A primer on quantum security

Analysts - Owen Rogers, Garrett Bekker

Publication date: Thursday, January 17 2019

451 Research is establishing a new cross-discipline Center of Excellence for Quantum Technologies. In preparation, this report provides a beginner's guide to quantum key exchange based on what Einstein called 'spooky action at a distance.' This isn't a distant dream – big players like Toshiba, Mitsubishi, NEC, NTT, Huawei and IBM are investing in R&D, while new players like Whitewood, Quantum Exchange, ID Quantique, MagiQ Technologies, QuintessenceLabs and Sequrenet already have commercial offerings for sale.

The 451 Take

Quantum key distribution guarantees the secure transmission of a key, but it is still susceptible to other attacks – if an unauthenticated malicious caller rings the holder of the key, for example, and persuades the holder to email it to them, the benefit of quantum technology goes out the window. As such, it is not a panacea, but another technology in the security toolbox to be considered on a case-by-case basis. Considering the complexity, immaturity and expense of quantum technologies, suitable cases will be few and far between. But for government and highly confidential communications, such an investment might be worth it, especially when quantum computing becomes more available.

Spooky action at distance

Imagine a marble in a clear sealed tube of just a few inches. The tube is angled such that the marble can only remain at either end of the tube no matter the orientation of the tube, so the marble has two states – it is either on the left or right. The tube only ever contains one marble.

We paint half the tube so that one side can't be seen and spin the tube so that the marble randomly settles in a left or right position. Can we determine which state the marble is in from looking at just the transparent half of the tube? Yes. If there is no marble at the visible end, we know it is at the other end.

Imagine we now stretch the tube from just a few inches to a few thousand miles. We still have two states, left and right, and the net number of marbles in the tube remains one. The position of the tube is affected randomly by the air pressure, weather, seismic activity and the like, such that it is constantly changing the marble's state. But we can always know the state of the hidden side by observing the visible side, even though we are miles apart.

This is where it starts to become more complicated. Imagine we cut the tube so the marble can't flow from left to right. But somehow, the ends of the tube continue to know the state of the other side. It's almost as if the marble is continuing to move between the endpoints of the tube via some secret magic passage we can't see.

This happens in so-called 'quantum entanglement.' Remember our Primer on Quantum Computing, where we referred to Schrodinger's Cat, which was both alive and dead in its box until its state had been measured? The cat was in a state of so-called 'superimposition.' In the tube model, the position of the marble is superimposed until we look at the tube – we only know the position of the marble by observing one side of the tube when we automatically know the position of the other side of the tube. More bizarrely, we can say that the marble is in a state of superimposition of both sides of the tube. It is only when we look at one of the sides, that the other side instantly knows if the marble is there.

This isn't a mathematical quirk; it really happens at a subatomic level. This is quite mind-bending, and Einstein himself described it as 'spooky.' In quantum communications, the zeros and ones are represented by characteristics of a subatomic particle. Let's say in Schrodinger's box, we put a subatomic particle with no spin (angular momentum). The particle decays into two new particles and must retain the characteristics of the particle from where it came, so one particle takes on an anti-clockwise spin and the other takes on a clockwise spin (the net sum of the spin is zero). These spins now represent 0 and 1. We now stretch the box across the globe. At either end of the box is a superimposed state of the original particle – we don't know which particle we will observe when we open it. But if we open the end of the box, we then observe one of the particles, and it is no longer superimposed. Thus, we instantly know the state of the other one even if it's at the other side of the world (or even more incredibly, the universe).

A crucial distinction to make here is that entanglement lets two places have the same state instantaneously, but it doesn't let us dictate the states – the moment we dictate one side, we measure it, and the entanglement collapses. They are no longer superimposed. Essentially, when we take a subatomic particle and it decays into two, the universe dictates randomly which states the particles have. As such, we must use this randomness as a key, rather than defining our own key. This sensitivity to collapse is a crucial function in quantum communications because it identifies when a man-in-the-middle has interacted with the communication. In fact, some vendors use this inherent randomness in quantum particles to generate random numbers for traditional security applications.

The quantum 'no-cloning' theorem says that we can't copy an unknown state, we can only copy an outcome. Let's go back to Schrodinger's Cat. If we want to duplicate the state of the cat, we have to open the box and measure it. We can't copy the cat's state without measuring it. Once we've measured it, the superimposition of the dead and alive cat collapses and we end up with the result.

Why is this important? If we introduce a man-in-the-middle watching our quantum communication, the superimposition will take place early. The man-in-the-middle will essentially open Schrodinger's box before we do, and the entanglement collapses. And the random digits the person at the end receives will be different from the ones sent. And this means our interpretations of the random numbers will be different.

If we were exchanging cryptography keys, we would know the key had been observed because it wouldn't work when we went to verify it over a regular communication medium using a checksum, etc. This is called quantum key distribution (QKD). Our quantum channel provides the ability for two parties to see the same random digits, so we can both have the same secure key. We must verify our keys over a traditional speed-of-light-bound channel to ensure the key exchange took place securely (using traditional hashes, etc.). If the key is observed by a third party, the digits each party receives will be different, and the validation will fail.

Entanglement isn't necessarily needed to exchange keys securely. Keys can be transmitted over an optical fiber today using polarized packets of light that, when observed, change state and provide protection from man-in-the-middle attacks. But entanglement takes this a step further – the information is really difficult to view because it is being transmitted over a channel that cannot be seen and is not really understood. This process is called quantum teleportation because information is essentially being teleported 'Star-Trek style' from one place to another. In particular, quantum key distribution provides some protection from cloud computing algorithms that are used to hack an encryption key (more on this in a moment).

But does it mean quantum data can be transmitted faster than light? Alas, no. You can't choose what data you are sending down the quantum channel because as soon as you do that, it is measured, and the particles are no longer entangled. We can just use the channel to make sure that both parties have the same random set of digits (which is exactly how it is used in key exchange).

The channel allows both you and the sender to see the same random data at the same time (which seems to suggest the communication is going faster than light). But you can only verify that you both have the same data once you use classical methods to communicate (a phone call, an internet communication, etc.). As such, the communication isn't faster than light because you must communicate in a traditional light-bound fashion to validate it.

Protection from quantum computing

Quantum computing (opposed to quantum security/communications, which is the focus of this report) potentially provides the ability to solve the complex math currently used in encryption today. The problem that quantum computing introduces is primarily with asymmetric encryption, not symmetric. Of the two types of encryption, symmetric has been around for millennia and is really good for encrypting data at rest. It is very hard to break since both users have the same key (hence the term symmetric), but the main problem is how to securely exchange those keys. In the past, this was mainly done manually, either in person or via courier, for example.

Asymmetric encryption was developed mainly to deal with the problem of distributing keys securely over networked connections, and as the name implies, each user does not have the same key, they are different. More specifically, there is a 'pair' of keys, one public and one private. Anyone can encrypt data using the public key, but it can only be decrypted using the private key. The public key (which encrypts the data) is essentially formed by taking two prime numbers and multiplying them together. To decrypt the data, you need to know the original primes (which are part of the private key). If you don't know the private key, to reverse-engineer that number into the two original prime numbers is incredibly difficult using technology today – to brute force the public key into its two primes would take an amount of time that would render the activity useless.

However, a quantum computer can find the two primes much quicker because (as shown in the primer) it can analyze all the possibilities at once using the uncertainty of the universe. As such, asymmetric encryption is highly vulnerable to quantum algorithms. Symmetric encryption doesn't have this problem because there is no inherent mathematical function that relates the keys held by the two parties (they are the same). All you have to do to increase the security of symmetric encryption is double the key length, and it should remain secure, even with quantum computers. Data at rest that is encrypted with symmetric algorithms should be relatively safe.

Since asymmetric encryption is mainly about key distribution, it follows that the main problem that quantum computing will introduce revolves around key distribution; hence, the interest in QKD. Using QKD, if the communication is hacked, at least you know it has been hacked.

Practicalities

ID Quantique, Quantum Exchange (building a QKD network under the Hudson), MagiQ Technologies, QuintessenceLabs, Sequrenet, SecureRF and Whitewood Security currently use quantum technologies in the secure communications arena, but QKD is generally still an area of research by the likes of Toshiba, Mitsubishi, NEC, NTT, Huawei and IBM. Partnerships with telecommunications providers such as BT, Telefonica and UPM demonstrate the commercial interest.

The US Defense Advanced Research Projects Agency (DARPA) has run a 10-node QKD network since 2004, and the EU has its SECOQC project, which links six sites over a fiber network. China is getting in on the act, too, operating a satellite-based quantum channel from China to Vienna with a link of 4,700 miles using its QUESS space mission. A fiber optical network provides the validation, and the project is aiming for a global QKD network enabled by 10 satellites by 2030.

The highest bandwidth currently achieved by a QKD network is 1Mbps over 12 miles of optical fiber and 10Kbps over 62km of fiber. Signal noise is a major problem, which reduces the distance achievable. Repeaters that resend the signal at regular intervals are one solution, but these aren't ready for widespread use today.

Quantum computing is a threat to public key infrastructure and security systems that rely on PKI, since PKI is based on asymmetric encryption, and PKI is ubiquitous in security. If quantum computing becomes accessible to malicious parties, then cracking the keys upon which PKI relies becomes relatively simple. QKD is just one way to deal with the threat from quantum – some firms are developing 'quantum resistant' algorithms, and NIST is in the process of evaluating 60 different algorithms for contention in its standards process, which will likely take a few more years.

Let's say there's a 20% chance there will be a workable quantum computer in 5-10 years. If so, and if you need data to be secure for at least 10 years, and it will take five years to implement and re-tool your infrastructure to support it, you need to hope you have 15 years before quantum can break it and strong quantum becomes available. In other words, if 'X + Y is greater than Z', you had better worry. Firms need to start preparing now if they think workable quantum computers could be around in five years.