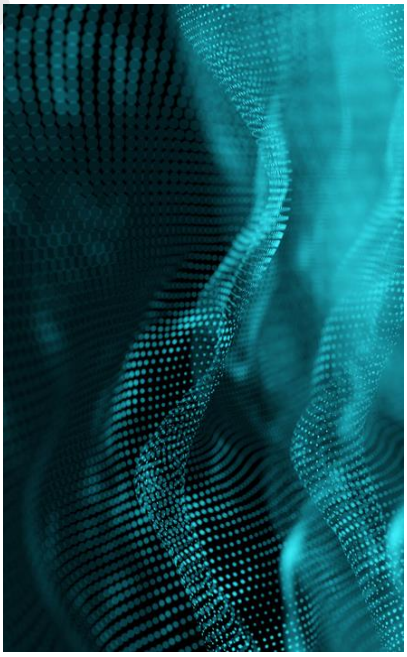
www.pipelinepub.com
Volume 22, Issue 2

The Importance of Simulation in Quantum Network Evolution

By: Michael Cubeddu



Today's telecommunications providers face enormous cybersecurity challenges: from advanced AI-powered attacks to quantum computing threats. These threats are already here in the form of Harvest Now Decrypt Later (HNDL) attacks, where adversaries intercept and store encrypted data now with the intention of decrypting it as more sophisticated technology becomes available.

Telco operators face major threats now and in the future from HNDL

Encryption and authentication are the pillars of our digital security. Today's classical encryption (RSA, ECC, Diffie-Hellman) is based on mathematical problems that are increasingly vulnerable to threats from quantum computing, and authentication methods are increasingly vulnerable to AI-powered attacks.

The most timely and urgent issue that quantum networks address is the threat of advanced attacks on our secure network infrastructure. The date for Q Day, the day a cryptographically relevant quantum computer (CRQC) is capable of breaking public key infrastructure, is continually changing, but it could be anywhere from three to ten years away. Gartner recently estimated that a CRQC could arrive by 2029, and that asymmetric cryptography could be fully broken by 2034. The timeline estimates for Q Day significantly shorten with every milestone in quantum computing hardware and improvements to quantum algorithms, error correction, and Google's recent work on shrinking the resource requirements for CRQC attacks.

With HNDL attacks, adversaries can harvest and store today's encrypted communications, often undetected, and later decrypt that information by leveraging a CRQC. There are some security issues specific to telecommunications that make these organizations more vulnerable to HNDL attacks. They are highly regulated with many laws requiring encrypted data to be stored for set amounts of time.

A Global System for Mobile Communications Association (GSMA) whitepaper on quantum's impact on the telecommunications industry noted that "traditional networking equipment (VPNs, routers), OS, custom equipment and applications, [and] legacy equipment" could be at risk. Nokia's Road to Quantum-Safe Networks whitepaper went into more detail, outlining the types of symmetric and asymmetric cryptography at risk in lower (data link, network layers), upper (transport and application), and telco application layers. They state, "Telecom networks are composed of multiple security domains, ranging from the data plane (carries user data), the control plane (handles network signaling and controls how user data is forwarded), and the management plane (monitors and configures network resources) to the user equipment itself. The recent addition of exposure interfaces to enable network programmability through APIs adds a new attack surface."

Clearly, telecommunications networks are at risk. They often carry sensitive information for government, finance, and healthcare organizations that must remain secure for decades, making quantum risk mitigation a priority. These could include data such as transaction histories, customer records, and encryption keys. A breach in the not-so-distant future could retroactively expose decades of confidential data.

But how can operators address these issues now?

One size does not fit all

There are several technologies available today that can protect sensitive data from HNDL attacks and the arrival of powerful quantum computers: Post-Quantum Cryptography (PQC), Quantum Key Distribution (QKD), and Quantum Secure Communication (QSC).

PQC consists of standards for integrating novel math-based algorithms that replace the legacy math-based algorithms that are used in public key encryption. While not provably immune to future attacks, PQC significantly improves upon the quantum-resistant security of legacy algorithms such as RSA. NIST finalized a set of candidate standards in 2024.

QKD leverages quantum physics to establish and distribute shared keys. Using single encoded photons, also known as qubits, QKD creates encryption keys that are more secure against quantum attacks than those generated by classical methods. This is what is referred to as prepare-and-measure QKD: a point-to-point security mechanism that requires trusted relay points to extend the coverage of QKD over longer distances.

QSC is an ultra-secure physics-based methodology that leverages quantum entanglement networks for more advanced key distribution and authentication protocols that are provably immune to quantum attacks.While all of these approaches have pros and cons, a layered approach that combines PQC with a quantum network architecture is the best approach for providing comprehensive security across the physical layer, the cryptographic layer, the network architecture layer, and the application layer. SK Telecom is supporting and developing this approach, noting that integrating QKD and PQC will be key for enhanced security for current and future 6G networks.

A layered approach provides two desirable features for an organization's security posture: defense-in-depth and cryptographic agility. As the attack landscape evolves over time, so will the standards, algorithms, and protocols – building flexibility into quantum-safe network systems will be critical.

The problem of scale? Meet simulation

Organizations can begin deploying quantum-secure infrastructure now, well before CRQCs become mainstream, but the importance of design and simulation cannot be overstated. Finding the components to build quantum networks can be costly in both time and financial commitment, and it's difficult to test and evaluate all of the pieces at scale.

There are a number of issues related to entanglement that can make testing difficult, including sensitivity to noise, fiber characteristics, hardware imperfections, and architectural decisions. As a result, real-world performance can differ substantially from theoretical predictions, especially as these networks grow more complex. This is why modeling and validating quantum network designs before and during physical deployment is so important.

Enter Quantum Network Simulation. At a high level, these tools allow organizations to assess quantum vulnerabilities and needs, establish proof of value, design to their requirements, and obtain guidance on how to best implement quantum networks – starting at the device level, then expanding to the global view. But when we dive deeper, simulation tools provide telecommunications providers with an opportunity to hone the full stack of quantum network operations, from physical-layer quantum communication to high-level security services (e.g., key distribution, authentication, eavesdropper detection) across diverse topologies, before purchasing any hardware. These simulators can model real-world characteristics such as fiber attenuation, noise, environmental factors, interference, and traffic load. They can also be modeled using existing fiber infrastructure.

Additional benefits of simulation include:

The ability to test different network topologies and configurations, assess their respective performance and underlying services to identify the most cost-effective and resilient architecture tailored to an organization's physical footprint, security requirements, and constraints.

Interoperability and flexibility testing. This ensures the hardware chosen will integrate with classical infrastructure and scale to support future quantum-powered security services. Organizations can also validate the compatibility of multi-vendor quantum components with each other, and test a variety of quantum network protocols and hardware components to ensure crypto-agility and scalability.

Planning for incremental deployment and scaling up. Organizations can model how quantum network performance scales with added nodes, longer distances, or increased data throughput to guide future upgrades, as well as rapidly test and iterate on different quantum services before investing in them.

Mitigating deployment risks. With simulation tools, organizations can identify issues early in the development of the quantum network to prevent costly hardware missteps and reduce operational risk. They can also validate the behavior of the quantum network across metro, long-haul, satellite, and hybrid networks in realistic situations.

Improving workforce readiness. Quantum network simulations provide a training ground for engineers and technicians to become well-versed in quantum principles ahead of a quantum network deployment. This is new technology. Having engineers who are versed in classical and quantum networking will be a benefit to any organization.

Setting the stage for additional use cases

Beyond preparing for changing attack vectors and HNDL attacks, quantum networks will help telecommunications providers move beyond the limitations of current encryption and authentication protocols to keep data secure, while simultaneously adding novel quantum capabilities to core networks and end customers. A quantum network simulator allows them to accurately model realistic quantum networks, evaluate performance under varying conditions, and optimize integration with existing infrastructure, as well as helping to validate, budget, and train for future deployments. This work also provides a foundation for additional applications, including secure access to clouds and data centers, position-based authentication, networking of quantum computers, and networking of distributed quantum sensors.