Aliro™

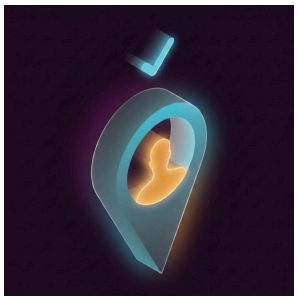
Making Location a Security Credential:

Using Entanglement for Position Verification

Aliro

www.aliroquantum.com

Making Location a Security Credential:
Using Entanglement for Position Verification



Summary

Post-quantum cryptography has made progress toward protecting the integrity of secure communications. However, there is a dimension of trust that classical security protocols leave unaddressed: location. Where is the device that sent this message? Is it really where it claims to be?

Quantum Position Verification (QPV) answers that question using the laws of physics. QPV makes it physically impossible for colluding adversaries to spoof a claimed location by incorporating quantum states into a challenge-response protocol. A January 2026 experiment conducted by NIST demonstrated device-independent QPV for the first time, marking a decisive shift from theoretical construct to experimental reality.

This white paper explains how QPV works, why classical alternatives are fundamentally insufficient, what the current security landscape looks like, and what the path to real-world deployment requires.

How Classical Position Verification Is Broken

The Global Navigation Satellite System (GNSS), of which GPS is the most widely known implementation, is the backbone of modern positioning. Dozens of satellites in orbit broadcast precise timing signals. Receivers on the ground triangulate their position by measuring the arrival time of signals from multiple satellites. The system is elegant, globally adopted, and deeply embedded in everything from consumer navigation apps to military asset tracking.

However, GPS is a positioning system, not a verification system. It estimates where a is located. It does not prove that the claimed position is authentic.

To add verification to positioning, classical protocols use techniques like distance bounding (measuring round-trip timing of a challenge-response exchange), multilateration (triangulating from multiple verifiers), and neighbor discovery. These methods rely on certain assumptions about the trustworthiness of the infrastructure, the timing systems, and the integrity of cryptographic keys used to authenticate claims.

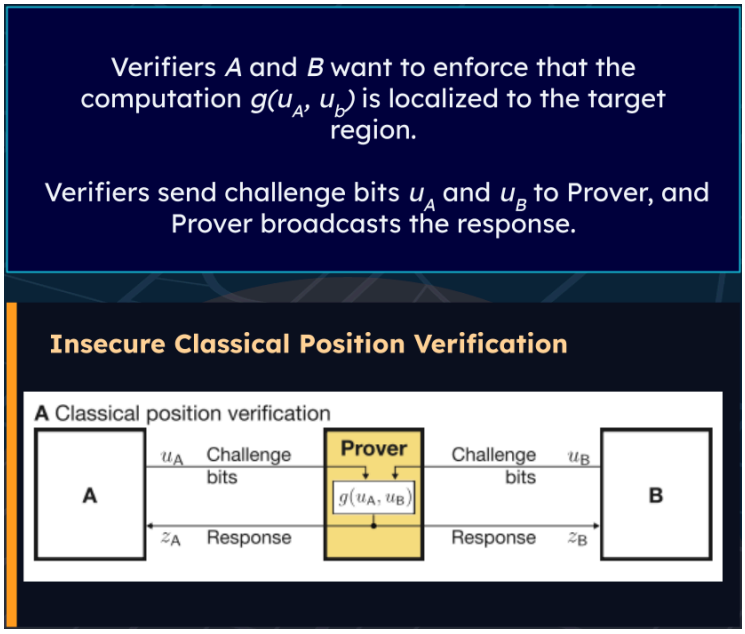
The flaw of these systems exists at the physical level, not the cryptographic level. Because classical bits can be perfectly copied, two colluding adversaries can intercept the challenge signal, clone it, relay to each other, and respond within the timing window, essentially fooling the system into believing the communication is secure when it has been intercepted. Because of this flaw, no classical position verification protocol is secure against colluding adversaries.

Chandran et al. published a seminal proof at CRYPTO 2009 proved that no classical position verification protocol is secure against colluding adversaries. Regardless of protocol complexity, any set of adversaries who can intercept a classical challenge signal, copy it, relay it to a partner, and respond within the timing window can successfully spoof a location. No amount of engineering changes this, because it is a consequence of the physics of classical information.

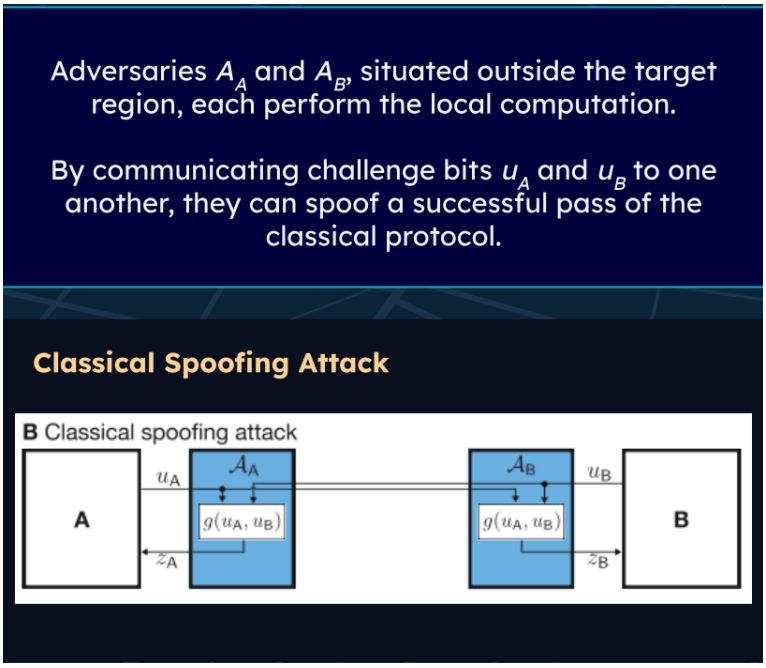
Exploiting this vulnerability and performing GPS spoofing doesn’t take expensive hardware and specialized techniques. Software-defined radios costing as little as $300 can generate fake GPS signals that overpower legitimate satellite transmissions. Receivers lock onto the fraudulent signals and compute incorrect positions. Thousands of ships and aircraft have been affected by adversarial spoofing operations documented since 2019.

A common misconception is that encrypted GPS signals are immune to this style of attack. They are not. Authentication prevents impersonation, but it cannot stop a physical relay attack. Classical physics offers no defense.

Consider the standard challenge-response setup: two verifiers (A and B) want to confirm that a prover is within a target region. They send challenge bits to the prover; the prover computes a response function and broadcasts it back. The verifiers check that the response is correct and arrived within the expected timing window.



Now consider two colluding adversaries positioned just outside the target region. They intercept the challenge bits before they reach the prover, relay them to each other, independently compute the response function, and broadcast the results within the accepted window. The protocol accepts. The prover's location has been successfully spoofed, and there is nothing in the classical protocol that can prevent it.



This is not a weakness of a particular protocol or implementation. It is a fundamental consequence of classical physics. As long as challenge information can be perfectly duplicated, colluding adversaries can coordinate responses that are indistinguishable from those of an honest prover at the claimed location.

Unlike classical information, quantum states cannot be perfectly copied. This property, known as the no-cloning theorem, changes the security model entirely and opens the door to protocols that can verify location in ways that are impossible in the classical world. Quantum position verification leverages entanglement and the laws of quantum physics to overcome the fundamental limitations that make classical position verification insecure.

How Quantum Position Verification Works

The security of QPV is in part due to the no-cloning theorem, proved independently by Wootters, Zurek, and Dieks in 1982. It states that no physical process can create an identical copy of an unknown quantum state.

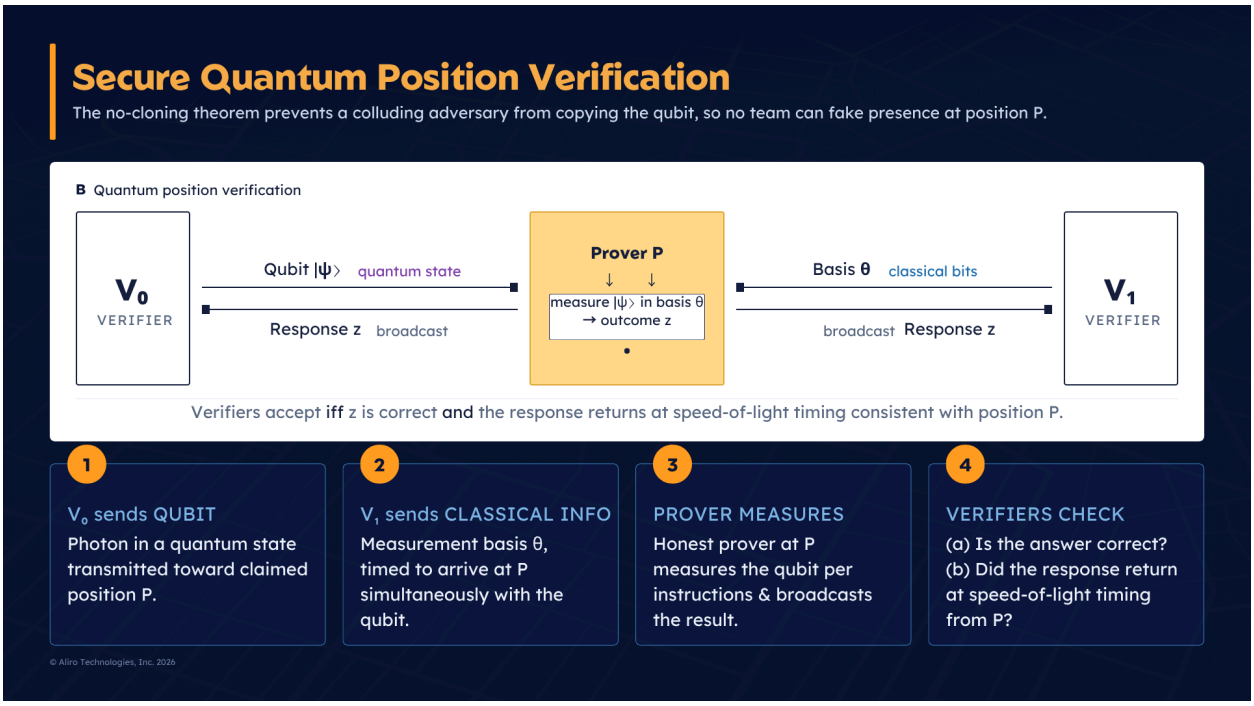
In the context of position verification, this creates a critical asymmetry. A classical challenge bit is like a spoken password: anyone who intercepts it can copy it, relay it, and repeat it as many times as needed, all within the timing window. A quantum challenge, a single photon in a specific quantum state, is like a key that disintegrates when copied. An adversary who intercepts a qubit must choose: keep it, or forward it. They cannot do both. This single constraint breaks the relay attack that defeats every classical scheme.

A common criticism of Quantum Position Verification (QPV) is that theoretical attacks exist in which multiple colluding adversaries share very large amounts of pre-distributed entanglement. In this model, attackers can use sophisticated quantum protocols to coordinate their responses and potentially impersonate a prover at the claimed location. However, these attacks assume access to effectively unlimited entanglement resources, requiring the generation, distribution, storage, and maintenance of enormous numbers of high-fidelity entangled states across a network. Such capabilities would demand quantum memories, quantum processors, and quantum networking infrastructure far beyond what is currently practical and, for many proposed attacks, beyond what is realistically achievable. While unlimited-entanglement attacks are important from a theoretical perspective, QPV remains one of the most promising approaches to position verification because its security is grounded in the laws of physics rather than the computational assumptions that underpin classical cryptographic systems.

How a QPV Exchange Works

A basic QPV protocol involves two verifiers (V0 and V1) and one prover (P). The exchange proceeds in four steps:

- **Step 1 —** V0 transmits a quantum challenge: a photon in a specific quantum state, sent toward the prover's claimed position.
- **Step 2 —** V1 simultaneously sends a classical challenge: measurement basis instructions timed to arrive at position P at the same moment as the photon from V0.
- **Step 3 —** The prover measures the qubit using the instructions from V1 and immediately broadcasts the result.
- **Step 4 —** Both verifiers check two things: (a) is the answer correct, and (b) did the response arrive within the speed-of-light timing window from position P?



An adversary not located at P would need to intercept the qubit from V0 and the classical instructions from V1 simultaneously, perform the measurement, and respond – all faster than an honest prover at P could. The no-cloning theorem prevents the adversary from copying the qubit to share with a partner; quantum teleportation could theoretically help, however, as explained above, this is beyond what is realistically achievable.

The QPV Timeline: From Theory to Experiment

QPV has a rich theoretical lineage. Kent, Munro, and Spiller first proposed the concept of 'quantum tagging' in 2002 (patented in 2004). The Chandran impossibility proof for classical PV arrived in 2009. In 2011, Buhrman et al. showed that adversaries with unlimited entanglement can theoretically break QPV, but also proved that with zero adversary entanglement, QPV is unconditionally secure. Bluhm, Christandl, and Speelman's 2022 Nature Physics paper established that bounded adversary entanglement makes QPV practically unbreakable. In 2025, Escola-Farras and Speelman proved loss tolerance for single-round QPV — a critical step toward deployment on real, lossy fiber networks.

The Security Landscape

It is important to be precise about what QPV guarantees and under what adversarial assumptions. The security of quantum position verification (QPV) depends fundamentally on the capabilities of the adversary. Classical position verification has been proven impossible under general adversarial models because colluding attackers can always defeat the protocol through relay attacks (Chandran et al., 2009).

Early analyses of QPV similarly demonstrated that unconditional security is impossible against adversaries possessing unlimited pre-shared entanglement, as they can exploit instantaneous nonlocal quantum computation to perfectly emulate an honest prover (Buhrman et al., 2011). However, the security landscape changes dramatically once realistic resource constraints are considered. When adversaries possess no pre-shared entanglement, QPV protocols are provably secure because the attacks fundamentally require entanglement as a resource (Buhrman et al., 2011).

More recent work has extended this result by showing that even bounded-entanglement adversaries cannot efficiently compromise practical QPV protocols, as successful attacks require an amount of entanglement that grows exponentially with the protocol parameters (Bluhm et al., 2022).

Finally, when QPV is combined with secret keys that are periodically refreshed using quantum key distribution (QKD), the protocol can maintain security indefinitely, even in the presence of increasingly capable adversaries, because compromised keys are continuously replaced with fresh information-theoretically secure keys (Kent, 2011; Cowperthwaite & Kent, 2023).

Practical Security: The Entanglement Barrier

The practical question is whether the 'bounded entanglement' assumption is realistic. The answer is emphatically yes!

To break a 256-bit QPV protocol, an adversary would need 2^256 entangled pairs — a number that exceeds the number of atoms in the observable universe. Today's most advanced quantum computers hold approximately 1,000 high-quality qubits. The 2025 protocols by Escola-Farras and Speelman further show that QPV can tolerate qubit error rates up to 3.6%, putting it within reach of current and near-term hardware.

This is a fundamentally different kind of security claim than RSA or elliptic-curve cryptography. Those classical protocols rest on computational hardness assumptions (P != NP). QPV's security is anchored in physics: to break it, an adversary must possess a resource: entanglement at cosmic scale. This is not just computationally hard to acquire but physically impossible.

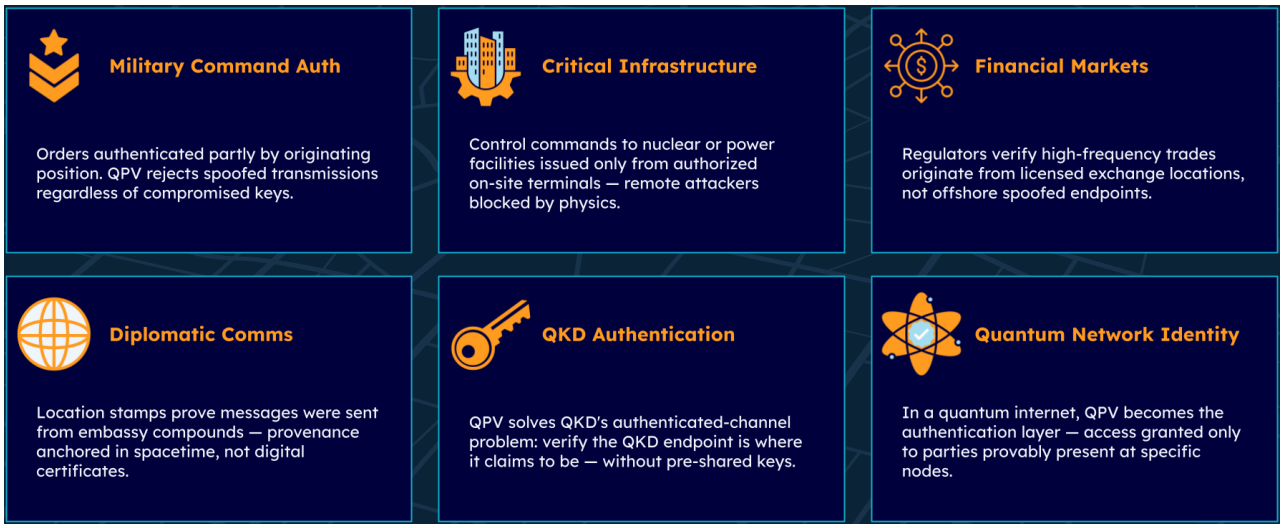
Location as a Cryptographic Credential

Traditional authentication factors are something you know (password), something you have (token), and something you are (biometric). QPV introduces a fourth authentication factor: somewhere you provably are, verified by physics, not by trust in infrastructure or cryptographic keys.

QPV is not only a location verifier; it is a spacetime verifier. The protocol does not simply ask 'is the prover at position X?' It asks 'was the prover at position X at time T?' This temporal dimension adds a new axis of authentication that has no classical equivalent.

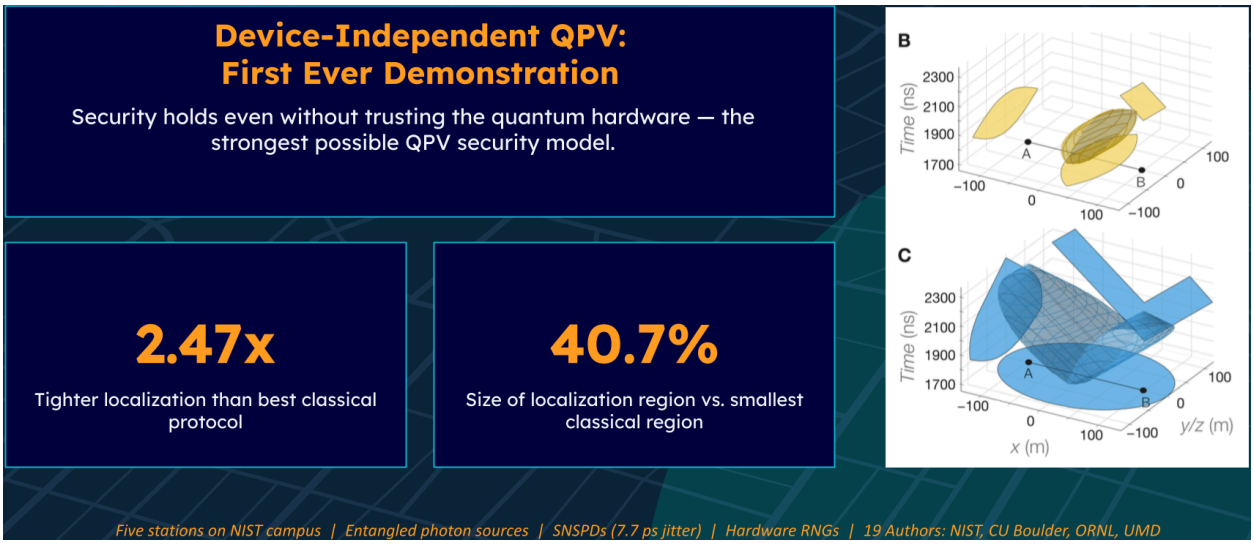
Who Needs QPV, and Why

- **Military Command and Control:** Operational orders carry higher trust when their originating position can be cryptographically verified. QPV rejects spoofed transmissions from adversaries impersonating authorized positions, even if the adversaries have compromised the encryption keys.
- **Critical Infrastructure:** Control commands for power grids, water systems, and nuclear facilities should only be issuable from authorized on-site terminals. QPV enforces this at the physics level — a remote attacker who has stolen credentials but is not physically present cannot pass the protocol.
- **Financial Markets:** Regulators increasingly require that high-frequency trades and high-value transactions originate from licensed exchange locations. QPV provides a cryptographic receipt proving that a transaction was initiated from a specific physical location at a specific time.
- **Diplomatic Communications:** Sensitive government-to-government communications carry higher integrity when their originating location can be verified. Digital certificates alone cannot provide this; if the keys are compromised, the location claim fails.
- **QKD Authentication:** QKD distributes secret keys but relies on an authenticated classical channel. QPV solves this problem by verifying the physical location of a QKD endpoint without requiring pre-shared keys — the nearest-term practical application for QPV.



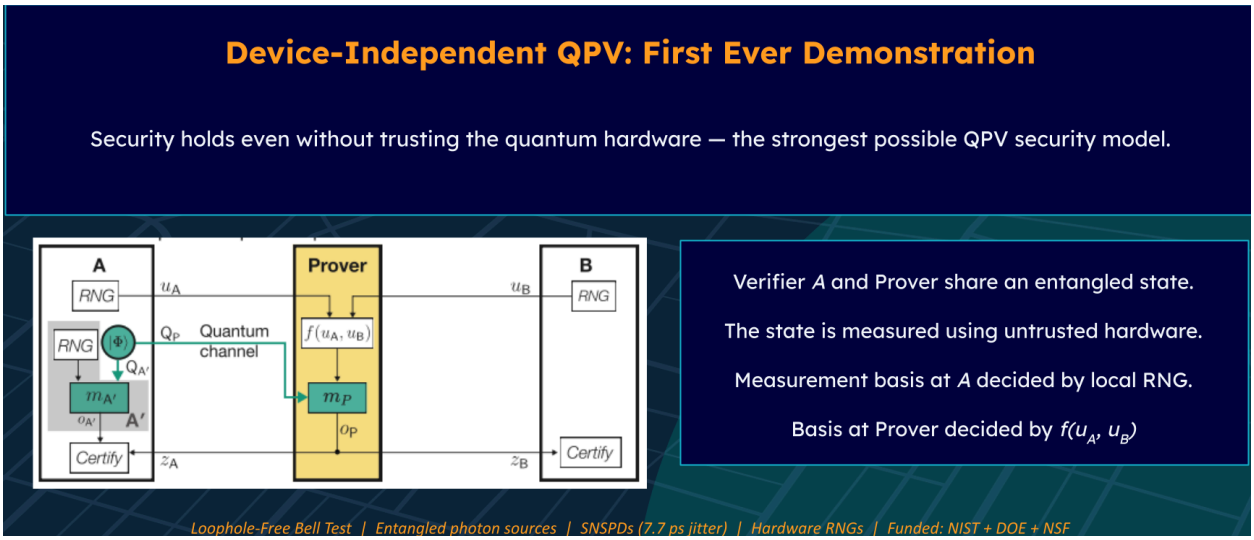
The January 2026 NIST Milestone: Device-Independent QPV

In January 2026, NIST and collaborators from CU Boulder, Oak Ridge National Laboratory, and the University of Maryland published the first experimental demonstration of device-independent QPV, the strongest possible QPV security model.



Device independence means that security holds even without trusting the quantum hardware performing the measurements. In standard QPV, an adversary who cannot break the protocol directly might instead compromise the hardware. Device-independent QPV removes this attack surface entirely by deriving security from a loophole-free Bell test rather than assumptions about hardware behavior.

The NIST experiment used five stations on the NIST campus, entangled photon sources, superconducting nanowire single-photon detectors (SNSPDs) with 7.7 picosecond timing jitter, and hardware random number generators. The results showed 2.47x tighter localization than the best classical protocol, with the verified region reduced to 40.7% of the smallest classical verification region.

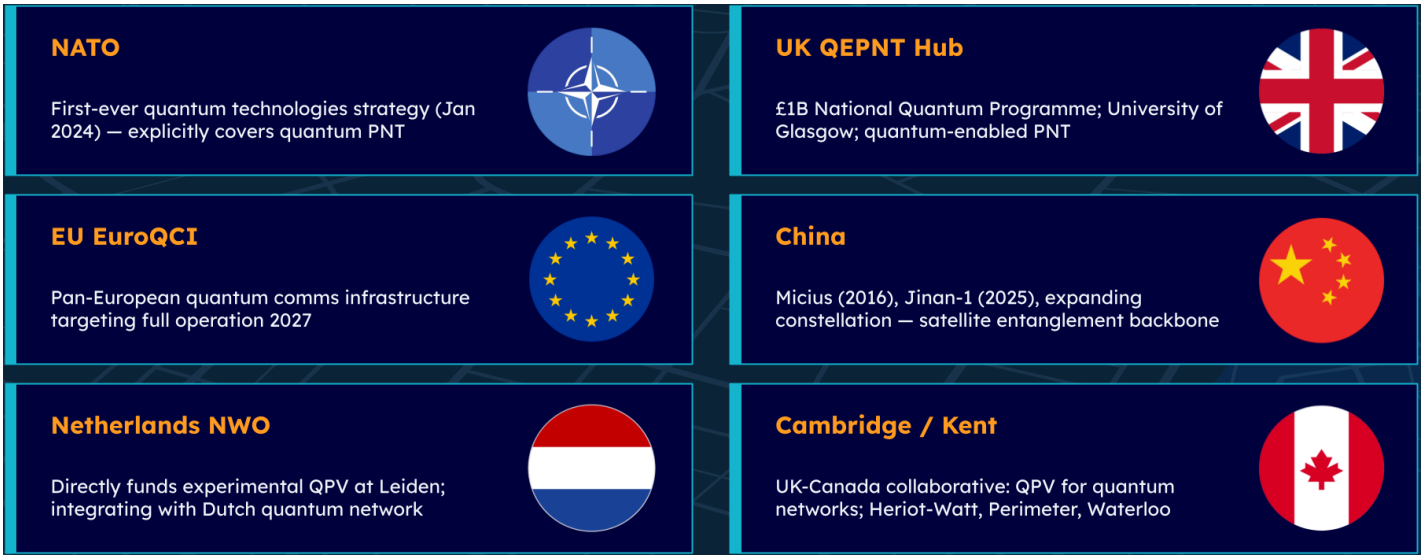


This is a landmark result demonstrating that QPV is theoretically sound, and it works in the real world, on real hardware, with measurable and superior localization compared to any classical alternative.

The Global Race to Build QPV Infrastructure

The NIST experiment is one node in a rapidly accelerating global effort:

- **NATO:** First-ever quantum technologies strategy (January 2024) — explicitly covers quantum PNT.
- **UK:** GBP 1B National Quantum Programme; dedicated quantum-enabled PNT hub at the University of Glasgow.
- **EU EuroQCI:** Pan-European quantum communications infrastructure targeting full operation 2027.
- **China:** Micius (2016), Jinan-1 (2025), and an expanding constellation building the satellite entanglement backbone.
- **Netherlands NWO:** Directly funds experimental QPV at Leiden University, integrated with the Dutch quantum network.



Clearing Up the Biggest Misconceptions

QPV is a new, technically dense topic, and because of that, several misconceptions have taken hold.

Misconception 1: QPV is just GPS.

GPS is a positioning system; it provides a location estimate. QPV is a verification protocol; it takes a claimed position and outputs a cryptographic yes/no verdict. QPV is not a navigation technology. It does not tell you where you are; it confirms whether you are where you claim to be.

Misconception 2: QPV is another form of QKD.

QKD distributes secret keys. QPV verifies physical location. They are complementary, not equivalent. QPV solves QKD's authenticated-channel problem; QKD can in turn refresh the keys used in QPV schemes that incorporate a shared-secret component.

Misconception 3: QPV is unconditionally secure.

Strictly speaking, this is false. Adversaries with unlimited entanglement can theoretically break QPV. But 'unlimited' means exponential in the protocol's input size, placing the required resources far beyond the capacity of any foreseeable adversary. QPV is practically unbreakable, and the security level is a tunable parameter analogous to choosing between 256-bit and 512-bit key sizes in classical cryptography.

Misconception 4: QPV is a universal defense against GPS spoofing.

QPV defends specifically against location fraud: a fake claim of physical location. It is not a general-purpose defense against GPS jamming, signal spoofing at the RF layer, or network-layer denial of service. QPV should be understood as one precisely targeted tool within a broader security architecture, not a universal cure.

The Engineering Roadmap

Deploying QPV at scale requires advances across the quantum networking stack, including photonic hardware, timing systems, detectors, quantum repeaters, and eventually satellite infrastructure. Encouragingly, none of these challenges require fundamentally new physics. Instead, they represent engineering problems that are already being addressed through rapid progress in quantum networking research and development.

Five Hardware Challenges

Although the theoretical foundations of Quantum Position Verification (QPV) are now well understood, practical deployment depends on continued advances in quantum networking hardware. Fortunately, many of the remaining challenges are engineering problems rather than fundamental scientific barriers. Progress across photonics, timing systems, quantum repeaters, and satellite infrastructure continues to move QPV toward real-world deployment.

Challenge 1: Photon Loss

(Status: Largely Solved)

Optical fiber networks inherently suffer from attenuation, with standard single-mode fiber exhibiting losses of approximately 0.2 dB/km. For many years, photon loss represented one of the primary obstacles to practical Quantum Position Verification because lost quantum challenges reduced protocol reliability in real-world networks. Recent advances in loss-tolerant QPV protocols have largely addressed this challenge by introducing protocol variants that remain secure even when photons are lost during transmission. As a result, channel loss is no longer viewed as a fundamental barrier to deployment, placing practical QPV within the reach of current and near-term quantum networking hardware operating over existing fiber infrastructure.

Challenge 2: Timing Precision

(Status: Advancing)

Accurate position verification depends on extremely precise timing measurements. Because light travels approximately 30 centimeters per nanosecond, verifying location with sub-meter accuracy requires synchronization on the order of picoseconds. Recent experimental demonstrations have shown that this level of precision is achievable. A NIST implementation, for example, demonstrated timing jitter as low as 7.7 picoseconds using superconducting nanowire single-photon detectors (SNSPDs). Moving from laboratory demonstrations to operational networks will require maintaining this precision despite environmental effects such as temperature-induced fiber expansion, vibration, and other sources of timing drift through continuous calibration and compensation.

Challenge 3: Single-Photon Detectors and Entangled Photon Sources

(Status: Advancing)

High-performance photonic hardware remains essential for practical QPV systems. Superconducting nanowire single-photon detectors currently offer detection efficiencies of approximately 80–90% together with extremely low timing jitter, but they require cryogenic operation at temperatures near 3 K, increasing deployment complexity and cost. Although room-temperature single-photon detectors continue to improve, they currently provide lower efficiency and higher noise. At the same time, device-independent QPV protocols require entangled photon sources capable of producing high-rate, high-fidelity entangled photon pairs with long-term operational stability. Continued improvements in both detector and source technology will directly improve the practicality and scalability of deployed QPV systems.

Challenge 4: Quantum Repeaters

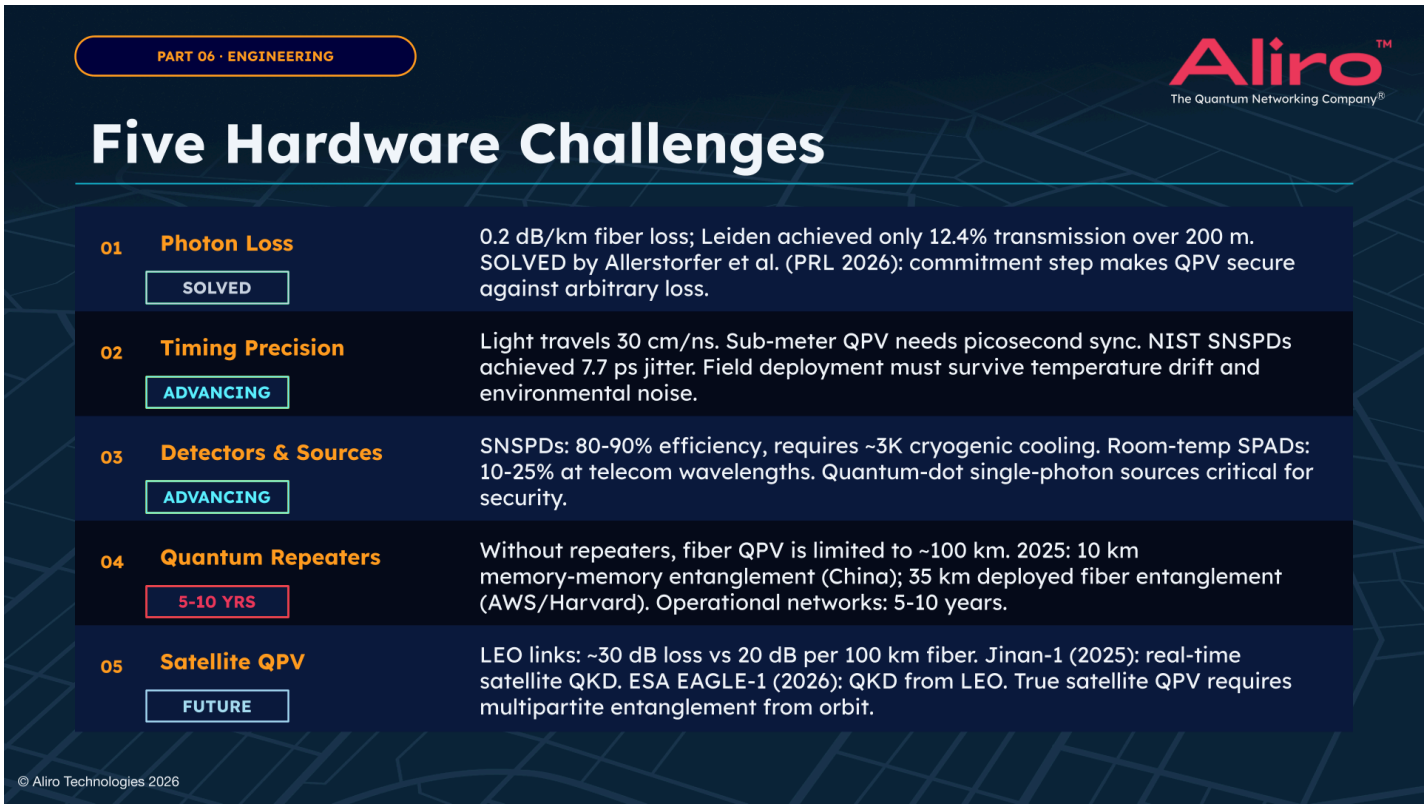
(Status: Medium-Term)

The operational range of fiber-based QPV is ultimately constrained by photon loss. Quantum repeaters overcome this limitation by extending entanglement over long distances through entanglement swapping and quantum memory technologies. Although fully functional repeater networks have not yet been deployed, important milestones have recently been achieved. Demonstrations of entanglement swapping by Qunnect in New York and remote ion-ion entanglement experiments in China represent significant progress toward practical memory-assisted quantum repeater architectures. As these technologies mature, metropolitan and regional QPV deployments will become increasingly feasible.

Challenge 5: Satellite-Based Quantum Networking

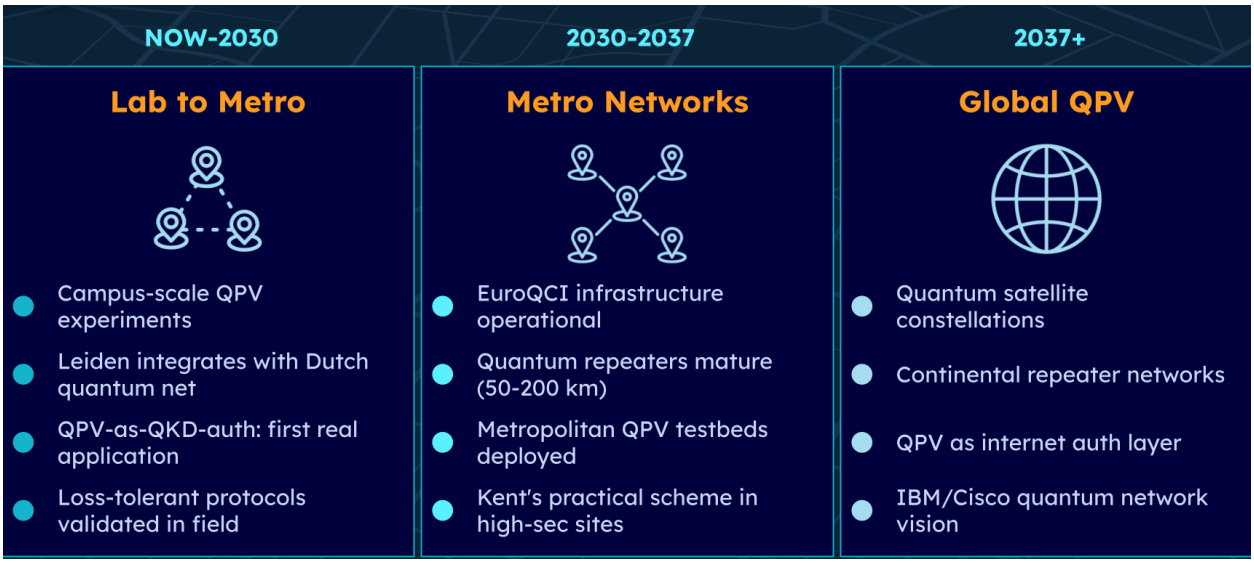
(Status: Long-Term)

Global-scale QPV will ultimately depend on satellite-based quantum networks capable of distributing entanglement across continental and intercontinental distances. Multiple national and commercial quantum satellite programs are currently under development, with approximately ten missions expected to be operational by 2030. As satellite-based entanglement distribution matures and integrates with terrestrial quantum networks, QPV will evolve from a regional authentication capability into a globally deployable security technology capable of verifying locations anywhere on Earth.



Realistic Deployment Timeline

The path to widespread deployment of QPV will mirror the broader evolution of quantum networking infrastructure. As enabling technologies, including timing systems, entangled photon sources, quantum repeaters, and satellite-based quantum communications continue to mature, QPV is expected to progress from laboratory demonstrations to regional deployments before ultimately becoming a global authentication capability.



Now – 2030: Lab to Metro

The near-term priority is moving QPV demonstrations out of the lab and into controlled metro-region testbeds. Minimum viable QPV requires three nodes (two verifiers, one prover) on short metro-region fiber or free-space links with calibrated timing systems. The first real application will be QPV as a QKD authentication layer.

2030 – 2037: Metropolitan Networks

As quantum repeaters mature (targeting 50-200 km range), QPV expands to metropolitan-scale networks. EuroQCI infrastructure comes online. Kent's practical scheme becomes viable in high-security fixed-location environments.

2037+: Global QPV

Quantum satellite constellations enable continental and eventually global QPV. QPV matures as a foundational authentication layer for quantum internet infrastructure.

Three Insights for Practitioners

The recent advances in Quantum Position Verification have important implications for organizations evaluating future quantum networking technologies. Three conclusions are particularly relevant for practitioners planning long-term security architectures.

1: Practical QPV is feasible with current technology.

Recent advances have produced practical QPV protocols that can be deployed with current quantum networking technology. As discussed earlier, these protocols address key implementation challenges such as channel loss and make QPV practical for high-security fixed-location environments, providing a realistic path from laboratory demonstrations to operational deployments.

2: QPV Provides a Fundamentally Different Security Model.

The security of QPV differs fundamentally from that of conventional authentication primitives because its security is tied to physical spacetime constraints, not just computational hardness. Under realistic threat models, any spoofing attacks on QPV would require exponentially increasing quantities of pre-shared entanglement, placing the required resources far beyond any foreseeable technological capability. The only

way to pass the QPV check is to be physically present at the claimed location. For organizations planning security infrastructure with multi-decade lifetimes, QPV represents a new and different approach to authentication than conventional cryptographic techniques, such as digital signatures.

3: QPV's nearest-term value is QKD authentication.

QPV addresses one of the longstanding challenges of Quantum Key Distribution (QKD): authenticating the physical location of communicating endpoints without relying on pre-shared secret keys. As organizations begin deploying QKD networks, integrating QPV provides a natural extension that strengthens endpoint authentication while preserving the information-theoretic security properties of the overall system.

Conclusion

NIST's January QPV experiment demonstrated a fundamental shift in how identity and trust can be established in distributed systems. Rather than relying solely on cryptographic credentials or computational assumptions around digital identity, QPV leverages the laws of quantum mechanics to verify a previously unattainable property: the physical location of a communicating device. By combining quantum information with spacetime constraints, QPV enables a new class of authentication protocols that are inherently resistant to the relay attacks that render classical position verification fundamentally insecure.

Over the past fifteen years, QPV has evolved from a theoretical concept into a maturing technology. Early work established both the impossibility of secure classical position verification and the security limits of QPV against adversaries with unlimited entanglement. More recent research has demonstrated that under realistic assumptions—including bounded adversarial resources, loss-tolerant protocols, and practical implementation models—QPV can provide incredibly strong security guarantees using technologies that are becoming increasingly available.

For QPV to become a globally-deployed technology, significant engineering progress needs to be made, particularly in timing synchronization, photonic hardware, quantum repeaters, and global entanglement distribution. However, these challenges are no longer questions of fundamental physics breakthroughs. Instead, they are engineering milestones that closely parallel the broader development of quantum networking infrastructure. As quantum networks mature over the coming decade, the technologies required to support practical QPV are expected to mature alongside them.

The first practical deployments of QPV are likely to emerge as an authentication layer for Quantum Key Distribution (QKD) and other high-security quantum communication systems. Beyond these initial applications, QPV has the potential to become a foundational service for a quantum-enabled internet, enabling secure authentication of users, devices, data centers, financial transactions, defense operations, critical infrastructure, and autonomous systems based not only on *who* they are, but also on *where* they are.

The evolution of cybersecurity has historically followed advances in computation and communications. Quantum networking enables practical Quantum Position Verification, allowing physical location to become a cryptographically-verifiable credential. As organizations prepare for a future built on quantum communications, QPV has the potential to become an essential component of the next generation of trusted network infrastructure.

From Research to Deployment

While broad deployment of QPV will depend on continued advances in quantum networking hardware, many of the foundational technologies required to support future QPV applications are already being developed and deployed today. Organizations investing in quantum networking infrastructure, including entanglement

distribution, QKD, quantum network management, and network simulation are building the technological foundation that will enable QPV as the technology matures.

Aliro provides the software platform for designing, simulating, deploying, and operating entanglement-based quantum networks. The Aliro Simulator enables organizations to evaluate network architectures, model protocol performance under realistic operating conditions, and validate designs before investing in hardware. As quantum networking comes to support applications such as Quantum Secure Communications (QSC), QPV, and distributed quantum computing, the AlirOS control plane software will play an increasingly critical role in coordinating network operations across diverse hardware environments. Aliro Orchestrator provides a unified management plane for quantum networking services through a single interface. It enables operators to configure, monitor, automate, and optimize multi-vendor quantum networks while orchestrating quantum resources and supporting the deployment of both today's production applications and tomorrow's emerging quantum networking capabilities.

Aliro works with commercial enterprises, government agencies, research organizations, and technology partners to evaluate quantum networking use cases, develop deployment roadmaps, build pilot quantum networking environments, and deploy their full-scale quantum network. Whether the objective is Quantum Secure Communications, networking quantum processors, distributed quantum sensing, or emerging applications such as Quantum Position Verification, early planning and experimentation will position organizations to take advantage of the capabilities offered by the next generation of quantum networks.

Key References

- Chandran et al., "Position-Based Quantum Cryptography: Impossibility and Constructions," CRYPTO 2009
- Buhrman et al., "Position-Based Quantum Cryptography," CRYPTO 2011
- Bluhm, Christandl & Speelman, Nature Physics, 2022
- Escola-Farras & Speelman, 2025
- Allerstorfer et al., Physical Review Letters, 2026
- NIST Device-Independent QPV Experiment, January 2026

About Aliro Quantum

Aliro provides the full-stack software platform for quantum-powered security and quantum-connected devices.

Aliro's products help organizations achieve their quantum goals faster. Aliro Simulator, Aliro Orchestrator, and AlirOS enable teams to plan, manage, and operate quantum networks in real-world deployments for applications including interconnecting QPUs and quantum-powered security.

Headquartered in Boston as a Harvard spin-out, Aliro is backed by leading deep tech investors including Cisco and Accenture, and is actively engaged with financial services, defense, telco, and utility customers on the path to commercialize quantum-powered network infrastructure.

Customers include Boeing, Cisco, EPB of Chattanooga, the Air Force Research Laboratory, Brookhaven National Laboratory, and Stony Brook University.

Contact: info@aliroquantum.com