Digital Quantum Key Distribution (dQKD) for Quantum-safe Key Exchange

Accelerating the World's Transition towards a Quantum-Safe Future with Software-Defined Quantum-Safe Key Exchange

Introduction

As quantum computing advances, today's encryption methods will soon be rendered obsolete. Secure Key Exchange is the foundation for an secure network; however, it must evolve to resist quantum attacks tomorrow.

— The need for evolution in cybersecurity is immense.

— The cost of a breach is increasing exponentially.

Product Overview

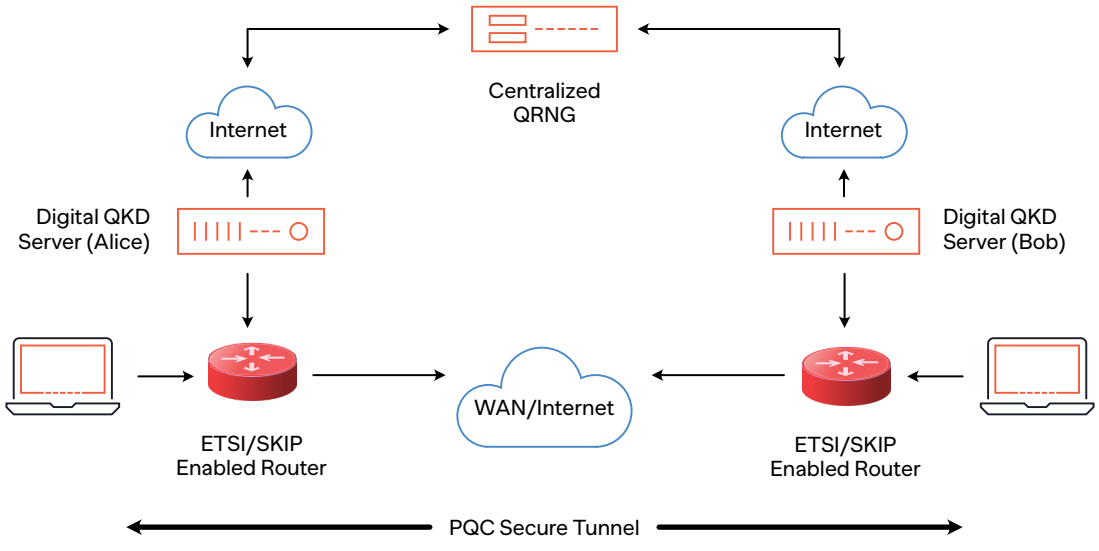
— QNu Labs' **Digital QKD (dQKD)** is a software-defined, Quantum-Secure Key Distribution system that delivers the strength of quantum security without the need for quantum hardware or channels.

— Uses **Quantum Random Number Generators (QRNGs)**, advanced entropy extractors, and post-quantum algorithm ML-KEM and QNu Labs Proprietary **HODOS (PQC).**

— Seamless integration into enterprise IT and Cloud Infrastructures.

— Scalable, compliant, and ready for deployment today.

Network Architecture



Digital QKD Network Architecture

Product Overview

- **Hardware-free Quantum Security:** Achieve quantum-grade protection without the cost or complexity of physical qkd systems. protects against shor's and grover's algorithms.com
- **Future-Proof Architecture:** Combines Quantum Random Number Generator (QRNG) with Post-Quantum Cryptography (PQC) to resist both classical and quantum attacks. Automated key rotation, expiry, and destruction.
- **Cloud & On-Prem Ready:** Cloud-first and fully compatible with AWS, Azure, and private networks.
- **Global Scalability:** Securely exchange keys across any distance (from metro to intercontinental links)
- **Compliant & Interoperable:** Built in alignment with ETSI GS QKD 014, SKIP, and TLS 1.3 standards.

Traditional QKD vs Digital QKD

Aspect	Traditional (Hardware-based) QKD	Digital QKD (QNu Labs)
Infrastructure	Uses **dedicated optical fibre links** to transmit quantum states directly between nodes.	Operates securely over **existing IP/TLS networks**, without requiring dedicated fibre.
Hardware	Involves **specialized quantum transmitters and receivers** (photon sources, detectors, etc.).	Implements QKD principles through **software-defined cryptography**, minimizing dependence on specialized hardware.
Distance	Typically effective up to **100–200 km** in point-to-point links; can be extended using trusted nodes or quantum repeaters.	Provides **global, cloud-agnostic coverage** through networked and virtualized architectures.
Scalability	Expansion requires **additional optical infrastructure**, making scaling complex and costly.	**Linearly scalable** across multiple nodes using standard network protocols and hybrid PQC-QKD integration.
Integration	Often relies on **custom or vendor-specific interfaces** and formats.	**Compliant with ETSI, SKIP, and PQC standards**, enabling seamless interoperability with classical and post-quantum systems
Use Case Strength	Ideal for **ultra-secure point-to-point links** and **research-grade quantum networks.**	Best suited for **large-scale, cloud-integrated, and geographically distributed environments**.
Aspect	**Traditional (Hardware-based) QKD**	**Digital QKD (QNu Labs)**

Technical Specifications & Performance Benchmarks

Parameter	Value/Performance
Key Size	256 bits
Key Generation Time	~3 seconds per key
Key Throughput	~1200 keys/hour
Key Retrieval Latency	0.01 – 0.028 seconds
Entropy Source	Quantum Random Number Generator (QRNG)
Key Derivation Methods	HKDF-SHA512, ML-KEM, HODOS
Network Compatibility	IPv4, HTTPS, TLS 1.3
System Integration	Works with existing Key Management Systems (KMS)
Storage Method	In-memory hash tables
Key Generation Latency	~3 seconds
Key Retrieval Time	< 0.03 seconds
Throughput 1200 keys/hour (linear scalability)	1200 keys/hour (linear scalability)
Distance Support	Global coverage over public & cloud networks
Cloud Tested Platforms	AWS (Singapore), Azure (Global)

Q→NU

QNu Labs is revolutionizing cybersecurity with cutting-edge quantum-safe solutions, making India a leader in quantum cryptography. Through its patent-protected products - Armos and Tropos, QNu Labs is at the forefront to enable quantum secure key generation & distribution for secure data transmission.

With its innovative QShield platform, which is based on NIST complaint PQC algorithms, QNu offers quantum-secure services such as VPN, messaging, file sharing & key management (QHSM).

QNu Labs is at the forefront of quantum security, shaping the future of secure communications & protecting critical infrastructures like finance, defence, and telecom from future quantum threats.

Have a trusted advisor get in touch with you to explore how QHSM can protect your operations from quantum cyber threats.

Request a Demo

Scan for more details

Registered Office:

QuNu Labs Private Limited, Centenary Building, 2nd Floor, East Wing, #28 MG Road Bengaluru - 560025

CIN: U72900KA2016PTC096629