BANK POLICY INSTITUTE

Why Is Quantum Computing Attracting So Much Attention?

Andrew Kennedy | May 27, 2022

BITS[1] recently held a virtual Symposium on quantum computing for its member companies. Over a hundred members registered for the event, mirroring the interest seen at other recent industry events. The BITS Symposium featured subject matter experts from the government, private sector and academia to discuss how organizations are preparing for post-quantum computing, strategies and resources that may be immediately leveraged, and the opportunity for better cybersecurity and technological innovation.

But why is there so much interest in a topic that is years, perhaps over a decade, away from meaningfully affecting cybersecurity? In our view, there are several drivers:

1. The consequences of quantum are potentially astronomical. Quantum computers hold the promise to exponentially speed up the computations necessary for cybersecurity such as integer factorization, which forms the basis for most public-key cryptography schemes used today. If a large quantum computer became available today, many — perhaps the vast majority of — online services we take for granted would become immediately less secure. Online services such as shopping and travel sites would become increasingly risky to use, and expectations of privacy on wireless networks would cease to exist, just to imagine some first-order effects.

2. There is a sense of scientific progress. Major technology firms are making announcements and setting ambitious near-term targets for computational sophistication and computing power. This may be peak mania in the current localized hype cycle, but it isn't unwarranted. As one of our distinguished speakers said, "The level of concern is not equal to the advancement of technology."

3. The opportunities, at least for the moment, are boundless. Whether it is vastly improving financial prediction and forecasting models via Monte Carlo simulations, expediting stronger AI to improve customer services or to process and spot patterns in data more rapidly than classical machines, the green fields appear endless. And while cybersecurity may be initially threatened, quantum key distribution and quantum random number generation may prove to make communication more secure than ever before.

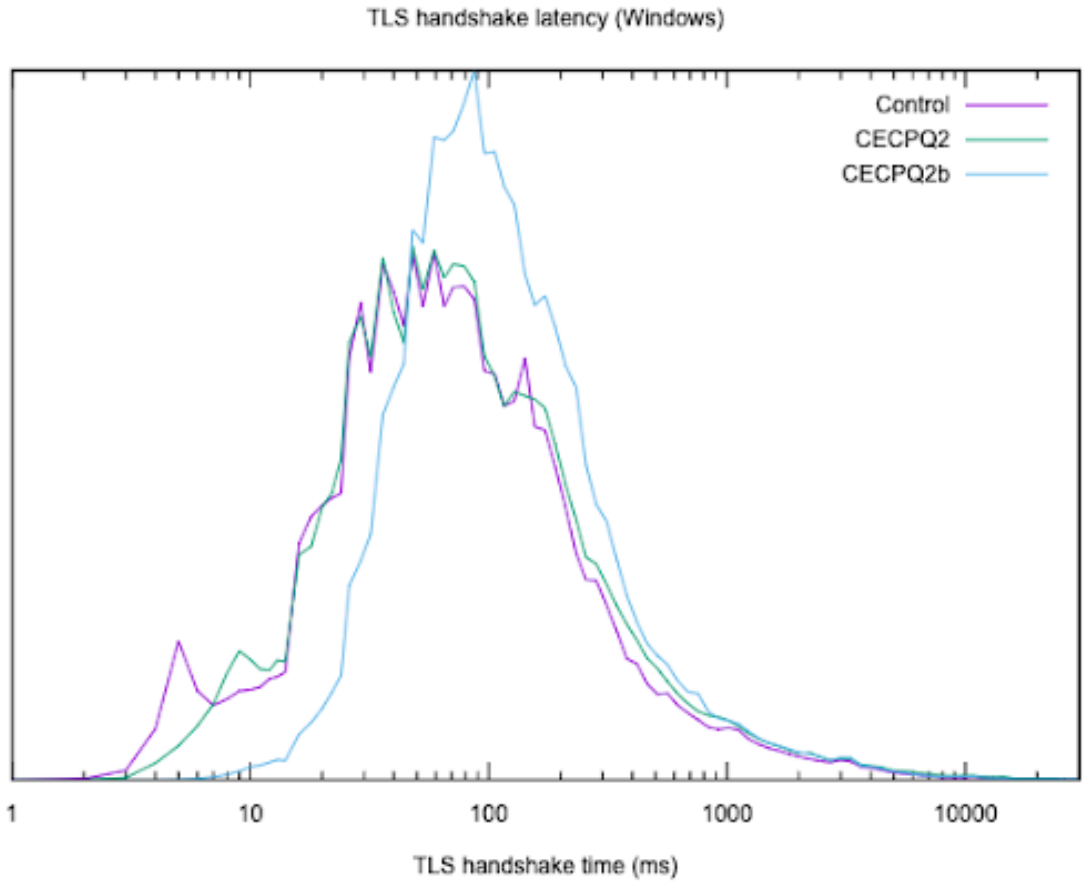
This isn't lost on the highest levels of the U.S. government, which issued two new directives May 4 on quantum. The Executive Order on Enhancing the National Quantum Initiative Advisory Committee is designed to keep the U.S. in the continued quantum information science leadership role, building upon the National Quantum Initiative to enhance public sector organizational strategies and fund quantum research and training activities to build out a

[1] BITS is the technology policy division of the Bank Policy Institute.

quantum-ready workforce. The President also signed a National Security Memorandum setting requirements for agencies to plan and update their cryptographic systems, enhance public-private collaboration and safeguard intellectual property.

The global race is on to not only develop a quantum computer, but also to develop the new cryptographic standards that will keep us safe in a post-quantum world. The transition to these standards will likely be a slow and arduous process if history is a guide. It took nearly two decades to move off 3DES, a standard thought to be weak as early as 1999. Further, there isn't certainty whether there will be one or more cryptographic transitions, meaning industry may have to update cryptographic systems at scale multiple times. This may add pressure on organizations to implement the concept of 'crypto-agility'; the ability to quickly transition to new cryptographic primitives without significantly changing other core parts of systems in an environment where most applications and systems today are not designed with crypto-agility in mind. Research indicates quantum-ready solutions may significantly degrade performance, generating issues with response time, customer satisfaction and potential competitive issues. The exhibit below demonstrates the effect of quantum-resistant solutions on business solutions like a website. Using Transport Layer Security (TLS) — the protocol securing virtually all modern websites — as a measure, the exhibit demonstrates a significant decline in performance between the control and experimental quantum computing encryption solutions such as CECPQ2/b. Finding the right architecture that carefully balances security with business and customer satisfaction will be paramount.

The Effect of Experimental Quantum Computing Encryption on Website Performance



Source: ImperialViolet

It takes time to plan, inventory, budget, benchmark and integrate modern cryptographic primitives into new and existing systems safely and securely — perhaps more time than we have before a quantum computer appears.

For today, 2022, the key message is that action can be taken for organizations of all sizes to start preparing for a post-quantum computing world. These include collecting information on affected systems, developing a concept of crypto-agility (for classical and post-quantum updates) or starting the discussion and potentially contracting process by asking third parties what they are doing to be prepared. Taking steps today, no matter how minute, will lower the burden and urgency of being prepared for tomorrow.

_____

Disclaimer: The views expressed do not necessarily reflect those of the Bank Policy Institute's member banks, and are not intended to be, and should not be construed as, legal advice of any kind.