Q*bird
quantum
connectivity

# Q*Bird QKD Falqon® Series

## NEXT-GENERATION QUANTUM CRYPTOGRAPHY

## Key Features of the MQ4000 Line

| | |
|---|---|
| Maximum length of quantum channel (typ. @ 0.2 db/km) | 200 km (40 db) |
| Secret Key Rate (with 0.2 dB/km) | ≥ 500 bps at 125 km |
| Protocol | Measurement Device Independent with Decoy States |
| Fiber requirements for Quantum and Service channel | 1 fiber pair total |
| Wavelength | C Band (1530-1580 nm), or O Band (1310 nm) |
| Key delivery interface | ETSI GS QKD 014 v1, and customer specific upon request |
| Pulse repetition rate | 1.25 GHz |
| Auto-recognition of eavesdropping attack | yes |
| Secure key handover to encryptors / Secure Application | yes, using MTLS |
| Connector for quantum channel | LC / SC / FC |
| WDM compatibility | yes upon request |

## Environmental and Physical Parameters

| | |
|---|---|
| Form factor MQT4000 2 U | 2 U Nodes |
| Dimensions | 19 inch x 70 cm |
| Interfaces | 2x simplex fiber<br>4x 10-gpbs Ethernet Ports<br>(keys/encryptors, control, management, ipmi)<br>1x USB (console) |
| Power supply | 200 W, 100-240 V |
| Weight | 30 kg |
| Temperature range | 18 C – 35 C |
| Relative humidity range | 30% to 60%, non-condensing |

## Management and Monitoring

| | |
|---|---|
| Remote management interfaces | NETCONF, RESTCONF, SNMP, CLI |

Q bird
quantum connectivity

Delftechpark 1
2628 XJ, Delft
The Netherlands

Interested?
Contact us!

www.q-bird.nl

# Introduction

Quantum key distribution (QKD) enables two parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages. QKD relies on the laws of quantum physics to prevent any third party from gaining knowledge of the secret key during transmission without being detected.

# System Overview

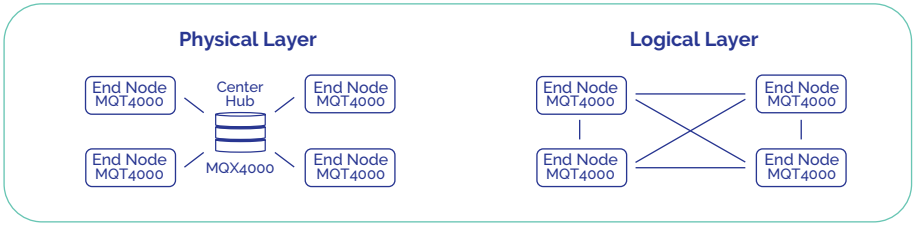
The Falqon® Series is composed of two main elements: User Nodes and Center Hubs. From an implementation point-of-view, Nodes are quantum-sending and Hubs are quantum-receiving. Any pair of Nodes can generate QKD keys, which remain secret to all other devices in the network.

In the Q*Bird system, a Center Hub facilitates QKD key distribution between two User Nodes, each of which are directly connected to the Center Hub via an optical fiber pair, Hubs are only present to establish quantum connectivity across the QKD link and form a Multi-Point-to- Multi-Point network of multiple User Nodes. Importantly, the secret QKD keys are never present at the Center Hub. The Center Hub cannot learn the secret keys. This is possible by the Next-Gen QKD Protocol in Q*Bird devices.

- Next - Gen QKD Protocol
- Multi-point to Multi-point Networks without Trusted Nodes
- Validated technology in pilot networks
- Immunity against detector hacking
- Provably secure key distribution with tapping detection
- Small form factor: 2U devices (Endnodes)
- Production, Maintenance, Service is EU27
- Non-Disruptive data communication channels
- QKD in complex networks (e.g. stars, rings, etc.)
- Embedded Key Management System (KMS)
- Cost Effective Scaling
- Remote Management and Configuration
- Easy installation and remote support
- Multiplexing option with DWDM

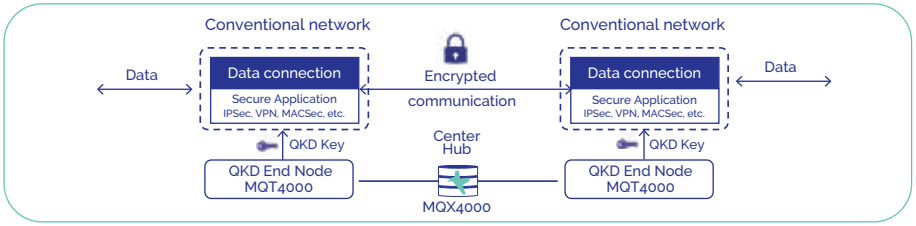
# Network Topology

At the physical layer, the Falqon® Series naturally operates in a multi-point-to-multi-point star network topology, with each User Node having a single connection to the Center Hub. Rings and point-to-point networks are easily configurable. With a single connection to the Center Hub, each User Node can establish QKD sessions with every other User Node in the network. At the logical layer, the network appears as a fully connected mesh network.




# Network Integration and Interop

The Falqon® Series interfaces with encryptors and cryptography applications via both standardized interfaces, such at ETSI, as well as customer specific solutions. The Q*Bird team has done integration projects with major network equipment vendors such as Cisco and Juniper.




# WDM Integration

Q*Bird's QKD systems can be integrated with conventional optical communication equipment via standard DWDM devices and technology.