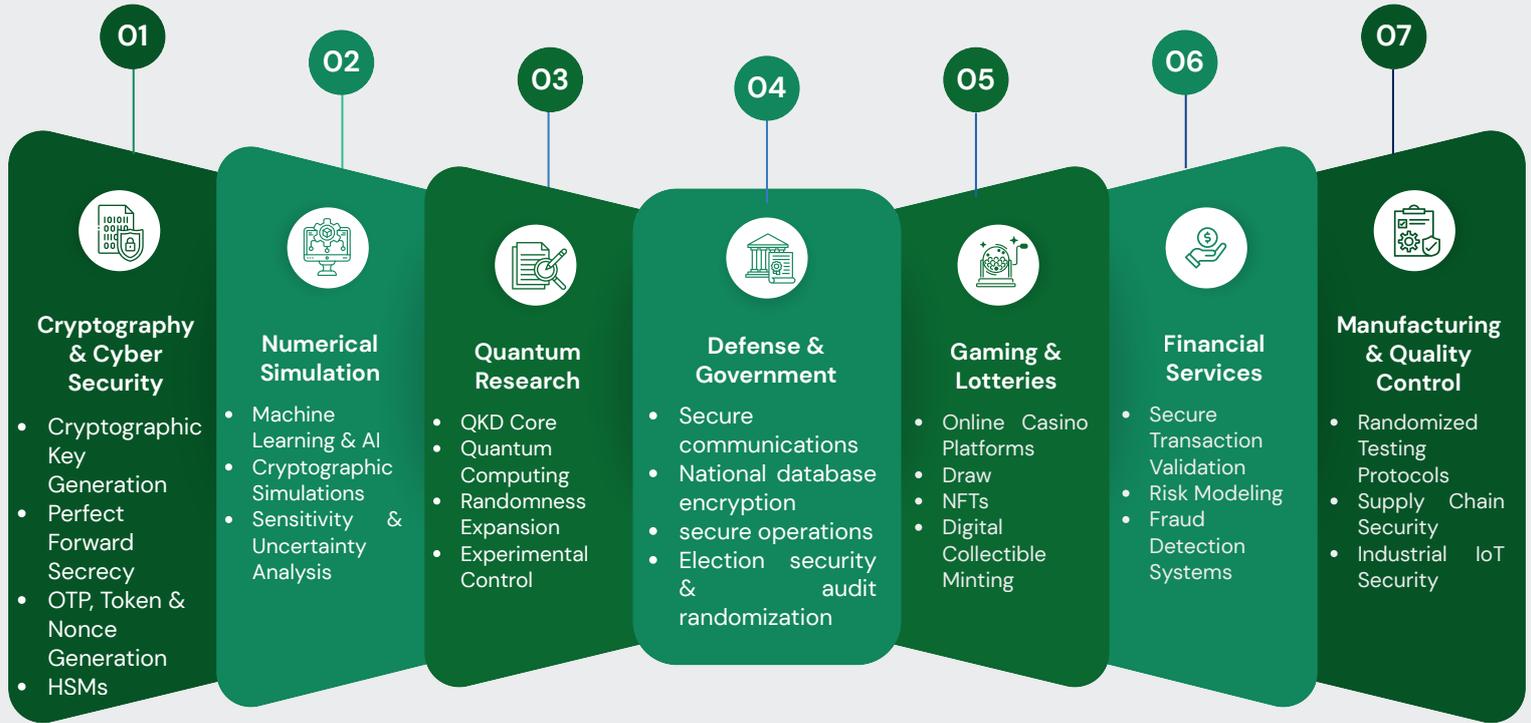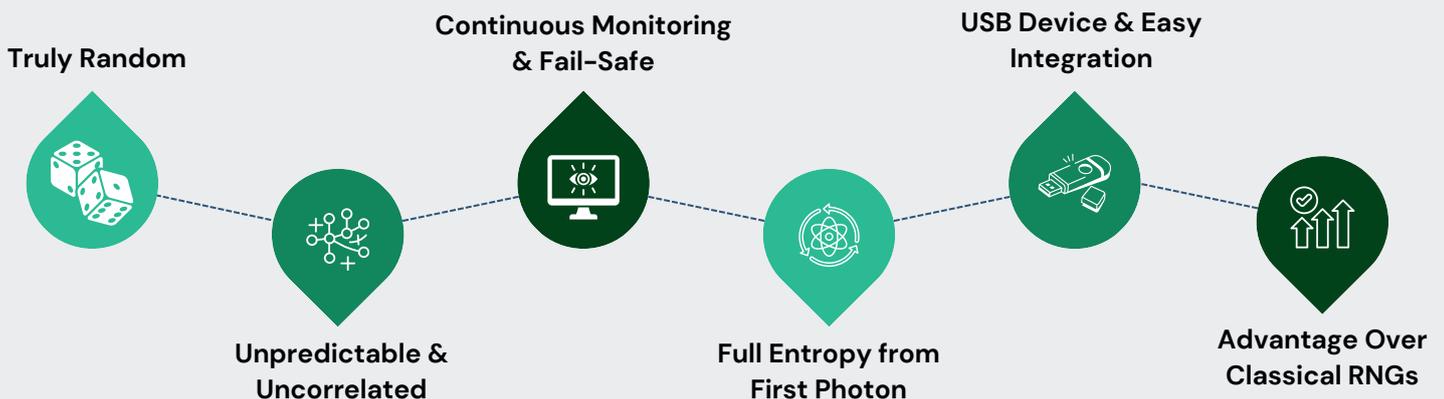# Q-Drive

Q-Drive USB harnesses the fundamental unpredictability of quantum mechanics to generate truly random numbers, unlike algorithm-based generators. It delivers guaranteed, full-entropy randomness instantly, features continuous self-monitoring for fail-safe operation, and offers simple plug-and-play integration across all major operating systems.

Where Quantum Randomness Matters

Critical applications across industries

01

Cryptography & Cyber Security

- Cryptographic Key Generation
- Perfect Forward Secrecy
- OTP, Token & Nonce Generation
- HSMs

02

Numerical Simulation

- Machine Learning & AI
- Cryptographic Simulations
- Sensitivity & Uncertainty Analysis

03

Quantum Research

- QKD Core
- Quantum Computing Randomness Expansion
- Experimental Control

04

Defense & Government

- Secure communications
- National database encryption
- secure operations
- Election security & audit randomization

05

Gaming & Lotteries

- Online Casino Platforms
- Draw
- NFTs
- Digital Collectible Minting

06

Financial Services

- Secure Transaction Validation
- Risk Modeling
- Fraud Detection Systems

07

Manufacturing & Quality Control

- Randomized Testing Protocols
- Supply Chain Security
- Industrial IoT Security

Core Features

Truly Random

Unpredictable & Uncorrelated

Continuous Monitoring & Fail-Safe

Full Entropy from First Photon

USB Device & Easy Integration

Advantage Over Classical RNGs

Q-Drive

Specifications

True Quantum Randomness	Generates randomness from quantum fluctuations ensuring inherent unpredictability and non-repeatability.
NIST 800-90A/B/C Compliant for Cryptographic Assurance	Meets globally trusted security standards, guaranteeing that randomness is suitable for high-security encryption and key generation.
High Data Output for Real-Time Security Applications	• 5.88 Mbps quantum noise sampling • 1.47 Mbps true random number output
Plug-and-Play USB Design for Instant Deployment	Requires no external power source. USB-powered, portable, and universally compatible with laptops, servers, embedded systems, etc.
Ultra-Portable, Rugged, Metallic Casing	Pocket-sized, weighing less than 0.3 kg device with a hard metallic shell engineered for field use, mobility, and long-term durability.
Secure Hardware Root for Cryptosystems	Acts as a dedicated high-entropy source, the first building block of secure cryptographic systems, enhancing key generation and reducing attack surfaces.
Reliable Performance across Wide Temperature Ranges	Designed for real-world operational conditions with stable performance between 0°C to 40°C and storage capability up to 60°C.
Ideal for High-Security and National-Grade Use Cases	Perfect for government, defense, telecom, banking, cloud, and secure communication environments needing quantum-grade entropy
Indigenous Quantum Hardware Engineered in Pakistan	Local innovation ensures superior support, controlled supply chain, and compliance with national cybersecurity and sovereignty requirements.
Minimum Entropy per Bit	0.997

DON'T WAIT FOR ENCRYPTION TO FAIL

Stay Connected

📞 +92 51 8852886   ✉ info@quantumronics.com

📞 +92 321 9112230   📍 107, First Floor, Evacuee Trust Complex, Agha Khan Road, F-5/1, Islamabad

www.quantumronics.com