G7 CYBER EXPERT GROUP STATEMENT ON PLANNING FOR THE OPPORTUNITIES AND RISKS OF QUANTUM COMPUTING

September 2024

The G7 Cyber Expert Group (CEG) advises G7 Finance Ministers and Central Bank Governors on cybersecurity policy matters of importance for the security and resilience of the financial system. The G7 CEG has identified quantum computing as an area of both potential benefit and risk to the financial system. The CEG encourages jurisdictions to monitor developments in quantum computing, to promote collaboration among relevant public and private stakeholders, and to begin planning for the potential risks posed by quantum computing on some current encryption methods.

Quantum Computing & the Financial System

Quantum computers are being developed that are expected to be able to solve computational problems currently deemed impossible for conventional computers to solve within a reasonable amount of time. Financial institutions may benefit from the computational speed that quantum technology enables through the optimization of market trading, investment processes, including those for risk management, internal operations, and prediction strategies. Moreover, quantum computing may support more efficient payment processing as well as dynamic optimization of portfolio holdings. Technologies such as quantum key distribution may also help organizations to better secure their digital communication systems.[1] Financial institutions will need to prepare to manage the potential risks of these new quantum applications as they are deployed. In addition, the introduction of quantum computers may provide an opportunity for nefarious actors to exploit the technology for malicious purposes in a way that creates both organizational and systemic risks in the financial system.

Risks to Public-Key Cryptography

Digital communications and IT systems are safeguarded by encryption. Complex algorithms ensure that communication between multiple parties are private and secure, and that identities are assured. In the future, cyber threat actors could use the unique properties of quantum computers to solve some of the mathematical problems that underpin conventional encryption, and, hence, defeat certain cryptographic techniques used in secure communications, potentially exposing financial institution data including customer information. In anticipation of large-scale quantum computing becoming prevalent, threat actors may be implementing a "harvest now, decrypt later" scheme to intercept confidential data now with the intent of decrypting it once quantum computers become more capable and widely available.[2] This scheme also poses a threat to traditional cryptographic algorithms protecting digital communications, IT systems, and data, potentially providing threat actors with access to confidential data at a future date, which could undermine the integrity of an organization's reputation and customers' privacy.

[1] The International Organization for Standardization (ISO) has published standards for quantum key distribution security to provide guidance to authorities and industry, which are available at ISO/IEC 23837-1:2023 - Information security — Security requirements, test and evaluation methods for quantum key distribution — Part 1: Requirements

[2] Project Leap: quantum-proofing the financial system (bis.org)

Post-Quantum Cryptography (PQC) Standardization

Post-quantum cryptography (PQC) is a field of work focused on efforts to develop cryptographic systems that are secure against quantum computing risks to encryption algorithms and that can interoperate with existing communications protocols and networks.[3] There are several ongoing PQC efforts across government and industry at the national and international levels, with a particular focus on development of security and interoperability standards. The National Institute of Standards and Technology (NIST) in the U.S. has explored developing PQC public-key algorithms to secure current systems against the risks posed by quantum computers and classical computers as their power increases.[4] NIST launched a public competition in 2017 to identify quantum-resistant algorithms that will form the basis of new encryption standards. The first ones were published in August 2024.[5] The European Union Agency for Cybersecurity (ENISA) has published a study on the current state of affairs on the standardization process of PQC, which highlights work at organizations such as NIST and the International Organization for Standardization (ISO), and a report on post-standardization challenges and protocol recommendations.[6]

Further international coordination can mitigate the risk of regulatory gaps and asymmetries across the G7 jurisdictions. The World Economic Forum has been investigating quantum resilience through a collaboration with the United Kingdom's Financial Conduct Authority, and, with the participation of several global financial authorities, released a report discussing global regulatory approaches.[7]

Recommendations

An operational quantum computer (or hybrid computer) is viewed as increasingly possible within a decade, although its capability to undermine existing cryptography, at least initially, remains uncertain.[8] It may take significant time and economic effort, however, for public and private sector entities in the financial sector ("financial entities") to coordinate activities to mitigate vulnerabilities in anticipation of a post-quantum environment. Given the long lead time to do so, entities should ready themselves to handle impending threats as soon as possible.

Financial entities should consider taking the following steps to address this emerging risk:

1. **Developing a better understanding of quantum computing, the risks involved, and strategies for mitigating those risks.** Financial entities may consider outreach to vendors, third parties, and other subject matter experts to better understand the risks of quantum computing and potential technology solutions, with a particular focus on cryptographic risks. Issues they may want to focus on include the timelines for quantum technology development, the evolution of the threat landscape, and existing and emerging quantum resilience

[3] Next steps in preparing for post-quantum cryptography - NCSC.GOV.UK
[4] Post-Quantum Cryptography | CSRC (nist.gov)
[5] NIST Releases First 3 Finalized Post-Quantum Encryption Standards
[6] Cryptography — ENISA (europa.eu)
[7] Quantum Security for the Financial Sector: Informing Global Regulatory Approaches | World Economic Forum (weforum.org)
[8] 2022 Quantum Threat Timeline Report # Global Risk Institute

technologies and approaches. Financial entities should consider processes to track developments in these areas as they change over time.

2. **Assessing quantum computing risks in their areas of responsibility.** Financial entities should develop a sound understanding of quantum computing risks to their particular areas of responsibility, whether that is an individual company or a jurisdiction. The goal of this is to identify the level of effort the entity should dedicate toward the issue and the specific area(s) where it should focus. For entities that are ready to do so, this may involve beginning to inventory critical data and current cryptographic technologies in use within their organizations and key third parties on which they are dependent in order to identify and prioritize areas for mitigation. For others, a starting point may be discussions with the entity's information technology leadership and key service providers prior to conducting a more in-depth analysis. They may also wish to discuss their risk tolerance for protecting critical data before quantum technologies become more mature.

3. **Developing a plan for mitigating quantum technology risks.** Financial entities should consider establishing governance processes, identifying key stakeholders and their roles and responsibilities, and establishing milestones for key actions based on the anticipated deployment of a cryptographically relevant quantum computer. As noted above, such future actions may include creation of an inventory of cryptography use within the entity and its third parties. It may also include planning for the orderly replacement of vulnerable technologies with those that are quantum resistant. The Canadian Government has developed a Quantum Readiness Guide that can help entities prepare for the quantum threat.[9]

The G7 CEG encourages financial authorities to work closely with firms and other relevant parties in their jurisdiction to raise awareness of the importance of the transition to quantum resilient technologies. The G7 CEG remains committed to this topic with the aim to foster dialogue with all the relevant public and private stakeholders in the financial system to prioritize areas of intervention and to exploit synergies among the G7 jurisdictions and standard setting bodies.

[9] Quantum-Readiness Best Practices