ETSI/IQC Quantum Safe Cryptography Event

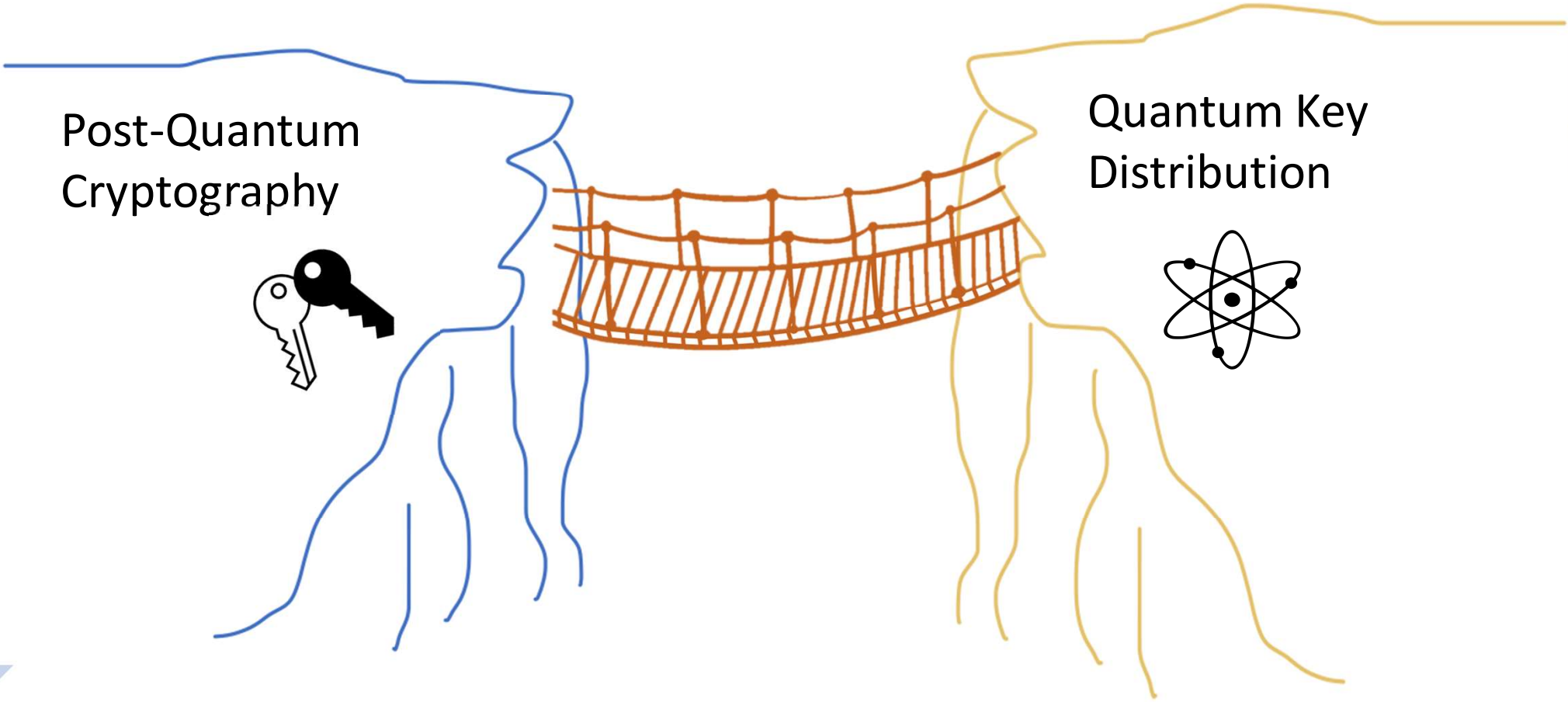
BasQuaNA: Building a Standardized Quantum-Safe Networking Architecture

Dr Sarah McCarthy

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

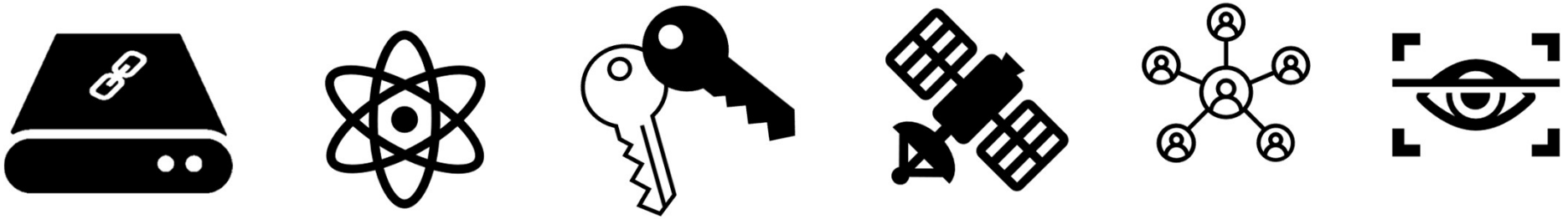
14/02/2023

The Challenge



BaSQuaNa is bananas! what do they want?

- Allows quantum security to span oceans
- Secure in multiple threat models
- Can be supported by users without special purpose QKD hardware
- Meets performance requirements of use-cases
- A de facto standard for all industry users
- Leveraging the expertise of leaders in key industries



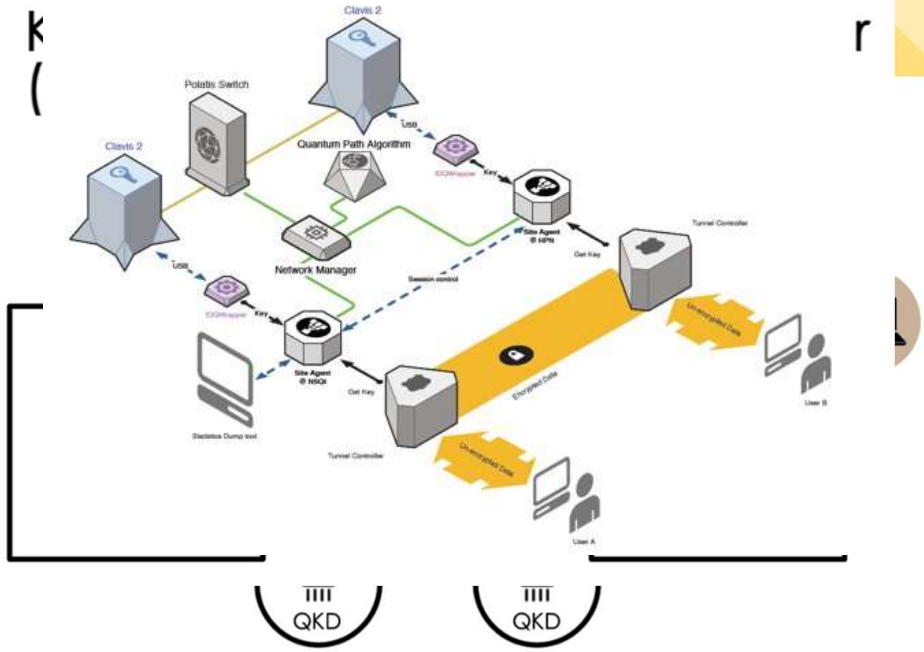
Extending the OpenQKDNetwork Architecture

HOSTS LAYER

KEY MANAGEMENT SERVICE

QKD NETWORK LAYER

QKD LINK LAYER

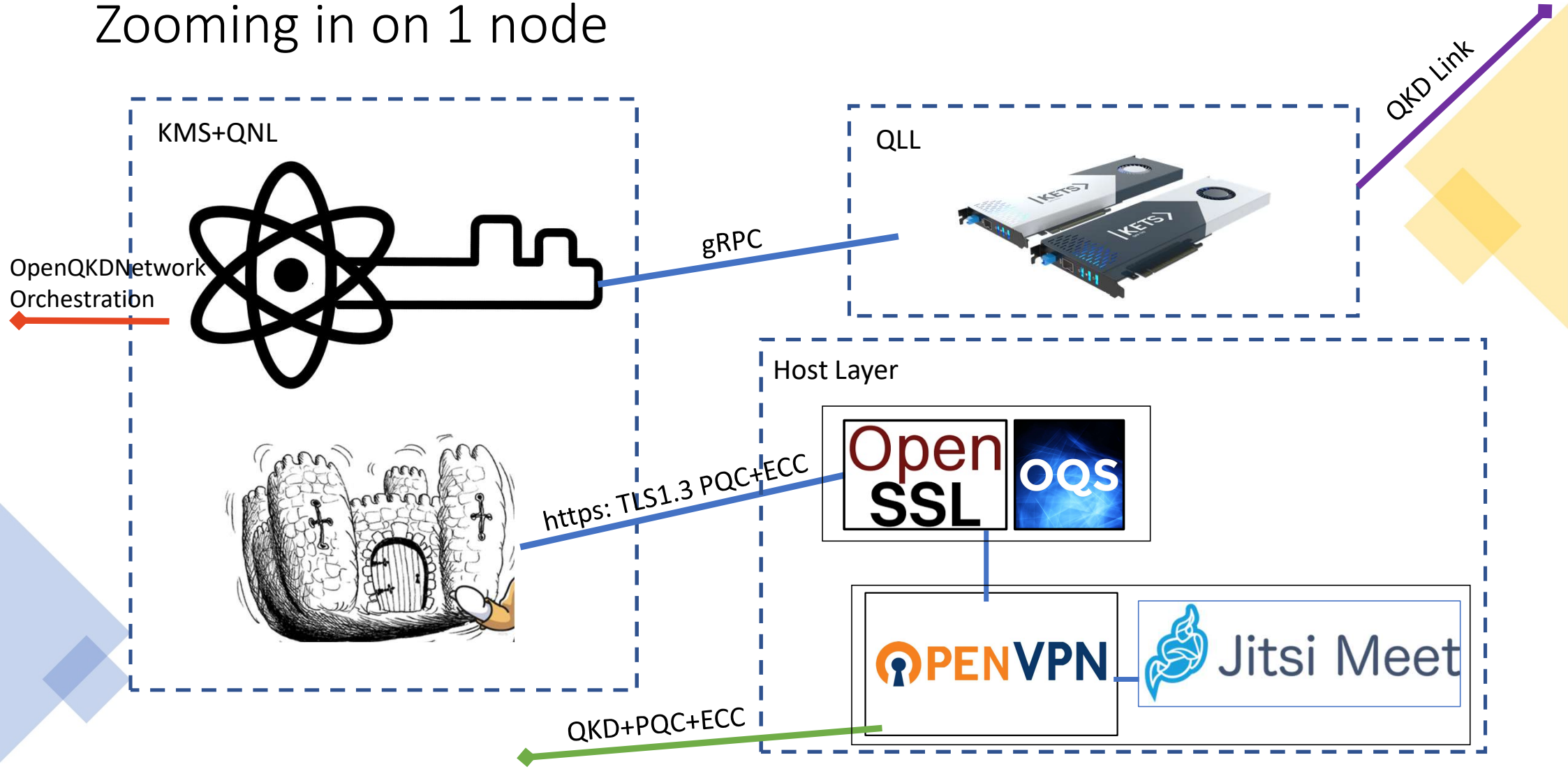


CQP Toolkit

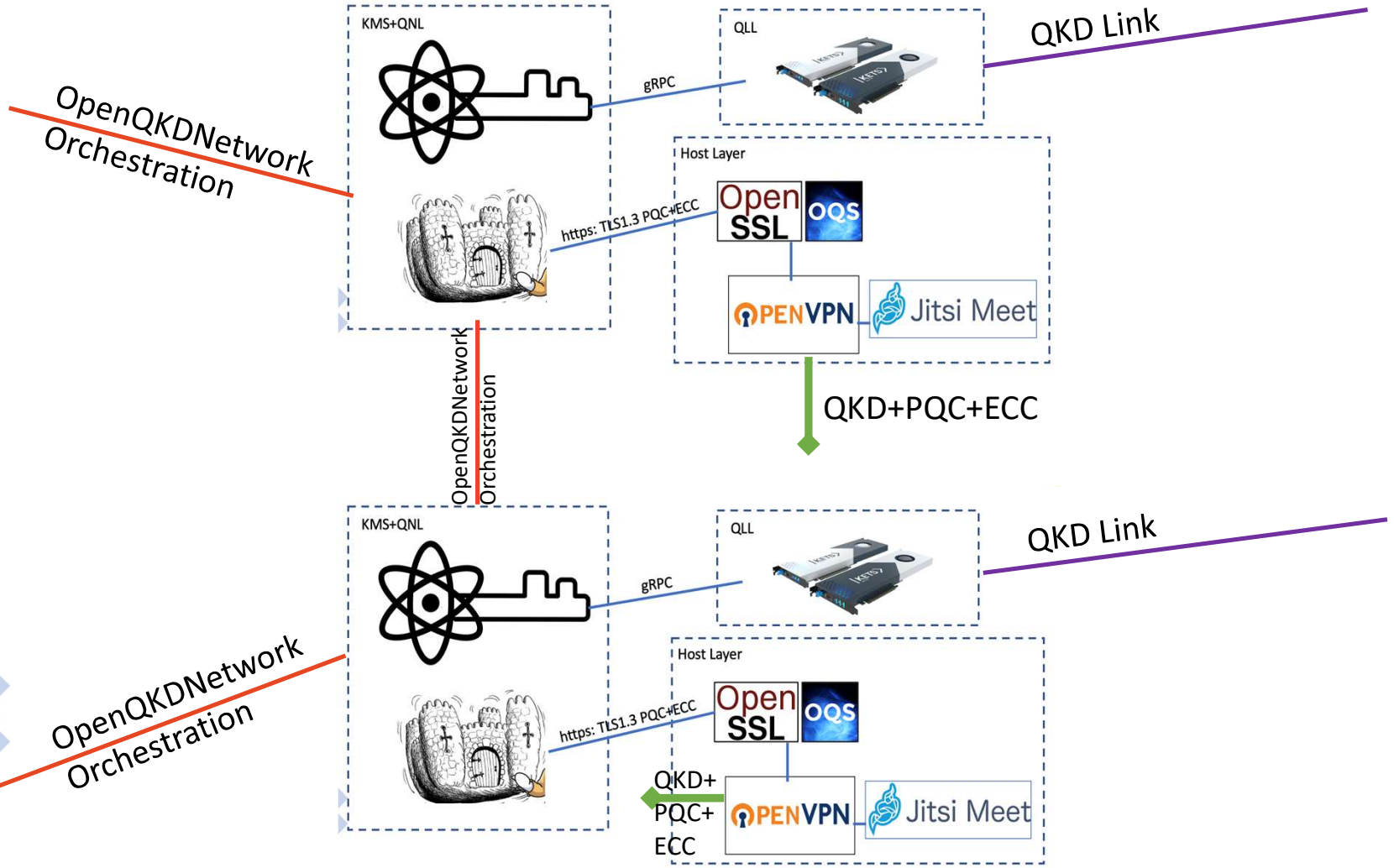
Extending the OpenQKDNetwork Architecture cont'd.

- Implements REST API according to ETSI 014, with concrete recommendations for design choices
- gRPC calls between QLL and QNL
- https using hybrid TLS1.3 (PQC + ECC) between OpenQKDNetwork to get QKD key
- Bouncy Castle-OpenSSL (Java) interoperability with liboqs-OpenSSL (C)
- Open-VPN link quantum-safe link - triple key exchange (ECDH + PQC + QKD) + AES
- Kyber and Dilithium provide PQC as per latest NIST recommendations

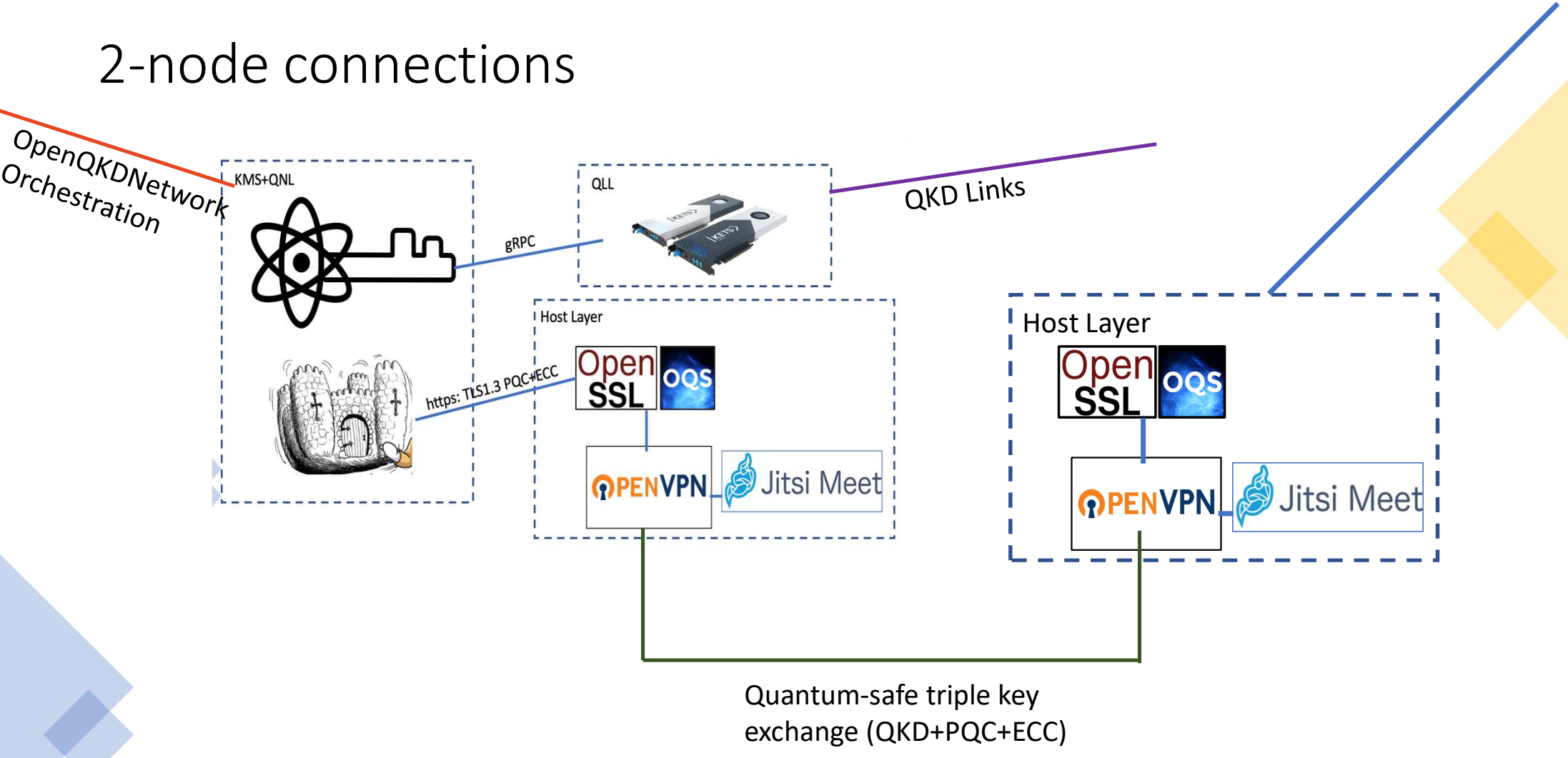
Zooming in on 1 node



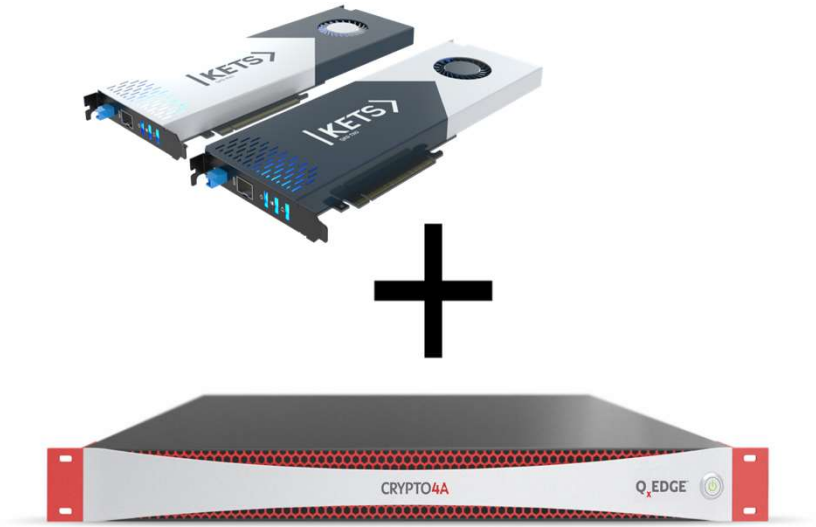
2-node connections



2-node connections



Securely storing QKD keys



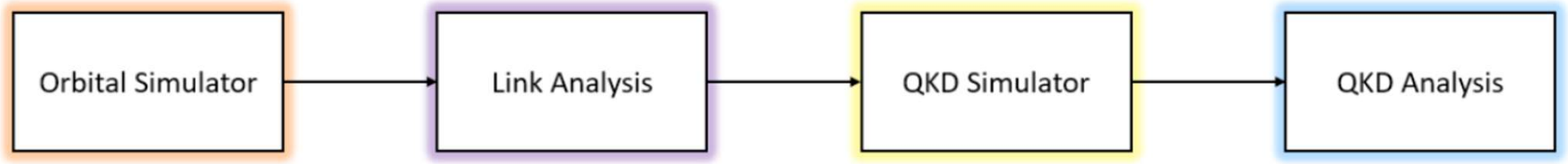
- **Development of a prototype KETS-Crypto4A combined QKD-HSM device**
- Each node contains a KETS TX0 and KETS RX0
- Secure QASM could be used for key storage
- ETSI 014 device level interface developed as a proof-of-concept
- KETS' QKD device drivers integrated into Crypto4A's QxEDGE
- Demo'd 3-node QKD network with one of these nodes running on a QxEDGE emulator
- Developed rack-mounted testbed

Securing beyond the QKD network

Kyber: 3x faster
Dilithium: 1.6-2.9x faster

- **Benchmark post-quantum cryptography algorithms in a hardware security module environment**
- Target platform: ARM Cortex A53 processor with ARMv8 NEON and crypto (AES and SHA-2) extensions
- Optimized versions of the symmetric key building blocks AES and SHA-2
- Added optimized implementations of the Kyber and Dilithium post-quantum scheme that make use of instructions available in the ARMv8 NEON extensions.
- A substantial amount of this performance improvement comes from the use of NEON optimizations for the NTT multiplication operations in Kyber and Dilithium, based in part on work by Becker et al. (TCHES 2022).
- Up-to-date benchmarks available on OpenQuantumSafe website

Transporting keys through space



Lat: 51.3441
Long: 2.7778
Alt: 30

Lat:45.5196
Long: -73.3939
Alt: 17

Sun Synchronous, Low Earth Orbit
Alt: 550 $\times 10^3$

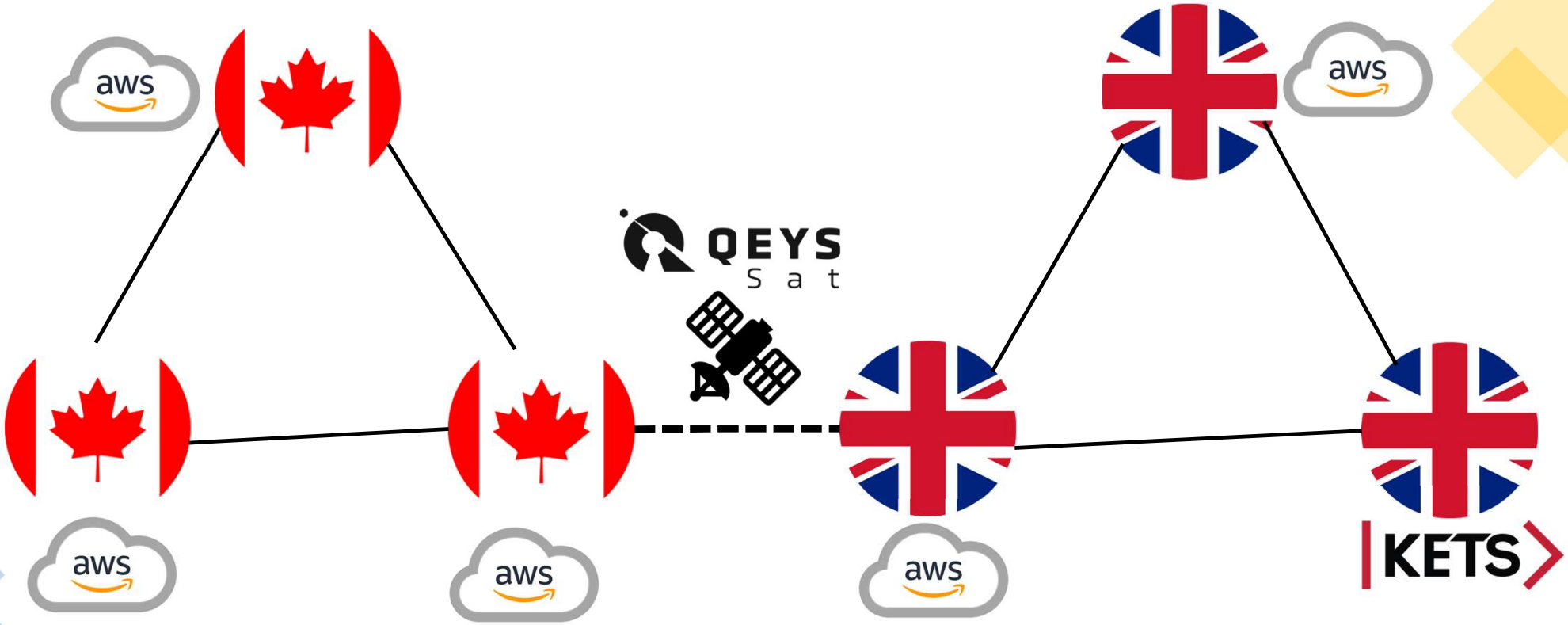
Parameters:

- Moon phases
- Background light
- Wind speed
- Atmospheric conditions
- Link type
- Pointing Error

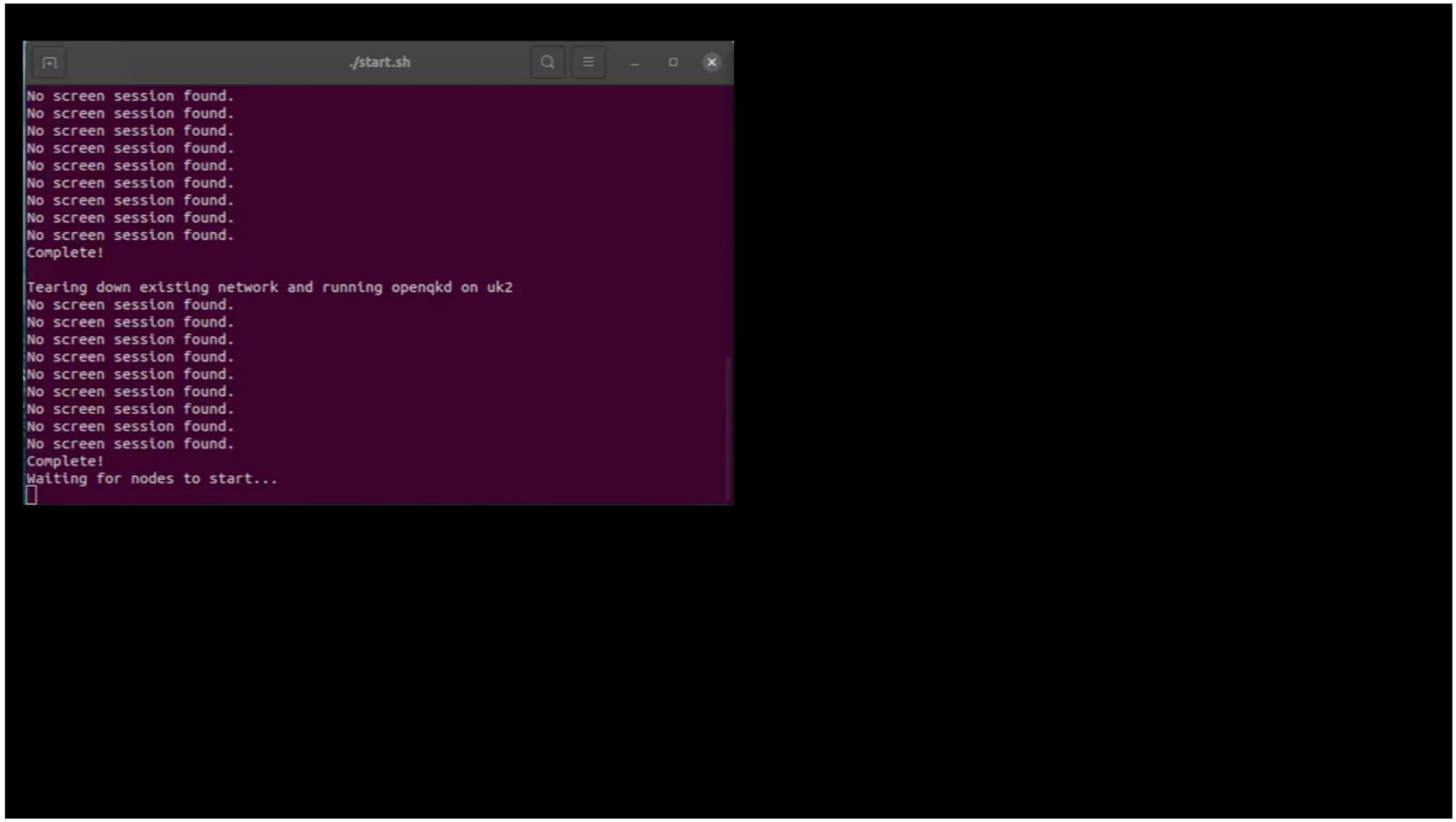
Signal-Decoy BB84 protocol with a Weak Coherent Pulse (WCP)

Generate key length per pass

The 6-node set-up



Demo


./start.sh
No screen session found.
No screen session found.
No screen session found.
No screen session found.
No screen session found.
No screen session found.
No screen session found.
No screen session found.
No screen session found.
Complete!
Tearing down existing network and running openqkd on uk2
No screen session found.
No screen session found.
No screen session found.
No screen session found.
No screen session found.
No screen session found.
No screen session found.
No screen session found.
No screen session found.
Complete!
Waiting for nodes to start...

BaSQuaNa

Building a Standardized Quantum-Safe Networking Architecture

Live Webinar

March 24th, 2023
10am EST // 3pm GMT

www.qkdnetworkcanadauk.com/signup

Michele Mosca and myself are around for the rest of the conference!

[Sign up here]