



QUANTUM
COMMUNICATIONS
HUB

Quantum Key Distribution

Modern society is becoming increasingly reliant on the security of transmitted information and communications. Data security is currently largely delivered through the use of cryptographic keys. So, the protection of sensitive information is ultimately determined by the security of these keys.

In conventional encryption, an algorithm is used to encrypt information, making it unintelligible to anyone who intercepts it during transit. The algorithm uses keys – long strings of random numbers – for the sender to encrypt and also for the intended receiver to decrypt the data. The encryption and decryption keys are identical for symmetric cryptography, but different for asymmetric cryptography on which all our current public key infrastructure (PKI) is built. This PKI is secure for now; however, advances in quantum computing pose a severe threat. It is widely accepted that, when these are built, sizeable quantum computers will be able to break all current PKI by running Shor's algorithm. Clearly, for information which is only required to be secure for a short time, this threat is just looming. However, for information which requires long-term security, the threat is real now. Sensitive information which is currently encrypted could be intercepted today, stored and then decrypted by suitable quantum computers when these become available. It follows then that new approaches to security are required, which are "quantum-safe" – that is safe in a future world where all forms of quantum technology exist.

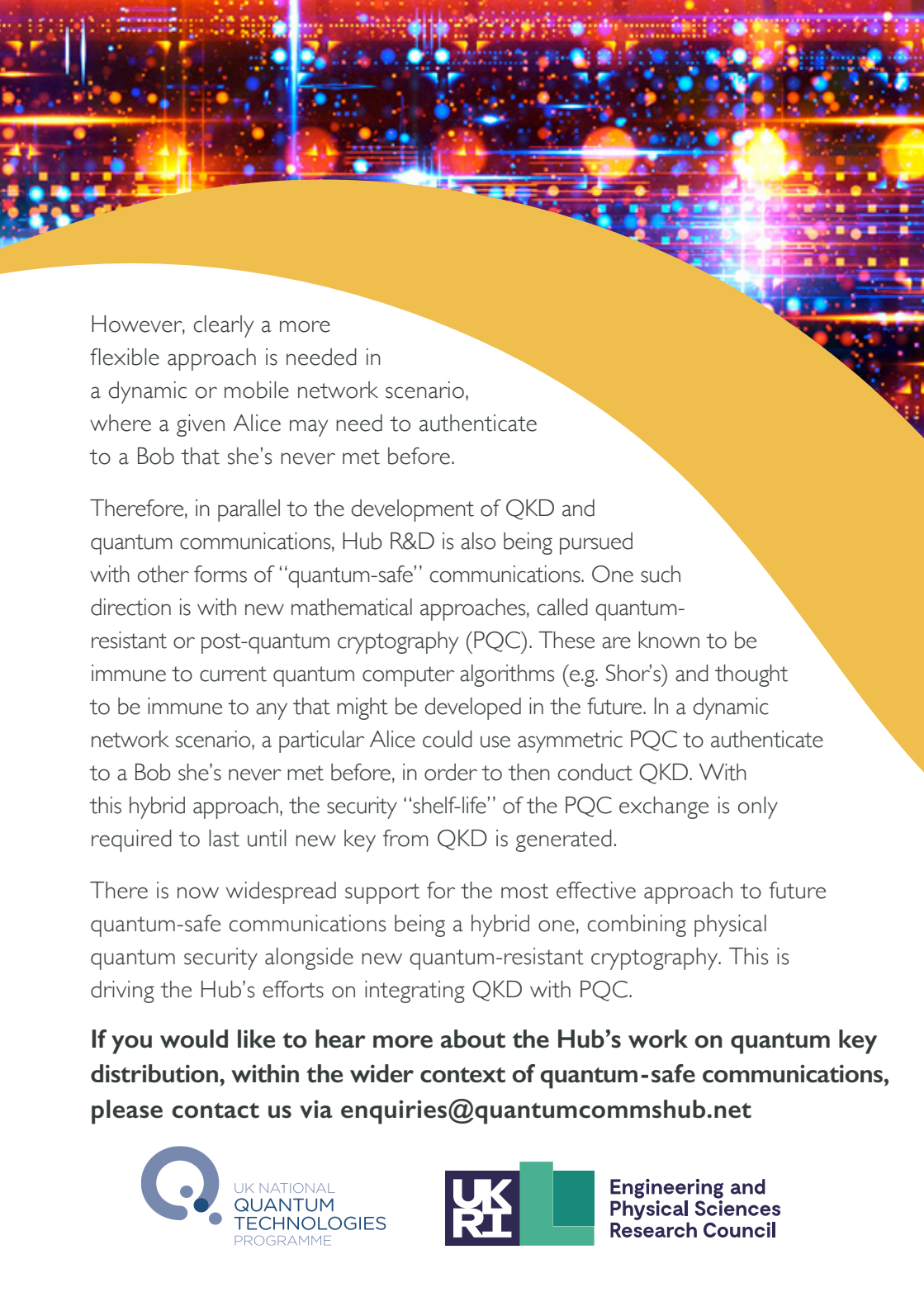
In order to utilise symmetric cryptography, the transmitter – usually described as "Alice" – and the receiver – usually described as "Bob" – use the same key which must be secret and known only to them. Therefore, the security of their subsequent communications is determined by the security of the key distribution mechanism. This is where the quantum technology comes in – it provides a quantum secure method of key distribution, or "quantum key distribution" (QKD) for short.

To share a key through QKD, the basic idea is that Alice transmits a long sequence of quantum light pulses to Bob. These may be sent down an optical fibre or through free space, whichever technology provides the best solution, but either way any adversary – usually called "Eve" – can only gain information on the transmitted light signals by measuring them in some way.

Quantum physics dictates that Eve cannot avoid introducing disturbance to some of these signals through her measurements, so she cannot avoid exposing her eavesdropping. Clearly, Bob also has to measure the quantum light signals that he receives in order to establish a key shared with Alice. Nevertheless, Alice and Bob can afterwards identify an intact subset of shared data to keep, which are those which Alice knows Bob will not have disturbed by his measurements. They can do this without exposing the actual data values, which are then used to create the key. Alice and Bob can locate and correct errors in the data that they keep, and then mathematically compress down to a final shared secret key. These subsequent communications do not have to be encrypted (although they could be) – the security of the final shared key is not compromised even if Eve overhears all this discussion.

Once Alice and Bob have shared secret key data, they can use this in a range of approaches. For secure communications the ultimate (information theoretically secure) protection would be through the use of one-time-pad encryption. A much more economical use of the keys is to drive a symmetric encryption system like the Advanced Encryption Standard (AES) – this approach is compatible with current high-speed telecommunications infrastructure. Other symmetric key applications include single-use PINs, or passwords, or entry codes. Two important things to note are: (i) that almost certainly the key use will be "once only" to maintain security (and so afterwards used keys should be irreversibly deleted); (ii) the use of the keys is conventional, requiring no quantum technology. It is the distribution, or replenishment, of the keys that is quantum.

While QKD is a mature quantum technology, it does not perform initial authentication. This means that, used in isolation, the technology could be vulnerable to man-in-the-middle attacks, due to Alice and Bob being unable to identify each other as friend, rather than foe. One simple solution to initial authentication is for Alice and Bob to be provided with some initial shared secret (or "seed") key material. As has been demonstrated, this approach enables QKD to work securely in a fixed network scenario, such as an optical fibre network.



However, clearly a more flexible approach is needed in a dynamic or mobile network scenario, where a given Alice may need to authenticate to a Bob that she's never met before.

Therefore, in parallel to the development of QKD and quantum communications, Hub R&D is also being pursued with other forms of "quantum-safe" communications. One such direction is with new mathematical approaches, called quantum-resistant or post-quantum cryptography (PQC). These are known to be immune to current quantum computer algorithms (e.g. Shor's) and thought to be immune to any that might be developed in the future. In a dynamic network scenario, a particular Alice could use asymmetric PQC to authenticate to a Bob she's never met before, in order to then conduct QKD. With this hybrid approach, the security "shelf-life" of the PQC exchange is only required to last until new key from QKD is generated.

There is now widespread support for the most effective approach to future quantum-safe communications being a hybrid one, combining physical quantum security alongside new quantum-resistant cryptography. This is driving the Hub's efforts on integrating QKD with PQC.

If you would like to hear more about the Hub's work on quantum key distribution, within the wider context of quantum-safe communications, please contact us via enquiries@quantumcommshub.net