Q*Bird Falqon QKD Systems

NEXT-GENERATION
QUANTUM CRYPTOGRAPHY

Introduction to Quantum Key Distribution

Quantum Key Distribution (QKD) adds an entirely new layer to the IT security systems protecting an organization's digital infrastructure. Today, hackers already employ "harvest and decrypt" techniques, wherein communication is recorded, and data is stored with the goal of decrypting it in the future. Advances in supercomputers, new techniques in cryptanalysis and even quantum computers will make decrypting data stored today possible. QKD is here to add protection against these kinds of cybersecurity threats today. As QKD is the only known key distribution technique with 100% forward security, a QKD layer of security protects digital infrastructure against the attacks of today as well as of tomorrow.

Advanced digital security is desired in many sectors: For telecommunication service providers, critical infrastructure, banking, finance, and public sector networks to protect their digital infrastructure against tampering. For commercial and industrial sectors to protect high-value IP data during transmission. For public, government and health networks to protect high-value long-term sensitive data.

Q*Bird Falqon QKD Series Overview

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

Q*Bird has developed next-gen QKD systems composed of two main elements: User Nodes and Center Hubs. Through the exchange of quantum signals, Falqon User Nodes generate secret keys known only to them. Hubs are present to facilitate quantum connectivity between User Nodes and form a Multi-Point-to-Multi-Point network of multiple User Nodes.

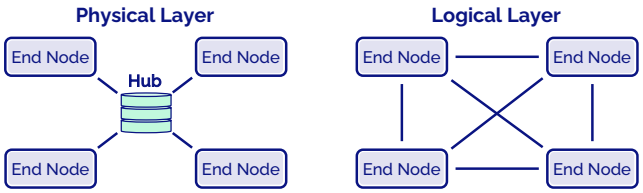
QKD keys can be used by a cryptographic application e.g. encryptor cards, IPSec, etc via standardized or customer-specific interfaces. Within a Q*Bird network, any pair of Nodes can generate QKD keys, which remain secret to all other devices in the network (including Hubs).

The Falqon system operates over standard fiber networks and at standard telecommunication wavelengths. The 19" rack-mounted 2U User Nodes are designed for standard digital infrastructure locations and integrate with conventional networking equipment.

Falqon Series – QKD System

Multi-Point to Multi-Point Network Topologies

The Falqon Series operates in a multi-point-to-multi-point network topology, with each User Node having a single connection to the Centralized Hub. Star, Hub-and-Spoke, Ring, and point-to-point networks are easily configurable. With a single connection to the Center Hub, a User Node can establish private QKD Keys with any other User Node in the network. At the logical layer, the network appears as a fully connected mesh network, with each pair of User Nodes appearing to have a dedicated QKD connection.

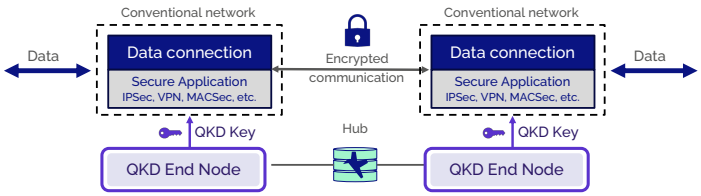


Advantages of the Falqon Series

Employing a next-gen QKD protocol (MDI), Falqon offers cost-effective scaling, as Users Nodes only need a single fiber pair to enjoy complete connectivity within the network. Moreover, the system contains an embedded Key Management System for multiple Users to connect to same QKD Node, and remote Configuration.

Network Integration

The diagram below shows an example integration architecture, with a crypto application receiving QKD keys from a QKD system to encrypt high-bandwidth data.



The Q*Bird team has done integration projects with major network equipment vendors such as Cisco and Juniper, as well as integration with DWDM technology and conventional optical data streams.

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

Q*bird quantum connectivity

Visiting address
Delftechpark 1
2628 XJ, Delft
The Netherlands

Postal address
Delftechpark 1
2628 XJ, Delft
The Netherlands

q-bird.nl
info@q-bird.nl
linkedin.com/company/q-bird/