



Q-VIKRAM

Compact 1 Gbps Post-Quantum Network Encryptor
Quantum-safe protection for mission-critical data in transit

1 Gbps | FIPS 203 ML-KEM Security Level 5 | AES-256-GCM | L2/L3 Protection



QUANTUM-SAFE
NIST FIPS 203
ML-KEM + AES-
256-GCM +
TRNG

**MISSION-CRITICAL
APPLICATIONS**
Defense • Power •
Nuclear • Space •
BFSI

**ATMANIRBHAR
BHARAT**
Indigenously
designed,
developed and
fabricated in India

Q-VIKRAM a.k.a. CPQE is an FPGA-based **1 Gbps network encryption device** providing post-quantum protection for **Layer 2 (Ethernet) and Layer 3 (IP) data**. It combines **NIST FIPS 203 ML-KEM** with **AES-256-GCM** and a **hybrid session-key derivation** mechanism based on **NIST SP 800-56C Rev. 2**, supporting pre-shared keys and optional **QKD-provided key material**. Its enhanced **IPsec framework** supports up to **1,024 Security Associations (SAs)** and **point-to-multipoint deployments**, delivering high-performance, standards-aligned protection for **mission-critical data in transit**.

Q-VIKRAM

Compact Post-Quantum Network Encryptor

Quantum-safe protection for mission-critical data in transit

Crypto Features

- FIPS 203 ML-KEM-1024 (NIST Level 5 Security)
- AES-256-GCM symmetric encryption
- Hybrid session-key derivation based on NIST SP 800-56C Rev. 2
- Supports pre-shared keys and optional QKD-provided key material
- NIST SP 800-90B-aligned TRNG
- FPGA-based HDL implementation of cryptographic algorithms and TRNG
- Red-Black separation for symmetric cryptographic processing
- Field-upgradable symmetric encryption algorithm FPGA IP core
- Crypto Agility – Support for proprietary cryptographic IP cores

Networking Features

- 1 Gbps encryption throughput
- Layer 2 Ethernet frame protection with MACsec-compatible framework and OOB ML-KEM
- Layer 3 IP packet protection with enhanced IPsec ESP tunnel mode
- Up to 1,024 IPsec Security Associations (SAs) between peer Q-VIKRAMs
- Point-to-multipoint network support
- LC-LC and RJ45 data interfaces
- OS2 single-mode fiber & CAT5e Ethernet cable support
- QKD & NMS interfaces with OM3 multimode fiber
- GUI and Console Ports

Security and Tamper Protection

- Side-channel leakage attack resistant cryptographic HDL implementations
- Active physical tamper monitoring under powered and unpowered conditions
- Emergency key erasure using keylock and toggle switch
- Multi-factor authentication using a security token, Numpad and password
- Secure key-loading port with dedicated security connector
- Secure algorithm-loading port with dedicated security connector

System Features

- FPGA-Based • High Throughput • Low Latency
- Tabletop / 19-inch rack-mountable
- Industrial-grade components
- Convection cooled
- Alarm LED panel and Buzzer
- Field-replaceable Li-SOCl₂ battery for tamper monitoring and RTC
- 2× AC + 2× DC hot-standby power supplies
- 18–75 V DC / 90–264 V AC 50/60 Hz
- 2U | 3.5" H × 19" W × 23" D | <10 kg
- Operating temperature: –20°C to +45°C



Centre for Development of Telematics

Corporate Office:
C-DOT Campus, Mehrauli,
New Delhi - 110 030, India
Phone: +91 11 2680 2856
Fax: +91 11 2680 3338

C-DOT Campus, Electronics City,
Phase-I, Hosur Road,
Bengaluru - 560 100, India
Phone: +91 80 2511 9001
Fax: +91 80 2511 9601

www.cdote.in

