



QUANTUM  
COMMUNICATIONS  
HUB

# Quantum-Safe Secure Communications

**Digital infrastructure permeates every sector and part of society. Cyber security refers to the protection of all this infrastructure – communications, remote connections, computing, IoT devices, etc. Current security is built on conventional cryptography. However, threats to current cryptographic techniques created by major advances in quantum computing are widely acknowledged as both real and forthcoming. Although quantum computers large enough to undertake hacking do not yet exist, retrospective decryption is a very real threat and critical data requiring long-term security should be protected now. Information which is encrypted with current cryptographic techniques can be intercepted, stored and decrypted once large quantum computers arrive. There is a clear and urgent need to make all aspects of cyber security “quantum-safe” – that is safe in a future world where all forms of quantum technology exist, including large quantum computers. Quantum Communications Hub researchers are working to address this need.**


There are two forms of conventional cryptography: symmetric and asymmetric (the latter of which provides our current public-key infrastructure (PKI)). Both approaches utilise cryptographic keys at the transmitter (“Alice”) and receiver (“Bob”) ends of the communication, along with a known mathematical algorithm for Alice to encrypt the data with her key and Bob to decrypt it with his key. In symmetric cryptography, Alice and Bob use the same key, which has to be kept secret from everyone else if their information is to remain secure, so they also need a mechanism to securely share this key. Asymmetric cryptography uses pairs of keys: Alice uses a public key (“public” because it is not a secret and available to everybody) to encrypt the data, whereas Bob uses a private key (secret and known only to him) to decrypt. Current real-world internet and other communications often rely upon a combination of the two approaches: asymmetric PKI first, to establish shared secret keys that are then used symmetrically to secure the communications or transaction. This two stage approach is clearly essential if Alice and Bob have never corresponded before. The looming problem is that current asymmetric PKI will be vulnerable to attack from a large quantum computer.

This PKI has been built on so-called “one-way” mathematical functions, so it is easy to work out a public key from the corresponding private key, but essentially impossible (with conventional technology) to work out the private key given only the corresponding public key. However, it is now known that a sizeable quantum computer running a quantum algorithm devised by Peter Shor will be able to efficiently determine a private key from the corresponding public key. So, the days are numbered for current PKI, deployed worldwide.

Two major advances are being developed to counter this threat and to progress cyber security to being quantum-safe.

1. Quantum key distribution (QKD) enables Alice and Bob to generate shared symmetric keys, with the security of these keys underpinned physically because they were established from the communication of quantum light signals. QKD does need Alice and Bob to have some initial shared secret (or “seed” key material), to provide authentication. However, two very important features of QKD are that: as long as they have a suitable seed, Alice and Bob can grow as much new key material as they want; and this new key material is (quantum) random and so cannot be deduced from the seed by anyone else.
2. Quantum-resistant, or post-quantum cryptography (PQC), comprises new mathematical encryption techniques that are immune to attack by Shor’s algorithm and are thought to be resistant to other quantum algorithms that may be developed in the future. The National Institute of Standards and Technology (NIST) in the US is currently overseeing a worldwide process for the establishment of a suite of new PQC techniques, which will be made available for widespread use.

Clearly in order to address the vulnerability of current PKI and to do so in a flexible manner appropriate for the internet and mobile networks, it is essential to provide a quantum-safe solution for Alice and Bob who have never met, and to future proof this solution. A combination of PQC and QKD provides a very appealing solution. If Alice and Bob seed a QKD session with new, asymmetric PQC, the quantum keys they establish will remain secure even if the PQC were to be subsequently broken, by the emergence of a new quantum algorithm. So any secure transactions or communications reliant on these symmetric quantum keys will remain secure. With communications, the ultimate information-theoretic security can be achieved by using quantum keys in a one-time-pad arrangement.



For more economical use of the key material, Alice and Bob can use their quantum keys to drive a symmetric conventional encryption system such as the Advanced Encryption Standard (AES). Such symmetric encryption is more resistant to quantum computer attack than current PKI.

Quantum Communications Hub researchers are currently working on asymmetric PQC development and its hardware implementations. Work is also progressing on hybrid systems, integrating PQC with QKD for a future proof approach to quantum-safe communications. There is a clear need for this approach to handheld and consumer technologies, with many Alices, rather fewer Bobs and a high demand to seed new Alice—Bob pairings. So Hub “consumer QKD” technologies provide one direction for deployment of a quantum-safe hybrid approach. In addition, Hub investigators are also trialling the integration of PQC with quantum communications networks, to enable quantum-safe communications across longer distances via optical fibre.

**If you would like to hear more about the Hub’s work on QKD and PQC, please contact us via [enquiries@quantumcommshub.net](mailto:enquiries@quantumcommshub.net)**

*NB Post-Quantum Cryptography is also commonly known as quantum-proof, quantum-safe or quantum-resistant cryptography.*



**Engineering and  
Physical Sciences  
Research Council**