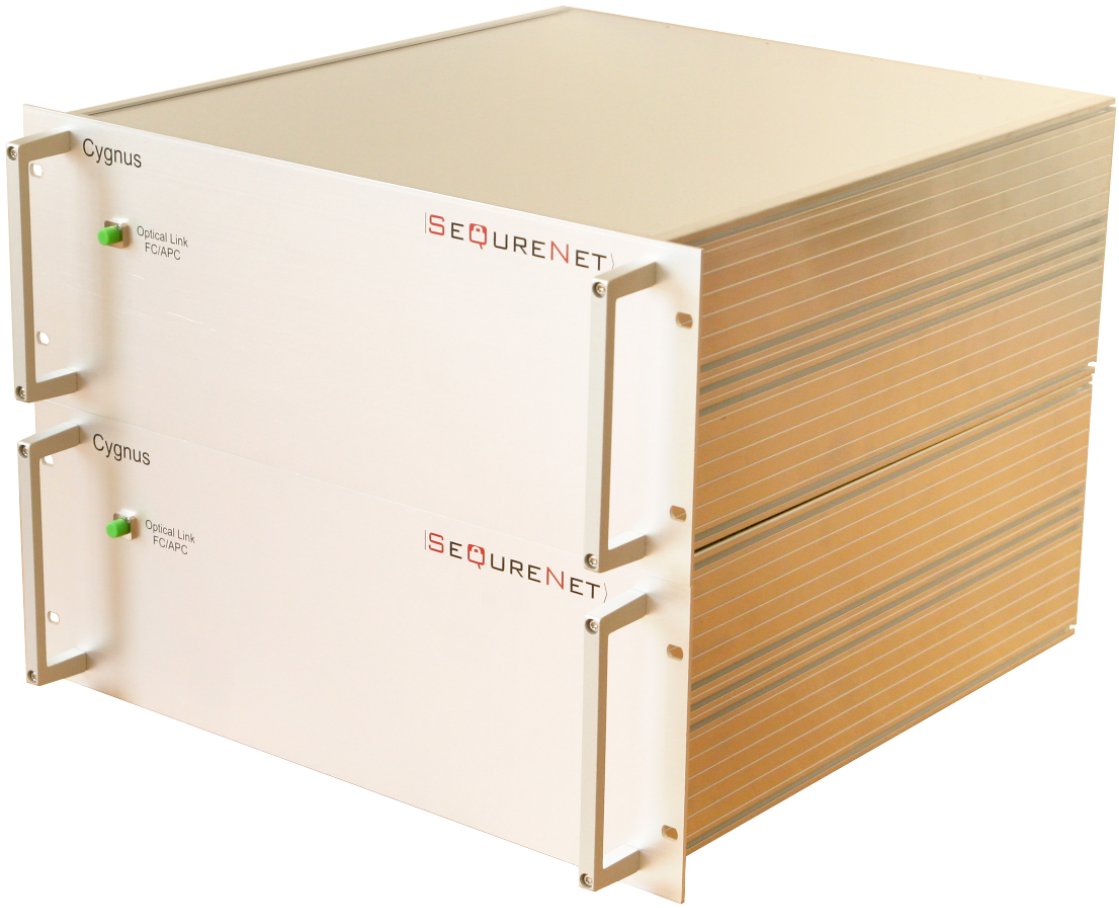
SeQureNet SARL
Bat B, 12 villa de la croix Nivert, 75015 Paris, France
www.sequrenet.com

Cygnus

State-of-the-art Continuous-Variable Quantum Key Distribution Module



SeQureNet SARL
Bat B, 12 villa de la croix Nivert, 75015 Paris, France
www.sequrenet.com

Quantum key distribution, relying on the uncertainty principle of Quantum Mechanics, enables the unconditionally secure distribution of secret values. Quantum Key distribution devices on the market are Discrete Variable implementations using single-photon detectors. SeQureNet proposes the first commercial implementation of Continuous Variable Quantum Key Distribution, relying on Gaussian modulation of coherent states and homodyne detection. The implemented protocol has a security proof against collective attacks with practical key rates. The range of the product (80Km / 16dB) is much greater that previous CVQKD implementations, enabling deployment in realistic conditions.

Highlights

- State-of-the-art CVQKD implementation with long range
- High-Efficiency LDPC-based error correction
- Many user-controlled parameters
- Access to a wide range of system data

Research applications

- Side-channel attacks and countermeasures
- Implementation of new protocols
- Education and training

IT security/networking applications

- QKD interoperability / field tests
- Pilot networks
- The produced keys can be used directly or as secret material for classical cryptography algorithms

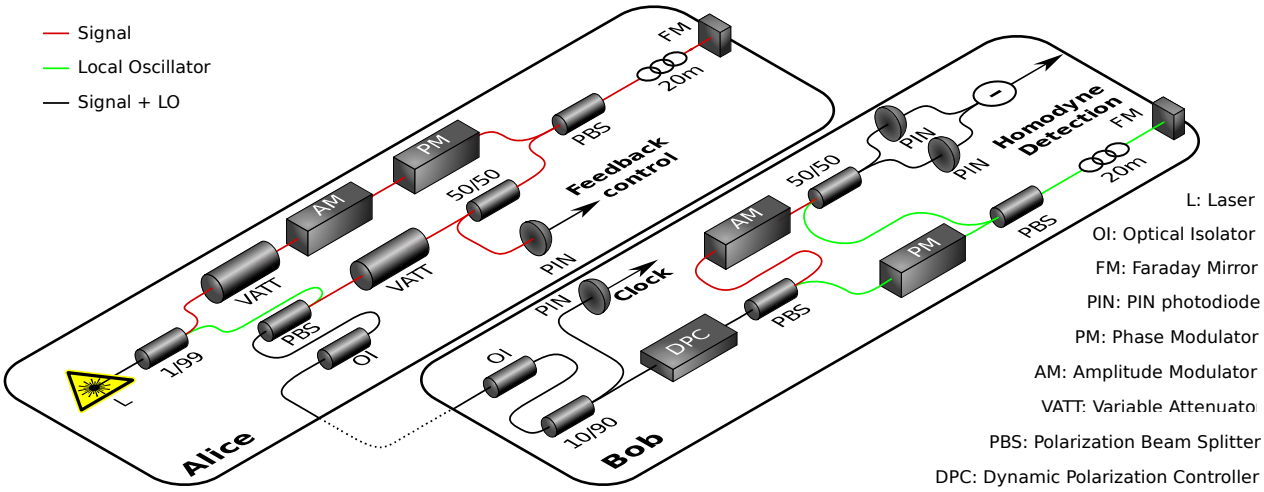
Optical Scheme

Cygnus is based on a patented interferometric setup. Alice sends both weak modulated light pulses and strong light pulses that are time and polarization multiplexed. After demultiplexing on Bob's side, they interfere on a shot-noise limited balanced pulsed homodyne detector.

Performance/Range

- @ 80Km: 100 bit / sec
- @ 20Km: 10 Kbit / sec

SeQureNet SARL
Bat B, 12 villa de la croix Nivert, 75015 Paris, France
www.sequrenet.com



Research-oriented Functionality

- Access to raw measurement data
- Access to key system parameters
- Synchronization and measurement signals available
- LabView compatibility

Customization, Devices Options

- Programming interfaces can be devised to provide access to internals of the equipment or to enable to override some specific protocol operation.
- IdQuantique Quantum RNGs can be included for randomness generation.
- Warranty extension (beyond the first year) can be purchased.
- GPUs can be included for fast error-correction.

Software

- Gaussian protocol
- Evaluation of parameters for large data blocks, key rate computation with finite-size effects
- Multidimensional reconciliation
- Error-correction: LDPC-based (CPU or GPU as an option)
- Privacy Amplification: fast universal hashing
- Key material storage on hard disk, or on smart cards as an option
- Encryption module (AES or One-Time Pad) as an option

SeQureNet SARL
Bat B, 12 villa de la croix Nivert, 75015 Paris, France
www.sequrenet.com

Equipment data, optical enclosure

- Size (W x H x D, mm): 483 x 177 x 466
- Weight: 10Kg
- Standard 19” rackable enclosure, 4U
- Power supply: 110/220V 50/60Hz, 20W (Alice) / 60W (Bob)

Equipment data, processing unit

- Standard 19” rackable PC, 4U
- Power supply: 110/220V 50/60Hz, 600W PSU
- 32-bit GNU/Linux OS