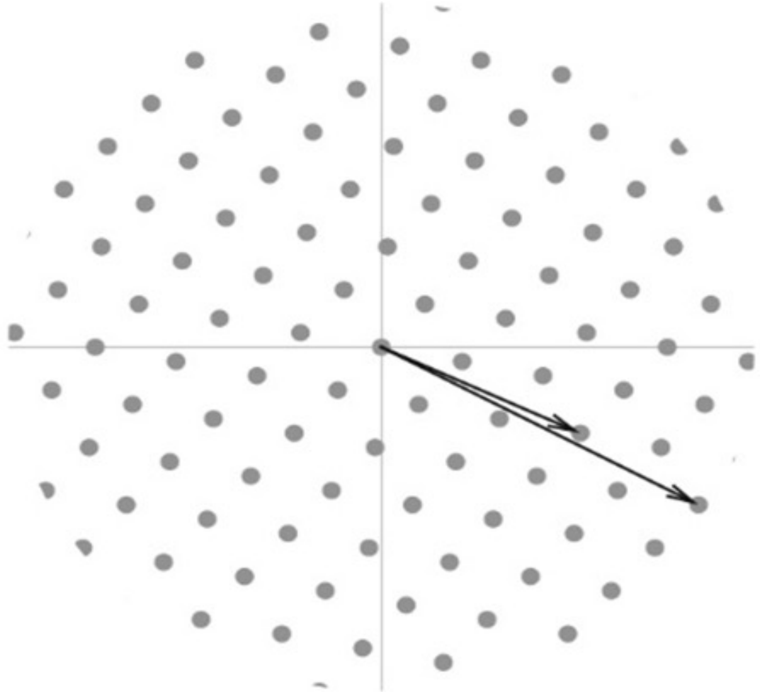
A LATTICE PROBLEM

Given a basis and some non-lattice point in its space find a nearby lattice point.

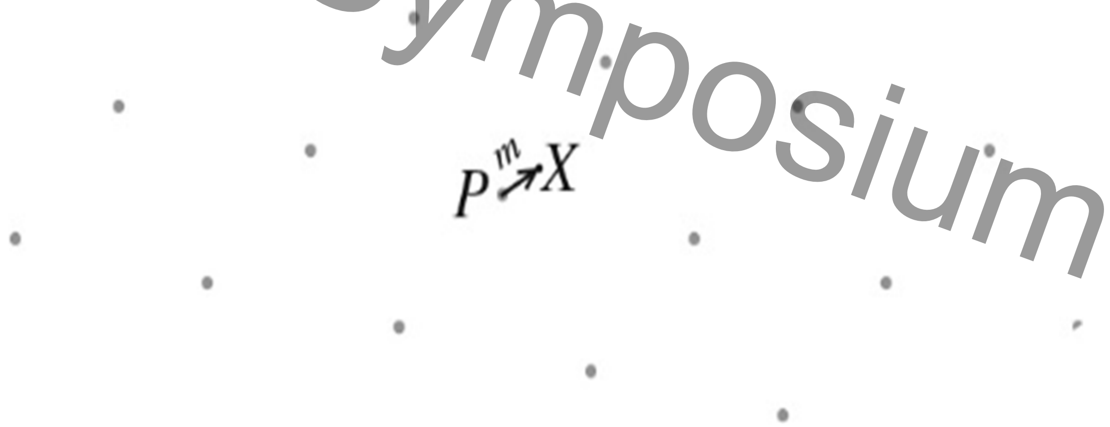
1. Alice uses Bob's public key to select a lattice point $\boldsymbol{P}$ and computes $\boldsymbol{X} = \boldsymbol{P} + \boldsymbol{m}$, where $\boldsymbol{m}$ is a "small" n −dimensional vector.
2. Alice sends Bob: $\boldsymbol{X} = \boldsymbol{P} + \boldsymbol{m}$
3. Bob uses his private key to find the nearest lattice point to $\boldsymbol{X}$ that is $\boldsymbol{P}$ and computes $\boldsymbol{X} - \boldsymbol{P} = \boldsymbol{m}$.



Bob's Private key: good basis



Bob's Public key: bad basis



Message m encoded as offset from Lattice point P

*Network Security, C. Kaufman, R Perlman, M Speciner, R. Perlner, 2023

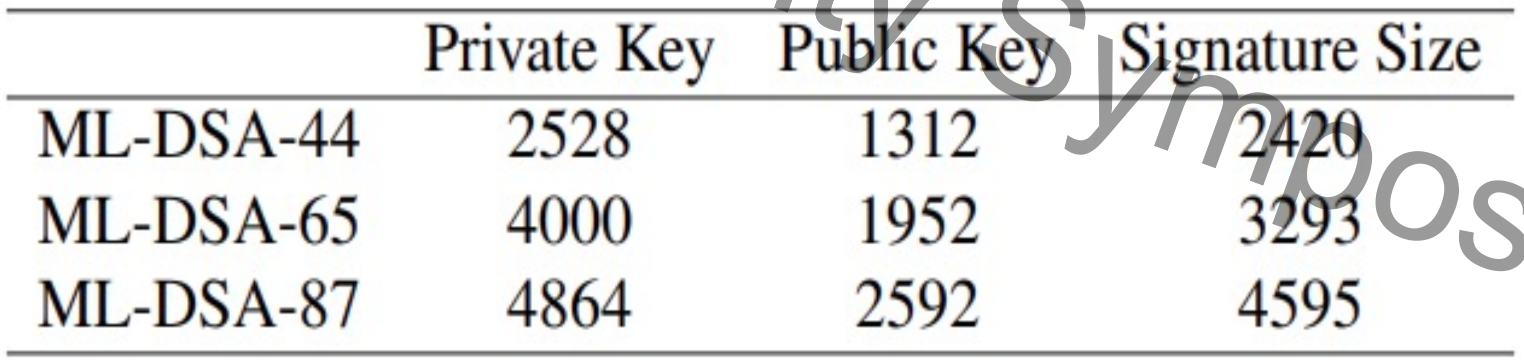
FIPS 203, ML-BASED KEM, LATTICE PROBLEMS, CTD

- *A lattice* $L \subset R_n$ is a set of integer linear combinations of n linearly independent vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$: $L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n) = \sum_{z_i \in Z} z_i \boldsymbol{b}_i = \mathbf{Bz}$, $\mathbf{z} \in Z^n$, with $\mathbf{B} \in R^{n \times n}$ a matrix with the *basis vectors* as columns.
- *L* is *cyclic* if $\forall\, a \in L$: $rot(a) \in L$, where $rot(x)$ is a rotational shift of a. Cyclic lattices correspond to ideals I in the polynomial ring $Z[x]/(x^n - 1)$. Then
  - $L_{\mathrm{I}} = \left\{ \left((a_0, \ldots, a_{n-1}) \mid \sum_{i=0,n-1} a_i\, x^i \in I \right) \right\} \subset Z^n$.
- *Learning with Errors (LWE) problem*: find a (*secret*) vector $\boldsymbol{s}$ given matrix $\boldsymbol{A}$ and vector $\boldsymbol{b} = \boldsymbol{As} + \boldsymbol{e}$ (infering $\boldsymbol{A}$ from noisy samples $\mathbf{Az}$, using basis "$\mathbf{A}$").
- Lattices are *standard* if they are based on LWE; they are *ideal* if $\boldsymbol{A}$ is cyclic.
- Modular lattices (ML) exploit a tradeoff between the efficiency of ideal lattices and the security of standard lattices.

FIPS 204, ML-BASED DSA STANDARD

High-Level Overview

- Security is based on the hardness of finding short vectors in lattices (the hardness of Module-LWE and Module-SIS (Short Integer Solution for lattices)
- A Schnorr-like lattice-based signature scheme
- All operations over $R = Z_q/(X^{256} + 1)$ for $q = 2^{23} - 2^{13} + 1 \ (= 8{,}380{,}417)$
- Three versions.



	Private Key	Public Key	Signature Size
ML-DSA-44	2528	1312	2420
ML-DSA-65	4000	1952	3293
ML-DSA-87	4864	2592	4595

Sizes in bytes

FIPS 204, ML-BASED DSA STANDARD, CTD

Schnorr signature

An interactive proof between a Prover P who knows g, the generator of a group and a value x, and a Verifier V who knows g and $y = g^x$. P demonstrates knowledge of x to V in three steps.

- *Commitment*: P generates a random positive integer r and commits to it by sending g^r to the V.
- *Challenge*: V sends a random positive integer c to P.
- *Response*: P returns $s = r - cx$, and V checks whether $g^s \cdot y^c = g^r$.

To make this non-interactive c is derived from the hash of the commitment.

FIPS 204, ML-DSA STANDARD, BASIC IDEA

Build a signature scheme from an analogous interactive protocol, where a prover P who knows matrices $\boldsymbol{A} \in Z_q^{K\times L}$, $\boldsymbol{S}_\mathbf{1} \in Z_q^{L\times n}$and $\boldsymbol{S}_\mathbf{2} = Z_2^{K\times n}$ with *short coefficients*, demonstrates knowledge of $\boldsymbol{S}_\mathbf{1}, \boldsymbol{S}_\mathbf{2}$ to a Verifer V who knows $\mathbf{A}$ and $\boldsymbol{T} \in Z_q^{K\times n}$, with $\boldsymbol{T} = \mathbf{A}\boldsymbol{S}_1 + \boldsymbol{S}_2$. Such an interactive protocol would proceed as follows:

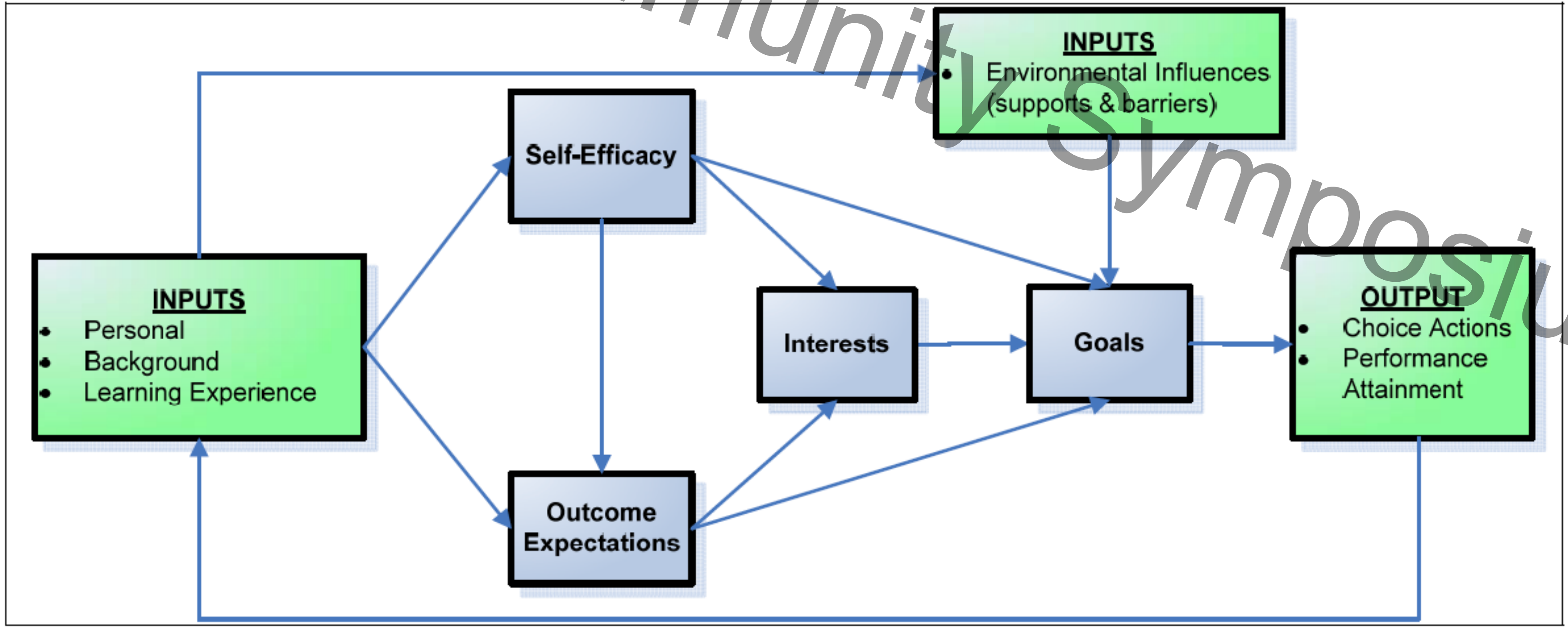
- *Commitment*: P generates $\mathbf{y} \in Z_q^L$ with short coefficients and commits to it by sending $\mathbf{Ay}$ to V.
- *Challenge*: V sends a vector $\mathbf{c} \in Z_q^L$ with short coefficients to P
- *Response*: P returns $\mathbf{z} = \mathbf{y} + \boldsymbol{S}_1\mathbf{c}$, and V checks whether $\mathbf{Az} - \mathbf{Tc} \approx \mathbf{Ay}$.

The public key is $(\mathbf{A}, \mathbf{T})$ and the private key is $(\boldsymbol{S}_1, \boldsymbol{S}_2)$.

ML-DSA uses several transformations to reduce the size the key size and signature size.

THE FRAMEWORK AND CURRICULUM ACTIVITIES

- The framework is based on the SCCT theory
  - The Social Cognitive Career Theory
  - The students need to take one quantum computer course
  - In addition, they need to be involved in solving problems using quantum computing through individualized research programs



SUMMARY

- We plan to make our curricular materials available to every CAE Institute that would be interested in having their program
- As NSF is pushing to have programs that incorporate quantum computing, having such a program could enhance proposals potentially