Practical Integration of Quantum Key Distribution with Next-Generation Networks

Overview

QKD Refresher

Networks of the Future

Emulating a Software Defined Network

Time-Sharing QKD Systems

Distributing Virtual Network Functions

Next steps
QKD Refresher

Shor’s algorithm can be used to attack conventional key distribution methods.

Grover’s search strengthens brute force attacks.

Need a quantum-secure method of key distribution to use alongside conventional ciphers reinforced against Grover’s.
QKD Refresher


QKD Refresher


One Time Pad
Mathematically secure
Infeasible for day-to-day communications

AES
Secure enough
Widely used in day-to-day communications
AES

Enciphers and deciphers messages in 128-bit blocks with 256-bit keys for post-quantum security. Can perform full encryption when operating in the correct mode (e.g. CTR).

Future networks will be software-defined, deploying data handling rules as software rather than hardcoding them in the firmware of devices, allowing global reconfigurability of the network from a single location as and when required.
Networks of the Future

Application Plane
- SDN Application

Control Plane
- Network OS

Data Plane
- Network Device
- Network Device

Northbound API
- Control-Data PI

SDN Controller
Emulating a Software Defined Network
Emulating a Software Defined Network

# possible switch configurations \(=10^{10^{438}}\)

- set wavelength
- set power
- 1 classical fibre
  - 1 quantum fibre

Best case: Negligible cross-talk
Worst case: \(49.1 \times 10^3\) counts/s
Time-Sharing QKD Systems

Diagram showing multiple Alice and Bob setups with optical switches and different wavelengths (1551.7 nm and 1310 nm). Graph showing the relationship between average initialization time and distance (km) and attenuation (dB).
Distributing Virtual Network Functions

10 km data centre: Secret key rate = 825 bits/s, QBER = 2.96 %
Distributing Virtual Network Functions

Transmitted AES-encrypted Windows VM (14.831 GiB), Ubuntu VM (0.178 GiB) and CentOS OVS_LC (0.716 GiB).

AES GCM encrypts $\leq 64$ GiB per key/IV pair.

$606 \pm 2$ s to generate each $223 \pm 1$ kbit set of VNF keys allows $79$ Alices per Bob in 10G networks.
Summary and Next Steps

 Demonstrated compatibility of QKD with the software defined networking paradigm.
 Utilised the SDN framework to time-share commercial QKD systems.
 Secured the transfer of virtual network functions using quantum keys.
Summary and Next Steps

The Bristol is Open metropolitan-scale SDN relies on VNF distribution to maintain a versatile infrastructure.