quantumbusinessnews.com

Cybersecurity in a Post-Quantum World

Maria Korolov

15–19 minutes

Experts agree that future quantum computers will break most current encryption when they become sufficiently powerful. The code to do this – Shor's algorithm – has already been written. It just needs a powerful enough quantum computer to run on.

According to the Cloud Security Alliance (CSA), a suitable quantum computer will be available by 2030. The CSA created a quantum-safe security working group in March 2023 and even has a “cryptopocalypse” countdown clock on its website.

A November 2022 memorandum from the U.S. Office of Management and Budget requires federal agencies to migrate to quantum-resistant cryptography by 2035 and to have a plan in place by May 2023.

But that doesn't mean that the threat is still years away. Malicious actors such as large criminal groups or foreign governments can collect encrypted traffic today and decrypt it later, once sufficiently powerful quantum computers are available, an attack known as “harvest now, decrypt later.”

"Imagine if anyone can read my data ten years from now," said

Insight analyst Phil Young.

He added that early versions of quantum computers are already available via cloud services and that once commercial-quality quantum computers are available, they'll be accessible via the cloud as well. This means attackers wouldn’t even have to own their own quantum computer, they could rent time on one for a few dollars to run their decryption algorithms. This means that companies with sensitive data that will retain its value for years into the future need to start looking at upgrading today.

Young added that the problem isn't just for external communications. Companies that store critical data on-premises use symmetric keys to make sure it's as safe as possible. But many wrap up both the data and the symmetric keys with asymmetric keys for easier key management, he said. That's the equivalent of having a strong key on every file cabinet in your storage room, but then the room itself is locked with a much weaker key – and once you get into that room, all the file cabinet keys are right there.

"The door to the file room has a key that changes quickly," he said. "That's the asymmetric key."

That means that both data at rest and data in motion are vulnerable to quantum decryption attacks. And it's not just data security that is at risk, identity and authentication are as well, he added.

"Today, people trust that they can log into their banks because their operating system has a copy of the bank's public key in what's called an SSL certificate," he said. "Those certificates are public keys, used to identify the entity and as part of exchanging keys to

encrypt traffic. So we are back to the same problem. How, in a post-quantum world, can I be sure I am talking to the entity I think I am talking to?"

There are three main alternatives for quantum-safe encryption. The first, and relatively easiest, is to upgrade the current encryption to use quantum-safe algorithms. The second option is to stop using the easily-breakable, asymmetric, public key encryption systems and use only the much more secure symmetric keys. The third, and most expensive and difficult option, is to use quantum communication networks.

There are several projects underway to find a quantum-proof alternative to today's asymmetric keys. Asymmetric keys are the foundation of our current public key infrastructure system, all internet communications and all digital certificates.

Asymmetric keys come in pairs. One key encrypts the message, and the other key decrypts it. Companies distribute the keys that can encrypt the message, known as the public keys, to the... well, to the public. Anyone who wants to send the company a message uses the public key, but only the company itself can read it because it keeps the decryption key, the private key... well, private.

The system uses math to keep people from figuring out the private key if they know the public key. One common strategy is using large prime numbers. It's very easy to multiply two large numbers, but very difficult to figure out what the divisors of a large number are. Well, difficult for today's computers. Not difficult for quantum computers running Shor's algorithm.

The plan is to replace the "factoring large numbers" problem with another math puzzle, one that's harder for quantum computers to

solve.

Last July, the U.S. National Institute of Standards and Technology (NIST) proposed four candidate encryption methods that aim to be able to stand up to decryption by quantum computers.

The four algorithms are Crystals-Kyber, Crystals-Dilithium, Falcon and Sphincs. Four other algorithms, BIKE, SIKE, Classic McEliece and HQC, are being considered as possible future candidates.

The final recommendations are expected to arrive next year. SIKE, one of those alternate candidates, was cracked on a single-core computer in an hour, about a month after the algorithms were released. And, last month, a team from Sweden's Royal Institute of Technology discovered that Crystals-Kyber is vulnerable to AI-powered side-channel attacks.

Internet encryption provider Cloudflare announced last month that it will provide post-quantum cryptography for free by default to all its customers.

"We hope that others will follow us in making their implementations of PQC free as well so that we can create a secure and private Internet without a 'quantum' up-charge," Cloudflare quantum researchers Wesley Evans and Bas Westerbaan said in the announcement.

Cloudflare uses the Crystals-Kyber algorithm – the one that was found wanting. But according to Cloudflare, it's not the algorithm itself that was broken. A side-channel attack goes after the way the algorithm is implemented, and all it means is that technology providers have to be more careful in how they secure the whole system.

"There is a big difference between a direct break of cryptography and a power side-channel attack," Cloudflare researchers wrote. "Kyber is not broken, and the presented power side-channel attack is not cause for alarm."

But there's always the possibility that another method will be discovered to break the encryption, said Insight's Young. "All mathematically-based encryption is vulnerable to 'Oh, wow, I didn't know you can do that!'"

What this means is that companies looking to upgrade their encryption should be ready to switch out their encryption algorithms quickly if they're discovered to be weak– or if better ones come along.

Better yet, they should use vendors that have migration plans in place for post-quantum cryptography, and make sure that those vendors' crypto infrastructure is flexible enough to handle changes in encryption standards.

"You don't want to roll your own," he said. "Encryption is generally not something people want to implement on their own. You want to talk to your vendors, understand what's possible and what the standards are."

In addition, companies should immediately move to the strongest current encryption that's practical, and, for systems that they are developing and managing, make sure that they can be migrated to post-quantum encryption at some point, he said.

“Now that early-stage standards exist, it makes sense to start planning laboratory condition testing," said Kevin Bocek, VP of security strategy and threat intelligence at Venafi, a cybersecurity company. "Choose a single application and understand the

performance impact of the new algorithms."

He suggested that, at first, companies might want to take a hybrid approach, running post-quantum encryption systems alongside the classic ones during the transition, adding that it's similar to the way hybrid cars are helping the transition to electric vehicles. In fact, we're likely to see hybrid systems in use for decades until the transition is complete.

The Symmetric Key Alternative

Another option for enterprises that have high-value communications that need to be secure is to get rid of asymmetric public-private keys altogether and just use symmetric keys.

The problem with this approach is getting the symmetric key to the other person in the first place. If they're all employees of the same company, then the key system could be directly installed on their company equipment. For example, each employee could be issued a giant list of symmetric keys, with a formula of which key to use and when. The next time they're at the office, the list gets updated with a fresh set of keys.

Or, companies could physically mail out thumb drives with keys on them. This approach can quickly get very challenging, logistically.

To solve the problem of how to distribute symmetric keys securely, vendors are coming up with different solutions. The downside here is that both parties have to be using the same vendor. Plus, you have to change all your processes to use symmetric keys instead of asymmetric ones – something that is very inconvenient.

One company offering a key distribution system is Qrypt, which has a method of creating and distributing secure symmetric keys.

Qrypt uses the principles of physics to create truly random numbers, namely interference patterns created by merging laser pulses and interactions with vacuum fields.

Once it has a list of random numbers, it sends the lists out to its customers. Those customers then pick a number from the list, select a recipe to apply to that number, then use the key that's generated to encrypt and decrypt communications with counterparties. The key itself is never shared – the counterparties just share the recipe they used to create the key from the lists they both have.

Qrypt can currently generate 50 terabytes worth of random numbers per day, which offers enough randomness to create 250 million secure keys per second and the architecture is designed to scale up as needed.

The pools of random numbers are shredded every hour, said Chris Schnabel, the company's VP of product.

"And you’re not actually transmitting the encryption key you’re relying on," he said. "So because you’re not doing that key exchange, if someone harvests that data, that key was never exchanged. So you can’t decrypt it."

The initial communications between Qrypt and its customers, and between the counterparties themselves, are secured with today's public key infrastructure. But as long as quantum computers aren't going to be invented within the next hour, he said, "we can establish long-term data security."

The system is functionally equivalent to quantum key distribution in terms of security, he said, but without the distance limitations and other challenges that QKD is currently facing.

Qrypt said that it's currently working with a dozen organizations, including some of the world's largest banks, telecoms and consulting firms, but, because of the sensitive nature of the technology, none of them were willing to talk about their implementations.

The most difficult and expensive of the three alternatives, and the one that's the furthest from commercial availability, is quantum key distribution or other quantum networking technologies. But this is the option that also promises to be the most secure for the long term.

With quantum key distribution, a quantum network is used to transmit the symmetric key. Once the networks get cheaper and faster, maybe they can handle more kinds of traffic. These networks use the principle of quantum entanglement to guarantee that nobody else can listen in to the communication. Most approaches use entangled photons, which means that they can work over existing fiber optic lines.

Unfortunately, they need special – and expensive – sending and receiving equipment. Currently, every vendor has its own, different, quantum network, but in the future, the different quantum networks will be interoperable.

"We already are working together," said Vanesa Diaz, CEO at LuxQuanta, a quantum key distribution company. In Europe, for example, every national security agency can certify the quantum communication vendors in each country, and those certifications will cover all of Europe.

"And we will, eventually, be able to interconnect systems between different vendors," she said.

Standards bodies are working on all aspects of quantum key distribution systems, she said, including how different machines interact with each other, what trusted nodes look like, and so forth.

"That is one of the biggest priorities for all the vendors," she added.

Quantum networks also have a bandwidth challenge, she confirmed. They can currently support key distribution, but not all messages. Plus, the devices are large and expensive.

Today, though, the quantum key distribution routers from LuxQuanta and other vendors are designed to be set up in data centers. LuxQuanta's device, for example, fits into a standard data center rack where it takes up three spaces.

Eventually, she said, quantum key distribution, and then quantum networks, can be compact and inexpensive enough to fit inside home Internet routers.

Another problem with quantum networks is that they typically work over relatively short distances. The way traditional networks deal with it is by moving messages through a series of hops. But when quantum communications hit a junction, they have to drop out of quantum mode -- which creates security vulnerabilities.

Quantum Bridge Technologies is working on a quantum repeater, which will allow quantum communications to transmit over longer distances.

"A repeater will allow bigger networks," said Mattia Montagna, the company's co-founder and CEO. "Real, scalable networks."

However, since the point at which the technology can be commercialized is still in the future, Quantum Bridge is also

working on securing classical communication infrastructure with its own encryption software solution.

The company has centralized key servers that distribute key lists to all participants. The participants then agree with each other about which particular key they're using, and how they're modifying it. An outside attacker might be able to listen in to the recipe, but without that list of keys, it's worthless. And the list of keys itself changes constantly, which would make it extremely difficult for an attacker in the future to figure out the correct decryption.

If there are multiple key distribution hubs, then participants can combine keys from different sources, he said, which will eliminate the need to trust any one particular key service. Organizations can use the technology to set up their own key servers, Montagna said, adding that the Canadian government is currently testing the system

Then, in the future, as quantum key distribution becomes more mainstream, these centralized key hubs can be replaced by QKD systems.

"It's the first step towards building a quantum infrastructure," he said.

Some companies are already experimenting with using quantum networks for quantum key distribution. Ernst & Young, for example, is using QKD to secure communications between two offices in

The U.S. does have working quantum networking testbeds –a 124-mile network in Chicago being the longest – but it’s been lagging behind Europe and China.

By comparison, China's QKD network – which combines optical

fiber with two ground-to-satellite links –can achieve QKD over a distance of 4,600 kilometers, or about 2,860 miles.

This year, two companies are planning to deploy the first U.S.-based commercial quantum key distribution networks – EPB Quantum Network in Chattanooga, Tennessee, and GothamQ in New York.

GothamQ, deployed by Qunnect, will connect the Brooklyn Navy Yard to New York University in Manhattan and is expected to be finished this year and will serve customers in the financial services, critical infrastructure, and telecom industries in the New York metropolitan area, according to a January press release.

Meanwhile, in Tennessee, a new commercial quantum network from EBP, an Internet and power company, and quantum networking company Qubitekk, is scheduled to go live this summer. The Tennessee location is because Qubitekk has been working with the Oak Ridge National Laboratory, located in the area, which has been working on quantum technology with Qubitekk and EPB since 2016.

Both of these networks are tiny -- more demonstration projects than actual workable systems. And they pale in comparison to China's deployment.

But the future is bright for quantum key distribution. According to a June report by quantum industry analyst firm IQT research, the worldwide market for quantum networks will be near $1.5 billion in 2027 and go to over $8 billion by 2031, and QKD will be the main revenue driver.