Facing the quantum threat

Facing the quantum threat

People have been keeping secrets for millennia. In the information age where data is currency (literally, in some cases) the need to keep these secrets safe is more important than ever.

Over the last century we've developed sophisticated cryptographic methods to attempt to hide our information from prying eyes, but each generation finds novel ways of overcoming these safeguards, whether through mathematical ingenuity or sheer brute force.

We are now approaching another revolution in computing that will not only transform our ability to solve complex problems and understand the world around us but will shake the pillars of modern cryptography, again challenging us to find new ways of keeping our information safe.

We are entering the age of quantum computing.

Quantum computers harness the strange properties of quantum physics to radically change the way in which we can solve certain types of problems. Much of the information which is encrypted across networks today is susceptible because it relies on asymmetric keys created by algorithms in Public Kye Infrastructure, or "PKI". These keys derive their security from mathematical problems which, while difficult to solve using a classical computer, can be efficiently solved using a quantum computer. What might today take thousands of years to decrypt could be done in hours. This is a separate risk to the problems that have resulted recently from the use of a legacy system that was not designed to operate in a hyperconnected World (see our "PKI in a Hyperconnected World" paper).

A huge effort is underway globally to win the race to create a large-scale quantum computer, funded by both nation states and large companies such as Google, Microsoft, Honeywell and IBM, and a range of interesting start-ups like PsiQuantum and IonQ, with global investment in the government sector alone estimated at $22.5bn[1]. There are major benefits for the winners, and unfortunately one of the advantages offered to the first to achieve so-called "Universal Quantum Computing" is the capability to break the algorithms in PKI. Estimates vary on the time it will take to reach this milestone but according to some sources it could be as soon as 2025[2]. Regardless of the date at which universal quantum computing is achieved, NIST has recommended that "we need to be prepared for it as many years in advance as is practical"[3]. Thus, governments and businesses need to act now to safeguard their data.

[1] Qureca. (2021, January 22). Overview on quantum initiatives worldwide. https://www.qureca.com/overview-on-quantum-initiatives-worldwide/

[2] Quantum computing could end encryption within five years, says Google boss. The Telegraph. https://www.telegraph.co.uk/technology/2020/01/22/googles-sundar-pichai-quantum-computing-could-end-encryption/

[3] NIST (2021 April 28) Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms. https://doi.org/10.6028/NIST.CSWP.04282021

Contents

What is the quantum threat?

A quantum advantage

Classical computers operate on *bits,* which are values that are either 0 or 1. Quantum computers use quantum bits – *qubits* – which are not limited to the binary states 0 and 1, but rather can take an infinite number of intermediate values between 0 and 1, an effect called superposition. The ability to operate on these superposition states allows some algorithms to be run in a massively parallel fashion, dramatically shortening their run time and solving certain problems much faster than a classical computer. While the set of these problems is fairly small, it happens to include some important operations used in cryptography today.

Two of the most widely used cryptographic methods are RSA and Diffie-Hellman. RSA is typically used in identity certificates – cryptographically signed digital assets which prove the identity of an endpoint or device – although it's still used widely in e-mail encryption. Diffie-Hellman is the most commonly used public key-exchange method, used in almost all encrypted web sessions to establish a shared key between the client and server. There are several variations, including elliptic-curve Diffie-Hellman. Almost all internet traffic uses these encryption methods, and it's also used in many other communication protocols.

Both of these methods rely on one-way or "trapdoor" functions: easy to compute in one direction, but hard to reverse. For example, it's easy for a computer to multiply two numbers together, even very large ones. However, it's much harder to calculate the reverse operation, i.e. given a very large number, find the two numbers which were multiplied together to arrive at it (called factors). It's the difficulty of reversing the multiplication operation, called factorisation, that gives RSA its security. Diffie-Hellman relies on a different mathematical function, but the principle is the same.

Both RSA and Diffie-Hellman are examples of asymmetric cryptography, where one key is used to encrypt data (the public key) and another key is used to decrypt it (the private key), related by the trapdoor function. The encryption key can be made public because the trapdoor function makes it extremely difficult to compute the private key from the information revealed in the public key. However, quantum computers are able to efficiently reverse the trapdoor function for both RSA and Diffie-Hellman, effectively replacing it with a revolving door, computable in both directions. That means information encrypted with either of these methods can be decrypted easily with a quantum computer.

Usually, the data itself is not encrypted using asymmetric keys directly, rather this is used as a way to transfer symmetric keys between the two parties, a process called key encapsulation. In symmetric encryption, methods like AES and ChaCha, both parties have the same key, and it employs functions that are, by design, easily computable in both directions. These keys are known to be safe against quantum attack. But while the data itself is encrypted with a secure symmetric key, the data is still insecure because the key was encapsulated for exchange using an asymmetric method.

One application where asymmetric keys are used directly is in identity certificates. This is another application at threat from quantum computers and would mean anyone with access to a quantum computer could fake these certificates and pretend to be someone they are not.

So symmetric keys are currently not used at scale for key exchange (physical couriers being the only safe method) but there are currently uses for such keys, which means that symmetric encryption is already built into most networking software standards. These keys are secure once delivered, but the delivery is not quantum safe. Below is a comparison of the main current uses of symmetric versus asymmetric cryptography.

		Symmetric cryptography	Asymmetric cryptography
Data encryption	Summary	Widely used, can encrypt and decrypt information very quickly and efficiently. But compromised by Asymmetric method of key exchange to begin with, unless physical couriers used.	Not widely used due to slower speed and larger size of key.
	Examples	AES-256, ChaCha	RSA
	Quantum-secure	Yes, with sufficient key lengths	No
Key exchange	Summary	Not widely used on public networks, used widely in enterprise. Requires a third party for negotiation.	Widely used, especially over the internet.
	Examples	Needham-Schroeder	Diffie-Hellman, ECDH
	Quantum-secure	Yes*	No
Data authentication	Summary	Used widely where devices already share a key.	Used in digital signatures and certificates, particularly with Public Key Infrastructure (PKI).
	Examples	HMAC	RSA
	Quantum-secure	Yes*	No

Table 1: A summary of cryptographic methods and their uses.
*This assumes the links with the third party are quantum secure, e.g. using a pre-shared symmetric key.

Quantum Computing Market Background

A large number of companies and government institutions are developing quantum computers. The global resources invested by publicly avowed government programs is at least $22.5bn. Industrial investment is harder to estimate accurately. In the US alone, Google, Microsoft, Honeywell, IBM, AWS and others are pursuing assertive strategies. A rapidly growing field of start-up have raised significant amounts of capital including IONQ ($698m), PsiQuantum ($509m), DWAVE ($216m)[4].

Whilst large-scale universal quantum computer may still be some years away, the technology is advancing rapidly. Google were the first to announce quantum supremacy in 2019[5], meaning they had reached the point where quantum computers were able to demonstrate an exponential speed-up compared with classical computers. The University of Science and Technology of China made a similar claim in the following year[6]. The problem solved was different from factorisation (the basis of PKI), but it's an important step towards being able to realise more complicated problems.

[4] source: Crunchbase

[5] Arute, F., Arya, K., Babbush, R. et al. (2019). Quantum supremacy using a programmable superconducting processor. Nature 574, 505–510. https://doi.org/10.1038/s41586-019-1666-5

[6] Simonite, T. (2020, March 12). China Stakes Its Claim to Quantum Supremacy. Wired. https://www.wired.com/story/china-stakes-claim-quantum-supremacy/

When to act

We aren't yet at the point where a quantum computer can break encryption, but does that mean we don't have to worry? Some estimates put the realisation of a quantum computer powerful enough to break encryption at around 2025, and so there are compelling reasons to act now, given the time it takes to plan, procure and make fundamental changes to IT. The latest advice from NIST reiterates this position[3].

The National Information Technology Laboratory (NIST) in the US is widely regarded as being at the forefront of international technical and scientific standards. They have been conducting a process since 2018 to identify new so-called "post-quantum algorithms" or PQA for standardisation, expected to run until around 2023–24. These algorithms are the best publicly known response the World has thus far had to the Quantum threat. However, in a White paper released in April 2021, NIST made several conclusions which suggested that the process is not satisfactory.

Firstly, NIST noted that data is not only vulnerable in future, it is also at risk today, because data encrypted using PKI today could be stolen in its encrypted form and decrypted in future:

> "all secret symmetric keys and private asymmetric keys that are now protected using current public-key algorithms, as well as the information protected under those keys, will be subject to exposure. This includes all recorded communications and other stored information protected by those public-key algorithms. Any information still considered to be private or otherwise sensitive will be vulnerable to exposure and undetected modification."

It is widely held that PQAs can never be described as "quantum safe" – i.e. provably and unconditionally secure for all time against quantum attack. This is because they are created using mathematical processes. Just as RSA is defeated by Shor's Algorithm running on a Universal Quantum Computer, any PQA which is introduced is likely at some point in the future to be the subject of a new attack algorithm capable of breaking it – we just don't know when. Therefore, PQAs can never give the assurance of long-term security:

> "These algorithms are sometimes referred to as quantum resistant, but our understanding of quantum computing's capabilities is almost certainly incomplete."

NIST notes that even accepting that incomplete level of assurance, all of the PQAs thus far brought forward have significant barriers to adoption:

> "There are multiple candidate classes for post-quantum cryptography. Unfortunately, each class has at least one requirement for secure implementation that makes drop-in replacement unsuitable".

On top of that, any fundamentally new cryptosystem poses serious adoption problems:

> "Updates to protocols, schemes, and infrastructures often must be implemented when introducing new cryptographic algorithms. Consequently, algorithm replacement can be extremely disruptive and often takes decades to complete."

But NIST believes the problem to be urgent:

> "We cannot accurately predict when a quantum computer capable of executing Shor's algorithm will be available to adversaries, but we need to be prepared for it as many years in advance as is practical. As previously stated, when that day comes, all secret and private keys that are protected using the current public-key algorithms—and all available information protected under those keys – will be subject to exposure."

Given the urgency that NIST communicates, given the incomplete and impermanent solution that PQAs present, and given the disruptive effect of implementing a new cryptosystem, finding a way to use, at scale an existing system like symmetric key encryption which is known to be quantum safe would be an extremely important advance for the World.

How to protect data from quantum attack

There are two main areas of concern for security researchers addressing the quantum threat: key exchange (particularly where the two parties communicating don't know each other in advance), and data authentication. There are two potential groups of solutions being researched today, namely post-quantum algorithms (PQA), and quantum key distribution (QKD).

Post-quantum algorithms or quantum-resistant cryptography: A new set of mathematical algorithms and protocols using asymmetric keys which are hoped to be more resistant to quantum attack than PKI.

Quantum key distribution: A method of distributing symmetric keys whose security derives from fundamental physical laws, not mathematics, and is therefore an unconditionally secure way of creating a shared key between two parties. These keys can then be used in quantum-secure communication.

In this section we'll focus on key exchange and how both of these methods propose to put pairs of symmetric keys on devices in a secure way. Once those keys are established the two devices can encrypt and decrypt data using standard protocols like AES-256 which are known to be resistant to quantum attack. We'll also look at one other method which uses a trusted third-party to negotiate symmetric keys using existing protocols.

Post-quantum Algorithms

Post-quantum algorithms (or sometimes called post-quantum or quantum-resistant cryptography) covers a wide range of techniques, some of which were first discovered decades ago, which use the same principles as existing asymmetric methods but implemented in ways that are designed to make it harder for quantum computers to attack them.

In 2018, NIST opened a competition to narrow the field of potential algorithms by exposing them to public scrutiny and peer review[7]. Sixty-nine algorithms were submitted in the first round, which has now reduced to seven finalists (with eight alternates) in the third round.

The algorithms share many aspects despite differing greatly in their implementation details. We'll examine some of the key challenges faced in their deployment, focussing on the algorithms submitted in the NIST competition since they are the most likely to reach international standardization.

Software-based encryption

Like almost all cryptography today, PQA is software based. This means it can be implemented without specialist hardware. This applies particularly where the algorithm is used only as a key encapsulation method, since the underlying data encryption can take place exactly as it did before once the symmetric key is unwrapped. While this makes it more likely for a PQA to be compatible with existing

[7] National Information of Standards and Technology. (2021, March). Post-Quantum Cryptography. U.S. Department of Commerce. https://csrc.nist.gov/projects/post-quantum-cryptography

cryptographic software, in practice it's extremely unlikely that one would be a drop-in replacement for an algorithm like Diffie-Hellman. NIST itself recognises that there are multiple candidate classes for post-quantum cryptographic algorithms, but each class has at least one requirement for secure implementation that makes drop-in replacement unsuitable[3].

Enterprise-grade cryptography often does use specialist hardware to perform encryption. This makes the process much faster since chips can be specifically designed with particular algorithms in mind. It's also safer since information about the implementation can be stored in hardware, preventing theft if the encryption device became physically compromised. These devices would need to be upgraded or replaced to work with PQC.

Not provably secure

There are very few encryption algorithms that can be proven to be completely secure, meaning that we don't know whether at some point in the future we'll discover a way to break them. This doesn't necessarily render them useless since we can still have a degree of certainty that an algorithm is safe, until that is, it becomes know that an attack algorithm has been written which successfully compromises it's mathematical construction.

This is especially true of algorithms which are in their infancy as sometimes issues only become apparent after years of exposure to the cryptographic community and to financially or scientifically motivated hackers. This is also evidenced by the NIST competition itself, where many of the algorithms have already undergone several iterations as small flaws are found in their implementation.

Since our understanding of quantum information science is developing it is reasonable to assume that new quantum computing algorithms will appear which can break some PQA methods. It is thus a misnomer to refer to any PQA as "quantum safe", but in finding solutions to the problem NIST can only use what is presented to it in public.

Rate of adoption

It took nearly two decades for us to deploy public key infrastructure. The April 2021 NIST cybersecurity whitepaper states "experience has shown that, inthe best case, 5 to 15 or more years following the publication of cryptographic standards will elapse before a full implementation of those standards is completed"[3]. The replacement of algorithms generally requires changing or replacing cryptographic libraries, implementing validation tools, developing hardware that implements or accelerates algorithm performance, modifying dependent operating system and application code, changing communications devices and protocols, and user and administrative procedures. Security standards, procedures, and best practice documentation also needs to be changed or replaced, as do installation, configuration, and administration processes and documentation. And this work only begins once a candidate is chosen, which may take another 2–4 years."

Hardware requirements

Despite individual differences among candidates, all PQA has greater hardware requirements than existing methods. This is due to two factors: larger key sizes, and more complex algorithms. Different PQA candidates trade these off to different degrees, but broadly all of the candidates will take longer to process and require more memory and bandwidth to use.

This might not seem like an issue at first glance because generally compute power, memory, and bandwidth are increasing each year. However, this overlooks the proliferation of small, low-power, IoT devices in networks. The increased hardware requirements for PQA poses a real challenge for these devices which in some cases are designed to be deployed once and never refurbished, meaning that their components may need to last for years.

Summary

PQA offers the same advantages as existing asymmetric algorithms, but with additional resistance against quantum attack – until compromised. However, they bring significant

problems, particularly their computational complexity and the disruption of an initial replacement cycle and the possibility of an emergency replacement cycle if a quantum attack becomes known.

Symmetric keys with quantum key distribution

Another way to create a pair of symmetric keys between two parties (traditionally called Alice and Bob) is by using quantum key distribution (QKD). This is a fundamentally different approach to key sharing using PQA. Rather than hiding the symmetric key behind difficult mathematics, the key is shared in the open using quantum bits – i.e. by encoding data into the quantum mechanical properties, like polarisation, of individual particles. The security of QKD in general relies on two fundamental physical laws that emerge from quantum physics[8].

No-cloning theorem. This states that it's impossible to perfectly copy quantum information, for example the information encoded within the properties of a photon, meaning that an eavesdropper can't just make a copy of the information as it passes between Alice and Bob. This rules out "Man-in-the-Middle" attacks.

Heisenberg's uncertainty principle. Roughly speaking, this states that making a measurement of a quantum state necessarily perturbs the state. If an eavesdropper tries to measure the information passing through the channel they perturb the information, and this perturbation can be detected by Alice and Bob.

Together, these principles ensure that Alice and Bob can detect anyone eavesdropping on their communication and be certain that only they have the final shared symmetric key. Alice and Bob can then proceed with standard symmetric key encryption.

The first practical QKD concept was proposed in 1984 with the QKD algorithm called BB84. We won't explain the full protocol here as there are many very good explanations elsewhere[9]. However, in summary, information about the key is encoded onto fundamental physical particles (usually in the form of individual packets of light called photons) and sent through a channel from Alice to Bob (such as an optical fibre or a satellite link). Since quantum information cannot survive transmission by fibre at distances exceeding around 400km (with 2021 technology its less than 150km), the only way to transmit keys at large distance is to use satellites.

However, BB84 by satellite has one overwhelming flaw. In order to transmit the same key to Alice and to Bob by satellite, the satellite must first send a key to Alice, agree the key with her then store the key until it is geo-located over Bob and send it to him. This means that the satellite is a "trusted node" – i.e. if a mal actor were able to gain access to the satellite payload he could steal the key. Thus, the security advantages of BB84 quantum transmission are rendered largely pointless by this trusted node status.

The E-91 protocol addressed that Trusted Node problem. It uses entangled photons to establish a shared key between Alice and Bob. The entangled states are perfectly correlated. This means that if Alice and Bob both measure the polarisations of the individual photons they receive from each pair, they always get the same answer with 100% probability. This correlation is only maintained as long as there is no interference from an eavesdropper in the process. Any attempt at eavesdropping by Eve destroys these correlations in a way that Alice and Bob can detect.

In practice the requirement to distribute entangled photons to separate parties compounds the losses experienced in the quantum channel. This substantially reduces key rates. But the main penalty for the use of E91 is that whilst the trusted node problem is solved, Alice and Bob must be in simultaneous line of sight of a satellite. Given the high loss rate, only a very low earth orbiting satellite is feasible, and this means that Alice and Bob cannot be more than several hundred kilometres apart.

---

[8]There are schemes that use an additional quantum property called entanglement to derive their security. While the physical mechanism is different, the outcome is the same. Therefore, for simplicity in this paper we'll focus on BB84-style protocols.

[9] ETSI Industry Specification Group on QKD. (2015). Quantum Safe Cryptography and Security [White paper]. ETSI. https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

Thus, the two main protocols for satellite QKD are either trustless, or global, but cannot be both. This makes them both impractical.

Arqit invented a new protocol called ARQ19 which solves these problems, and also facilitates high throughput of key distribution, and the ability of groups of counterparties to create keys. Thus, the Arqit version of Satellite QKD IS practical.

Symmetric key exchange with a third-party

Both PQA and QKD offer the means to create shared symmetric keys on pairs of devices, whilst offering different levels of assurance against the quantum threat. One other method uses a trusted third-party to aid devices in negotiating keys.

The most familiar protocol of this type is Kerberos[10], which consists of a centralised key distribution centre (KDC) that each device communicates and authenticates with. If a client wants to talk to a server it requests a ticket from the KDC. The ticket contains an encrypted symmetric key that the client can use to communicate with the server.

This depends on the KDC being able to establish its own secure connection with each device on the network. This can be accomplished using pre-shared keys manually injected into each device on the network. This is more feasible than it would be without the KDC because now each device only needs to share a key with the KDC, rather than with every other device on the network. This dramatically reduces the number of pre-shared keys required for large networks. Device authentication is provided by the KDC since each device must authenticate with it.

In practice the KDC is a weak link, meaning that if it were compromised it would be possible to eavesdrop on all traffic in the network and impersonate any user. Kerberos has also been hacked many times and there are several known vulnerabilities that have to be worked around.

Despite this, Kerberos is still widely used today, in particular for authentication in both Microsoft Windows and Apple macOS operating systems, as well as Linux and other UNIX variants.

QuantumCloud™ from Arqit

Is there a way to combine these different approaches into a single solution?

Arqit offers an ARQ19 QKD solution to some of its customers, mainly data centre operators, telcos and government customers for whom unconditional and provable security guaranteed by the laws of physics are required for certain mission critical uses cases.

But Arqit also created a second domain of ground-breaking innovation. QuantumCloud™ is a cloud-based solution available to any device that is connected over a network. It enables us to deliver substantially all of the benefits of provable security to any device, using encryption methods which rely on ARQ19 in the core, but extend digital keys to any form of device on any form of network.

QuantumCloud™ is composed of a group of nodes distributed globally, each of which acts as a local exchange for devices to authenticate and negotiate keys with other devices on the network. Communication with the node happens over API calls, either called directly from the device or through the QuantumCloud™ SDK. Each node is connected with other nodes in the network using quantum-secure symmetric keys. By using a fully symmetric key infrastructure, QuantumCloud™ protects data today and into the future.

When a device first registers with QuantumCloud™ it uses a secure pre-shared key that was created on device registration using a patented Arqit technique. Once devices are registered and authenticated with QuantumCloud™ they can access its services, such as creating a shared symmetric key with another device on the network or taking part in a group key session. The network traffic between devices happens directly over a network, e.g. using TCP/IP, and the final keys used in that communication aren't known to QuantumCloud™.

With Arqit, customers now have an alternative to increasingly problematic legacy PKI, which is also secure against quantum attack in future, without the uncertainty and complexity of the unsatisfactory and unpredictable developments of PQA. Symmetric

[10] Kerberos does not preclude the use of asymmetric cryptography, but it's not a requirement of the protocol.

key encryption is already well understood, simple, and incorporated into most networking software systems which greatly minimises the disruption of moving to QuantumCloud™.

Given the threats and opportunities described above, all organisations can start making a plan today, regardless of which solution is eventually implemented. QuantumCloud™ provides advantages in security and simplicity over PKI today, with security from quantum attack built in.

Conclusion

Arqit is only just beginning to educate the market about its inventions, having innovated in secret since 2017. We will gradually release more information, but for the moment, the deep detail is reserved for customers. If you are concerned that legacy PKI is letting you down, and that PQAs do not represent a viable pathway to security against the quantum threat, get in touch.