FIJISHI

# Quantum-Secure Communications for Financial Networks.

*India, 22 May 2025/ 17:14 PM IST*

**Case Study: Quantum-Secure Communications for Financial Networks**

**Industry:** Financial Services & Cybersecurity

**The Challenge:** A leading global bank, processing trillions in transactions daily, was acutely aware of the looming threat posed by quantum computing to current cryptographic standards. Their existing communication infrastructure, while robust by today's standards, was vulnerable to future "harvest now, decrypt later" attacks. They needed a future-proof, quantum-resilient solution to protect sensitive financial data and ensure transactional integrity across their distributed network, including highly decentralized trading platforms.

**The FiRIS Solution:** The bank integrated FiRIS-Guard into its core network and private cloud infrastructure, focusing on securing the underlying communication pathways and data flows.

- **"FiRIS-Guard" – Quantum-Resilient & Proactive Threat Anticipation:**
  - **Integrated Post-Quantum Cryptography (PQC):** FiRIS facilitated the seamless integration and management of PQC algorithms across the network, ensuring that all data in transit was encrypted with quantum-safe methods, protecting against future decryption by quantum computers.
  - **RF Anomaly Detection & Threat Mapping:** Beyond traditional cyber security, FiRIS monitored the physical RF layer for unusual patterns that could indicate advanced eavesdropping attempts or electromagnetic interference attacks designed to disrupt transactions.
  - **"Deceptive Counter-Propagation":** In a highly innovative move, FiRIS was configured to deploy deceptive RF signals in response to detected anomalies, creating false targets or obscuring actual data flows, effectively misleading potential attackers at the physical layer.
  - **Zero-Trust Micro-Segmentation:** FiRIS enforced a granular zero-trust model, micro-segmenting the network down to individual transaction flows and devices. This minimized the lateral movement of any potential threat, even if a part of the network was compromised.
- **Integrated Risk, Governance, and Compliance (GRC):**
  - **Dynamic Risk Assessment & Mitigation:** FiRIS continuously assessed the network's security posture against evolving threats and regulatory changes, automatically adjusting security policies and mitigation strategies in real-time.
  - **Transparent Audit Trails & Reporting:** Automated generation of immutable audit trails provided comprehensive evidence of security measures and compliance with stringent financial regulations (e.g., GDPR, PCI DSS), crucial for internal and external audits.

**Impact and Benefits:**

- **Future-Proofed Security:** Established a leading position in quantum-resilient communications, assuring clients and regulators of long-term data integrity.
- **Enhanced Threat Intelligence:** Gained unprecedented visibility into physical layer threats, enabling a more holistic security posture.

- **Reduced Compliance Burden:** Automated GRC simplified adherence to complex financial regulations, lowering operational overhead.
- **Stronger Client Trust:** The bank could market its superior security capabilities, fostering greater trust among high-value corporate clients.
- **Operational Continuity:** Proactive threat anticipation and deceptive counter-propagation reduced the risk of service disruption from sophisticated cyberattacks.

**Key FiRIS Features Highlighted:**

- "FiRIS-Guard" (Integrated Post-Quantum Cryptography, RF Anomaly Detection & Threat Mapping, Deceptive Counter-Propagation, Zero-Trust Micro-Segmentation)
- Integrated Risk, Governance, and Compliance (Dynamic Risk Assessment & Mitigation, Transparent Audit Trails).