QUANTUMXCHANGE

DATA SHEET

PHIO

Prepare for the quantum threat with Phio™ by Quantum Xchange

THE FIRST AND ONLY QUANTUM-SAFE KEY DISTRIBUTION SYSTEM

As the provider of unbreakable key exchange, ultra-secure communications, and quantum-ready solutions, Quantum Xchange gives commercial enterprises and government agencies the ultimate defense to keep high-value data safe — today, tomorrow, and long into the future. Offering the first commercially-viable quantum-safe network, your organization will enhance your existing encryption infrastructure while making it quantum ready, crypto agile, and resistant to quantum attack.

The Quantum Threat Is Real and Here Today

As technology heavyweights like IBM, Microsoft, Google, and governments (domestic and foreign) engage in a cyber arms race for quantum supremacy, bad actors are stockpiling encrypted data now, to be deciphered in the near future by quantum computers. This means that critical SSL-protected data, that today can be easily scraped and stored, will be available for complete decryption in the near future. Therefore, all secrets that are protected today with SSL (or public-private key cryptography such as ECC) will be compromised. Quantum computers will fundamentally change how organizations secure their most sensitive data. Shor's algorithm published in 1994 uses a quantum computer to factor an integer N into its prime number factors. It proves that what once took eons to compute using modern computers will only take seconds using a quantum computer. Large prime numbers, that form the underpinnings of today's public-private key encryption protocols, will be easily and quickly factored by quantum computers, leaving mission-critical data exposed and at risk. As the computing and threat landscapes continue to evolve and change, organizations without a well-articulated, quantum risk management plan will begin to lose business, confidence, and trust to organizations that do.

Why Quantum-Safe Key Distribution?

There is a solution, available today, that does not require ripping and replacing existing encryption solutions. It enables enterprises to build a dynamic, crypto-agile network that can easily scale to meet current needs while preparing for quantum cryptography at any time.

Phio™ TX by Quantum Xchange separates the data and key delivery channel, making a brute force, quantum computer attack practically impossible. Combining keys delivered inline by traditional methods and out-of-band with quantum-safe key distribution allows for unobtrusive deployment on existing networks, while significantly increasing the encrypted channel's resistance to attacks.

PHIO
By QUANTUMXCHANGE

Phio Solutions by Quantum Xchange

Quantum Xchange offers end-to-end quantum readiness through our innovative Phio system, which you can deploy today to sit side-by-side with your current network and encryption infrastructure. Choose just Phio TX or Phio QK, a combination of both, or opt for our managed services and dark fiber.

Phio TX

Our patent-pending, out-of-band symmetric key delivery technology that enables encrypted, fault-tolerant and load-balanced point-to-multi-point key transmissions for both traditional and QKD keys across any distance.

- Enhanced quantum security both with and without fiber
- Multi-path key routing
- Exchange keys using QKD or over regular Internet/network connections
- No distance limitations
- Dedicated point-to-point connection not needed to exchange keys
- Incorporate QKD at any time for critical segments

Phio QK

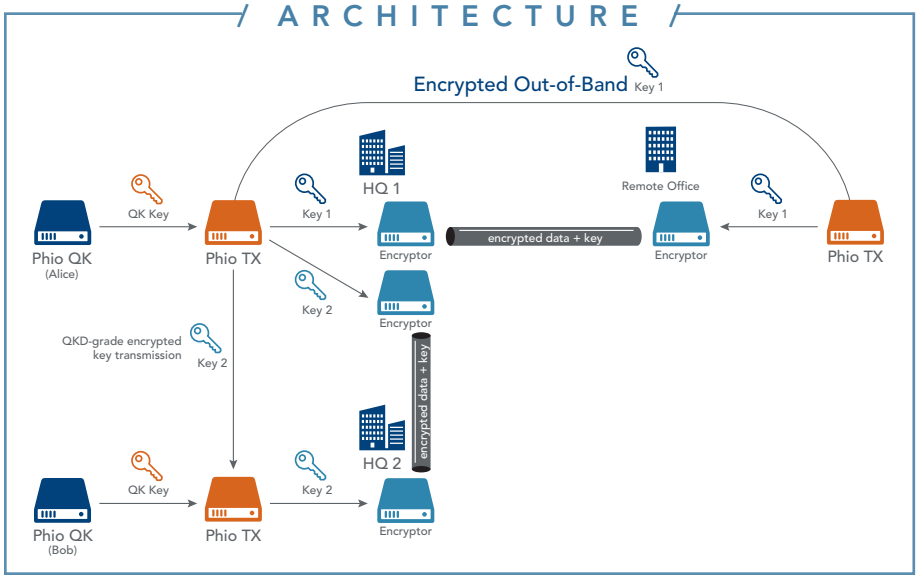
Our Quantum Key Distribution (QKD) hardware, Phio QK, allows for the sending of unbreakable quantum keys. Coupled with Phio TX, QKD is now possible across any distance and using any network.

- Uses the quantum properties of single photons to exchange keys between two locations
- Keys are derived from the exchanged quantum information
- Any attempt to read a photon is detected because of the change in quantum state, and that photon's bit is rejected
- Provably secure: Security is based on the laws of physics, not on difficult math problems
- Forward security: Implementing QKD provides secure key exchange is the foundation for all future encryption

Phio Network and Managed Services

Our quantum-secured network, Phio Network, is the first of its kind in the United States, and allows keys to be securely shared over a wide-ranging network, making large-scale quantum-safe key distribution possible and practical.

- Access to 1,000 kilometers of existing optical fiber and 19 co-location centers along the Boston to Washington route, including key connections to the financial markets on Wall Street with back office operations in New Jersey. Although Quantum Xchange manages the QKD fiber network, you (the customer) retain absolute control and visibility over your encryption keys and critical data using Quantum Xchange's fiber quantum network.
- Our Managed Services offering allows enterprises to easily and quickly deploy quantum-safe key distribution with Phio QK, Phio TX and the Phio Network of dark fiber.



PHIO
By QUANTUMXCHANGE

BUILD YOUR QUANTUM RISK MANAGEMENT PLAN

CHOOSE YOUR DESIRED QUANTUM PROTECTION LEVELS BASED ON RISK TOLERANCE

Our advanced out-of-band key delivery offers multiple crypto options through Phio TX and/or point-to-multi point QKD with no distance limitations with Phio QK.

STRENGTHEN YOUR EXISTING ENCRYPTION

Phio operates seamlessly with your existing crypto and networks. Extend the life of your current encryption by making them quantum-safe now, and easier to layer in QKD in the future.

ENABLE QUANTUM-SAFE INTEROPERABILITY BETWEEN FIBER AND NON-FIBER LOCATIONS.

Phio extends unparalleled security over any TCP/IP link. Independent network key distribution virtually eliminates quantum hacking threat.

Quantum-Safe Transmissions — At Any Distance, Over Any Network

Quantum Xchange saw the opportunity to bring QKD out of the lab and into an enterprise setting. To do so, it had to solve QKD's distance limitations and point-to-point only transmission capabilities. Phio Trusted Xchange (Phio TX) is the first commercially viable quantum-safe network to provide both traditional key-transmission services and Quantum Key Distribution (QKD) via point-to-multi-point transmission across any distance.

Due to Phio's unique design, enterprises can now get quantum-safe key distribution across their existing network and crypto infrastructure. By selecting a level of protection based on their individual risk tolerance and resource availabilities, Phio TX enables organizations to start simple, then grow as the need arises by layering in QKD, thereby making QKD practical and affordable. It is uniquely capable of making traditional crypto-keys quantum safe.

Utilize Quantum Xchange's future-proof, quantum keys to avoid:

SSL scraping attacks — SSL traffic (or messages/data encrypted using PKI) are copied and stored for later decryption

Potential backdoors and yet-to-be-discovered vulnerabilities

Quantum-computing nullification of public/private encryption key transfer methods

PKI vulnerabilities