ARMOS

The Ultimate Shield for Confidential Data in Transit!

Armos protects critical infrastructure unconditionally, providing quantum resilience while ensuring data is always safe in transit.

ARMOS QNL-X210 G

INTRODUCTION

Armos, QKD (Quantum Key Distribution) is a state-of-the-art appliance which provides unconditional security for your critical data by leveraging the principles of quantum physics.

This product enables to create secure encryption keys for any two ends of a communication link for Symmetric Key Encryption system without ever sharing the actual keys on any links. The basic principle is to exploit the peculiarities of quantum mechanics by utilising encoded photons or “Qubits" from one end (Alice) to the other (Bob) over a single fibre core called the quantum channel.

Key distribution has always been an area of vulnerability holding the highest value of compromise. Though strong keys may be used for encryption, the sharing of the secret key has always been a point of vulnerability and challenge – this results in less frequent rotation of keys via manual processes indirectly leading to decreased flexibility in type, length and periodicity of key usage. Key generation and distribution forms the basis for cryptographic infrastructure and secured digital usage of it increases the use-cases when higher security can be applied for maximum benefits. With PKI breakdown and rampant theft of critical data, organizations world over are focusing on adopting more secure methods with quantum cryptography. There are only two proven ways of securing data in transit, one is Quantum Key Distribution (QKD) and the second is with Quantum One Time Pad (QOTP), both of which in combination provide the highest level of security possible against the attacks experienced today while addressing potential threats of future.

Key Applications	Key Benefits
Transition to Secure Digital Key Transfers	Secure key generation and distribution digitally without any manual process or intervention. Key rotation can be more frequent, enhancing security.
Data Centre to Data Recovery Data Transfers	Secure key generation, distribution to protect all data transfers between DC-DR locations over any third-party links.
Critical Infrastructure Control Systems	Detection of eavesdropper / Man-in-the-Middle
Quantum Safe Networks	Complete un-hackable data path with utmost security.
5G Back Haul using QKD Network	5G core network protection with best-in-class security

__USE CASES

TRANSITION TO SECURE DIGITAL KEY TRANSFER

Armos QKD offers quantum safe key generation, distribution and usage in encryption for the transport of confidential ciphers across any network in real time. This can lead to total transformation of secure key distribution in the defense and allied sectors while offering strategic advantage.

DATA CENTRE (DC) TO DATA RECOVERY (DR) DATA TRANSFERS

Armos creates a virtual air gap given the quantum layer, it creates the separation of quantum keys from the classical encryption layer making it potentially harder for attacks to take place on both cryptography primitives at the same time. Additionally, any communication between any two locations including DC to DR data transfers can be unconditionally protected by utilising Armos.

CRITICAL INFRASTRUCTURE CONTROL SYSTEMS

Sensitive data is communicated across different points in a critical infrastructure. It is important that all the points are inter-connected for effective communications to occur and that data is exchanged using the highest level of encryption possible with detection of any eavesdropper trying to perform man-in-the-middle attacks on the quantum channel. Armos provides secure and trusted key generation and distribution between any critical points or locations that require utmost transit security.

QUANTUM SAFE NETWORKS

Terrestrial networks that span agency, state, or country require end-to-end encryption, thereby providing unconditional security for any communication over classical channels. Armos enables creation of completely quantum safe network to enable highest level of trust in data that traverses such networks.

5G BACK HAUL USING QKD NETWORK

5G provides higher speed and better connectivity but also has an Achille's heel in the form of data security. Armos QKD helps in securing the communication between the various base stations to secure critical data without impacting the actual communication.

DENSE WAVELENGTH DIVISION MULTIPLEXING (DWDM)

Parameter	
Channel Wavelength (nm)	ITU 100GHz Grid
Center Wavelength Accuracy (nm)	± 0.05
Minimum Channel Spacing (nm)	0.8
Insertion Loss (dB)	< 3.2
Adjacent Channel Isolation (dB)	> 30
Non-Adjacent Channel Isolation (dB)	> 40
Insertion Loss Temperature Sensitivity (dB/°C)	< 0.005
Wavelength Temperature Sensitivity (nm/°C)	< 0.002
Polarization Dependent Loss (dB)	< 0.1
Directivity (dB)	>50
Dimensions	355mm x 270mm x 31.2mm

CRITICAL ANALYSIS AND RESEARCH PLATFORM (CARP)

CARP allows observation and working of the QKD system in real time. A user-friendly Graphic User Interface (GUI) provides a platform to initiate, observe and understand various parameters. The system can be connected to a server for logging outputs and studying the system for a longer period of time depending on the capacity and usage.

CARP provides an excellent framework to study and experiment with some of the parameters which are essential to understand Quantum Key Distribution protocol – Differential Phase Shift in QKD.

Below are the list of experiments:

- Experiment on weak coherent source, for example Hanbury Brown and Twiss (HBT) test
- Impact of source characteristics on QKD performance can be experimented
- Experiment to study quantum visibility
- Applying non ideal parameters and studying its impact on QBER (Quantum Bit Error Rate)
- Effect on self-interference outcomes due to the variable encoding
- Change in the key rate can be studied by varying the attenuation and pulse width of the optical pulse
- The control can be done through UI with a pre-defined set of variables
- Impact of quantum channels of different length on the system performance
- Key generation is the important part of the process. It will be checked if the same keys are generated at Alice and Bob
- Platform will display the error rate, key rate etc. on every execution
- The error corrected key will be compressed by an algorithm to generate final secure key. The provision will be provided to check the randomness of the shifted key using NIST test suite
- Experiment to show fundamental ability of QKD to create randomness

Q→NU

qnulabs.com

qnulabs.com/schedule-a-demo/

MAKE IN INDIA

CIN - U72900KA2016PTC096629

DIPP: DIPP5607 dt 21/07/2017

MSME: KR03B0149274

DSCI: DSCI/AM/2018/08

NASSCOM: NSCM/2018/11/5396