www.pipelinepub.com
Volume 20, Issue 1

Evolving The Network to Prepare for Q-Day

By: Jim Ricotta

Experts estimate that quantum technology capable of breaking current encryption algorithms and intercepting communications will be possible no later than 2030. The day the first quantum computer (or a network of quantum computers) is able to decrypt security schemes currently in-use is widely referred to as Q-Day, and due to the complexity of upgrading these systems, network operators and other organizations need to be taking steps now to prepare for this looming threat to existing networks and communications encryption.

Why worry about Q-day

If Q-day might not happen until the end of the decade, many organizations may believe that they have years before they need to worry about quantum attacks. To understand why this isn't true, let's take a look at how we currently protect information.

Asymmetric encryption like RSA, ECC, Diffie-Helman, and public key security are standards that most organizations rely on today to keep data safe. They are used for authentication and key distribution and are absolutely vital to cybersecurity. Shor's algorithm has been around for 30 years and has been proven to efficiently crack these security schemes. It's just a matter of time before quantum computing technology is advanced enough to run Shor's algorithm on large inputs.

What does this mean in real terms for those organizations—the governments, network operators, other businesses, and individuals using these standards today? Essentially, all information that is sent across the Internet will be rendered unsecure by future quantum computers. Defensive military, intellectual property, financial, medical, and even infrastructural information are all at risk.

It's easy to imagine just how disastrous it could be if this information falls into the wrong hands, but just as easy to push this into some “future” bucket. Unfortunately, the information we are sending today is also a risk due to “Harvest Now, Decrypt Later” attacks—in which an adversary steals encrypted data that they can't currently decrypt. The adversary holds onto this encrypted data until they're able to decrypt the data, when they have access to a quantum computer capable of running Shor's algorithm.

Think about the kinds of information that needs to remain secure for long periods of time: military and defense, intellectual property, and financial and medical information, among others.

Because of the looming threat of Q-day, and the immediate threat of “Harvest Now, Decrypt Later” attacks, organizations need to come up with a countermeasure to this quantum threat as soon as possible.

Three Solutions to Address the Looming Threat

At this point in time, there are three main solutions proposed to address the challenge of preparing for Q-day: post-quantum cryptography (PQC), quantum key distribution (QKD), and quantum secure communication (QSC). With PQC, the idea is to replace the end-use classical security algorithms that are going to be broken by quantum computers with classical security algorithms designed to be quantum safe. These new security algorithms are based on math problems that are believed to be difficult for quantum computers to solve. This is a purely classical solution, and it can be deployed over the classical internet. PQC is thought of as a good short-term solution because it's relatively quick and easy to implement. PQC algorithms have been heavily scrutinized for years, and they're believed to be secure. Unfortunately, they are not mathematically proven to be secure and could be broken in the future by quantum or even classical computers. Two of the most promising PQC algorithms, RAINBOW and SIKE, were already broken by standard classical computers.

QKD is a physics-based solution, relying on the properties of superposition and measurement, and uses quantum properties to always be able detect the presence of an eavesdropper. In theory, at the protocol level, this works great. The implementation vulnerabilities though—like the requirement for trusted relay nodes if you want to distribute a key between nodes that are far apart—makes QKD much less secure in practice. The "trusted" part of this term is misleading. Trusted relay nodes are not nodes you can trust, but nodes that you need to trust, and if they become compromised, your key will become compromised as well. QKD networks may also require the deployment of additional resources, such as QKD devices and additional optical fiber. They also only support the single purpose of key distribution.

QSC refers to the entanglement-based quantum security protocols that run over and are enabled by entanglement-based quantum networks. This is a physics-based solution, relying on the property of entanglement and measurement. Similar to QKD protocols, quantum properties can always detect the presence of an eavesdropper when communicating a quantum message. Organizations can create an encryption

key that no unwanted party can access. The implementation of QSC is also secure because of quantum teleportation, which allows the communication of quantum information between users of a network without that quantum information actually ever being exposed on the network. This means that even if a midpoint of the network is compromised, the quantum data will not be. The security schemes exist and have been verified, and entanglement-based quantum networks that are capable of running these schemes exist and are being built today.

A Solution with the Least Implementation Vulnerabilities and Multi-Purpose Application Possibilities

In an ideal world, the best solution to the Q-Day threat is one without implementation vulnerabilities and one that can add value with other application possibilities beyond protection. The QSC security schemes had been around for decades, just waiting for the technology to develop so they could actually be used. The same entanglement-based networks that enable QSC are also the ones that will enable the networking of quantum computing, future distributed quantum sensing applications, and connectivity to blind quantum compute.

Quantum networks exist today, and have actually been around for quite some time. The first quantum communication protocols were established in 1984, and the first quantum network in the US went live in 2003. Toward the end of the 2010s, there was renewed interest when the catastrophic security threats associated with quantum computers started to become known. This renewed interest drove an increase in funding and investments to companies and organizations developing and deploying quantum networks at scale, and the technology continues to develop very quickly. Entanglement- based quantum networks are starting to pop up all over the world with some of them testing and running QSC.

In 2022 alone, ten new quantum network deployments were announced or were operating in North America. This includes the EPB Quantum Network℠, America's first industry-led, commercially available quantum network. These networks and testbeds all started small—some just two to three nodes—but then they scaled the networks to many nodes, and will continue to scale and connect to other networks across the country.

Integrating Quantum into Existing Networks

Entanglement-based quantum networks are also compatible with a lot of existing classical networking infrastructure, including standard telecom fibers and frequency bands, optical transport, network components, and existing encryption devices. Building entanglement-based quantum networks will not require a complete infrastructure overhaul or upgrade, which makes them easier to build and scale up. A great way to think about this is to remember when the classical network was originally used only to make telephone calls, and then transitioned to the internet—yes, you can still make calls, but now the network can be used for much more than that.

The progression from previous quantum networks to entanglement-based quantum networks will likely be the same. QSC can be used now and in the future for enhanced quantum computing capabilities and distributed quantum sensing. It will also be the foundation for the Quantum Internet, the global scale entanglement-based quantum network that will be able to support all known quantum applications, as well as all of the distributed quantum applications that haven't even been invented yet.

Quantum networking will also help improve metro and wide area networks. With a wide area network, organizations can connect quantum devices together and run distributed quantum applications. So, for example, if it wanted provably secure communication between parties on this wide area network, it would need entanglement-based quantum networks to run QSC. If it wanted to do blind computing—the only secure option for transmitting data on the cloud—one of the applications of distributed quantum computing, entanglement-based quantum networks will be needed.

Address The Threat Now, Reap the Advantages Later

While it makes sense to address the current threat from quantum computers, organizations that evolve their networks now can capitalize on the advantages that will come with quantum computers, quantum networks, and other quantum technology. QSC is provably secure, meaning mathematically proven to be secure against all types of cyberattacks. Put another way, it means that at no time in the future will algorithms, quantum computers, classical computers, or future technology, be able to break these schemes. These technologies promote faster computing, bolster the cybersecurity, and will enable the global Quantum Internet.