Q→NU
Proactively Quantum

ARMOS (QKD)

The Ultimate Shield for Confidential Data in Transit!

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

Introduction:

Armos Quantum Key Distribution (QKD) stands at the forefront of quantum security, offering resilience against sophisticated attacks, including photon number splitting and side channel attacks. Leveraging the fundamental principles of quantum physics, this state-of-the-art appliance establishes an unbreakable shield for critical data transmission using Decoy based Differential Phase Reference protocol.

Photon number splitting, a well-known attack vector in quantum communication, attempts to intercept quantum signals by exploiting the imperfections in the weak coherent sources. However, Armos QKD incorporates advanced countermeasures to thwart such attacks using decoy pulses. This proactive defense mechanism ensures that any attempt to split or intercept photons is immediately detected and mitigated, preserving the security of the quantum keys.

Moreover, Armos QKD's design prioritizes security against side channel attacks, which are non-invasive methods that seek to extract information from the physical characteristics of the quantum hardware or the surrounding environment. The appliance employs rigorous tamper-evident mechanisms and physical safeguards to protect against side channel vulnerabilities. Additionally, cryptographic protocols within Armos QKD are meticulously engineered to be resilient to information leakage through side channels, ensuring that the quantum keys remain uncompromised even when subjected to these covert attack vectors.

Armos QKD provides an exceptionally robust defense against photon number splitting and side channel attacks, reaffirming its position as a cutting-edge quantum security solution. By seamlessly integrating quantum physics principles with comprehensive security measures, it offers organizations an unprecedented level of protection for their critical data, safeguarding against both known and emerging threats in the quantum era.

Key Applications and Benefits:

Key Applications	Key Benefits
Transition to unconditional secure symmetric Key generation	Secure key generation eliminating manual processes and intervention. It Enables more frequent key rotation, enhancing security.
Data Centre to Data Recovery Data Transfers	Secure key generation and distribution to protect all data transfers between data center (DC) and data recovery (DR) locations, even over third-party links.
Critical Infrastructure Control Systems	Detection of eavesdroppers and prevention of Man-in-the-Middle attacks. Security consideration at every level of deployment. This establishes Quantum Safe Networks with the utmost security.
5G Back Haul using QKD Network	Provides 5G core network protection with best-in-class security through Quantum Key Distribution (QKD).

Use Cases:

- Transition to unconditional secure symmetric key generation
- Data Centre (DC) to Data Recovery (DR) Data Transfers
- Quantum security to the critical infrastructure
- 5G Back haul using QKD Network
- End-to-End Encryption

Specifications

Model	Armos QNLX 150G	
Physical	Dimensions	560mmx424mmx85mm (Alice) 560mmx424mmx85mm (Bob)
	Enclosure	2U 19” rack mountable
	Weight	14.5 kgs
Operating Conditions	Operating Temperature Range	15°c - 25°c (ambient), 60% RH
Weak Coherent	Source	DWDM DFB Laser with VOA
QKD Protocol	Protocol	Distributed Phase reference with Decoy
Quantum Channel	Fiber Type	SMF-28
	Fiber Transmission Loss (typical)	0.2db/km | 30 db (Max - 150km)
	Secret Key Rate (typical)	11520 AES 256 key per hour
Clock Synchronization	Fiber Type	SMF-28
	Connector	ST/UPC
Configurations / Topologies	• Supports Hub N Spoke config with 5 Alices connects to 1 Bob • Supports extensions of QKD distance using trusted node technology	
Interfaces	Key Interface and External Applications	ETSI GS QKD 014 V1.1.1 with KMS Cisco Skip Protocol
	Host Computer Interface	GUI, Browser bases
QKD Software	Authentication	3 Factor Authentication
	Error Correction, Privacy Amplification, Reconciliation	QNu proprietary algorithms optimized for execution on high-performance FPGA and co-processor compute engine
Security	• Tamper proof hardware • Provably secure key distribution and instantaneous intrusion detection • Robust against photon number splitting attack (Emulation) • PQC enabled pre authenticated classical channel • Resiliency against side channel attacks	
Management and Monitoring Functions	• Diagnostics and operational status reporting along with system configuration & recovery • Auto-calibration • Programmable key parameters: VOA, Temperature, QBER and IP address • Built in test equipment (BITE)	
Power	Input Voltage	Auto ranging 100-240VAC @ 50/60Hz
	Connector	EAC 309, Power Entry