QET Labs
Quantum Engineering Technology Labs

Practical Handheld QKD

Rather than a single vulnerable key (such as a password), Quantum Key Distribution (QKD) systems and specialist software can provide a continuous supply of provably secure keys.

Public key is vulnerable to the computing power of quantum computers and their ability to reverse engineer the key. A quantum computer could solve the key within a practical time, such as hours or days, depending on the available power of the computer. Symmetric encryption is much less vulnerable but has been impractical so far. Since some symmetric encryption schemes use a specific numerical key, it would take an unreasonable amount of time an effort to guess the key.

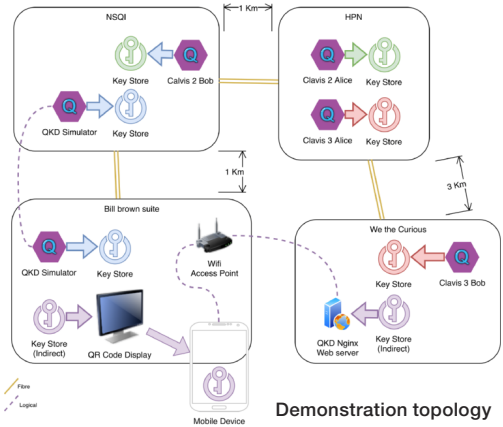
QKD allows a new approach to symmetric encryption by enabling users to generate shared, truly random symmetric keys from different locations on the network. A database of keys is built up continuously in the key store and a new key can be used for each data transfer. This communication link can detect an eavesdropper, thereby preventing interception of the key and allowing long term secrecy.

Quantum Engineering Technology Labs

The mission of QETLabs is to take quantum science discoveries out of the labs and engineer them into technologies for the benefit of society. The group brings together £50M worth of activity that covers theoretical quantum physics through experiment, engineering and skills and training toward concept demonstrators of quantum technologies.

Researchers in the Quantum Technology Engineering Labs (QET Labs) have developed open source software, 'CQP Toolkit', capable of incorporating various QKD solutions into current networking infrastructures. The Toolkit will be used in this demonstration to show a real-world application of secure communication using QKD, i.e. creating encrypted custom VPN tunnels between computers with the *QTunnel* program.

It will demonstrate how QR Code technology can be used to exchange keys between a client and the local keystore emulating a Quantum ATM. In time, this will be replaced with the Handheld Quantum Key Distribution system being developed by the consortium comprising of the University of Bristol, the University of Oxford and Cognizant Worldwide Limited.



Demonstration topology