Arqit Myth Busters

Since Arqit was founded in 2017, we have seen quantum technologies move from scientific research to commercial applications at scale.

The science behind quantum-enabled services in computing, communications, security, sensing and timing is complex and not easily understood by the non-expert. Quantum technologies have potentially broad applications and use. There are a great variety of processes (although those in cyber security are advancing quite quickly out of necessity) and the taxonomy of language used is scattered and inconsistent (e.g. "Quantum Safe"). As a global leader in post quantum cryptography, Arqit is uniquely positioned to bring clarity for anyone coming new to the subject and to bust some of the common myths around quantum technology. Of course, the problem statement is not only about quantum computing. Public Key cryptography has been compromised many times and is no longer fit for the purpose. Neither is it able to keep secure the surge of internet of things (IoT). But this paper mainly concerns itself with the quantum threat.

First, some explanation of terminology.

In cryptography, the community generally uses the phrases Quantum Resistant, Quantum Safe, Provably Secure, Quantum Weakened and Quantum Broken.

Here we define what "Provably Secure" means to us

"Provably Secure" refers to a key distribution process or encryption technique for which there exists a recognised mathematical or physical proof demonstrating that either:

An attack by an adversary with computationally unbounded quantum or other computing resources on a cryptographic algorithm would be unsuccessful at breaking the encryption regardless of any unknown future advances in attack algorithms.

An attack by an adversary on the key distribution process would alert those authorised to share the key that an attack was taking place.

We encapsulate this in the following diagram.

Descending Degrees of Quantum Safety

Provably Secure

- One-time pad
- Universal 2 Hash
- Symmetric Encryption

Quantum Resistant

- Post-quantum algorithms (e.g. NTRU, R-LWE, McEliece)

Quantum Broken

- All protocols that require use of RSA, Diffie-Hellman, ECDH. E.g TLS

Terminology

Quantum Domain

Refers only to information which is travelling in quantum form, i.e. in the quantum mechanical polarisation properties of photons.

Quantum Safe

An algorithm that provides a permanent level of security against an adversary with access to a quantum computer.

Quantum resistant

A problem for which it is believed that, given a universal quantum computer, no efficient algorithm currently exists for solving instances of the problem, but the existence of such algorithms cannot be ruled out. The non-existence of such algorithms is required to be a conjecture. Quantum-resistant constructions include post-quantum cryptography protocols and common symmetric algorithms, but do not include problems for which the existence of such algorithms can be ruled out, such as information-theoretically secure problems.

Provably Secure

Refers to a key distribution process or encryption technique for which there exists a recognised mathematical or physical proof demonstrating that either:

1. An attack by an adversary with computationally unbounded quantum or other computing resources on a cryptographic algorithm would always be unsuccessful at breaking the encryption regardless of any unknown future advances in algorithms.

2. An attack by an adversary on the key distribution process would alert those authorised to share the key that an attack was taking place.

Quantum Weakened & Quantum Broken

An algorithm is quantum weakened if, in order to guarantee this level of security against an adversary that has a quantum computer, the necessary increase in key length is deemed acceptable (in terms of the consequential computational cost). If the necessary increase in key length is unacceptably high, we say that the algorithm is quantum broken.

Post quantum algorithm (PQA)

A PQA is an algorithm which is quantum resistant, i.e., believed to defy efficient solution by any existing quantum algorithm, but which no proof is known to guarantee this.

"Quantum Safe" is a very high bar which hardly anyone who uses the phrase manages to achieve. Always ask the question: Could an actor with a Universal Quantum Computer and a mind like Peter Shor's potentially crack this algorithm? The day that an adversary breaks your mathematical algorithm, you won't know until it's too late, and it will happen"

David Williams - Founder, Arqit.

Myth 1.

The quantum threat is years away so I don't need to worry

Until quite recently, quantum computing was considered a threat on the distant horizon, due to the challenges in developing such advanced technology. We look at timelines below.

Quantum computers don't have to be operational for there to be a threat. 'Harvest now, decrypt later' attacks mean malicious actors are harvesting large quantities of encrypted data today, which can then be decrypted once quantum computers are developed. Importantly, TLS/SSL which is used to encrypt most data transmissions between software applications, may include recognisable identity data in plain text which would allow an adversary to "zero-in" on the traffic they want to attack.

For this reason, security against quantum computing needs to be deployed even before quantum computers become powerful enough to break public encryption.

The lifecycle of data means storage times for encrypted data need to be considered and re-encryption is required to preserve the security and confidentiality of data.

Shor's algorithm (the threat to public key cryptography) succeeds using polynomial time and resources.

Polynomial time is the ultimate goal of cryptanalysis because it means that key sizes simply cannot scale at a rate to keep ahead of the attack. The tongue-in-cheek design "post-quantum RSA" estimated key sizes of one Terabyte would be needed to be secure against a quantum threat. These keys required roughly four days to generate and the encryption process took about 100 hours. Worse still, if the technology behind quantum computers grows at a rate commensurate with the growth rate of classical computers, the byte length of these keys would have to increase by over 12% each year. This is not a feasible approach.

Any organisation with an obligation or duty to keep data safe for five years or more should consider themselves to be in breach of that duty by virtue of the Quantum Harvest Now, Decrypt Later exploit.

When we started Arqit in February 2017, most commentators on quantum computing were drawn from academic and government scientific circles. The consensus then was that universal quantum computing would not be viable until around the 2040s. We disagreed and bet that it would happen by 2027. The commentators back then were not wrong, they just used the wrong assumptions. They assumed a slower pace of innovation based on the limited resources available for research. In October 2017 the Government of China invested $10bn in Pan Jianwei's quantum technology research laboratory at the University of Science and Technology in Hefie, a 92-acre campus. This served as a catalyst for the expansion of the efforts of others in the commercial and state sector. The acceleration of research into raw technology and its applications, especially in fields like error correction has greatly compressed the timetable to make a wide variety of quantum technologies viable. For more detail on this see the **Arqit paper on Quantum Speedup**.

The acceleration in the development of quantum technologies is evident as more money is invested across a wide range of projects.

Recent announcements show we are nearer to universal quantum computing than many previously thought.

Google announced it had built a quantum computer last year that could shave 10,000 years off the computational time of the fastest classical computers.

Amazon soon followed with an announcement of its own.

China made its own "quantum supremacy" statement using a very different system to the big US tech companies (photonic-based computation).

PsiQuantum and more recently CEA have spoken about bringing semiconductor-based quantum computing to market within five years.

Some experts caution that a secret "Manhattan project" level of effort could be even further ahead than the recent public successes.

The engineering of the "quantum supremacy" projects and their growing physical qubit numbers are not the only way in which full scale quantum computing is being brought closer:

- Improvements in the lifetime and fidelity of qubits increases the ratio of logical to physical qubits leading to fewer physical qubits needed for a fully capable computer.
- Advances in quantum error correction also mean the timetable is accelerating for similar reasons.
- Algorithmic improvements in the cryptanalytic algorithms that break public key cryptography similarly cause estimates of the time to a cryptanalytically relevant quantum computer to reduce.
- In April the U.S. Department of Defense's outgoing chief data officer, David Spirk called for the Pentagon to make urgent investments to defend against potential espionage from quantum computers, stating that that the Pentagon needs to speed up efforts to counter adversaries who are developing quantum computing tech. He said "I don't think that there's enough senior leaders getting their heads around the implications of quantum. Like AI, I think that's a new wave of compute that when it arrives is going to be a pretty shocking moment to industry and government alike. We have to pick up pace because we have competitors who are also attempting to accelerate."

"How good is your crystal ball into the future? Cryptography is the foundation of the Internet's security, underpinning all authentication, integrity, and confidentiality. Would you bet the safety, continuity, and profitability of your businesses, critical infrastructures, and government services on your crystal ball being able to predict, not just if, but when an operationally viable quantum computer is being turned on by a deep-pocketed APT? I wouldn't."

Phil Quade, COO Evolution Equity and former Chief of the NSA Cyber Task Force

---

"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. We need to determine where, why, and with what priority vulnerable public-key algorithms will need to be replaced, and we need to understand the constraints that apply to specific use cases. These initial steps in developing and implementing algorithm migration playbooks can and should begin immediately."

NIST, Getting Ready for Post-Quantum Cryptography, April 2021

Myth 2.

Quantum key distribution can secure the Internet

Arqit does not sell QKD because, as agencies like NSA and NCSC have observed, it is presently neither practical nor secure at scale. QKD cannot provide a useful service beyond some niche use cases. Arqit learned this in 2017 and so developed a hybrid model combining quantum effects with new cryptographic protocols based not on mathematical hardness but on secret sharing.

Scientists have demonstrated that QKD works over fibre optic cable telecoms infrastructure in certain conditions. Whilst there are certain narrow use cases for fibre QKD, it is unlikely to be universally used within our lifetime to encrypt mass market internet transmissions due to significant technological and economic limitations. To send a key via a quantum channel, a single-photon laser beams a signal, one photon at a time, via a fibre optic cable. This method is slower than current telecommunication technologies and requires a dedicated fibre optic cable between the two parties.

For example, Amazon could not secure customer transactions using quantum encryption because it would require dedicated cables between its servers and individual mobile devices that make purchases. Distance is also a factor, with current fibre struggling to move single photons reliably and at usable data rates over more than 100 miles. The longest distance so far achieved was an experiment claiming transmission of single photons at 600km - but that was achieved at a data rate of eight bits per second ("bits" – not even "kilobits") and in lab conditions that could not be replicated in the real world. This data rate is a very long way from being of any use.

When fibre optic cables are used to transmit data, as in your home internet and cable systems, they use repeaters to send the data over longer distances.

However, those repeaters disturb the delicate quantum state that is crucial to QKD, and so current repeaters act exactly like a man-in-the-middle attack on the quantum transmission. Thus, the quantum states must be decoded to digital at classical computing devices at the termination point of each cable, then re-encoded to quantum for the next leg. These devices are generally classified as "Trusted Nodes" – meaning that there is no benefit of quantum mechanics in them, they are just ordinary computers containing ordinary bits and can therefore be attacked in a classical way. Thus, long distance quantum encryption via fibre does not have Provable Security.

There is currently no physical way to **'trustlessly'** relay the information across multiple links. A quantum repeater would be required to do this. It would have to recognise the quantum states transmitted from the A end when they reach the B end and instantly transfer those states to new quantum particles from transmission form B to C. These devices do operate at tiny scale at present – for example it is possible to hold quantum states in memory under lab conditions for microseconds in very small data rates transmitted at sub-micron distances. But to scale this up for quantum transmission for hundreds of kilometres and with data rates in the Mb per second is likely many decades away, if it is possible at all.

Fibre Based QKD can secure transmission across single fibre spurs. There are some narrow use cases for this in certain Critical National Infrastructures, but presently trust-free long-distance fibre QKD is not viable.

Furthermore, it is difficult to imagine QKD as a technique having application in end-to-end communications. Even if we accepted the use either of trusted nodes or quantum repeaters at every network aggregation point (which seems either prohibitively expensive or farfetched) there is still a problem of addressability. Photonic transmission has a point-to-point topology. Photons are not IP addressable so we cannot tell photons to travel across a network path of its own choosing and find their way to a desired end point. That is the biggest barrier of all in creating a quantum photonic internet. Satellite QKD does not solve these problems. In Satellite QKD, there is one additional major problem and several secondary problems. In the previously known protocols, there were two ways of delivering QKD.

First, using a protocol called E91/2, which relies upon a satellite flying in low earth orbit at approximately 700 kilometres, entangling two photons and transmitting them to the 'a' and 'b' point. The satellite doesn't need to remember the photonic information in its quantum form; the information is delivered in quantum form to the 'a' and 'b' point and therefore the transmission is quantum-safe, and the satellite does not need to remember the information.

However, because the satellite must be in low earth orbit to deliver sufficient information to the 'a' and 'b' point, basic geometry determines that the 'a' and 'b' point cannot be separated physically by distances greater than approximately 700 kilometres, largely because of the curvature of the earth. Therefore, in this entanglement protocol, QKD can be delivered in a quantum-safe way, but it can't be delivered at distance. This renders it impractical in the modern style as switched IP networking. Furthermore, entanglement protocols have extraordinarily high loss rates because of the requirement to deliver the same information to 'a' and 'b'; 'a' and 'b' both achieve different losses of different particles and securing an identical set of information at both the 'a' and 'b' end renders the aggregate loss of the system much greater. Therefore, entanglement protocols are also very impractical for sending reasonably high volumes of key data.

The second protocol, the "prepare-and-measure protocol" or BB84, attempts to overcome this distance problem but in doing so, renders the satellite a trusted node. The satellite delivers key information to the 'a' point, it undergoes a key agreement process with the 'a' point, where 'a' and the satellite called 'c', now agree and know a key. 'C' remembers the key during its overpass in low earth orbit until it is geolocated over the 'b' point ('a' could be in London and 'b' could be in Sydney).

At this point, the satellite 'c' point, delivers that key information to 'b' and 'b' and 'a' now have the same key. Thus, the key delivery is done on a global basis. However, the satellite, the 'c' point, has remembered the key during its overpass. It is, therefore, a trusted node. It is a classical computer remembering the key in classical, digital ones and zeros and therefore a malicious actor can hack this computer and would know the key. Whereas the transmission of quantum information from the 'c' point to both 'a' and 'b' benefits from information theoretic security of the quantum states, the satellite as a trusted node, renders the expense and the difficulty of establishing the quantum infrastructure pointless. The end-to-end system is not quantum-safe and can be hacked.

QKD does not solve the problem, Arqit agrees with agencies such as NCSC and NSA that QKD is not a suitable technology for large scale secure and efficient encryption. As mentioned, Arqit does not sell QKD, it sells a symmetric key agreement software platform.

"Arqit agrees with NCSC and NSA - there is presently no viable mass market technology within the field of fibre or satellite QKD for addressing quantum information point to point with zero trust operation or usable efficiency. The world does not want to rip up all its infrastructures to replace them with something else which does not deliver any real improvement. It wants software which is easily integrated into the current infrastructures. That's why Arqit does not do QKD and why we invented the QuantumCloudTM software platform to deliver a symmetric key agreement service with light weight software that works at any endpoint."

Dr Barry Childe, *CIO, Arqit Quantum Inc*

ARQIT

Myth 3.

Post-quantum algorithms (PQA) are a good way to secure the 21st century Internet

When understanding about the imminence of Quantum threat began to grow, it was important that the world started to figure out an alternative. A year after we founded Arqit, the US Department of Commerce National Institute of Standards and Technology (NIST) began a process, through competition, to find the best way to protect data from the quantum threat. One might say that the answer was already there. Modern symmetric encryption has been used for decades and is known to be quantum safe. But at that point no one felt that there was a way, using QKD or any other technique to create zero trust symmetric keys at end points. No-one could have predicted the creation of the Arqit hybrid tech stack in 2018. So NIST has been doing important and necessary work to the best of its ability but, by its own admission, the project has not been a complete success. There are some use cases for PQAs that are rational, but comprehensive adoption for all encryption uses cases looks unlikely.

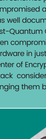
"Unfortunately, the implementation of post-quantum public-key standards is likely to be more problematic than the introduction of new classical cryptographic algorithms. In the absence of significant implementation planning, it may be decades before the community replaces most of the vulnerable public-key systems currently in use."

NIST, Getting Ready for Post-Quantum Cryptography, April 2021

The most obvious problems are summarised below, and well detailed here by NIST itself in April 2021

Getting Ready for Post-Quantum Cryptography

a. PQAs will take a decade to implement. Historically, it has taken about two decades to deploy modern public key cryptography infrastructure and, according to NIST, the process of testing and adopting a new algorithm, like PQAs, could take an additional 10 or more years. Arqit is not opinionated about encryption algorithms. AES 128 or 259 happen to work perfectly now; others may arise in future and Arqit is happy for its key agreement platform to be used in any algorithm. But the world needs to adopt a viable solution today, not in ten years' time.



"There is insufficient maturity in our understanding of PQAs to have confidence that they will solve any of the problems facing us. However, there are good ways to encrypt data using very standard and provably secure symmetric encryption methods, and a novel way to create the keys locally is a really big step forward for the world which does offer a solution now."

Dr Taher Elgamal, *Marconi Prize Winner "The Father of SSL"*

b. After four years of competition, there is no single algorithm which has even been deemed to be a least-bad option for universal adoption, let alone quantum safe.

"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"

NIST, Getting Ready for Post-Quantum Cryptography, April 2021

c. PQAs are not Provably Secure. Any algorithm that relies on mathematical systems is in danger of eventually being compromised by a quantum or classical attack. It's inevitable the security of these systems will degrade as the understanding of algorithms matures. Government and banking users place the greatest faith in the globally standardised AES-256 algorithm to find a way to securely distribute their keys. The assessed security of AES is essentially unchanged after over 20 years of cryptanalysis. By contrast, the candidates in the NIST PQA process are constantly re-evaluating their security as novel ideas are presented. Furthermore, the novel ideas are purely classical and little effort has been made to consider quantum attacks on these systems. For this reason, NIST, wisely, does NOT use the phrase "Quantum Safe" and anyone who does, in describing PQAs should be treated with caution.

No so-called Post Quantum Algorithm, which constructs keys through the operation of multiparty algorithmic mathematical computation can ever pass the Provably Secure test. It's indisputable that a well-motivated actor with a quantum computer and sufficient mathematical processing skills may be able to break any PQA. The next Peter Shor is already out there working on it. In fact – to explain the fallibility of PQAs most simply, several such schemes proposed have already been broken. Publicly, The Campbell-Groves-Sheppard attack compromised a variety of "lattice based", "fully homomorphic" and "multilinear map" encryption schemes and was well documented here in 2015. One of the three finalist signature schemes shortlisted by the NIST Post-Quantum Cryptography Standardisation project, called Rainbow was revealed in February 2022 to have been compromised, not in theory by a future quantum computer but in practice using basic computing hardware in just a weekend by an IBM researcher. In April 2022, a new analysis by the Israeli Defence Force Center of Encryption and Information Security (MATZOV) suggested that improvements to the dual lattice attack considerably reduces the security levels of Kyber, Saber and Dilithium, the LWE/LWR based finalists, bringing them below the thresholds defined by NIST.

"We need to maintain defence and industrial secrets – such as government classified information, designs and code, and personal data such as DNA secure for a lifetime – 80 years used to be the test in government. We don't even know if PQAs will keep them safe for 5 years."

Air-Vice Marshal Peter "Rocky" Rochelle, *former Chief of Staff Capability, Royal Air Force*

d. PQAs will have huge key sizes. For example, a paper by one promoter uses Falcon with level 1 NIST security (which is AES-128 equivalent), by creating a signature size of 5328 bits with a public key size of 7176 bits. However, this is not sufficient for many applications that require level 5 NIST security (which is AES-256 equivalent). The problem here, however, is that using level 5 NIST security doubles the size of the keys and almost doubles the size of the signatures. The bandwidth required by these methods is a poor fit for the modern internet and as a result, protocol designers are looking for ways to minimise the use of such cryptography.

"These PQA schemes will not work with small IoT devices and it is questionable if they are suitable for 5G. Never in the history of ICT have we willingly accepted such vast increase in latency and processing cycles as is contemplated by the deployment of PQAs. To do so without even achieving the desired level of security for all devices seems unwise."

Toby Redshaw, *Former SVP Innovation, Verizon, and Global Chief Information Officer American Express*

e. PQAs require a massive amount of processing. The additional processing power required to properly execute a post quantum signature algorithm has been demonstrated in several papers as being very significant. Creating a Crystal-KYBER encryption with the equivalent (claimed) key strength of AES-256, for example, would consume 1,732,000 cycles compared to 1164 cycles for AES!

See the paper **"Assessment of Quantum Threat To Bitcoin and Derived Cryptocurrencies"** by Professor Liqun Chen and Stephen Holmes of University of Surrey.

f. PQAs require a deep understanding of the complex mathematics involved to implement safely. Public Key Infrastructure (PKI) has been broken many times in the past due to mistakes in the implementation. This is because software developers can't be expected to understand the nuanced university-research-level mathematics that makes it safe. We expect no difference with implementations of PQAs. In particular, digital signatures using lattice algorithms need to be used very carefully to avoid leaking information about the private key. The knowledge of what this entails is held by a very small number of researchers.

g. Post-quantum cryptography can be broken. There are two types of security notions that we use to show that protocols are secure: complexity theoretic security and information theoretic security. Information theoretic is a very strong notion of security. On the other hand, complexity theoretic security is much weaker, and typically results in statements of the form "My new problem is as hard as this well-studied old problem".

PQAs are all based on complexity theoretic security statements. The security of post-quantum comes from showing that breaking the encryption is as hard as solving a particular mathematical computation. The computation is believed to become very hard as the size of the numbers involved grows. However, there is no concrete understanding of exactly how hard that makes the specific instances of the cryptography being proposed.

The security of the designs is being constantly reassessed and lowered in light of new ideas. When the designers speak of the schemes meeting a certain level of security, they mean the amount of work required by the best attack that is currently known. Worse yet, almost all the analysis focuses on classical attacks with few researchers able to grasp the possibilities offered by quantum computation. By contrast, the information-theoretic security of one-time pads, symmetric encryption keys and quantum communications provide guarantees of the work required by all possible attacks, whether currently specified or not.

"There are many reasons why the PQAs in the NIST Standardization project are not suitable, but the immature understanding of their security is the most concerning".

Dr Daniel Shiu, *Former Head of Cryptographic Design and Quantum Information Processing, GCHQ*

ARQIT

Myth 4.

Quantum random number generation solves the problem

Although there have been many instances of security failures through weak random number generation, good physical solutions already exist for generating random numbers. Random numbers generated from existing good processes are no easier for a quantum computer to recover than random numbers generated by quantum methods.

To be clear, **quantum random number generators** can produce very good quality random numbers and this quality can potentially be tested using the laws of quantum physics. It is important to have assurance on the quality of randomness in a system. But that is not at all difficult to do and there are many ways to achieve it.

However, the creation of random numbers is not the major cryptographic challenge of the quantum age; putting the same random number in two different places is. Prior to the creation of Arqit, it was impossible to securely put random numbers simultaneously in multiple locations. A quantum random number encapsulated within a post-quantum algorithm is just as weak and impractical as the PQA and therefore broadly pointless. Anyone promoting this as Quantum Safe is not using that phrase accurately.

"Too many people confuse random numbers with security. The creation of randomness is not particularly hard, and you don't need a quantum computer to do that. The zero-trust creation of randomness simultaneously at many end points is the holy grail of cyber security, and that is what Arqit's incredible international team achieved."

Daryl Burns, *Formerly Deputy Chief Scientific Advisor for National Security, UK Government and Chief of Research & Innovation, GCHQ*

Myth 5.

AES is not quantum-safe

AES and other symmetric algorithms are occasionally described as vulnerable to Grover's algorithm.

This is a very generic quantum algorithm for inverting arbitrary functions with fewer operations than a classical computer needs. However, Grover's algorithm does not parallelise at all well in comparison with classical methods. To run Grover's algorithm ten times as fast requires using one hundred times as many quantum computers. This means that although a powerful quantum computer might hope to break AES-128 in 700 years, to break it in a single year would take roughly half a million such quantum computers. This is not feasible.

One might ask whether a different quantum algorithm might perform better than Grover's algorithm. However, the excellent work by Zalka has shown that Grover's algorithm is optimal for solving questions of this sort, both in terms of number of operations and parallelism.

For reasons such as these, the NIST post-quantum cryptography project has declared AES to be the standard of security that other quantum-resistant algorithms should match. Even if quantum technology ever looks to be close to threatening AES-128, the much stronger AES-256 algorithm used by Arqit will be secure beyond any conceivable security timeframe. Moreover, AES-128 & AES-256 is already standardised in most networking software systems in the World. No major global co-ordinated software upgrade is required to use symmetric keys within AES256.

"Taking these mitigating factors into account, it is quite likely that Grover's algorithm will provide little or no advantage in attacking AES, and AES 128 will remain secure for decades to come."

NIST, *"To protect against the threat of quantum computers, should we double the key length for AES now? November 2018"*

"Arqit's biggest advantage is ease of use. It's one thing to have paradigm shifting tech. But customers must be able to easily buy and use it. Arqit's tech, remarkably, requires no major upgrade cycle. Rather than trying to re-invent the software that we all use every day, Arqit found a way to merely change the way keys are delivered into it and to serve customers with a SaaS model. This is one of the smartest pieces of innovation I have ever seen."

Dr. Alison Vincent, *Formerly Group Chief Information Security Officer HSBC & Chief Technology Officer Cisco*

Myth 6.

5G Is
Secure

5G is a cloud native SDN network and therefore the scale of edge computing is now rising exponentially.

This edge computing facilitates a dramatic improvement in service capability in areas like AI at the edge. However, the expansion of the edge also grows the cyber-attack surface and whilst 5G is more secure than 4G, it is a communications architected progression not a security anchored effort. There is nothing in the 5G specification about improving the security of data at rest or the infrastructure chain in this massive new edge compute cloud. This security weakness will be compounded by the explosion of IoT devices. 5G handles 1000x more sensors per unit area than 4G and this means that sensors become more capable and useful. Companies building sensor-based solutions are already realising that the very small flash memories built into such sensors are simply unable to run PQA's because of the high computational burden imposed by them. The growth in a new edge architecture expands the target space for cyber threats without a commensurate set of defences.

In all the excitement of ensuring 5G is deployed as quickly as possible for consumer use, some obvious holes have been left in the solution's security barriers. The fact that 5G can rely on such a wide variety of virtual networks and RAN partitions might make it faster and more efficient, but it also produces far more space for cyber criminals to target. As the number of components increases, so does the complexity of a network's supply chain. Complex supply chains provide an opportunity for experienced cyber criminals to exploit flaws left open by suppliers.

"The proliferation of edge computing and sensor networks both in civilian and military networks will generate astonishing gains in functionality as AI begins to process decisions in real time. But cyber security has been an afterthought. Without stronger, simpler encryption, these networks are all fatally compromised"

David Kumashiro, Former Director, National Security Commission on Artificial Intelligence

ARQIT

Myth 7.

Quantum computers can't hack cryptocurrencies

With a market cap of around $2 trillion, and regulatory and government involvement deepening, we can't ignore the impact of cryptocurrencies to the world economy or deny the possibility that blockchain technology could play an important role in many sectors in the future. In April 2022 the British government declared its intention to make the UK a hub for Digital Asset business.

While the blockchain aspect of most cryptocurrencies is what makes them so watertight against incursions, we are seeing a massive increase in crypto theft already happening and there are several vulnerability points, even without quantum computers' (QC) advanced decryption techniques. Broken down very simply, the asymmetric cryptography (one public and one private key) most crypto systems use is currently deemed impenetrable because it's simply mathematically nearly impossible to derive the private key in the exchange from the public key. Running Shor's algorithm on a quantum computer changes this. In the time it takes for an unprocessed transaction to be placed in a block in the chain (and it need only be milliseconds for a QC to 'break in') a quantum computer could break into the transaction. All blockchains using PKC are therefore quantum compromised.

"We cannot discount the possibility that malicious actors, sponsored by rogue organisations or criminal groups awash with ill-gotten gains from scams and ransomware attacks, can gain access to quantum computers to target blockchains within the next few years. Successful attacks will inevitably destroy all confidence in all blockchains and thus their value will fall to zero. All the custody and trading systems built to deal with digital assets will become worthless. A radical new approach to securing digital assets should therefore be a pre-requisite to any investment in such technology."

Mr Boon Hui Khoo, *Former INTERPOL President*

Myth 8.

Our national defence networks will not be threatened by quantum technology because they are ahead of the game

Several Arqit board members, former high-ranking military officers, now work for Arqit because they recognised that the defence apparatus in both the UK and the US needed to find private sector solutions to mitigate the quantum threat. Whilst it is true that defence institutions use symmetric keys widely already, they can't deliver these keys at scale or rotate them on demand or create them instantly with devices that have never been in contact before, three essential features in the future war theatre. The Military has its own "IoT" problem – called JADC2 (Joint All Domain Command and Control) in the USA and MDI (Multi Domain Integration) in the UK. There was no solution to the security layer problem of JADC2 before Arqit.

"Our job as senior leaders is NOT just to prepare and be ready for today's challenges but to anticipate and adapt to future challenges. As I look at the emerging technologies like AI, 5G, Blockchain, etc., I believe quantum computing has the potential to be the most transformative. Anyone ... from individuals to governments to businesses caught unprepared by a sudden quantum breakthrough will face enormous consequences."

General Stephen W. "Seve" Wilson, *Former Vice Chief of Staff of the US Air Force*

"Having had decades of involvement with security projects I am in no doubt that what Arqit offers is a set of capabilities of profound global significance."

Dr Geoffrey Taylor, *Former GCHQ Directorate Board member*

Arqit QuantumCloud™

We hope that you found this useful, and we are pleased to contribute to creating some common understanding of terminology and standardisation of thinking in this important but chaotic industry. But there is no free lunch, so a few words on why Arqit's QuantumCloud™ is so important, and why customers in Government, Defence, Telecoms and Financial services are concluding at scale that Arqit has the only answer to the quantum threat.

Who is Arqit?

A **pioneer and global leader** in quantum encryption.

UK headquartered, **NASDAQ listed** business with a market cap of **$2bn+.**

Category-defining technology protected by over **1,400 patent claims.**

World-leading team of **famous cryptographers** and engineers.

Blue-chip enterprise and government customers.

How the product works

Random numbers are distributed to data centres using a transformational new Quantum Satellite Protocol complemented by a novel terrestrial method.

QuantumCloud™ enables any device to download a lightweight software agent of less than 200 lines of code, which can create encryption keys in partnership with any other device – **from a mobile phone to a fighter jet.**

The keys are **computationally secure**, don't exist until the moment they are needed and **can never be known by a third party.**

QuantumCloud™ can create **limitless volumes of keys in limitless group sizes** and can regulate the secure entrance and exit of a device in a group.

QuantumCloud™ can be deployed as either a Private Instance or PaaS.

What problem do we solve?

- Legacy encryption is obsolete. PKI was designed decades ago.
- It was never intended to protect our hyper connected world.
- It has many vulnerabilities in its implementation for attackers to exploit.
- Quantum computers will soon compromise the mathematics at the heart of PKI.
- The world is being urged to create and adopt new protections.
- The efforts to make PKI more resistant to quantum attack are temporary, and pose grave problems in usability.

Leadership

David Williams
CEO & Founder
Former CEO & Co-Founder, Avanti plc. TMT Banker. Queens Award for Exports 2016

David Bestwick
CTO & Founder
Former CTO, Avanti plc. Marconi & Vega engineer. Astrophysicist. Royal Aeronautical Society medal winner

Nick Pointon
CFO
Former CFO, Privitar. Ex VP Finance, King Digital. KPMG ACA

Air Vice Marshal Rocky Rochelle CB
COO
Air Vice Marshal RAF Capability, highly decorated aviator & military leader

Dr Daniel Shiu
Chief Cryptographer
Former Head of Mathematics & National Technical Authority for Cryptographic Design & Quantum Information Processing, GCHQ

Dr Geoffrey Taylor, CB
Co-Founder, Adviser
Formerly 22 Years a Main Board Director at GCHQ. PhD in Quantum Molecular Dynamics

Daryl Burns
Inventor, Consultant
Former Chief of Research and Innovation, GCHQ and the Deputy Chief Scientific Advisor for National Security

Sir Iain Lobban
Adviser
Former Chief Executive, GCHQ

Dr Taher Elgamal
Director, Arqit Ltd
Inventor of SSL, Security CTO Sales Force, Operating Partner, Evolution Equity Partners

General VeraLinn Jamieson
Director, Arqit Inc
Former Deputy Chief of Staff for Intelligence, Surveillance, Reconnaissance, and Cyber Effects Operations, U.S. Air Force

Gen Seve Wilson
Director, Arqit Inc
Former four-star Vice Chief of Staff of the US Air Force. Retired 2020

David Webb
Chief Software Engineer
Former Engineering Director, McAfee UK Enterprise Data Protection

Patrick Willcocks
General Counsel
Solicitor and Barrister, former General Counsel Avanti plc, HP/EDS and banking lawyer

Paul Feenan
Chief Revenue Officer
Former Director, Jumo World and Avanti Government Services. British Army Officer who led the UK's Counter Terrorism Planning for 2012 Olympic Games

Dr Barry Childe
Chief Information officer
44 years' experience since winning the IBM prize aged 13 specialising in High Performance Computing

Manfredi Lefebvre d'Ovidio
Vice Chairman
Chairman of Heritage Group, and also Executive Chairman from 2001 to 2020 for Silversea Cruises.

Carlo Calabria
Non-Executive Director
Founder and Chairman of CMC Capital and Ex-Barclay's EMEA chairman of mergers and acquisitions.

Boon Hui Khoo
Adviser
Former Snr Deputy Secretary of Singapore's Home Affairs Ministry and Commissioner of Singapore Police. Ex-President of INTERPOL from 2008 to 2012.

Dr Alison Vincent
Adviser
Former Group CISO, HSBC & CTO, Cisco. PhD Cryptography. Fellow Royal Academy of Engineering

Scott Alexander
Chief Product Officer
Formerly a product strategist at Juniper, IBM and Nortel