QUANTUMXCHANGE™

PHIQ

SOLUTIONS BRIEF

"Anyone that wants to make sure that their data is protected longer than 10 years should move to alternative forms of encryption now."

May 2018

Arvind Krishna
CEO, IBM

"In a 5-10 year timeframe quantum computing will break encryption as we know it today."

Davos 2020

Sundar Pichai
CEO, Alphabet and Google

"Quantum computing has a one-in-seven chance of breaking RSA-2048 encryption by 2026. By 2031, that chance jumps to 50 percent."

September 2016 report, "Quantum Computing: A New Threat to Cybersecurity."

Michele Mosca
Co-Founder, University of Waterloo's Institue for Quantum Computing

A Response to NIST's Post-Quantum Cryptography Adoption Challenges and Planning Requirements

Cybersecurity is about to change. Public Key Encryption (PKE), the system that for years has protected our digital universe and communications networks is in danger of becoming obsolete. No one argues if a quantum computer will break today's encryption standards — Shor's algorithm has proven this to be true. How soon is almost beside the point. History shows past cryptographic transitions can take years, even decades to complete.

In 2005 and again in 2007, the U.S. National Institute of Standards and Technology (NIST) recommended through special report SP 800-57 that subscribers move from 1024-bit to 2048-bit RSA by 2010. In 2011, NIST upgraded their policy and issued special publication SP 800-131A to allow for a three-year transition period from 1024 to 2048 bits ending Dec. 31, 2013. It took more than 20 years for the Advanced Encryption Standard (AES) to completely replace Data Encryption Standard (DES) and 3DES.

Today, RSA-2048 encryption is considered the gold standard for PKE and critical to the protection of email exchanges, VPNs, secure webpage connections, digital supply chains, e-commerce, cryptocurrencies, passwords, and users accounts. If PKE enables more than 4.5 billion internet users to securely access 200 million websites and engage in some $3 trillion of retail e-commerce annually[1], why are so many organizations taking a lackadaisical, wait and see attitude to quantum readiness planning and execution? Many are relying on the Post-Quantum Cryptography (PQC) project sponsored by NIST to determine the set of PQC standards and migration guidelines needed to augment and ultimately replace RSA.

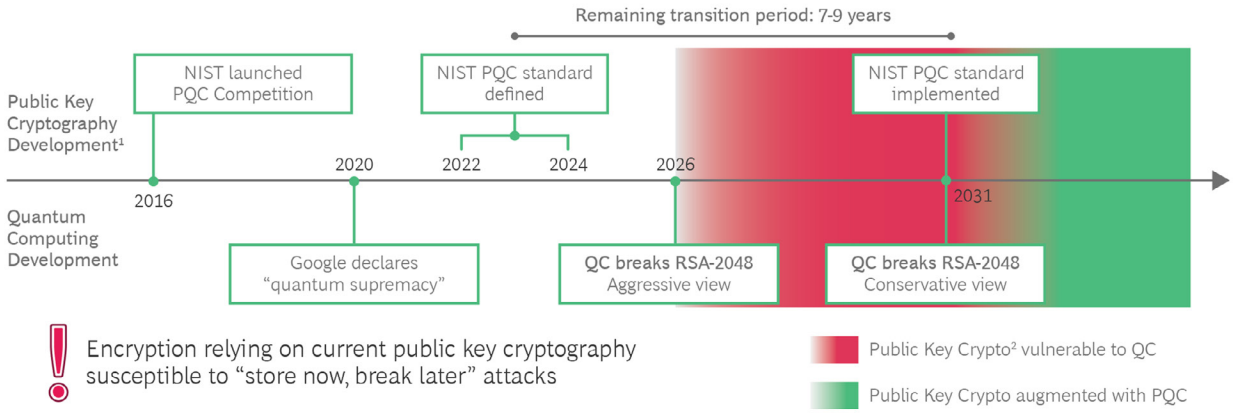
In the April 2021 report published by NIST, Getting Ready for Post-Quantum Cryptography the standards body outlines the challenges associated with adopting and using PQC algorithms after the standardization process is complete — which is currently on pace for selection by the 2022–24 time frame. As mentioned above, and reinforced in the NIST paper, experience has shown that in the best case, another 5–15 more years will be needed after the publication of the cryptographic standards before a full transition is completed.

This timing is problematic on three fronts:

- A quantum computer may be available before then.
- There is no guarantee that the cryptographic standards selected will not be broken by adversaries or vulnerable to implementation errors. Again, if we look to history, we will find that all past cryptographic standards have been broken.
- "Harvest today, decrypt tomorrow" attacks are happening now.

[1]BCG, "Ensuring Online Security in a Quantum Future," March 30, 2021

The Time Window for Upgrading Cryptographic Infrastructure is Closing Rapidly



Sources: NIST Post-Quantum Cryptography timeline, BCG analysis.

Note: PQC: Post-Quantum Cryptography. NIST: National Institute of Standards and Technology USA.

[1]Based on NIST PQC timeline.

[2]Public Key Cryptography (up to RSA-2048).

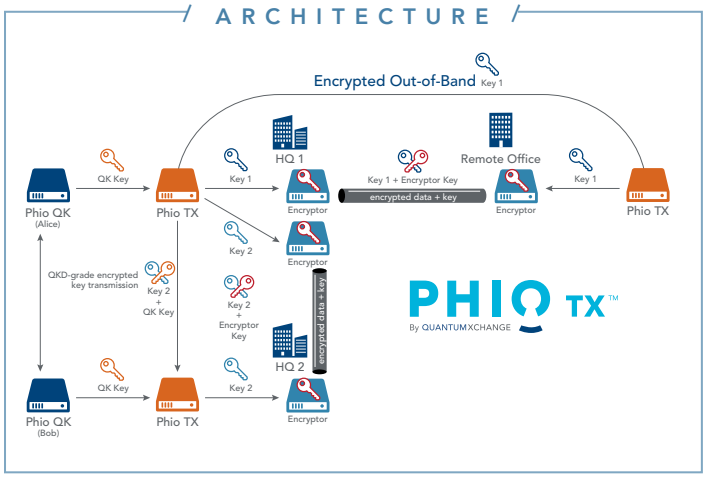
Image Source: BCG, "Ensuring Online Security in a Quantum Future," March 30, 2021

As NIST warns, cryptographic transitions are disruptive and resource intensive. The replacement of algorithms can require changing or replacing libraries, validations tools, hardware, operating systems, application code, device protocols, and user/administrative procedures. Most organization would prefer to avoid expensive rip and replace security projects in favor of an incremental transition toward quantum-safety.

Address Present-Day Data Protection Requirements and the Quantum Threat at Once

Quantum Xchange offers a better approach. It solves for the quantum threat architecturally and at the same time helps organizations overcome the inherent vulnerabilities of modern key-management practices. The company's groundbreaking key distribution system, Phio Trusted Xchange (TX), is a FIPS-compliant, simple architecture overlay that can be dropped into your existing encryption environment to deliver an infinitely stronger cybersecurity posture today and a scalable solution to increase quantum-protection levels as the threat landscape evolves and new risks associated with advances in computing and mathematics emerge.

Phio TX leverages its patent-pending, out-of-band symmetric key delivery technology to supplement native encryption with an additional key-encrypting-key (KEK) transmitted independent of the data path. An attacker must now know two keys are in play, steal them both, and understand when, where, and how they are paired — a near impossible feat even for a quantum computer.



Phio TX is the first key exchange to support quantum keys from any source, i.e., PQC, Quantum Key Distribution (QKD), Quantum Random Number Generated (QRNG), or a combination. Further crypto agility is achieved through Phio TX's support of all PQC Key Encapsulation Mechanism (KEM) candidate algorithms – meaning, customers can change PQC algorithms without disturbing their networks.

If desired, customers can even begin with PQC then eventually add QKD with no changes needed to the underlying infrastructure. There is no fiber required and no distance limitations on key delivery. With Phio TX, keys are continuously rotated and can be delivered point-to-multipoint over any media that can carry TCP/IP v4 or v6 traffic, i.e., fiber, satellite, 4G, 5G, or copper.

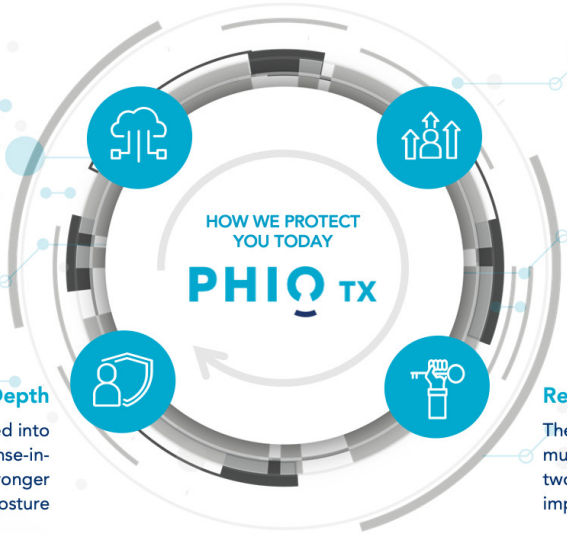
The following diagram captures the top-level challenges and concerns NIST has outlined to help organizations develop and implement algorithm migration playbooks that they warn "can and should begin immediately." See how Phio TX immediately addresses these issues, enabling organizations to easily extend the life of their existing crypto infrastructure and investment by making it immediately quantum safe and crypto agile.

PQC Adoption Issues Raised by NIST	Phio TX Solves/Avoids
Current key sizes and hardware/software limits on future key sizes and signature sizes	X
Latency and throughput thresholds	X
Processes and protocols used for crypto negotiation	X
Current key establishment handshake protocols	X
Where each cryptographic process is taking place in the stack	X
How each cryptographic process is invoked *(e.g., a call to a crypto library, a process embedded in the operating system, a call to an application, cryptography as a service)*	X
Whether the implementation supports the notion of crypto agility	X
Whether the implementation may be updated through software	X
Suppliers and owners of each cryptographic hardware/software/process*	X
Sources of keys and certificates	X
Contractual and legal conditions imposed by and on the supplier	X
Whether the use of the implementation requires validation under the Cryptographic Module Validation Program (CMVP)4	X
Support lifetime or expected end-of-life of the implementation, if stated by the vendor	X
Intellectual property impacts of the migration**	X
Sensitivity of the information that is being protected	X

* Quantum Xchange can provide a list of compatible products which reduces an enterprises effort to compile a list.
** Quantum Xchange's solution eliminates the intellectual property impacts of migration

There's Too Much at Stake to Wait

Contact Quantum Xchange to learn more about our risk free and economic friendly approach to post-quantum safety that provides instant security benefits to your organization and a key distribution system for the ages.



Out-of-Band Key Delivery
Symmetric out-of-band key delivery, over any TCP/IP connection, means your data is no longer sent with the key

Scalability & Crypto-Agility
Gives companies & governments choice and affordable infrastructure to easily upgrade defenses as the threat landscape evolves

Defense-in-Depth
Simple overlay architecture can be dropped into any crypto environment to enable a "defense-in-depth" approach for an infinitely stronger cybersecurity posture

Resilience
The Phio TX "hive" network provides multi-path key routing coupled with a two-key approach, making it virtually impossible to track keys