SUMMARY OF THE WORKSHOP ON CYBERSECURITY OF QUANTUM COMPUTING

Product of

The National Quantum Coordination Office

November 2022

About the National Quantum Coordination Office

The National Quantum Coordination Office (NQCO) coordinates quantum information science (QIS) activities across the U.S. federal government, industry, and academia. Legislated by the National Quantum Initiative (NQI) Act of 2018 and established within the White House Office of Science and Technology Policy, the NQCO oversees interagency coordination of the NQI Program and QIS activities; serves as the point of contact on Federal civilian QIS activities; ensures coordination among the consortia and various quantum centers; conducts public outreach, including the dissemination of findings and recommendations of the National Science and Technology Council (NSTC) Subcommittee on QIS, the NSTC Subcommittee on Economic and Security Implications of Quantum Science, and the NQI Advisory Committee; and promotes access to and early application of the technologies, innovations, and expertise derived from U.S. QIS activities, as well as access to quantum systems developed by industry, universities, and Federal laboratories to the general user community. More information is available at quantum.gov.

Director

Charles Tahan, OSTP

Staff

Gretchen Campbell, OSTP
Tanner Crowder, OSTP
Corey Stambaugh, OSTP
Thomas Wong, OSTP

Acknowledgements

This report was compiled by the NQCO. The NQCO thanks the Pittsburgh Quantum Institute and University of Pittsburg for hosting and leading the organization of the workshop, and the National Science Foundation (NSF) for co-organizing the workshop.

Executive Summary

The Pittsburgh Quantum Institute hosted a Workshop on Cybersecurity of Quantum Computing on behalf of the National Science Foundation (NSF) and the White House Office of Science and Technology Policy (OSTP) National Quantum Coordination Office (NQCO). The workshop, which took place on September 29 and 30, 2022, brought together roughly 40 experts from the cybersecurity and quantum computing communities to explore how quantum computing intellectual property (IP) can be protected, mechanisms to ensure that quantum computers are not used for illicit purposes, and opportunities for research on the cybersecurity of quantum computers.

Two panels provided a forum for discussions between the classical security and quantum computing communities. The first panel identified crucial IP in quantum computing systems. The panelists determined that the design and process for making quantum processors were key, while supporting technologies like cryogenic refrigerators can be outsourced. In addition, depending on the context, panelists identified quantum algorithms and/or their results as potential IP. They proposed that the biggest threats to quantum computing IP were traditional vectors like hacking to steal data and people leaving with expertise.

The second panel explored how to prevent quantum computers from executing unwanted algorithms, and the panelists identified several technical challenges to detecting quantum algorithms or restricting specific applications. The challenges include the ability to hide a quantum computation, the common techniques underpinning quantum algorithms, and the tendency for useful quantum devices to be capable of all quantum applications.

Participants noted that in cybersecurity, the best practice is to design systems with security in mind, rather than waiting until systems are developed to incorporate security considerations. They expressed the view that research programs that address the cybersecurity of quantum computing should be launched while quantum computers are still nascent. Breakout teams composed of both security and quantum computing experts identified research opportunities including, but not limited to:

1. Securing large-scale control and monitoring systems
2. Distributed high-performance quantum computing
3. Attack vectors on different types of quantum computers
4. Formal methods for safe and secure quantum computing systems
5. A multi-layered instrumentation framework for enforcing or verifying security-relevant properties of quantum computers
6. Ensuring that quantum algorithms do not enable undesired capabilities or behaviors

Participants lauded the opportunity to engage early in discussions about quantum computer security, and they agreed that there are interesting and important research problems in this new field.

1. Overview

From September 29-30, 2022, the Pittsburgh Quantum Institute hosted the Workshop on Cybersecurity of Quantum Computing[1] on behalf of the National Science Foundation (NSF) and the White House Office of Science and Technology Policy (OSTP) National Quantum Coordination Office (NQCO). The workshop brought together security experts and quantum computing experts from academia, industry, and government to explore how intellectual property (IP) in the nascent quantum computing industry can be protected, as well as mechanisms to ensure quantum computers are not used for illicit purposes.

Roughly 40 participants engaged in the virtual workshop, who were welcomed by lead organizer Dr. Robert Cunningham, Vice Chancellor for Research Infrastructure at the University of Pittsburg and the Deputy Director of the Pittsburgh Quantum Institute. Co-organizer Jeremy Epstein, Lead Program Officer for Secure and Trustworthy Cyberspace at NSF, introduced Dr. Margaret Martonosi, NSF's Assistant Director for Computer and Information Science and Engineering, to give opening remarks. Dr. Martonosi noted the uniqueness of the workshop in bringing together the security and quantum computing communities to discuss a new field of study. Dr. Charles Tahan, OSTP's Assistant Director for Quantum Information Science (QIS) and the Director of the NQCO, provided additional opening remarks. He describing the President's National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems,[2] which charged agencies with safeguarding QIS IP. Dr. Tahan noted the need to balance the promotion and protection elements in order to ensure that American innovation in quantum computing continues to accelerate, while acknowledging the dual-use nature of quantum computers, ultimately raising the question of whether we can ensure that quantum computers are not used for illicit means.

As described in Section 2, two panels of security experts and quantum computing experts initiated discussions on the following topics:

Panel 1: IP of Quantum Computing Systems

Panel 2: Recognizing Quantum Algorithms

As described in Section 3, three breakout sections spanning both days and composed of security experts and quantum computing experts identified potential areas of research on the security of quantum computers, centered on the following three topics:

Breakout 1: Hardware-Based Attacks and Defenses

Breakout 2: Software-Based Attacks and Defenses

Breakout 3: Recognizing Quantum Algorithms

2. Panel Discussions

Panel 1: IP of Quantum Computing Systems

The first panel focused on identifying critical IP in quantum computing systems. In a quantum

[1] https://www.pqi.org/events/workshop-cybersecurity-quantum-computing

[2] https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

computing system, the quantum processor can be quite small, with many technologies supporting it, such as cryogenic systems, lasers, electronics, and classical computers. Panelists expressed that the design and process for making the quantum processor was critical IP. For example, with superconducting quantum processors, this could include the materials science, surface chemistry, layout, and packaging of the quantum processor. The supporting technologies are still important, but perhaps less proprietary. For example, a panelist conveyed that they are currently outsourcing cryogenic refrigerators, and another panelist expressed the desire to purchase supporting optical devices rather than develop them in-house, but commercial options are not available. Panelists noted that the line between critical and important technologies may be different for companies that focus on hardware rather than software, with the quantum software being external and important, but not as critical to their business.

Panelists also noted that depending on the application, the algorithms or the solutions they produce could be the important IP. For example, for quantum machine learning, the algorithms to find solutions may be critical IP, but the solution to any one particular problem may be idiosyncratic. But with drug discovery, the output is important because the drug is the product. If a user is submitting algorithms to a quantum computer, there needs to be trust between the user and the quantum computing company that IP, whether it be the algorithms or solutions, are protected. As the field evolves, participants raised the idea that the standards for data protection for quantum computers will probably be similar to current high-performance computing (i.e., supercomputing) environments.

The discussion also branched into potential attacks, with panelists stating that the majority of the attacks are classical. For example, a panelist described a classical denial-of-service attack on an older quantum computing system, where someone inadvertently submitted “a million jobs,” which crashed the classical job-handling software and brought the entire system down. Panelists proposed that the biggest risks to quantum computers are similar to conventional ones, like hacking into computer systems to steal the critical IP, or leaving with knowledge of critical IP.

Panelists described protection measures already in place to prevent accidental damage to devices in the laboratory. One example given was restricting the power of pulses sent to a quantum processor, which can serve as a layer of protection for students who may be less familiar with the machines, but also for experienced user, where a typo could otherwise destroy a device. Panelists noted that users at higher levels of abstraction inherit these protections.

Protections for critical IP installed at uncontrolled facilities was also discussed. For example, one panelist’s company, which has deployed quantum computing systems in foreign nations, protects its IP by having its own employees perform the installation and maintenance, preventing unauthorized direct access to the hardware. The company also only sold to countries with a strong rule of law, so it is unlikely that a quantum computing system will be taken by force.

Panel 2: Recognizing Quantum Algorithms

The second panel focused on recognizing quantum algorithms and discussed the possibility of preventing malicious or unwanted algorithms from being run on a quantum computer. Panelists noted that what is considered malicious could be a matter of debate. An example given was Shor’s quantum algorithm for factoring, which can permit an attacker to read private information that was encrypted with the most common forms of public-key cryptography, but which could have benign use by research mathematicians studying number theory.

The notion of restricting algorithms or applications is a preexisting notion that is not unique to quantum computing. For example, panelists pointed out that restrictions are already employed in classical computing by service providers, such as those on smartphone applications, as well as restrictions on mining digital currencies on cloud computers.

Panelists gave three reasons why recognizing quantum algorithms may be technically challenging:

First, it may not be technically possible to implement such restrictions on quantum computers due to homomorphic encryption, which permits a user to efficiently hide a quantum computation. For some time, however, quantum computers will be resource limited, and the additional overhead needed to obfuscate an algorithm may make homomorphic encryption prohibitive. Despite this, panelists cautioned that methods with less overhead could be developed to evade detection schemes.

Second, common techniques are shared across different applications of quantum computation. A panelist gave the example of a technique called phase estimation, which underpins both Shor's algorithm and algorithms for quantum chemistry.

Third, the line between a special-purpose and a general-purpose quantum device is not very clear, and offering a device that is useful but not a full-fledged "universal" quantum computer may be a challenge. As a panelist explained, a quantum device restricted to solving chemistry problems can implement any other quantum algorithm, including Shor's algorithm, by encoding it as a chemistry problem. Panelists noted that the overhead needed for such encodings will make them prohibitive in the near term.

3. Breakouts

Breakout 1: Hardware-Based Attacks and Defenses

The first breakout focused on the vulnerability of quantum computers to hardware-based attacks and identified potential IP that a service provider or user may want to protect.

Participants noted that for the provider of the quantum computing system, IP may include the physical layout of the quantum device, its surface chemistry, the material stack, input/output configuration, cooling methods, controller architecture, error correction and mitigation methods, optimized pulse sequences, firmware architecture, orchestration, and workflow management. For the user, potential IP includes quantum circuits and results, runtime methods, and error mitigation and correction methods.

Potential hardware vulnerabilities include reset operations, crosstalk between qubits, having multiple tenants on a processor, manipulating the mapping process with regards to error rates, and reliance on untrusted hardware.

Despite these vulnerabilities, participants said that intentional attacks on current quantum processors are rare compared to accidents. An example of such an accident was provided in Breakout 2: electricians accidentally shut down the wrong electric panel, shutting down twelve quantum systems. This mistake required three days to correct.

The team also considered the risks due to attacks at various layers of the hardware stack. As one moves from the cloud computation at the top of the stack, to the quantum processor at the bottom, an adversary's ability to learn the IP of the quantum device goes from low to high.

Breakout 2: Software-Based Attacks and Defenses

The second breakout focused on vulnerabilities of quantum computers to software-based attacks.

Participants noted that by crafting the pulses or circuits sent to a quantum processor, it may be possible to learn some properties of the hardware. One example given was in the case of a superconducting quantum processor, it is theoretically possible to use pulse-level control to characterize the relationship between the processor's inputs and outputs, i.e., its "scattering matrix," from which an expert might infer some sensitive details about the hardware. Vendors can defend against this by restricting the frequencies of pulses or eliminating pulse-level control altogether.

The team discussed classical software attacks to render a quantum computer damaged or useless, with one example being the error connecting code. It is a classical algorithm, and it could be hacked so that it is not fault tolerant anymore.

Participants described unexpected attack vectors that can also arise despite protecting individual components. One example was that the translation from a quantum circuit element to a control stimulus should make it so that one cannot exceed power constraints, but an adversary might use repeated pulses, each within constraints, to asymmetrically heat a quantum processor, causing errors.

The team also considered risks due to multiple clients using the same quantum processor (i.e., multi-tenancy). They described a situation where one user using qubits in one part of a quantum processor could use spectroscopy-style quantum circuits to learn about another user's workload on other qubits in the same processor. They also examined multi-tenancy where one user employs a quantum processor for some amount of time, followed by a second user employing the quantum processor for another length of time. It might be possible for the first user to affect the results of the second user, such as by overheating the processor, or it might be possible for the second user to learn something about the first user's computation. One protection already in place at a company is performing a "hard reset" of the quantum computer between users to erase unwanted entropy from the processor.

The breakout team considered possible topics of research with the potential to address some of these challenges:

- **Secure Large-Scale Control Systems**. The scale of the classical computation involved in supporting a large-scale quantum computer can be extensive. This support includes control systems and error correction, but it can also include monitoring for intrusions. This research program explores scaling and securing classical control systems for quantum computers.
- **Distributed high-performance quantum computing**. Classical high-performance computing systems are typically multi-tenant and distributed. Addressing the security of multi-tenant and distributed quantum computers now can lay the foundation for more secure quantum computers when they achieve scale.
- **Attack vectors on different types of quantum computers**. This workshop provided only a cursory discussion on potential attacks on quantum computers. Deeper research into potential attack vectors for various quantum system models, such as whether adversaries only access quantum devices through a user interface, is needed to more fully understand how to secure quantum computers.
- **Formal methods for safe and secure quantum computing systems**. In computing, "formal methods" refer to rigorous mathematical techniques for specifying, developing, and verifying computer software and hardware. This research program involves developing formal methods

for quantum computing in order to achieve trustworthy quantum computing.

Breakout 3: Recognizing Quantum Algorithms

The third breakout team focused on whether it is possible to detect or restrict the use of specific quantum algorithms, whose output could enable unwanted capabilities.

The discussion reiterated a point from the second panel discussion, that it may be impossible to restrict certain quantum algorithms generally if we want to be able to solve some of the most pressing scientific questions that researchers want to address, with the example that algorithms for solving certain chemistry problems on a quantum computer can closely resemble Shor's algorithm, and vice versa.

Despite this, the breakout team explored some potential approaches to preventing quantum computers from being used for nefarious purposes. One is to only make modules available that are well-understood, and to only make new modules available as they are understood better. Another identified option would be having different categories of user access, where users only have access to the building blocks of certain algorithms depending on their level of trust. A third solution would be for users to disclose the purpose of their algorithm and provide sufficient information for the service provider to approve the use. This has privacy challenges, however, and requires that the user trust the service provider with their algorithm, which could itself be IP. The level of detail required for a service provider to verify user behavior and intent is an open question.

The breakout team raised two research areas with the potential to address some of these challenges:

- Developing **a multi-layered instrumentation framework** that allows security-relevant properties of quantum computers to be enforced or verified.
- Developing **the necessary tools for service providers to verify quantum algorithms** could not enable certain tasks, such as solve a particular problem, and that a quantum computer will not perform undesirable behavior, such as leak IP.

The breakout team raised the concern that restricting access to devices could slow US innovation and cause other nations to take leadership in the development of quantum computers and applications.

4. Conclusion

The Workshop on Cybersecurity of Quantum Computing brought together cybersecurity experts and quantum computing researchers for two days to begin exploring how quantum computers can be secured and whether it is possible to ensure that quantum computers will not be used for nefarious means. Many potential research programs were identified by the participants that address the scientific questions underlying these topics.

Some participants commented on the foresight of the workshop to involve security researchers while quantum computers are still nascent, lamenting that security was considered too late for other technologies. With this warning in mind, they expressed that launching research programs around the cybersecurity of quantum computing should be a priority.