Cybersecurity Considerations for The Quantum Information Science Technology (QIST) Workforce
April 20, 2022
NICE Webinar: Cybersecurity Considerations and the QIST Workforce

April 20, 2022

Dr. Corey Stambaugh
Senior Policy Advisor
National Quantum Coordination Office
Office of Science and Technology Policy

Whitehouse.gov/ostp
www.quantum.gov
@WHOSTP
The New SI and the Redefined Kilogram

The kilogram was based on the mass on artifact. Now the kilogram is realized through measurements traceable to the Planck Constant.

Chip contains about 300,000 superconducting Josephson junctions.

A distinguishing feature of superconducting quantum circuits is the usage of a Josephson junction.
Quantum mechanics enables new technology

- **Quantum 1.0: Quantum Theory**
  - Enabled by understanding of how to control quantum particles (electrons, photons, atoms)
  - Lead to semiconductor devices, lasers, atomic clocks, NMR imaging

- **Quantum 2.0: Quantum Information Science**
  - Enabled by quantum *superposition*, *measurement*, *entanglement*
  - Leads to Quantum Computers, Sensors, Networks

- **Quantum Mechanics** is one of the most accurate and predictive theories ever devised
Quantum computers represent a foundational shift in information technology

- Quantum algorithms take advantage of a quantum computer’s massive parallelism, interference, and internal structure of the problem to find the right answer.
- Only certain types of problems (e.g., where you can check the answer fast) seem amenable to quantum speedup.
  - Shor’s quantum factoring algorithm breaks public-key cryptography
- For most problems, quantum computers offer no speedup.
Quantum computers represent a foundational shift in information technology

- Quantum algorithms take advantage of a quantum computer’s massive parallelism, interference, and internal structure of the problem to find the right answer.
- Only certain types of problems (e.g., where you can check the answer fast) seem amenable to quantum speedup.
  - Shor’s quantum factoring algorithm breaks public-key cryptography
- For most problems, quantum computers offer no speedup.

Exponentially better is fundamentally disruptive

![Diagram showing the comparison between classical and quantum algorithms for factoring large numbers.](image-url)
The National Quantum Initiative - a National Priority

• **Getting the science right** by understanding the applications and timelines by which quantum information science and technology will benefit our society, and roadblocks we must overcome to get there;

• **Enhancing American competitiveness** by accelerating technology development toward useful economic and mission applications while also protecting our national security; and

• **Enabling our people** by building the necessary talent pipeline and ensuring that this field creates new opportunities for all Americans.

**Authorized:**
DOE – Establish centers and carry out R&D  
NSF – Establish institutes and support basic R&D  
NIST – Establish consortium and carry out R&D  
But many more agencies participate, and the NDAA supports additional efforts.

**Coordination and Support Bodies:**
• Subcommittee on QIS (SCQIS) *;  
• Subcommittee on Economic and Security Implications of Quantum Science (ESIX) **;  
• National Quantum Coordination Office (NQCO) *

* from National Quantum Initiative Act (PL 115–368)  
Building the U.S. Quantum Ecosystem

**Infrastructure**
- 5 DOE National QIS Research Centers
- 5 NSF Quantum Leap Challenge Institutes (+2 FY21)
- 3 DOD/IC QIS Centers (+1 FY21)

**Workforce**
- Key concepts for QIS learners
- Q-12 Education Partnership [http://Q12education.org/](http://Q12education.org/)
- Quantum profile videos
- Quantum Engineering Workshop
- Government Talent Workshop
- Workforce Strategy

**Industry**
- Quantum Economic Development Consortium (QED-C)
  NIST facilitated consortium continues to grow, supporting QIST industry and supply chain (now >170 organizations)
- Oct 2021 WH Summit on Quantum Industry and Society

**Security and International Cooperation**
- ESIX Report on Intl Talent
- Quantum Cooperation Statements (+2 FY22)
- QED-C engaging with international companies
The bill establishes a 10-year program to advance QIST and workforce development. To expand the number of researchers, educators, and students with training in QIST to develop a workforce pipeline; and (B) promote the development and inclusion of multidisciplinary curriculum and research opportunities for QIS at the undergraduate, graduate, and postdoctoral level;

SEC. 103. SUBCOMMITTEE ON QIS: (1) coordinate education activities and programs of the Federal agencies; and (2) establish goals and priorities of the Program, based workforce gaps ...;

Title III: NSF: using NSF programs, in collaboration with other Agencies... to (A) improve the teaching and learning of QISE at the undergraduate, graduate, and postgraduate levels; and (B) increase participation in QIST fields, including by individuals identified in S&E Equal Opportunities Act
The Challenges

Strong demand for quantum workforce

Breadth of Needed Skills

Limited exposure to QIST

0.5% of HS students in 2016 took AP 2 exam (i.e. quantum)

Report - S&E Indicators 2018 | NSF - National Science Foundation

Attracting and retaining talent

Developing a diverse QIST workforce

Why are efforts to boost the small number of Black U.S. physicists failing? | Science | AAAS
From workforce policy to coherent actions

- **Action 1:** Develop and maintain an understanding of 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
- **Action 4:** Make Careers in QIST and Related Fields More Accessible and Equitable

A broad, agile, and sustainable workforce that possesses the range of skills needed by industry, academia, and the U.S. Government, while being able to scale and adapt as the QISE landscape evolves.
Action 1: Develop and maintain an understanding of workforce needs in the QIST ecosystem, with both short-term and long-term perspectives.

- **Wide range of degree levels, and job roles**
- **Increasing number of learning opportunities from undergraduate classes and minors, to master degrees**
**Action 2:** Introduce broader audiences to QIST through public outreach and educational materials by:

Creating sustainable broadly available outreach, engagement and early educational opportunities that make QISE accessible.

**Action 3:** Address QIST-Specific Gaps in Professional Education and Training Opportunities:

Programs should include numerous and diverse educational on-ramps to meet the varied depth and disciplinary needs of QISE careers.

**Action 4:** Make Careers in QIST and Related Fields More Accessible and Equitable

U.S. needs a strong and growing workforce
Celebrating: QIS Concepts to Q-12 Education to K-12 Framework to QuanTime to Quantum Profiles

http://q12education.org/

QIS Key Concepts for Early Learners: K-12 Framework

Q-12 Education Partnership

Teach and Student Engagement

- Teacher Workshops
- Career Videos
- Quantum Crossing
- QuanTime

New NSF Programs

- Q2Work, 2 teacher conferences on quantum (Summer 2020)
- Convergence Accelerators for QIS Education
- QIS outreach embedded in centers and programs
- High School Students Learning QIS

• Announced August 2020
• 13 initial members: industry, professional societies, and academia
• Commits to expanding access to K-12 quantum learning tools
• Will work with the community to nurture a diverse and innovative quantum workforce

NSF Key Concepts Workshop

NQCO SCQIS Workforce Working Group

quantum.gov/world-quantum-day
Questions or Feedback?

SCQIS
Co-Chairs:
J. Stephen Binkley, DOE
Sean Jones, NSF
James Kushmerick, NIST
Charles Tahan, OSTP
Executive Secretary:
Denise Caldwell, NSF

ESIX
Co-Chairs:
J. Stephen Binkley, DOE
Barry Barker, NSA
John Burke, DOD
Charles Tahan, OSTP
Executive Secretary:
Brad Blakestad, NSA

National Quantum Coordination Office (OSTP)
Charles Tahan – Director of NQCO and AD for QIS at OSTP
Alex Cronin – Deputy Director for NQCO
Corey Stambaugh – Senior Policy Advisor
Tanner Crowder – Policy Analyst
Thomas Wong – Quantum Liaison
Q & A
Cornerstone of Cybersecurity in Quantum Era – Post-Quantum Cryptography

Lily Chen
Computer Security Division, Information Technology Lab
National Institute of Standards and Technology (NIST)
Cryptography – The Cornerstone of Cybersecurity

• Protect information transmitted over the links and stored in the devices
• Prevent from malware and malicious software attacks

- Public-key cryptography has been used to establish a secure and protected link
- Symmetric-key algorithms are used to protect data
NIST Cryptographic Standards – A Glance

• NIST developed the first encryption standards in 1970s
  • Data Encryption Standard (DES), published 1977 as Federal Information Processing Standard (FIPS) 46

• Over 40 years, NIST continues to evolve its cryptographic standards
  • Enable to respond the growing application demand
  • Enhance security strength to against more sophisticated attacks

Nearly all commercial laptops, cellphones, Internet routes, VPN servers, and ATMs use NIST Cryptography
Quantum Impact to Cybersecurity

• The security of public-key cryptography is based on hard problem assumptions, e.g., integer factorization for RSA
• Quantum computing changed what we have believed about the hardness
  • By Shor’s algorithm, factorization problem can be solved by quantum computers in polynomial time
• Quantum computing also impacted security strength of symmetric key based cryptography algorithms – manageable by increasing key size
How to Deal with Quantum Attacks?

• Need to find cryptographic algorithms which are secure against attacks by both classical and quantum computers
  • The algorithms must be based on hard problems which are hard for both classical and quantum computers
• In other words, we need quantum resistant cryptography, named by the researchers as post-quantum cryptography (PQC)

• Clarification
  • Post-quantum cryptographic algorithms are supposed to be implemented in “classical” computers in the same way as RSA, DH, and ECDSA
  • It is different from Quantum Key Distribution (QKD), which relies on quantum mechanics to distribute keys
NIST PQC Standards - Scope

- Cryptography standards
  - Public key based
    - Signature (FIPS 186)
    - Key establishment (800-56A/B/C)
  - Symmetric key based
    - AES (FIPS 197) TDEA (800-67)
    - Modes of operations (800-38A-38G)
    - SHA-1/2 (FIPS 180) and SHA-3 (FIPS 202)
    - Randomized hash (800-106)
    - HMAC (FIPS 198)
    - SHA3 derived functions (parallel hashing, KMAC, etc. (800-185)
  - Tools
    - RNG (800-90A/B/C)
    - KDF (800-108, 800-135)
  - Guidelines
    - Hash usage/security (800-107)
    - Transition (800-131A)
    - Key generation (800-133)
    - Key management (800-57)
NIST PQC Standards – Milestones and Timeline

2016 Criteria and requirements and call for proposals

2017 Received 82 submissions and announced 69 1st round candidates

2018 The 1st NIST PQC standardization Conference

2019 Announced 26 2nd round candidates

2020 Announced 3rd round 7 finalists and 8 alternate candidate

2021 The 3rd NIST PQC Standardization Conference

2022-2023 Release draft standards and call for public comments

2024 Publish PQC Standards
Cybersecurity in Quantum Era

- Quantum computers, once in a full scale, will crash cryptographic schemes used today, reveal yesterday’s secret, and attack tomorrow’s transaction
  - PQC is the cornerstone of cybersecurity in quantum time

- PQC standardization and migration are in a pipeline
  - Standardization: NIST PQC standardization process [www.nist.gov/pqcrypto](http://www.nist.gov/pqcrypto)
  - Migration and adoption: The National Cybersecurity Center of Excellence (NCCoE) has a project for [Migration to PQC](http://Migration to PQC) to support a head start on executing migration roadmap in collaboration with industry partners

If $y + x > z$, then we should worry.
- Michele Mosca

$y$ – time for PQC standardization and adoption
$x$ – time of maintaining data security
$z$ – time for quantum computers to be developed
Thanks

• Check out www.nist.gov/pqcrypto
• Sign up for the pqc-forum for announcements & discussion
• Contact us at: pqc-comments@nist.gov
Q & A
Complete Survey

https://www.surveymonkey.com/r/aprilnicewebinar
Thank You for Joining Us!

Upcoming Webinar:
“Showing Our Appreciation of Military Veterans and Spouses By Supporting Cybersecurity Career Opportunities”

When:
May 18, 2022, at 2:00-3:00PM ET

Register:
https://go.usa.gov/xuZ7k

nist.gov/nice/webinars