Using Quantum Network Simulation to De-Risk Quantum-secure Telecommunications

Aliro

www.alirotech.com

Using Quantum Network Simulation to De-Risk Quantum-secure Telecommunications

Executive Summary......1

The Quantum Threat and the Quantum Solution......1

Modeling and validating Quantum Secure Communications (QSC)......4

Aliro Simulator: Advancing Quantum Networking Through Comprehensive Simulation.... 5

Key Features and Capabilities......6

Simulation-Aided Design...... 6

Design Validation and Optimization...... 7

Benefits of Using Aliro Simulator...... 8

Conclusion...... 9

Executive Summary

Today's telecommunications providers face enormous cybersecurity challenges: from advanced AI 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.

Quantum networking technologies can be used to counter these threats today. Entanglement-based Quantum Secure Communication (QSC) offers the highest level of security: unbreakable by advanced threats from AI or a future quantum computer. Acquiring the components to build quantum networks can be costly in both time and financial commitment. However, using a quantum network simulator can significantly reduce these costs, while simultaneously providing other benefits.

Aliro Simulator helps telecommunications operators stay ahead of these sophisticated security threats by providing a safe, flexible environment to:

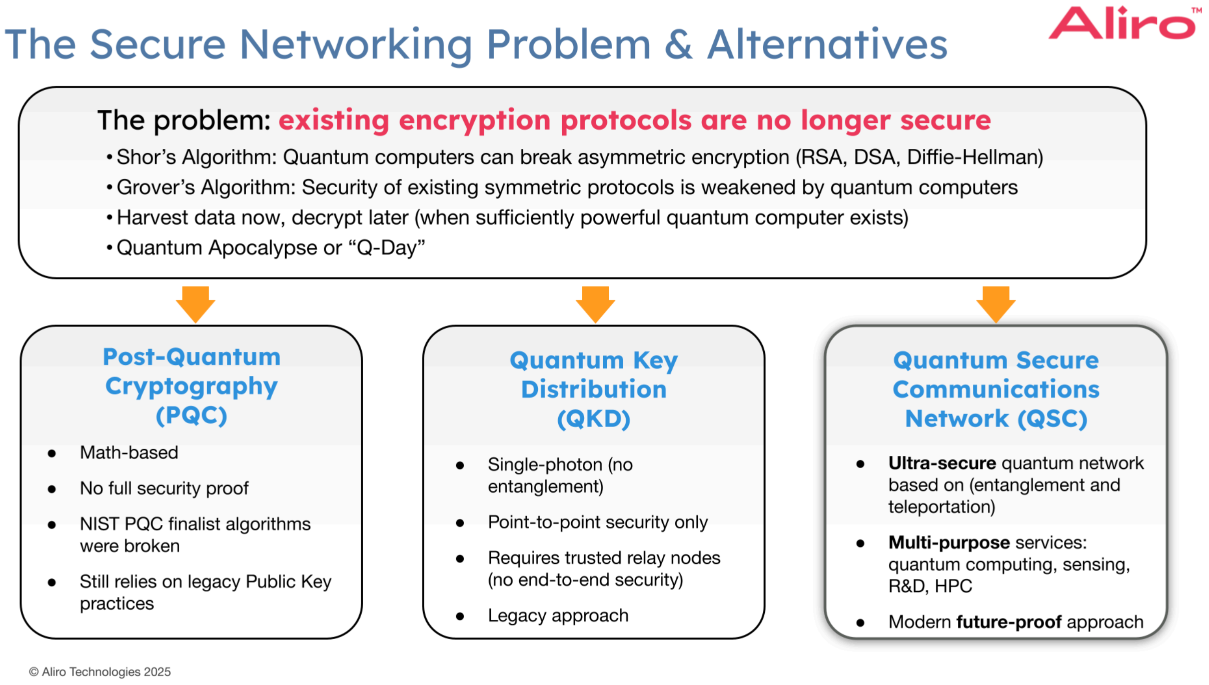
- Model quantum networks on existing fiber infrastructure, optimizing performance and cost.
- Test Quantum Secure Communication (QSC) protocols resistant to both classical and quantum attacks.
- Validate interoperability across hardware and protocols.
- Train technical teams on realistic, future-ready quantum network architectures.

Real-world deployments by leading carriers and government agencies have already demonstrated that quantum-secure telecommunications infrastructure is already in motion. This white paper explores how the telecommunications sector can use quantum network simulators to secure critical communications infrastructure to protect from HNDL attacks today, as well as future breakthroughs in AI and quantum computing.

The Quantum Threat and the Quantum Solution

As quantum computing advances, classical encryption protocols (especially those underpinning public key infrastructure) are increasingly vulnerable. Even before a cryptographically relevant quantum computer arrives, Harvest Now Decrypt Later (HNDL) attacks are already a serious threat. In HNDL attacks, adversaries intercept and store encrypted data now with the intention of decrypting it once quantum computers become capable. This threat underscores the urgency for telecommunications providers to adopt quantum-resilient technologies now.

Telecommunications networks often carry sensitive information for government, finance, and healthcare organizations that must remain secure for decades, making quantum risk mitigation a priority. There are several protections 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).



The Secure Networking Problem & Alternatives

Aliro™

The problem: existing encryption protocols are no longer secure

- Shor's Algorithm: Quantum computers can break asymmetric encryption (RSA, DSA, Diffie-Hellman)
- Grover's Algorithm: Security of existing symmetric protocols is weakened by quantum computers
- Harvest data now, decrypt later (when sufficiently powerful quantum computer exists)
- Quantum Apocalypse or "Q-Day"

Post-Quantum Cryptography (PQC)

- Math-based
- No full security proof
- NIST PQC finalist algorithms were broken
- Still relies on legacy Public Key practices

Quantum Key Distribution (QKD)

- Single-photon (no entanglement)
- Point-to-point security only
- Requires trusted relay nodes (no end-to-end security)
- Legacy approach

Quantum Secure Communications Network (QSC)

- **Ultra-secure** quantum network based on (entanglement and teleportation)
- **Multi-purpose** services: quantum computing, sensing, R&D, HPC
- Modern **future-proof** approach

© Aliro Technologies 2025

(2023-03-27, slide 35)

Post-Quantum Cryptography (PQC). PQC is a well known methodology today. PQC consists of 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 legacy algorithms such as RSA. The National Institute of Standards and Technology (NIST) has finalized a set of candidate standards following rigorous public testing. Several early contenders failed, with some unable to withstand basic decryption attacks using conventional laptops. PQC will become a pervasive tactic for protecting data, deployed across entire networks; this is the baseline of quantum secure infrastructure, but could also contain vulnerabilities that haven't been identified.

Quantum Key Distribution (QKD). QKD advances security by leveraging quantum physics to establish shared keys. Using single encoded photons, also known as qubits, QKD creates encryption keys that are more secure 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 distance of the links. Some vulnerabilities are introduced by these trusted relay points due to data being exposed in the clear at each relay. For links where QSC is not feasible but physics-based protections are needed, QKD can be a helpful method.

Quantum Secure Communications (QSC). QSC is an ultra-secure physics-based methodology that leverages entanglement and teleportation. This is the most secure implementation for protecting the high-volume links that carry the most sensitive data. QSC is modern and future-proof, and because it's entanglement-based this technology can carry out other applications such as interconnecting quantum computers, connecting distributed quantum sensors with one another, and other applications that we're not even aware of today. Overall, this provides the highest security level while maintaining flexibility for future advancements in quantum technology.

The timeline to Q-Day, the day a cryptographically relevant quantum computer (CRQC) comes online, is continually contracting. Since the advent of Shor's algorithm in 1994, researchers and governments have acknowledged the need to replace vulnerable encryption systems. NIST began the formal process of standardizing post-quantum cryptography (PQC) in 2016. In 2019, Google achieved quantum supremacy. And more recently, research from China and new hybrid quantum-classical algorithms suggest that the number of qubits needed to break RSA-2048 could be significantly lower than previously estimated. While conservative estimates project a CRQC to be 10 years away, aggressive forecasts suggest it could arrive in as little as 3–5 years. Gartner recently estimated that a CRQC could arrive by 2029, and that asymmetric cryptography could be fully broken by 2034.

Telecommunication providers that adopt quantum technologies proactively can confidently protect their networks against these threats by validating them under simulated real-world conditions before deployment. This is where quantum network simulators become indispensable. Simulators like the Aliro Simulator empower telecommunications providers to model entanglement-based networks, evaluate performance under varying conditions, and optimize integration with existing infrastructure. By enabling experimentation without physical risk, these tools provide the strategic foresight and operational assurance required to lead in a quantum-secure future. As the countdown to Q-Day accelerates, quantum network simulation lays the foundation for quantum-powered security.

Modeling and validating Quantum Secure Communications (QSC)

Deploying QSC presents technical and operational challenges that are unique to quantum networking due to its use of quantum entanglement, a phenomenon of quantum physics where particles remain interconnected across distances and can be used to generate secure keys without ever sending the key itself across the network - essentially replacing public key cryptography.

Entanglement is inherently sensitive to noise, distance, hardware imperfections, and architectural decisions. As a result, real-world performance can differ substantially from theoretical predictions. This is why modeling and validating quantum network designs before physical deployment is so important.

Quantum network simulators provide telecommunications providers with an opportunity to hone the full stack of quantum network operations, from physical-layer entanglement generation to high-level protocol behavior 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. Using a quantum network simulator to rigorously test quantum networking strategies in a controlled, virtual environment has many advantages, including:

- Run the numbers before you make significant financial investments. Model using your existing fiber infrastructure for your future quantum-secure network.
- Optimize the network design. Test a variety of network configurations, routing schemes, and error correction methods to identify the most cost-effective and resilient architecture for your situation. Determine the most efficient use of quantum hardware before investing in a purchase.
- Test for interoperability and flexibility. Ensure the hardware chosen for your network will integrate with classical infrastructure. Validate the compatibility of multi-vendor quantum components at different layers of the network. Test across a variety of protocols and hardware components to ensure the future flexibility of the network.

- Plan for incremental deployment and scaling up. Model how quantum network performance scales with added nodes, longer distances, or increased data throughput to guide future upgrades. Rapidly test and iterate different quantum services before investing in them.
- Mitigate the risks of deployment. Identify issues early in the development of the quantum network to prevent costly hardware missteps and reduce operational risk. Validate the behavior of the quantum network across metro, long-haul, or hybrid networks in realistic situations.
- Improve workforce readiness. Quantum network simulations provide a training ground for engineers and technicians to become well-versed in quantum networking principles ahead of a quantum network deployment.

Using a quantum network simulator gives telecommunications providers time to validate, budget, and train for a future deployment. Quantum network simulators help organizations make informed decisions about their quantum-secure roadmap. Insights gained from robust simulation reduce financial and operational risk, and accelerate the progress from concept to implementation. Using a quantum network simulator provides organizations with two important

Aliro Simulator: Advancing Quantum Networking Through Comprehensive Simulation

Entanglement-based quantum networking holds immense potential for secure communication, enhanced cloud access, and networked quantum computers. However, developing and deploying quantum networks presents significant challenges, demanding meticulous design, validation, and implementation. Aliro addresses these challenges with its robust Aliro Simulator, a scalable cloud platform and simulation pipeline designed to facilitate the development and optimization of quantum networks. This white paper provides an overview of the Aliro Simulator, highlighting its features, capabilities, and benefits for researchers and developers in the quantum networking space.

Key Features and Capabilities

Aliro Simulator offers a comprehensive suite of tools and functionalities to support the simulation and analysis of quantum networks. Key features include:

- Discrete Event Simulation: The simulator supports discrete event simulation, allowing users to model the dynamic behavior of quantum network components and protocols over time.
- Quantum Simulation: At its core, the Aliro Simulator provides quantum simulation capabilities, enabling the modeling of quantum phenomena and interactions within the network.
- Quantum Networking Protocols: The simulator supports the implementation and testing of various quantum networking protocols, allowing for the evaluation of their performance and effectiveness.
- Quantum Network Components and Noise Modeling Library: A comprehensive library of quantum network components and noise models is available, enabling users to create realistic simulation environments and analyze the impact of noise on network performance.
- Python Simulation Framework: The simulator leverages a powerful Python simulation framework, providing a comprehensive API for simulating network devices and protocols. The framework also includes tools for data collection, processing, and visualization.
- Scalable and Swappable Backend: The simulator offers a scalable and swappable backend, allowing integration with various quantum simulators, such as Cirq, QuTIP, and QSim. It supports multiple state representations, including State Vector, Density Matrix, and Stabilizer, and can scale on the cloud using parallel processing or GPU acceleration.
- Scalable Cloud Platform and Simulation Pipeline: The simulator is built on a scalable cloud platform, enabling efficient execution of complex simulations. Its streamlined pipeline simplifies the setup, execution, and visualization of simulation results.

Simulation-Aided Design

The Aliro Simulator plays a critical role in simulation-aided design, particularly for Entanglement Purification and Photon Sources (EPPS). By providing a virtual environment for testing and refining EPPS designs, the simulator enables developers to optimize performance and identify potential issues before physical implementation.

Design Validation and Optimization

Theoretical formulas for quantum network behavior can quickly become intractable, making simulation essential for design validation.

The Aliro Simulator facilitates:

- Verification: Ensuring that the network design aligns with theoretical principles and specifications.
- Sanity Checks: Identifying potential flaws or inconsistencies in the design.
- Optimization: Fine-tuning parameters and configurations to maximize network performance.
- Parameter Setting: Determining optimal values for network parameters.
- Design Choices: Evaluating different design options and their impact on network behavior.
- Alignment with Experimental Data: Comparing simulation results with experimental data to validate the accuracy of the model.

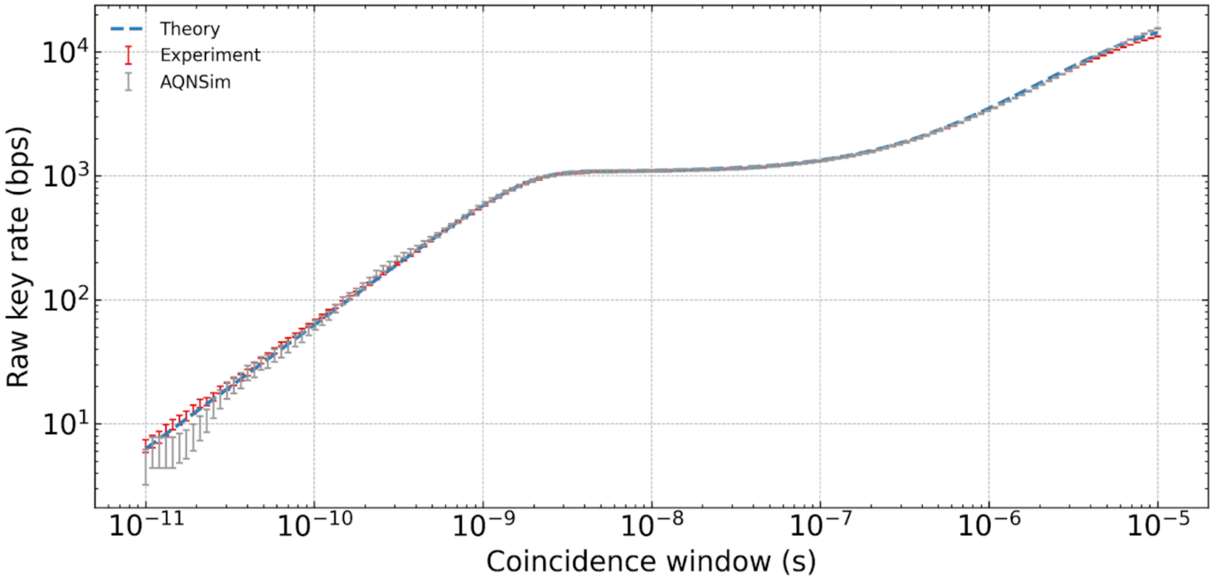


Figure 1. Comparison of Theoretical, Experimental and Aliro Simulation Results for Key Rate

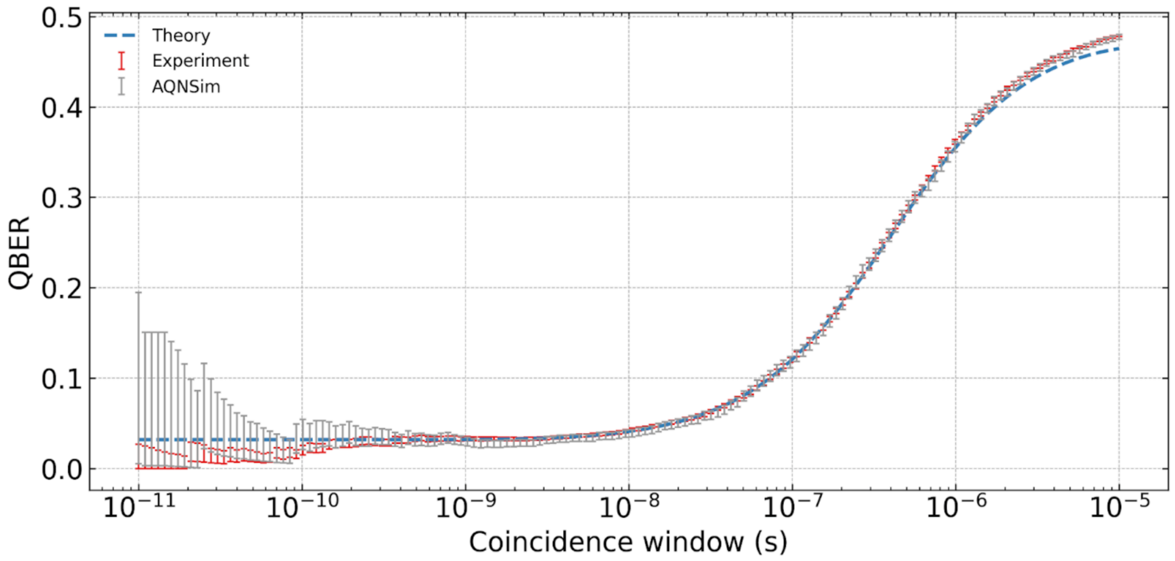


Figure 2. Comparison of Theoretical, Experimental and Aliro Simulation Results for Qubit Error Rate

Benefits of Using Aliro Simulator

- Accelerated Development: The simulator significantly reduces the time and cost associated with quantum network development by enabling virtual testing and optimization.
- Improved Design Quality: Simulation helps identify and address potential issues early in the design process, leading to higher-quality and more robust network designs.
- Enhanced Understanding: The simulator provides valuable insights into the behavior of quantum networks, enhancing understanding and facilitating innovation.
- Risk Mitigation: By enabling thorough testing and validation, the simulator helps mitigate risks associated with deploying complex quantum networks.
- Interoperability: The simulator's scalable and swappable backend ensures interoperability with various quantum simulators and state representations.

Conclusion

Aliro Simulator is a powerful tool for advancing quantum networking research and development. Its comprehensive features, scalable platform, and robust simulation capabilities empower researchers and developers to design, validate, and optimize quantum networks effectively. Aliro simulation results provide a tight correlation with both theoretical and hardware-based experimental results. By leveraging the Aliro Simulator, organizations can accelerate their journey towards realizing the full potential of quantum networking and its transformative applications.

info@alirotech.com www.alirotech.com