QUANTUMXCHANGE

PHIO

SOLUTIONS BRIEF

Ultra-Secure, Quantum-Safe Data Protection for Banking and Financial Institutions

Protect Critical Data and Communications Networks from Known and Yet-to-be-Discovered Threats with Quantum-Safe Solutions from Quantum Xchange

Banking on Quantum Computers — The Promise and The Peril

Major banks are betting that quantum computing can find them an investment edge. Goldman Sachs, Wells Fargo, and JPMorgan Chase are among the firms testing early stage quantum computers to solve complex and resource-intensive financial calculations. Currently quantum computers can still be beaten in most applications by traditional computers. But quantum power is growing at a dizzying rate. Some experts predict that quantum computers have the potential to speed up financial computations by more than a thousand times and could be here in the next 5–10 years.

With such promise comes peril. Q-Day, or the day in which a quantum computer breaks the Public Key Encryption (PKE) that protects most of our digital world and the personal data critical to banking, is approaching and could arrive much sooner than anticipated.

The banking and finance industry is already a top target for cybercriminal activity, costing U.S. banks $18.37 million annually according to Accenture.[1] Responses to data breaches are increasingly severe, with an average stock price decline of 6.8%, up from 4.4% in 2016 according to the 2020 Cost of a Data Breach Report by IBM and Ponemon Institute. The looming quantum threat, current cybercriminal activity waged against financial institutions, compounded by the pressures of an already highly regulated, risk-intense industry, means financial institutions should start preparing now for the quantum threat. There's just too much at stake to wait.

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

When a quantum computer is available that can break encryption standards is almost beside the point. Other driving factors point to the urgent need for ultra-secure encryption to protect transmitted data by financial institutions and their partners, these include:

- Current PKE systems, i.e., TLS/SSL and key management practices are rife with vulnerabilities putting today's data and communications networks at risk.
- History shows cryptographic transitions can take years to complete which is why The National Institute for Standards and Technology (NIST) put forth recommendations in 2016 encouraging all organizations to begin preparing then for the quantum cryptographic break.

PHIO TX™
By QUANTUMXCHANGE

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

Be immune to the nullification of public/private encryption key transfer methods by a quantum computer

Escape PKI vulnerabilities

- Any encrypted data that has been intercepted or stored will be vulnerable to decryption in the quantum era. This means a quantum computing system of sufficient power will be able to decrypt stored data with ease, an attack known as "harvest today, decrypt tomorrow."
- Long shelf-life data such as customer PII has the highest cost per record if stolen at $150.[2]

Future-Proofing the World's Data in Motion

In many ways staying ahead of the game in quantum computing is about being able to continue to provide the same core service to customers that banks always have — keeping customers' money safe. Only instead of protecting their money with a stronger vault or an armed guard, banks will have to protect themselves against a quantum computer in the hands of bad actors.

Quantum Xchange offers Phio Trusted Xchange (TX) the first and only quantum-safe key distribution system that provides true crypto agility by supporting quantum keys in any format both math and physics-based, i.e., PQC, QKD, QRNG. Perhaps even more striking is how its patent-pending, out-of-band key delivery technology is uniquely capable of making traditional encryption keys quantum-safe — bringing an immediate, heightened level of security to any network environment while offering the scalability most organizations prefer when evaluating a technology upgrade.

The first-of-its-kind technology provides secure key transfer protected by PQC and/or QKD, in a FIPS 140–2 validated implementation. Phio TX is vendor agnostic and integrates seamlessly with leading cybersecurity products; works within any existing crypto infrastructure avoiding capital-intensive "rip and replace" security projects; and can be deployed across any network media — copper, fiber, satellite, 4G or 5G. If or when maximum QKD-level security is desired, Phio TX can be used to overcome its distance and delivery limitations by enabling quantum keys to travel unlimited distances to multiple transmission points without the need for dedicated fiber.

Quantum Xchange offers leading banks and financial institutes a practical pathway to quantum readiness and an infinitely strong cybersecurity posture today. With our future-proof, unbreakable key exchange in place, financial firms can fully leverage data as a strategic asset and provide the protection and security that customers and partners expect and deserve.

Achieve an instant and infinitely stronger security posture for protecting transmitted data across communications networks and links.

[1] Accenture Ninth Annual Cost of Cybercrime Study
[2] 2020 Cost of a Data Breach Report by IBM and Ponemon Institute

Phio TX Delivers Ultra-Secure Key Distribution

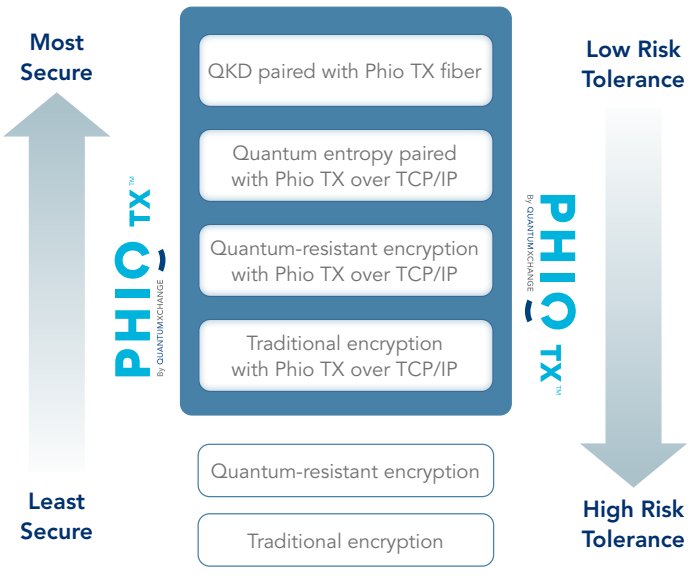
USE CASES

- Out-of-band key delivery over any TCP/IP connection
- Key delivery over extended distances, including satellite or undersea cable
- Enhances existing Layer 2 and Layer 3 solutions
- Key delivery with fiber (QKD) or without

APPLICATIONS

- Headquarters to main datacenter
- Headquarters to branch office and branch-to-branch
- B2B (partner to partner) transactions
- Enterprise locations to cloud services
- Connections from main datacenter to disaster recovery site
- Tamper evident critically sensitive fiber connections with QKD

Phio TX Offers a Wide Range of Data-in-Transit Security



Phio TX Boosts Security for All Forms of Encryption