QUANTUM KEY DISTRIBUTION SYSTEM PROTOTYPE

ANDARIEL TESTBED SERIES

Quantum Key Distribution (QKD)

The purpose of QKD is to provide cryptographic key material at both endpoints of an optical link. Provable security of the keys is provided by the means of quantum physics and information theory.

MAIN FEATURES

Function

Andariel Testbed Series is a quantum key distribution (QKD) system prototype. The system consists of two modules: A transmitter *Alice* and a receiver *Bob*. Their purpose is to perform a quantum key distribution protocol using quantum optical communication and classical telecommunication in order to grow a secret key between Alice and Bob, which can be used for cryptographic applications.

Transmitter and receiver modules consist of three subsystems each (cf. Figure 1):

- Quantum optical transmitter/receiver
- Quantum post-processing
- Key buffer

The purpose of the quantum optical transmitter and receiver is to send quantum states of light over a pair of optical dark fiber, convert the transmitted light to an analog electrical signal, digitize it and perform digital signal processing on the data.

The quantum post-processing unit processes the arbitrary modulation pattern (Alice) and the raw data (Bob) on both sides. Such, without revealing too much information on the classical channel, a secret key can be distilled at either end of the fiber link.

The key buffer stores the secret key data and labels it, such that key data labels are synchronized between Alice and Bob. In a typical network application, the keys are transferred to a key management system.

QKD Protocol

Andariel Testbed Series utilizes QKD based on continuous variables of the light field, also called CV-QKD. The term “continuous variables” refers to the type of detection used in the receiver, which is a form of coherent optical detection and yields a continuous measurement outcome when measuring the electrical field of light. This is in contrast to discrete-variable QKD (DV-QKD), which relies on single photon detection - a click or no-click single photon event, and thus a discrete measurement outcome.

More specifically, a quadrature phase shift keying modulation (QPSK) is employed. The transmitter thereby encodes a random sequence of QPSK modulated signals onto a continuous wave of light. The transmitter is equipped with a suitable demodulation unit in order to characterize the quantum states for later post-processing.

Advantages of CV-QKD

Since CV-QKD relies on coherent optical detection, both transmitter and receiver may be miniaturized using integrated photonics. Thus, CV-QKD takes advantage of the recent evolution of coherent telecommunication technology and thus greatly benefits from the availability of commercial-of-the-shelf components, and thoroughly established industry processes and -technology.

In contrast, DV-QKD systems rely on single photon detectors, which are currently a niche market product and require significant fundamental scientific advances for allowing photonic integration and thus miniaturization. Besides the miniaturization aspect, the technological synergy with standard coherent telecommunication also allows for a future scaling of the CV-QKD technology in terms of size, weight, power consumption and producibility, making it very attractive for wide-scale deployment.

CV-QKD detection mechanism

The detection mechanism of CV-QKD requires an optical interference of the quantum signal with a so-called local oscillator (LO). The LO is typically a narrow line-width laser which acts, due to its interference with the quantum signal, as a narrow spectral filter for photons. This adds passive filtering of unwanted photons from the fiber channel, which may be present due to noise and scattering of other optical signals present in the fiber. Potentially, this may lead to better QKD performance in wavelength-division multiplexing applications.

CV-QKD detectors are able to perform a continuous measurement of the impinging light. This is in contrast to DV-QKD, where single photon detectors (avalanche photo diodes) typically suffer from a dead time, once a photon has been detected. CV-QKD therefore is compatible to very high symbol rates (up to several GHz). In addition, in typical CV-QKD protocols, the secret key rate does not saturate at low quantum channel loss because of the absence of detector dead times.

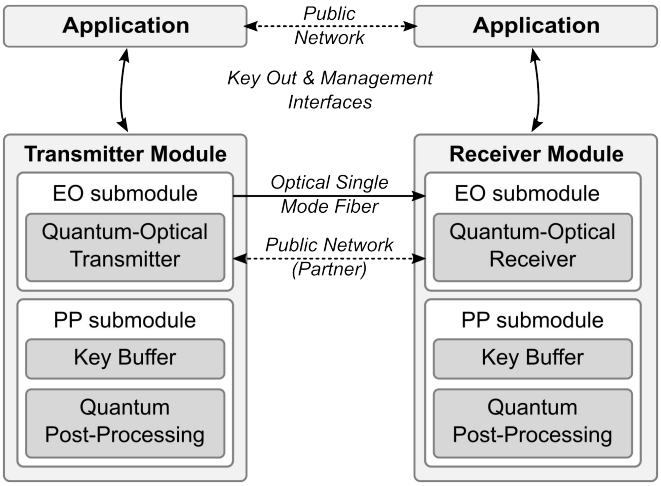

Figure 1: Andariel Testbed Series system block diagram connected to an application, e.g. a key management system (not contained). The transmitter and receiver modules consist of an electro-optical (EO) and a postprocessing (PP) submodule on each side, connected by a SM optical fiber and the partner network.

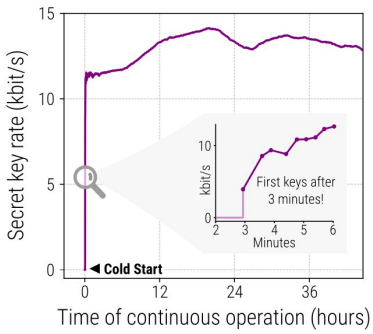

Figure 2: Continuous operation of the CV-QKD system with a key rate exceeding 10 kbit/s.

TECHNICAL PARAMETERS

Parameter name	Value	Condition/Comment
QKD Protocol		
QKD protocol	CV-QKD	QKD with continuous variables, similar to ideas presented by Grosshans and Grangier in 2002. Protocol and security proof are detailed in the system documentation delivered.
Quantum state encoding	Gaussian Modulation of Coherent States (GMCS)	possibly other modulation formats, such as Quadrature Phase Shift Keying (QPSK) or Quadrature Amplitude Modulation (QAM).
Detector technology	CV / coherent detection with LLO configuration and dual polarization readout.	LLO ("local local oscillator") configuration, i.e. local oscillator laser is not transmitted and part of the Bob/receiver module. Both TE and TM polarizations are detected.
QKD reach (max. tolerable loss on the quantum channel)	16 dB	Corresponds to 80 km reach in standard fiber (0.2 dB/km loss). More than 20 dB currently under development.
Secret key rate	10 kbit/s	(indicative value, non-binding).
Security parameter ε	tbd	Protocol and security proof are detailed in the system documentation delivered. The management GUI displays the ε_{PE} parameter.
Data co- or counterpropagation compatibility	tbd	Not specified. Please inquire if other data traffic present on quantum channel fiber.
Optical		
Required number of optical fibers	1	One dedicated dark optical fiber for the quantum channel.
Optical fiber connectors	SC/UPC	Other upon request.
Wavelength	1530 – 1560 nm	C-Band, DWDM channels 15.0 to 62.5 .
Key buffer		
Protocol for key delivery	ETSI GS QKD 004 ETSI GS QKD 014	
Management interface	Graphical web interface	Inquire for API and CLI options.
Electrical		
Network interface	Ethernet	3 RJ45 ports (Key Out, Partner, Management) for connecting to the relevant networks.
Mains power	230 V / 50 Hz	
Electric power consumption and heat intake	< 300 W < 1000 BTU / hr	Value for each Alice or Bob module, consisting of one EO and one PP submodule each.
Mechanical		
Height per QKD module (Alice or Bob module)	2 U (EO submodule) 1 U (PP submodule)	Alice and Bob modules consist of one EO and one PP submodule each. 1 U corresponds to one standard rack heigth unit.
Width	19 inch	Standard rack mount compatible.
Depth	425 mm	Excluding handles, cables and rack space needed for ventilation air flow.
Weight	< 12 kg per module	Value for each Alice or Bob module, consisting of one EO and one PP submodule each.

PHYSICAL INTERFACES

Figure 3: Andariel Testbed Series EO submodule front cover with interfaces.

On their front sides, the QKD modules offer two optical fiber interfaces and three ethernet interfaces (cf. Figure 3):

Quantum Fiber Port – Interface over which Alice sends quantum states of light to Bob. Here, weak laser pulses modulated in phase and amplitude are used.

Auxiliary Fiber Port – n/a.

Key Out ETH Port – Interface to the user application, for example a hardware encryptor or a key management system, which act as key sinks.

Partner ETH Port – Interface through which the QKD subsystems Alice and Bob communicate classically across the link. The port can be either connected directly, through a LAN, or the Internet.

Management ETH Port – Interface for local maintenance, monitoring and configuration. A web-interface is served through this port.

The back side of the QKD module holds the IEC 60320 C14 mains connector as well as the power switch. An M6 tapped through hole is provided for optional additional protective grounding. If a mains power cord is plugged in, case protective grounding is internally ensured via the PE conductor.

NORMS AND COMPLIANCE

The KEEQuant QKD System was developed and produced according to the EU directives

2014/30/EU:2014-02-26
2014/35/EU:2014-02-26
2011/65/EU:2011-06-08
2012/19/EU:2012-07-04
EU 2015/863:2015-03-31

and complies with and was tested according to the norms

DIN EN 55032:2015 + AC:2016 + A11:2020
DIN EN 55035:2017 + AC:2019
DIN EN IEC 61000-4-2
DIN EN 61000-4-3
DIN EN 61000-4-4
DIN EN 61000-4-5
DIN EN 61000-4-6
DIN EN 61000-4-11
DIN EN IEC 62368-1:2014 + AC:2015

TENTATIVE

CE

RoHS compliant

LIMITS OF APPLICABILITY – NOT FOR USE IN PRODUCTION NETWORKS

KEEQuant Quantum Key Distribution System Prototypes of the Andariel Testbed Series are fully functional but not hardened or certified for handling keys intended for encryption of security critical or classified information.

The intended use of Andariel Testbed Series devices is to provide operators and other companies or institutions with the ability to develop network architectures, test interfaces, key management systems, encryptors, and other components of a quantum communication infrastructure, in conjunction with a quantum key distribution layer.

Class 1 laser product according to IEC 60825-1. Wavelength 1530 – 1560 nm, output power less than 0.1 mW.

KEEQuant GmbH
Gebhardtstrasse 28
90762 Fürth
Germany

Phone: +49 911 9769 3 666
sales@keequant.com
www.keequant.com

Company Register
Amtsgericht Fürth HRB 18963

Managing Directors
Imran Khan

VAT-ID / USt-Id-Nr.
DE335326777