

CyCity Quantum Web Standard (CQWS)

A Plain-English Executive, Client & Layman's Orientation to Post-Quantum Cryptography & Physical Quantum Entropy

Target Audience: Business Owners, C-Suite, IT Directors & Clients	Standard Compliance: NIST FIPS 203/204/205, BSI, NSA CNSA 2.0
Hardware Entropy: Quantum Dice DISC™ True Photonic QRNG	Deployment Footprint: Zero-Downtime Linux Kernel Hook (< 850µs)

1. The 10-Second Executive Summary

Every modern website, bank portal, and corporate server relies on standard encryption (RSA or ECC) to secure user passwords, database records, and financial payments. These standard systems work today solely because traditional computers are too slow to guess the encryption keys.

The Imminent Danger: Quantum computers operate on quantum mechanics. When fully operational (known as **Q-Day**), a quantum computer will calculate and break standard RSA encryption in seconds. Today, state-sponsored cyber adversaries are aggressively intercepting and storing encrypted corporate internet traffic to decrypt it once quantum machines arrive—a strategy called **Store-Now-Decrypt-Later (SNDL)**.

■ **The CQWS Solution:** CQWS replaces vulnerable mathematical locks with **NIST-Standardized Post-Quantum Lattice Cryptography** and **True Physical Quantum Hardware Entropy**, rendering enterprise websites, databases, and network traffic mathematically impossible for a quantum computer to crack.

2. The Plain-English Analogy: Safe Lock vs. Living Light Maze

Standard Traditional Encryption (RSA / ECC) The Mechanical Combination Lock	CQWS Post-Quantum Cryptographic Shield The Living Quantum Light Maze
- Represents a safe with a 100-digit mechanical combination. - A classical computer tries one code at a time (taking 100 years). - A Quantum Computer tries trillions of combinations simultaneously, unlocking the safe in seconds. Result: Critical data becomes totally compromised at Q-Day.	- Represents a shifting glass maze whose internal corridors rearrange every microsecond based on real light photons fluctuating in a sub-atomic vacuum. - Even a quantum supercomputer cannot solve a maze that rearranges unpredictably according to the laws of quantum physics. Result: 100% Shor Immune & Quantum Secure.

3. Complete 3-Layer Defense: Transit, Rest, and Process

Layer 1: Data in Transit (Over the Internet / Wire) Every incoming and outgoing connection between client browsers, APIs, and servers is wrapped in NIST FIPS 203 (ML-KEM) lattice cryptography and Pauli XOR stream blinding. Eavesdroppers intercepting optical fiber cables see only pure mathematical white noise.
Layer 2: Data at Rest (In Databases & Storage) Customer databases, user records, and encrypted backups are secured using authenticated AES-256-GCM / ChaCha20 seeded with True Physical Quantum Entropy from Quantum Dice DISC™ PCIe hardware cards. Attackers cannot predict or reverse-engineer seeds.
Layer 3: Data in Process (In Server Memory & Operating Kernel) CQWS executes directly at Ring-0 in the Linux Operating System Kernel. Hostile automated bot probes, unauthorized port scans, and SYN floods are destroyed at line-rate (< 850µs) before consuming server memory or application sockets.

4. Exact Cryptographic Algorithms Used in CQWS

CQWS implements a rigorous, double-locked hybrid cryptographic stack combining the official final NIST standards (released August 2024), authenticated symmetric ciphers, and physical hardware entropy feeds:

Security Function	Algorithm / Specification	Standard & Level	Primary Role & Execution Silicon
Post-Quantum Key Exchange	ML-KEM-768 (formerly Kyber)	NIST FIPS 203 Security Level 3	Quantum-immune session key exchange executing at line-rate on standard classical server CPUs.
Post-Quantum Signatures	ML-DSA-65 / 87 (formerly Dilithium)	NIST FIPS 204 Security Level 3 & 5	Quantum-safe digital signatures, authentication tokens, and root certificate verification.
Stateless Hash Signatures	SLH-DSA (formerly SPHINCS+)	NIST FIPS 205 Stateless Hash	Fallback quantum-resistant signature scheme providing defense against mathematical monoculture.
Classical Hybrid Layer	X25519 (ECDH)	RFC 7748 Elliptic Curve	Classical elliptic-curve key exchange combined in hybrid mode for double-locked protection.
Symmetric Bulk Encryption	AES-256-GCM / ChaCha20-Poly1305	NIST SP 800-38D RFC 8439	High-throughput bulk encryption for data-at-rest and storage, accelerated via CPU AES-NI.
Information-Theoretic Blinding	Pauli XOR Masking	Shannon ITS $H(M C) = H(M)$	One-time dynamic entropy stream padding providing unconditional mathematical secrecy on the wire.
Wire-Speed Interception	Ring-0 Netfilter Hook	NF_INET_PRE_ROUTING Linux Kernel	Intercepts & drops hostile scans at line-rate (< 850µs latency) before memory allocation.
Physical Quantum Entropy	Quantum Dice DISC™ & ANU Labs	NIST SP 800-90B FIPS 140-3 Pass	True physical quantum optical vacuum fluctuation noise (7.999984 b/B) injected into kernel pool.

5. Scientific Distinction: PQC vs. Quantum-Inspired vs. Quantum Hardware

■ Why We Do NOT Use "Quantum-Inspired" Algorithms:

"Quantum-inspired" is a marketing term used by some vendors for classical software approximations (such as simulated annealing). These formulas run purely in software on predictable algorithms. They do **not** possess mathematical immunity against Shor's quantum attack and are **not accepted** by NIST, BSI, or NSA for post-quantum defense.

1. Standardized Post-Quantum (PQC) Algorithms	2. True Physical Quantum Hardware (QRNG)
• NIST FIPS 203 (ML-KEM) & NIST FIPS 204 (ML-DSA). • Mathematically proven Module-Lattice Learning With Errors (MLWE). • Runs at line-rate on standard classical server silicon (x86_64, ARM64) today. • Mathematically uncrackable by future Quantum Computers (QPUs).	• Quantum Dice DISC™ PCIe hardware & ANU quantum optical feeds. • Measures physical sub-atomic quantum vacuum phase noise. • Delivers 7.999984 bits/byte Shannon entropy. • 100% Non-deterministic physical random seeds (zero software PRNG formulas).

6. Simple 4-Step Logical Architecture Flow

STEP 1: Incoming Traffic Visitor web browsers, mobile applications, or hostile automated hacker bots connect to your public server IP address.
STEP 2: Ring-0 Kernel Netfilter Intercept Hostile port scans, malformed packets, and unauthorized connection attempts are instantly dropped at wire speed (< 850µs) directly at the network interface card.
STEP 3: Quantum Entropy & Lattice Key Exchange Legitimate connections negotiate a double-locked session key using NIST ML-KEM-768 seeded with true physical photon entropy from Quantum Dice DISC™ hardware.
STEP 4: Protected Enterprise Application Core Clean, verified requests reach your web application, microservices, and databases with absolute zero quantum decryption risk and zero CPU drag.

7. Comprehensive Comparison: Traditional SSL vs. WAF vs. CQWS

Evaluation Criteria	Traditional SSL/TLS	Cloudflare / Standard WAF	CyCity CQWS Shield
Quantum Computer Immunity	■ Broken by Shor's Q-Day	■ No Quantum Resistance	■ 100% Shor Immune (FIPS 203)
SNDL Attack Defense	■ Traffic Decryptable Later	■ Traffic Decryptable Later	■ Pauli XOR Blinded (ITS)
Operating Kernel Layer	Ring-3 (User Space)	Ring-3 (Reverse Proxy)	■ Ring-0 Linux Kernel Hook
Randomness / Entropy Source	Software PRNG Math	Standard OS Math	■ Physical Vacuum Photons
Port Scan Cloaking	Ports Exposed to Public	Filtered After Arrival	■ Stealth Cloaked at NIC
Processing Latency	Standard TLS Handshake	15ms – 45ms Proxy Hop	■ < 850µs Zero-Copy Hook
2030 Mandate Compliance	■ Non-Compliant	■ Partial / Third-Party	■ NIST FIPS 203/204 Standard

8. Executive & Operational FAQ

Q1: Do we need to buy quantum computers to use CQWS? Answer: No. CQWS installs as a lightweight software kernel driver on your existing classical Linux or cloud servers (AWS, Google Cloud, Microsoft Azure, Hetzner, or Bare Metal silicon).	Q2: Do we need to rewrite our application code or databases? Answer: Zero code changes. CQWS operates seamlessly in the Linux operating system kernel underneath your web apps, transparently shielding database logins, APIs, and payments.
Q3: What critical problems does this solve immediately? Answer: It halts Store-Now-Decrypt-Later (SNDL) espionage, renders servers invisible to hacker port probes, and guarantees immediate audit compliance with 2030 federal post-quantum mandates.	Q4: Will CQWS slow down our websites or APIs? Answer: No. Because packet inspection occurs natively at Ring-0 in the Linux netfilter subsystem, execution occurs in under 850 microseconds with 0.00% observable CPU drag.

9. Corporate Governance & Global Entity Provenance

CyCity Inc. (United States Entity) 8 The Green, Suite A, Dover, DE 19901, United States Corporate Website: https://cycity.space LinkedIn: https://www.linkedin.com/company/cycityinc	CyCity International Private Limited (India Entity) Mangalore – 575028, Karnataka, India Institutional Inquiries: info@cycity.space LinkedIn: https://www.linkedin.com/company/cycityinternationalprivatelimited
Official Executive Sign-Off: Merwyn Furtado, Founder & Chief Architect • CyCity Quantum Web Standard (CQWS) <i>All technical claims are verifiable from standard Linux CLI diagnostics. Document certified valid for 2026 enterprise procurement.</i>	