Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 14, Issue 2

# Quantum Key Distribution and the Crypto-Apocalypse

By: Tim Young

I am told that there was a time in which security—whether on the network or in physical space—was an expectation. Or, at least, it was considered a possibility.

But in an era of high-profile hacks and breaches, I think most adults with an ounce of healthy cynicism expect that, at some point, their sensitive data has been or will be compromised. The high-profile hacks, breaches, ransoms and leaks are too numerous to bother naming. Universities, voting boards, healthcare providers, intelligence agencies, emergency siren networks, font providers… It's been a busy year. I would say that I would bank on there being more coming, but my credit's been frozen since the Equifax hack, so I'm not banking on anything.

But as porous as security seems at the moment, the eventual rise of quantum computing promises to throw another wrinkle into this already wrinkly security Shar-Pei.

"Asymmetric cryptography relies on the assumption that computers today are not capable of solving  some difficult problem, for example the prime factorization of a very large number, in a reasonable amount of time," Rishiraj Pravahan, principal member of technical staff at the AT&T Foundry in Palo Alto, told *Pipeline*. "In fact, this assumption can be easily broken by using quantum computers."

Pravahan and others at the Foundry—AT&T's in-house innovation incubator—are among the thousands of motivated researchers working to head off the so-called "Crypto-Apocolypse".

There's been lots of encouraging progress on this front. MIT's Seth Lloyd proposed a model for a so-called "quantum enigma machine" back in 2013. Named for the famed WWII machine code, the quantum enigma device alters the properties of a photon wave in order to encode messages. It's called quantum data locking, and it does away with the old notion that a randomly generated key must be as long as the encrypted message itself.



It was only hypothetical until, last year, researchers Daniel Lum and John Howell at the University of Rochester created a prototype that put Lloyd's ideas into motion. While tremendously promising, however, this work—which would allow messages to be transmitted entirely through quantum channels—is still in its early days.

In the meantime, there have been massive strides of late toward something of a middle ground between traditional and quantum communications. Emerging as the most prominent among these middle roads is quantum key distribution (QKD).

QKD does not use an end-to-end quantum channel, instead opting to send an encrypted key through quantum channels which can be used to decrypt a message sent through traditional methods. Even attempting to measure the encoded photons changes their behavior, which makes any intrusion detectable.

“Strictly speaking QKD does not actually specify any particular encryption technique but simply provides a fully secure way of distributing a pair of keys to two parties who want to share information,” says Pravahan. “The two parties can then use the shared keys to encrypt their data using, for example, a one-time pad with the guarantee that the encrypted information will be impossible to decrypt.”

And QKD is not a new idea. It’s based on theories that are decades old and its practical examples date back to 2004, when researchers in Vienna used the method to make a bank transfer. DARPA has been running a quantum network since that same year, and the Secure Communication based on Quantum Cryptography (SECOQC) network, a project of the E.U., has been running since 2008. U.S. research non-profit Battelle has been making solid progress on QKD for years, and has had an encrypted fiber network in place since 2013.

And QKD is gaining steam. In February, SK Telecom and Nokia announced an agreement to conduct joint research that combines SK’s QKD acumen and Nokia’s next-generation optical transport. Toshiba announced in September that it had reached quantum key distribution speed in excess of 10Mbps, seven times faster than the speeds it had achieved only a year before. The quantum race has also been pushing increasingly into space, with China’s quantum satellite, Micius, being joined by Japan’s SOCRATES and others.

It’s those satellite advances that brought about one of the most noteworthy recent QKD headlines. In September, Chinese and Austrian researchers used Micius to facilitate a video conference between scientists 4,600 miles away from one another. The call connected Chunli Bai, president of the Chinese Academy of Sciences in Beijing, with Anton Zeilinger, president of the Austrian Academy of Sciences in Vienna. It built on work from earlier this year that saw researchers within China communicate over distances of 750 miles over channels secured by QKD.

This application is still a far cry from widespread adoption and use of QKD, but it’s part of a series of very encouraging early steps. “Insight must precede application,” University of Vienna Rector Heinz W. Engl said in the wake of the intercontinental call. He was quoting Max Planck, the founding father of quantum physics. “A telephone call illustrates today the innovative potential of fundamental research.”



But QKD isn’t a final answer. It’s only a beginning. Pravahan cites AT&T’s involvement in the INQNET initiative–which he co-founded in collaboration with Caltech and other academic, government, and industry partners– is “looking forward to building quantum networks where communication occurs between multiple nodes in a wide area network while preserving the

quantum correlations also called entanglement between the quantum bits (or qubits) that encode the information." He says that such a network will allow for QKD, but will eventually be capable of much more.

Pravahan notes that there are considerable costs associated with implementing and scaling applications that rely on QKD, but asserts that, given the impending emergence of widespread quantum computing, finding alternative methods of encryption is essential.

"I think, at least in the near future," Pravahan says, "QKD will play a very important part in network security, especially for highly sensitive communications."