Practical Handheld QKD

R. Collins, D. Aktas, D. Lowndes and J. Rarity

University of BRISTOL

QUANTUM COMMUNICATIONS HUB

EPSRC
Engineering and Physical Sciences Research Council

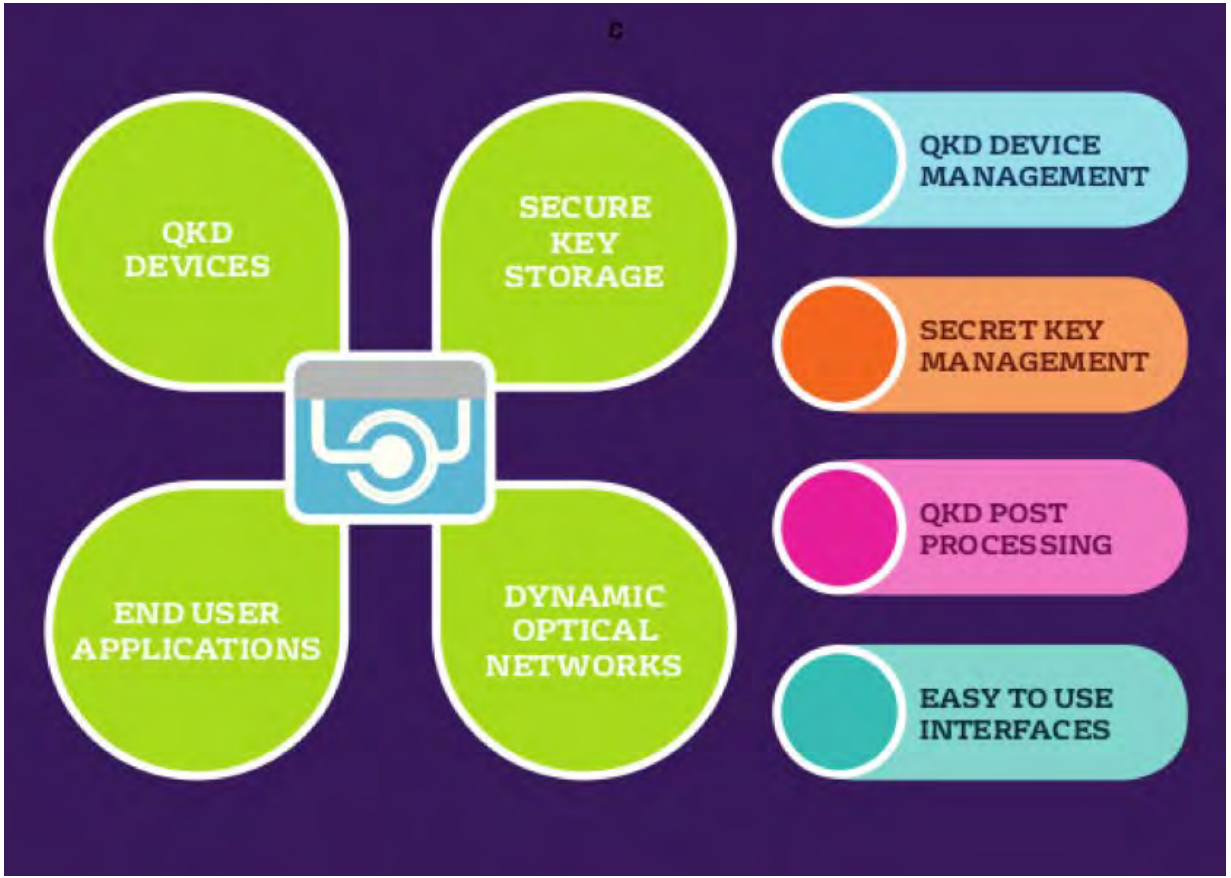
How do you create a permanently secure network that can be remotely accessed?

- Rather than a **single vulnerable key**, what if you had a continuous supply of **provably secure keys**?
- Quantum Key Distribution (QKD) systems and specialist software can address these issues.
- Our software allows for **a new key** to be used **each time** a remote worker connects.
- The CQP toolkit is designed to incorporate different QKD solutions in current networking infrastructures.

Bristol trusted-nodes

NSQI/HPN/One Cathedral Square/We The Curious/Bradley Stokes

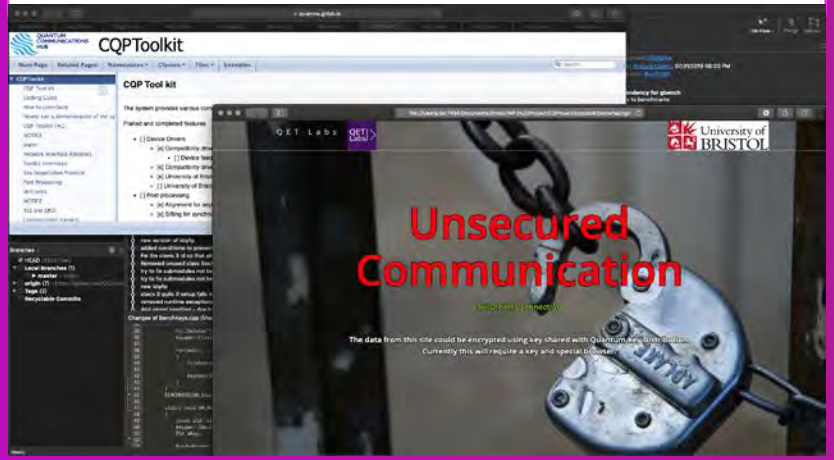
Trusted-Node QKD architecture in Bristol



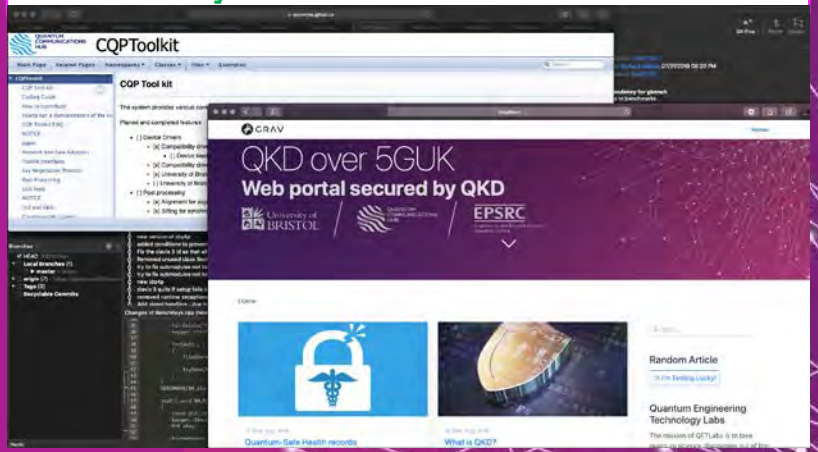
- Discover prototypes of future quantum technologies,
- Download the CQP Toolkit,
- Unlock a website with QKD & QR Codes.

open source initiative®

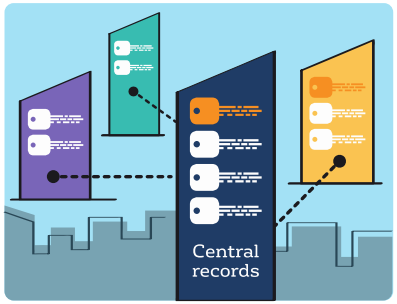
✗ Without the proper key



✓ With a key withdrawn at the keystore of a trusted-node



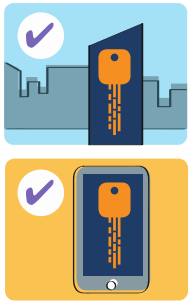
A quick guide to QKD and what's happening when you scan the QR code.



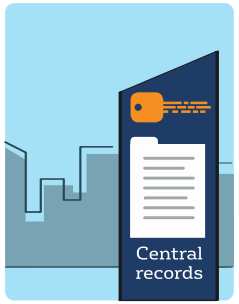
Network of trusted nodes are connected via a fibre network.

Keys are generated separately at each node.

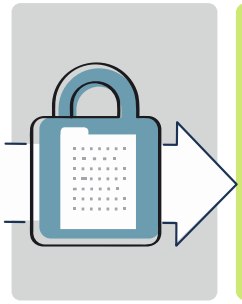
Keys generated locally at node transferred to mobile device via desktop terminal connection.



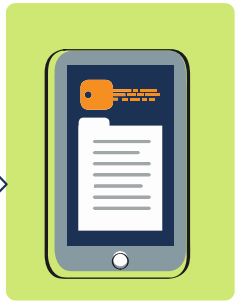
Secure communication allowed ONLY if matching pair of keys is found.



Data encrypted using this key. Key erased when encrytion completed.



Encrypted data sent safely via any connection.



Paired key on mobile device unlocks data. Key erased when decryption is complete.