What Is QEncrypt and How Does It Protect Your Data from Quantum Threats?

Understanding QEncrypt's approach to protecting sensitive data from current and future quantum risks.



Austin, Texas Oct 21, 2026 (Issuewire.com) - There is an unspoken expiry date on any encrypted file. While conventional encryption does its job of securing contracts, medical files and banking records, the calculus is set to be altered in the coming decade by a new breed of machine.

Quantum computers can work through certain problems at a speed classical system cannot match, putting the public-key algorithms behind most sensitive data at risk.

There is a method to the attackers' work: they are stockpiling encrypted files with an eye to the future. The security community has a name for it, "harvest now, decrypt later." To forestall such threats, a good number of organizations have made the move to quantum safe encryption, enlisting tools like QEncrypt as a form of insurance.

Why Quantum Computing Puts Current Encryption at Risk

The rule of online security is underwritten by public-key algorithms, RSA and elliptic curve cryptography (ECC) being the chief examples. They are what safeguard key exchange, the process by which two sides come to an agreement on a shared secret.

While a classical computer might be at it for thousands of years without success, a sufficiently powerful

quantum machine with Shor's algorithm can do in short order what would otherwise be impossible.

US federal policy has been influenced by that prospect. NIST's draft IR 8547 puts forward a plan to phase out algorithms susceptible to quantum threats, such as RSA and ECDSA, once we pass 2030, with an outright ban following in 2035. Those have become the baseline for planning purposes under federal directives like OMB memo M-26-15.

Symmetric ciphers prove more resilient. Take AES (Advanced Encryption Standard); with a larger key size like AES-256, there is still a good margin of safety from a quantum attack.

Harvest Now, Decrypt Later

There is no waiting on the part of attackers when it comes to this looming threat. They are already in the habit of making off with encrypted archives and putting them in storage at little cost.

The plan is to let quantum technology do its work once it has had time to develop and then crack open all of it in one go. One can see why they go after data that has a long shelf life like contracts, tax returns or health records; any file that needs to be kept under wraps for a decade is at risk today.

Quantum Encryption: QKD vs. Post-Quantum Cryptography

Quantum encryption is an umbrella term for two quite distinct methods. One is quantum key distribution, or QKD, which relies on the laws of physics to exchange keys. The system transmits key bits in the form of photons through open air or fiber optic cabling; should an eavesdropper try, the resulting disturbance to the photons will be noticed by both sides.

Then there is post-quantum cryptography (PQC). This is the method most would refer to as quantum safe encryption. Rather than hardware, it is a software solution for the phones and laptops already in use, built around novel mathematical problems that can withstand a quantum assault. NIST put the finishing touches on its first trio of PQC standards in August 2024. FIPS 203, for instance, lays out ML-KEM (the Module-Lattice-Based Key-Encapsulation Mechanism) using the CRYSTALS-Kyber algorithm as the go to standard for general encryption, with FIPS 204 and 205 handling digital signatures.

QKD has its place, but it is not without drawbacks. It demands specialized equipment and its own fiber links, with a range of mere tens of kilometres before one need relay node.

The Rising Cost of Weak Data Protection

Even in the absence of quantum threats, a breach is an expensive proposition. The 2025 Cost of a Data Breach Report from IBM shows that for the US, the average tab comes to a record $10.22 million.

In the healthcare sector it is worse still, with the industry's highest average at $7.42 million. And when quantum decryption is within reach, there is the prospect of a second wave of losses as old, harvested archives are used.

What Is QEncrypt?

QEncrypt is a file encryption app that makes use of NIST-standardized post-quantum cryptography for the files it protects. Compatible with Windows, macOS, as well as iOS and Android, the application is a good case study for how this kind of post-quantum defence can be brought to ordinary devices.

What sets the app apart is its concentration on data at rest; in other words, the material kept on one's computer or phone. That is distinct from data in transit like web traffic or messaging. Archives are of particular concern since they present the most attractive targets for an attacker to make off with. After all, one does not get rid of old photos, videos, spreadsheets and documents right away.

The method used here is in line with the sort of thing NIST and the NSA would have you do, using software algorithms instead of quantum hardware. In doing so, it demonstrates that the move to PQC is not confined to government networks but is also relevant for small business and personal use.

Core Functionalities and How They Protect Data

Each functionality below maps to a specific security principle. Understanding these principles helps readers evaluate any post-quantum tool, beyond this single example.

- *Hybrid Encryption: AES Plus ML-KEM*

By way of a hybrid design, the app makes use of AES in conjunction with CRYSTALS-Kyber, the algorithm at the heart of NIST's ML-KEM standard. Under this, AES is put to work on the file content, while ML-KEM is responsible for protecting the key to it. The result is that an attacker would have to overcome both algorithms to get at the file.

There is good reason security researchers are fond of such hybrid approaches in times of transition. Newer algorithms do not yet have the same depth of real-world testing behind them. One has only to look at SIKE, a post-quantum contender that was brought down by a classical attack in 2022. A hybrid model allows for a proven layer to remain as the more recent options mature.

- *NIST-Standardized Algorithms*

There is value in standardization, not least because it allows public scrutiny to uncover any shortcomings at an early stage. NIST, for instance, put ML-KEM through a global evaluation spanning several years before making it final. The quantum-resistant component of the app is built in accordance with that FIPS 203 standard. For those in regulated sectors, such alignment with standards makes the task of compliance planning a good deal simpler.

- *Local Encryption Engine*

By having the app's encryption engine operate on the user's device, we ensure files are encrypted and decrypted locally. It is a method that limits exposure; with all processing done in house, there is no plaintext data to be found on remote servers. The local nature of the work also means the owner has direct control over any key material.

- *Automatic Secure Deletion*

The original file must be put out of the way for encryption to be of any real use. Our app is designed to handle this: once a file is encrypted, the unencrypted one is automatically done away with. It is a simple measure that plugs a hole in security all too often left open. One might encrypt a copy and not think twice about the original sitting in a downloads folder, but the automatic deletion takes care of any such residual risk.

- *Folder-Level Encryption*

There is a tendency for gaps to appear when files are encrypted individually. By contrast, folder-level encryption will safeguard an entire directory in one go; it is the way to ensure that a body of related records, say a complete tax archive, remains undercover.

- *Quantum-Safe Sharing, Signing, and Verification*

Then there is the matter of sharing. Files make their way from colleagues to clients or family, and quantum-safe keys can be used to share them with confidence, preserving confidentiality in the process. Integrity is another concern altogether, addressed by file signing and verification. A digital signature serves as proof to the recipient that what has been received is exactly as the sender put it out, unaltered.

- *Modular, Updatable Architecture*

There is an inevitability to the way cryptographic standards evolve. “Crypto agility” is what security professionals refer to when they talk of the capacity to make a swift change in algorithms, and the app’s modular construction is built for exactly that. When NIST puts out fresh guidance, a tool with such modularity will get up to speed more readily than something less flexible.

- *Cross-Platform Consistency*

Then there are the sensitive files making their way from laptops to desktops and on to phones. To ensure the same level of protection follows them, we have native apps on all four of the major platforms. It is a matter of consistency; one device left without safeguards is invariably the weakest point in the chain.

Why QEncrypt Factors into Modern Security

In the way it is built, the app is an expression of some of the wider tenets of modern security. They are principles that any organization or individual would do well to keep in mind when they set about a post-quantum transition.

- **Defense in depth:** There is also the matter of layered encryption, which is as much a part of today’s security as it has ever been. One can see this in NIST’s draft guidance for the transition; by not including hybrid modes in what will be disallowed after 2035, the agency is making room for a migration that is both low-risk and phased in over time.
- **Breaking the harvest-now, decrypt-later chain:** There are three phases to the threat: first the data is harvested by attackers, then quantum computing comes of age, and then the decryption is carried out. Post-quantum encryption is what severs that link in the last phase; it puts up a wall of lattice-based mathematics that can withstand a quantum assault, even on a file that has been copied.
- **Software-based deployment:** As for migration, most plans put PQC at the heart of things. The reason is simple: PQC will work with the hardware you already have. QKD, on the other hand, demands its own optical infrastructure.
- **Algorithm transparency:** By making its algorithms a matter of public record, the app affords independent reviewers the transparency they need to measure up against NIST publications. It is the kind of openness that underpins an informed choice when it comes to security tools.

How to Evaluate Any Quantum-Safe Encryption Tool

When one is in the market to compare post-quantum tools, a straightforward checklist will do. Consider the following points:

- **Named algorithms:** any credible tool will tell you precisely which ones are in use.
- Standards alignment: there should be no ambiguity about support for NIST FIPS 203 (ML-KEM).
- **Hybrid design:** having a classical component like AES puts a safety net in place.
- **Processing location:** with local encryption, the device retains both the keys and plaintext.
- **Handling of originals:** secure deletion is necessary so that unguarded copies do not persist.
- **Update path:** crypto agility is what makes it possible to get on board with new standards as they come along.
- **Independent review:** for added credibility, third-party audits or some form of published security documentation are to be expected.

Conclusion

The day is coming when quantum computing will put a new spin on digital security, and that day is getting closer. The means to defend against it are here. NIST has put the finishing touches on its post-quantum standards and federal bodies have laid out firm dates for migration.

While quantum key distribution (QKD) has its place in certain niche networks, software solutions in the way of quantum safe encryption are a more expedient option for the average business or individual.

It is prudent to secure long-lived files before an attacker has the chance to make them legible. A sensible approach is to begin with the most sensitive records and work from there to cover every device.

In the end, any robust security posture today must account for quantum-era risks as well as ransomware. To see how hybrid post-quantum file encryption can be applied on Windows, macOS, iOS or Android, one can look to QEncrypt for a case in point.

Media Contact

FiveRivers Technologies

*********@fiveriverstech.com

+1 512-543-9093

6001 W Parmer Lane Ste 370 #734

https://fiveriverstech.com/

Source : https://qencrypt.app/

See on IssueWire