White Paper: Quantum Safe Framework

An Intra and Inter-agency Guide to Being Quantum Ready

ATARC Quantum Working Group

July 2021

Advanced Technology Academic Research Center
designed by government • led by government • attended by government

Table of Contents

Disclaimer: This white paper was prepared by the ATARC Quantum Working Group members in their personal capacity. The opinions expressed do not reflect any specific individual nor any organization or agency they are affiliated. This white paper is intended to be a helpful guidance relating to currently quantum technological capabilities.

Quantum Technology: History, Overview, Potential and Risks

The foundations of “Quantum Physics” started to evolve more than two centuries ago as the findings in the sciences of chemistry and classical physics converged. Although the term “Quantum Mechanics” was coined in the 1925 paper, “The Matrix Formulation of Quantum Mechanics”, authored by Werner Heisenberg, Pascual Jordan, and Max Born; it is actually the culmination of contributions from the great minds of scientists Niels Bohr, Max Planck, Albert Einstein, and Marie Curie (among others).

Despite its occasional misuse in popular culture and science fiction, the term “quantum” simply refers to laws and principles of physics at the atomic or sub-atomic level.

In 1994, a Bell (AT&T) Labs Mathematician, Peter Shor, wrote the groundbreaking paper, "Algorithms for quantum computation: discrete logarithms and factoring", that described a method for turning these properties into useful computing systems that may ultimately outperform conventional microprocessor (semiconductor based) technology by a significant factor.

For example, whereas classical gate based (semiconductor) computers are limited to binary states (1 or 0), quantum circuits in theory can maintain multiple states simultaneously (although at this time they are highly unstable and cannot maintain these states, their “coherence”, for indefinite periods of time). Furthermore, the operational speed of classical computers is limited by physical constraints of power density, heat dissipation, and other reactive forces of nature. However, quantum computing may also in theory overcome these limitations via such properties as superconductivity (zero resistance), and photonic entanglement (interactions between photons which have no mass).

Goals and Objectives

Current projections estimate the number of qubits required for gate-model systems to surpass conventional systems to be in the millions, although progress in developing hybrid quantum/classical systems might shorten these estimates considerably. For gate model quantum computers there currently is no quantum-based system that operates beyond the triple-digit qubit range. For annealing models (a type of adiabatic quantum computation), there are quadruple-digit (5000+ qubit) systems, but it is currently unknown whether (larger versions of) these systems could be used to break encryption.

The foundation of the security systems used by today’s IT infrastructure is based on encryption. Specifically, the ability to mathematically encode and decode data and communication protocols using large prime numbers as *keys*. Presently, the length of these *keys* makes it highly improbable for any unwanted actor to decode in a useful amount of time.

However, in an October 2020 interview with Nature Magazine, now a Massachusetts Institute of Technology (MIT) Professor Shor was asked if there was a risk that we will be caught unprepared (for the implications of quantum computing). His answer was:

> “*Yes. There was an enormous amount of effort put into fixing the Year 2000 bug. You’ll need an enormous amount of effort to switch to post-quantum. If we wait around too long, it will be too late…*”

With that sense of urgency in mind, the goals of this framework are to develop and guide in the implementation of a plan and structure to protect critical government IT systems (infrastructure and data) from the potential threat of the misuse of quantum computing technology and to provide guidance to government personnel in this endeavor. To reach this goal **a community of interest composed of government, business, and academia, must coordinate their efforts in vigilance, innovation and communication** via structured working groups and standard operating procedures. Its effectiveness and ubiquity are dependent upon the input from this community of interest.

Audience

The misconceptions about quantum computer technology can create the false perception that preparing for this potential threat may be too daunting for IT professionals who do not have a deep background in mathematics or physics. This is not nor should not be perceived as the case. To use a metaphor from chivalry, in sieges past, the knights charged with defending the castle were seldom the actual masons, carpenters, or blacksmiths that physically made these defenses and tools. Likewise, today's frontline IT management personnel and most other affected stakeholders, need only to properly use the tools provided to them by the subject matter experts and not necessarily know how to construct such tools.

Therefore, in addition to those with a technical background (i.e. programmers, engineers, scientists, and mathematicians), this framework is also intended to be used by the frontline government supervisor, or manager or, who is not necessarily a subject matter expert in those technical fields.

Approaches to Quantum Safe Security

NIST has been undergoing a standardization process to identify quantum-safe cryptographic algorithms. At this time there are fifteen (15) post-quantum cryptographic algorithms being evaluated with a high likelihood of usefulness. All algorithms have been independently developed by large companies such as the IBM, Intel, Microsoft, as well as international academic institutes and start-ups. The outcome/results of this competition must be incorporated into future readiness strategies.

Please go to https://csrc.nist.gov/projects/post-quantum-cryptography for more information.

Readiness Plan

At this time there are many entrants in the race to develop a relevant quantum computing system. In this race to prepare for the future, the U.S. government is investing heavily in research and development and workforce development on the technical side. Just because it is too soon to know which approach will be successful or dominant does not mean it is too soon to take proactive steps. As this race unfolds, all of the resources and tools, to be identified later in this document, must be utilized. Each organization, according to their mission and resources, must develop an actionable readiness plan or a list of best practices for a quantum resilient organization.

Malicious actors are trying to collect valuable and sensitive data today (even in encrypted form) in hopes that it can be decrypted in the future. A July 2020 article by Gregory Mone in the Communications of the ACM journal says:

"While the threat is theoretical, it still has contemporary implications. A malicious actor could store a cache of email encrypted with today's cryptographic approaches, and then use quantum computing to unlock them some 10 or 15 years in the future".

Although the fact that quantum technology is in its infancy does makes long term planning difficult but nevertheless the framework of a readiness strategy must be developed.

Therefore, the IT professional, frontline government supervisor, or manager must have and implement an agency and mission specific readiness plan that contains with the following basic steps:

1. **Acknowledge that basic practices will remain effective.** Although the deployment of quantum computing systems will inevitably require new procedures and protocols, traditional methods, such as carrying out scheduled and recommend upgrades, security patches and timely (or automatic) breach, anomaly, or compromise notifications cannot be minimized in importance.

2. **Keep a current inventory of applications, data, and hardware/infrastructure.** This action will facilitate what we and how we transition to the proverbial "post quantum" moving day.

3. **Archive system breaches and past vulnerabilities for continual forensic analysis and response.** Actions or incidents that may seem harmless today must still be logged and periodically reviewed (with the help of previously referenced tools to confirm whether or not some compromise did occur that may not have been obvious at the time. If data has been compromised it cannot be assumed that current encryption techniques would render that data useless to malicious actors

4. **Embed agility and flexibility in IT planning.** Past IT planning decision priorities were based primarily on accounting principles such as asset depreciation and/or return on investment as well as upgrades. IT professionals must face the reality that reactive (what until something happens) approach to cybersecurity is potentially disastrous. Even if existing infrastructure has not been fully depreciated or system applications are relatively new, their scheduled replacement must be based on the assessment of their vulnerability to attacks from quantum-based technology.

5. **Maintain awareness of progress and announcements being made by NIST Post-Quantum Cryptography initiative**. Follow https://csrc.nist.gov/projects/post-quantum-cryptography

6. **Stress test the system.** Just as financial institutions are audited and tested for their resiliency against threats to their liquidity and or solvency, it is possible even now to evaluate the robustness of conventional computing systems against future quantum-based threats via advanced simulation. This evaluation process will be further refined based on the outcomes of item 5 above. The results of these simulation can be used as metrics for preparedness.

7. **Require technology vendors and suppliers to address and certify government systems being quantum safe.** The April 28, 2021 NIST white paper "Getting Ready for Post Quantum Cryptography" provides a detailed study of possible migration paths for a post quantum cyber security.

Readiness Tools/Resources

Implementing the readiness plan will require tools and resources. Fortunately, we do have some of the tools and resources, right now. Currently, some of the tools and resources are:

1. **Boldly and proactively leveraging the full potential of conventional and cutting-edge technology (Moore's Law is still applicable).** Fortunately, the principle of Moore's Law (a doubling of computational power every 18 to 24 months) is still applicable and as such is the case the continual advancement in conventional computing systems subsequently allow for advancements in encryption and other cybersecurity techniques. Furthermore, NIST quantum-safe algorithms and quantum system modeling are techniques that can be deployed today.

2. **Leverage AI, Machine Learning, and Zero Trust.** Pattern and behavioral recognition as well as zero trust protocols can work in concert as an interim firewall.

3. **Fight quantum with quantum.** As stated previously there are other characteristics and applications of quantum physics such as de-coherence and entanglement that can be used to protect organizations from the threat of quantum computing systems. Examples of a readily available technologies are:

    a. Quantum random number generator, which uses quantum physics to deliver truly random keys.
    b. Quantum key distribution, which uses the laws of physics to protect key exchange, and as such is not vulnerable to quantum attacks.
    c. Hybrid system of quantum and classical computing systems can work in concert to detect, deter, and mitigate risks.

Quantum Safe Commission

The complexity and breadth of a transition to a quantum safe status across the government footprint, mandates that federal agencies must collaborate, unify and perhaps share resources to adequately protect the response of the US. to the quantum threat. Furthermore, because this is a technological race similar to that of the nuclear arms or the space race, the U.S. cannot afford to lose time or compartmentalize resources. Therefore, from a national level, an interagency panel must be empowered to:

    a. Provide guidance and standards. Support individual agencies in establishing and executing their mission specific framework, readiness strategy and readiness plan,
    b. Facilitate the exchange of ideas and best practices,
    c. Develop a list of public private partnerships which utilize quantum computing applications
    d. Receive and disseminate information on threat/vulnerability assessments, and recent or active incidents responses, and
    e. Monitor, track, and evaluate developments in quantum computing technology.

This interagency panel or ***Quantum Safe Commission*** should be composed of representatives of government, finance and commerce, private sector technology, academia and research and strategic support partners. The recommended commission members for this iteration are:

- The Department of Energy – To leverage the intellectual power of the national laboratories. *
- The National Institute of Standards & Technology (NIST) – To lead policy and standards development. *
- U.S. Cyber Command (DoD) and Cybersecurity & Infrastructure Security Agency (DHS-CISA) Their mission statements positions them uniquely to access and respond to potential threats. *
- Defense Advanced Research Project Agency (DARPA) and The National Science and Technology Council (NSTC) Subcommittee on Quantum Information Science (SCQIS)
- To leverage the power of advanced research.
- The Departments of Treasury and Commerce – To evaluate impacts and risks of a fiscal or financial nature.
- Research, Industry, and Technology coalitions such as the Quantum Industry Coalition (QIC) and or the Quantum Economic Development Consortium (QED-C) and or their member representatives (i.e. D-Wave, IBM, Google, etc.).
- Finance Industry representative(s) (i.e. Visa, Chase, PayPal, Wells Fargo, etc.)
- Strategic non-government support partner i.e. the Advanced Technology Academic Research Center (ATARC).

As of the writing of this document there are no commitments from the entities referenced and no specific representative from academia and or technology policy or think tanks have been identified.

Conclusion

The deployment of quantum computing systems, and all of the benefits and potential risks that come with it, is inevitable. Procrastination is not an option regardless of one's individual role in an organization's mission or IT environment. We do not have to be fearful or intimidated by this undertaking. There is a path forward. There are tools at our disposal today. There are already knowledgeable and ethical people of vision, who are working hard to meet this challenge. However, the institutions of our society must prepare now. This framework is a starting point that will assist the targeted audience and the U.S. as a whole, in mitigating the risks from, but more importantly enjoying the benefits of this new technology on the near horizon.

* Denotes voting member. All other representatives would be advisory with regards to policy statements and directives.