Qline

A Scalable Quantum Key Distribution Infrastructure

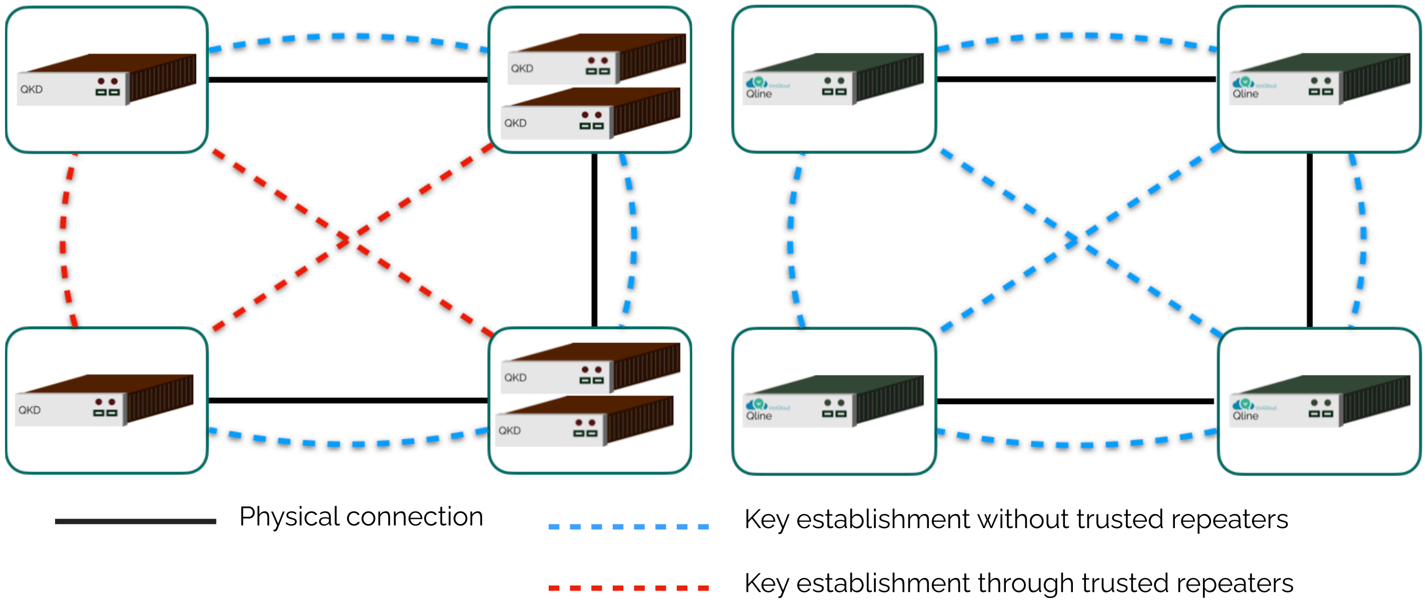
Current encryption technologies **do not offer reliable security guarantees** over long period of time. **Quantum Key Distribution (QKD) adresses this issue**.

QKD is only a **point-to-point** task, Scaling it to a network is **costly** and **injects vulnerabilities** due to the use of trusted repeaters.

Qline connects several nodes **over a single line of fiber**. It scales with **standard telecom components** and avoids using **trusted repeaters**.

A four-node QKD network

A four-node Qline


QKD
Qline
Physical connection
Key establishment without trusted repeaters
Key establishment through trusted repeaters

Concept

For a similar network topology, QKD uses **more hardware than Qline**. In Qline, each additional node uses only a standard telecom modulator. Moreover, in QKD, keys are revealed to intermediate trusted repeaters, putting them at risk. This trust assumption vanishes in Qline.

Qline uses a **new protocol** and **patented countermeasures** against side channel attacks.

Ref: Doosti et al. Establishing shared secret keys on quantum line networks: protocol and security. Apr. 4, 2023. arXiv: 2304.01881.

Use cases

In large scale quantum communication networks, Qline solves **the last-mile problem** by increasing the connectivity. By avoiding trusted nodes, it lowers the physical security requirements, making quantum cybersecurity **more accessible to end-users**.

In the local and metropolitan area scale, Qline can be used to tackle **several use-cases that are out of reach of standard quantum key distribution** methods.

Finally, it can be integrated in datacenters to ensure **quantum-safety for data-at-rest as well as data-in-computing**.

Datasheet

Qline version 0.2

June 2023

VeriQloud

Qline is a discrete variable quantum key distribution network. It consists of three different hardware modules: Alice, Charlie and Bob. Alice generates quantum states, Bob measures them and Charlie can only modify those states.

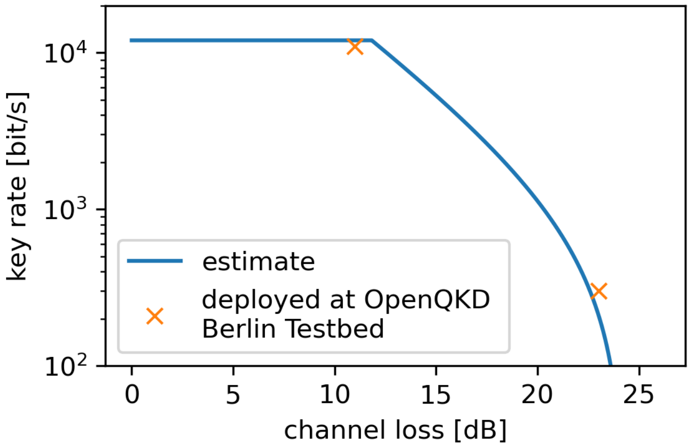
Qline requires one Alice and one Bob, but can have multiple Charlies. Optionally, several Alices can be connected to the same Bob. The key exchange is always pair-wise: Two players exchange keys while the others assist or idle.

Protocol and system specification

Protocol	BB84 with decoy states
User interface	ETSI14 standardized interface over ethernet
Authentication	preshared key or public key
Required fiber links (per qline)	one channel in dark fiber, one channel in bright fiber
Scheduling: who and when	automatic; customizable by request
Key management system (KMS)	included; customizable by request

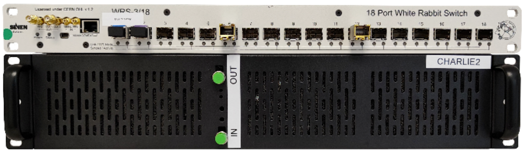
QKD performance

Repetition rate	80 MHz
Loss budget	22 dB
Loss per Charlie	5 dB
key rate	300b/s - 20kbit/s
Qber	3% - 7%
Operating wavelength	1530 - 1570 nm
Maximum temperature	30°C



Dimension and connectors

Alice	2U QL-box+1U White Rabbit Switch
Charlie	2U+1U
Bob	2U+1U+ detector Aurea SPD_OEM_NIR
Fiber connectors	FC/APC
User Interface	RJ45 Ethernet
QL-box to WRS	2x SMA; 1x RJ45
QL-box to detector	Bob only; 2x SMA; 1x USB; 1x fiber



Pre-production enclosure
Product similar