Entanglement for Security, Beyond QKD:
Physics-based trust in an evolving threat landscape of AI and quantum technologies

Qunnect, Inc.

Executive Summary

The security that underpins much of the world's critical digital infrastructure is at risk as adversaries with increasingly sophisticated technologies at their disposal threaten our current security protocols. Artificial intelligence has emerged as a tool for adversaries to levy multifold attacks at a speed and scope previously thought to be impossible. At the same time, quantum computers pose a novel threat to modern public-key encryption standards that are ubiquitous across industries.

There are steps that have been taken in response to the acceleration of these threats. Notably, the Cybersecurity and Infrastructure Security Agency (CISA) has published joint publications to address both the security of AI systems and the dangers they pose;[1] the US Government (USG) has mobilized in response to these emerging threats by mandating migration of government encryption to post-quantum cryptography (PQC).[2] Both of these steps, while addressing the immediate threat, are fundamentally limited: as they focus on securing the **digital** layer with mathematically-based cyber approaches, they still remain at risk to cyberattacks that bring greater sophistication to efforts to steal or alter critical data and operations.

To best address this growing threat, Qunnect introduces quantum networking as a **provably secure solution** to **physically protect** digital infrastructure from future threats that AI and quantum computing pose to security regimes. Quantum entanglement — a phenomenon that physically correlates two quantum particles, no matter how far apart they are — enables the construction of **entanglement-enhanced security (EES)**. EES leverages quantum networks to form a backbone of trust on top of telecommunications infrastructure that significantly boosts the resilience of existing security protocols without replacing them.

In this whitepaper, Qunnect describes three near-term capabilities of EES:

- **Who am I transacting with?**
  Quantum Factor Authentication (QFA) binds identity to hardware that cannot be cloned or modeled.
- **Is our communication channel actually secure?**
  Quantum Channel Protection (QCP) turns the communication fiber into a sensor with continuous monitoring to detect tapping, rerouting, and jamming in real time.
- **Is my transaction partner being spoofed?**
  Quantum Position Verification (QPV) produces a spacetime seal: cryptographic proof of location and time.

With these three answers, entanglement-enhanced security delivers physics-certified trust, dramatically broadening the security capabilities of quantum networks and the digital networks they support.

1. AI & Quantum Computing Dismantle Classical Security Assumptions

The threats that AI and quantum computing pose to current digital security lie in their ability to break assumptions that had held for decades. As our understanding of technology evolves, the abilities that new technologies have — some that were previously believed to be impossible — reveal the shortcomings in the assumptions that modern security infrastructure relies on.

Assumption 1: Computational hardness

The public-key cryptography used by most enterprises today for securing digital activity and data assumes the mathematical problems underpinning key generation, such as prime factorization, will remain computationally out of reach within a useful time frame for most adversaries. However, quantum computing directly dismantles this assumption.[3]

As a result, federal agencies in the US are mandated to migrate to post-quantum cryptography (PQC),[2] a necessary step that will significantly increase the resilience of digital systems. PQC, while mathematically secure, remains vulnerable to AI-led attacks from leading frontier models, which are increasingly capable of exploiting mathematical structures.

Key Takeaway

Post-quantum cryptography, while a necessary step in addressing the quantum threat in the near-term, is, ultimately, also vulnerable to the same vector of attack.

Assumption 2: Behavioral unpredictability

A physical unclonable function (PUF) derives identity from microscopic manufacturing variations in silicon, creating a physical fingerprint that is measured rather than programmed. However, many strong classical PUF constructions have proven vulnerable to modeling attacks when adversaries can collect sufficient challenge-response data.[5]

An attacker who gathers sufficient challenge-response pairs across a network can train an ML model to clone the device's behavior, predicting future responses with near-perfect accuracy. A 2020 review in *Nature Electronics* confirmed that contemporary classical PUF constructions are vulnerable to machine learning modeling attacks, identifying provably secure PUF design as an open problem.[4]

Key Takeaway

Machine-learning attacks have demonstrated that physical uniqueness alone is not sufficient when a PUF's challenge-response behavior is learnable.

Assumption 3: Human judgment

The historical last line of defense for enterprise security has been the human: an operator noticing a strange voice or an irregular email. As generative models improve, they have swiftly eliminated effective human vetting. With the

cost of creating convincing, real-time synthetic media ever-decreasing, any security control that relies on a human detecting an imitation can become an active point of failure.

Key Takeaway *The only way to circumvent human judgment errors is to build something that is physically unspoofable, such as entanglement.*

Assumption 4: Metadata security

The contextual signals used to validate digital transactions – location, time, and network route – have always been dangerously at risk:

- Location and identity can be masked through proxies, VPNs, or API gateway compromises.[6]
- Hardware identifiers and system clocks are routinely spoofed.[7]

Key Takeaway *Metadata was assumed to have been a certifiable stamp of digital events occurring, but it is increasingly malleable under sophisticated adversarial attacks.*

Assumption 5: Channel integrity

The physical pathways and routing mechanisms that carry digital communication are fundamentally exposed to hidden exploitation. Physical fiber-optic lines can be tapped using clip-on couplers operating under the tolerance threshold, allowing adversaries to siphon data without causing service disruption or detectable packet loss.[8] This silent interception enables **"harvest now, decrypt later" (HNDL)** attacks, where adversaries continuously stockpile encrypted data with the intent to decrypt it using future quantum or AI capabilities.

AI further increases the scale, speed, and adaptability of network-level attacks. By removing human bottlenecks, autonomous tools can now automate continuous traffic redirection and exfiltration attempts across entire infrastructures.[9]

Key Takeaway *The physical and routing infrastructure of networks is often assumed to be a secure conduit, but stealthy hardware taps and automated redirection attacks leave data continuously vulnerable in transit.*

Summary

Today, enterprises are facing an unprecedented security environment as **every primary assumption underlying classical defense is degrading simultaneously.** They face AI threats that operate at machine speed and QPUs will soon have the computational power to break codes previously thought to be secure. Continuing to rely on existing assumptions exposes our critical infrastructure to unacceptable systemic risk. **To maintain digital trust, security architectures must transition from being based in mathematical probability to physical law.**

2. Quantum Entanglement: A New Physical Layer of Digital Trust

A Note on: Quantum Entanglement and QKD

EES is enabled by our ability to leverage **entanglement**, a type of quantum information that can be carried by special pairs of light particles (photons) whose physical identities are highly correlated. This unclonable correlated pair can be used to build security protocols, as it is analogous to a physically-defined check bit. However, to do so, these sensitive particles and their correlation must be actively preserved as they are distributed across the network.

When entangled photons are distributed with high fidelity across a fiber optic network, they can be used for security protocols based on physical laws rather than computational assumptions, and guarantee that the answers are unspoofable. Historically, the most well known quantum security protocol is quantum key distribution (QKD). This can be performed with non-entangled or entangled photons. In 2020, the National Security Administration (NSA) identified several limitations with non-entangled QKD.[10]

It has been shown both theoretically and experimentally that quantum entanglement, as a complementing layer, can close the loopholes of QKD, providing a robust encryption solution for critical networks.[11] EES introduces a new suite of security applications beyond QKD. Like QKD, EES uses the security strengths of quantum networks to secure information. Unlike QKD, EES is not reliant on key exchange, and is therefore resilient to loopholes. We frame EES as a **necessary complement** to PQC, forming a layer of infrastructure security that enhances existing PQC-encrypted communication.

2.0 Entanglement-Enhanced Security In Practice

Establishing trust in a digital event or agent requires independent verification of four distinct variables:

1. **Identity:** Who is at the other end of the connection?
2. **Channel Integrity:** Has the fiber path been altered or tapped in transit?
3. **Location and Time:** Where and when did the event physically occur?
4. **Data Integrity:** Is the data safely encrypted between all parties?

Securing all of these variables simultaneously has been a consistent north star for security infrastructure, one that has been upended by advances in technology now available to adversaries. While researchers have developed digital-layer solutions to individual variables — PQC, for instance, is reliable at maintaining data integrity — there is a limit to how far software and mathematical-based solutions alone can protect a network.

This section will overview why having a physical protection layer on digital infrastructure can guarantee trust and

significantly enhance the security of any network and how quantum entanglement is uniquely suitable as a universal solution.

2.1 Quantum Factor Authentication: Identity Protection

Eliminating identity cloning, algorithmic modeling, and synthetic impersonation.

User authentication is highly vulnerable to impersonation, with traditional defenses like Two-Factor Authentication (2FA) and digital signatures increasingly threatened by AI deepfakes, social engineering, and future quantum computers. To eliminate these risks of identity cloning and algorithmic modeling, EES introduces **Quantum Factor Authentication (QFA).**

Rather than relying on easily compromised software solutions, QFA physically validates a user's identity using a combination of electronic fingerprints and quantum entanglement. While it utilizes pre-registered hardware similar to 2FA, QFA closes the interception and social engineering loopholes: the transmitted authentication data fundamentally carries no exploitable information for eavesdroppers. Even if a user is tricked into revealing a code, or if the request comes from a malicious source, the exposed data remains provably useless to anyone except the true authenticator.

The Quantum Mechanism

In this system, the authenticator sends a challenge code by sharing one half of each pair of entangled photons with the user. The user's hardware

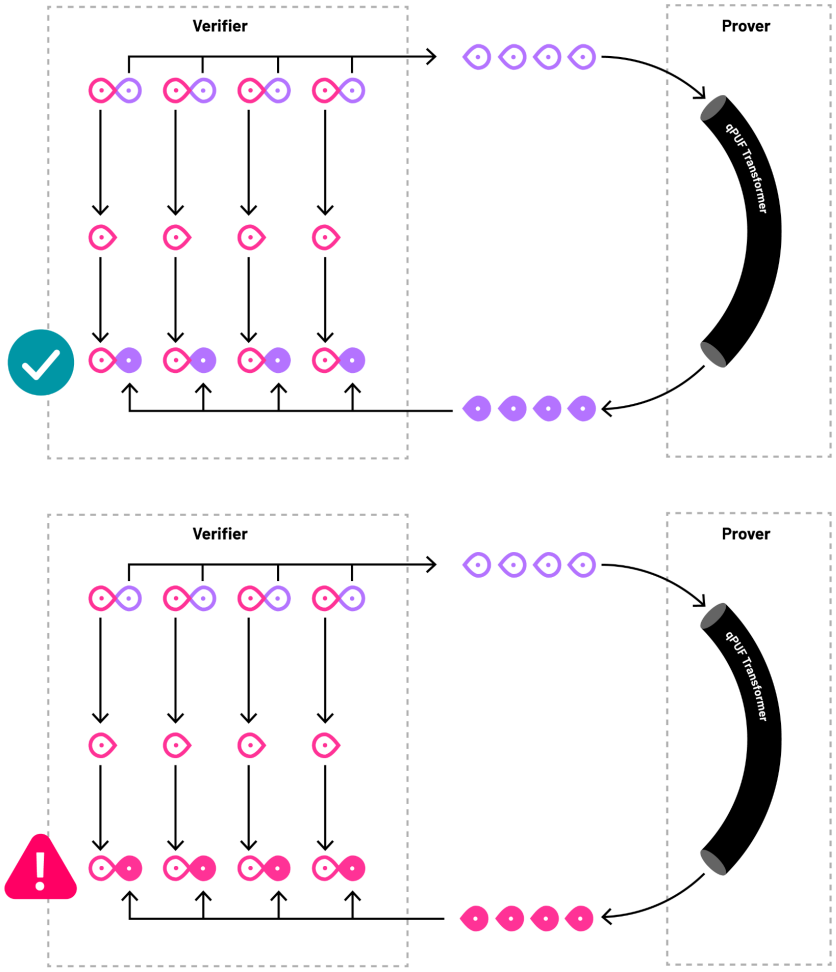


FIGURE 1 • Schematic of QFA: *The Verifier creates entangled pairs of photons (pink and purple infinity icons). The Verifier keeps half of each pair (pink) while sending the other half (purple) to the Prover. The Prover processes the received data (purple) with their unique hardware, and sends the result to the Verifier. The Verifier compares the Prover's result (filled pink or purple) to the expected result to authenticate the Prover.*

processes the code to generate an output, whose result is then sent back to the authenticator node. As the user publicly announces only the quantum measurement result, the channel yields zero useful information to eavesdroppers. Without the physical hardware to determine the measurement basis, intercepted photons appear as entirely random noise. Meanwhile, the authenticator — holding the other half of the entangled photons and knowing the expected classical output — can securely verify the measurement, making machine-learning impersonation fundamentally impossible.[4, 12]

There are three axes through which QFA guarantees security:

- **Un-clonable Communication:** The shared entanglement between the authenticator and the user creates a condition where the generated output is virtually meaningless to anyone except to the real authenticator. This is in sharp contrast with 2FA, where users are responsible to not expose their private codes since any hacker could use those to access their data.
- **Detection via State Collapse**: An adversary attempting to measure passing photons must guess the measurement basis. An incorrect basis choice collapses the quantum state, introducing a measurable error into the correlation checks between the endpoints.
- **Quantitative Confidence:** Verification is statistical. By measuring the Polarization Entanglement Error Rate (PEER) across a challenge sequence, the system computes an exact False Accept Rate (FAR). Optical fiber loss does not compromise security; it simply requires extending the photon sequence length to accumulate the target statistical confidence.

2.2 Quantum Channel Protection: Monitoring The Connection

Turning standard optical fiber into an intrusion detection sensor.

While Post-Quantum Cryptography (PQC) offers near-term software protection against quantum threats, it suffers from three critical vulnerabilities:

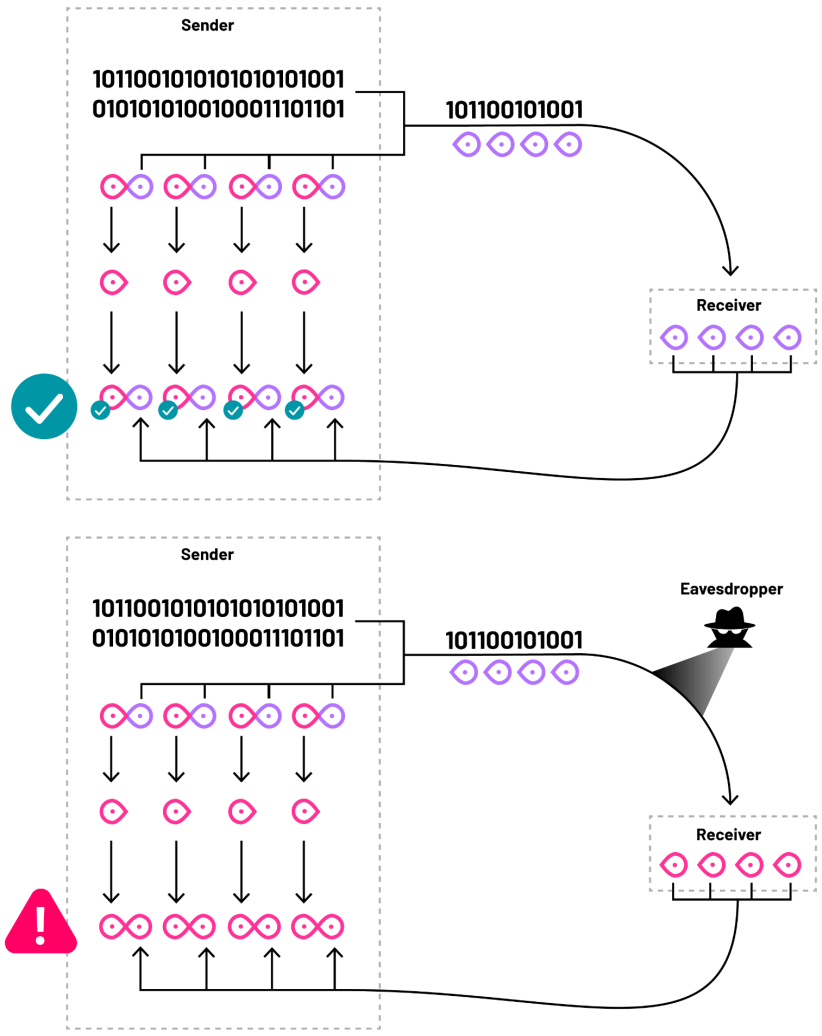
1. Susceptibility to future AI or quantum algorithms that enable "harvest now, decrypt later" (HNDL) attacks;
2. An inability to detect physical network breaches like Advanced Persistent Threats (APTs);
3. Significant processing latency that can force high-speed industries to bypass encryption altogether.

To protect the communication channel itself, physical security layers are required, yet classical monitoring methods are easily bypassed by stealthy optical taps or jamming that hide within a network's normal noise floor. Entanglement networks solve this by transforming standard optical fibers into ultra-sensitive intrusion detection sensors.

The Quantum Mechanism

Quantum Channel Protection (QCP) secures standard telecom networks by multiplexing high-purity entangled photon streams alongside active classical data. Rooted in the quantum no-cloning theorem, this approach guarantees that any tapping or jamming attempt will destroy the fragile quantum states, immediately exposing the intrusion to the communicating parties through detectable changes in the transmission rate and Polarization Entanglement Error Rate (PEER).

Beyond detecting data interception, QCP leverages time-energy entanglement to achieve picosecond timing and centimeter-level distance measurements between nodes tens of kilometers apart. This continuous, ultra-precise



monitoring of the physical channel makes it virtually impossible for hackers to covertly reroute the network or insert unauthorized nodes, ensuring complete structural and informational security.

In essence, any physical manipulation of the fiber — such as micro-bending, splicing, or physical rerouting — disturbs the entangled photon state and immediately elevates the link's baseline error rate.

Real-Time Detection: Identifies passive optical taps drawing well under 1% of signal power within seconds, and detects physical fiber rerouting down to centimeter-scale variations.

Defense-in-Depth Architecture: In current security architectures, quantum channel protection is designed to run alongside existing encryption rather than instead of it. Post-quantum algorithms protect the content; quantum channel protection assesses the integrity of the path the content travelled. It also adds capabilities such as distance detection or even threat triangulation that otherwise would not be possible using a pure software approach.

FIGURE 2 • Schematic of Quantum Channel Protection: *The Sender generates entangled photon pairs (pink and purple infinity icons) and keeps half of each pair (pink), while sending the other half (purple) with the digital data traffic in the same communication channel. The Receiver continuously measures the entangled photon stream and returns the result to the Sender, who compares it to the expected value. When an eavesdropper observes the data in the channel, it corrupts the data stream which triggers an alarm when it is not the expected values.*

2.3 Quantum Position Verification: Authenticating the Time and Location

Creating an unspoofable physical receipt for digital communication.

Proving where and when an action occurred, or ensuring that the agent you are talking to is where they say they are, is critical for regulatory compliance and national security.[13] Securely identifying where a communication is initiated from is a powerful tool against a large variety of financial scamming and spoofing attacks. Classical position verification (IP geolocation, GPS, timestamping) is vulnerable to VPN masking, clock manipulation, and DNS redirection. Furthermore, classical position verification is mathematically proven to be insecure when communication channels are intercepted by adversaries.

Quantum Position Verification (QPV) is the first-ever provably secure way to verify a network entity's location. It not only acts as a true example of quantum advantage, but also empowers the cybersecurity and compliance world with a powerful paradigm-shifting tool.

The Quantum Mechanism

Quantum Position Verification (QPV) cryptographically enforces a user's exact location and time by combining the absolute speed limit of light with the quantum no-cloning theorem. In this system, two "verifier" nodes simultaneously send a randomized process request to a "prover" and measure the roundtrip response time; because information cannot travel faster than light, this timing perfectly triangulates the prover's physical location.

While classical triangulation is vulnerable to coordinated spoofing by colluding hackers, QPV completely secures the process by having a verifier share entangled photons with the prover and demand real-time, randomized polarization measurements. Because quantum states cannot be copied or accurately intercepted without destroying them, hackers cannot impersonate the prover's location. When the verifiers confirm the measurement results match expected bounds, they guarantee the integrity of the transmission and the undeniable physical presence of the user.

- **Paradigm-Shifting Approach:** Classical secure position verification is provably impossible, making QPV a clear example of quantum advantage, adding an important layer to physical security and compliance.[13]
- **Adversary Prevention**: Because quantum states cannot be cloned, colluding adversaries outside the claimed region cannot intercept, copy, process, and relay the quantum states fast enough to simulate the prover without breaching the timing window.
- **A Digital Receipt:** Since time and space are complementary, QPV can be used to determine both the location and the time of a transaction. This expands the use-cases of the protocol way beyond compliance and fraud prevention into a true replacement for digital signatures. As a quantum signature, QPV is capable of certifying the position and time of the signatory.

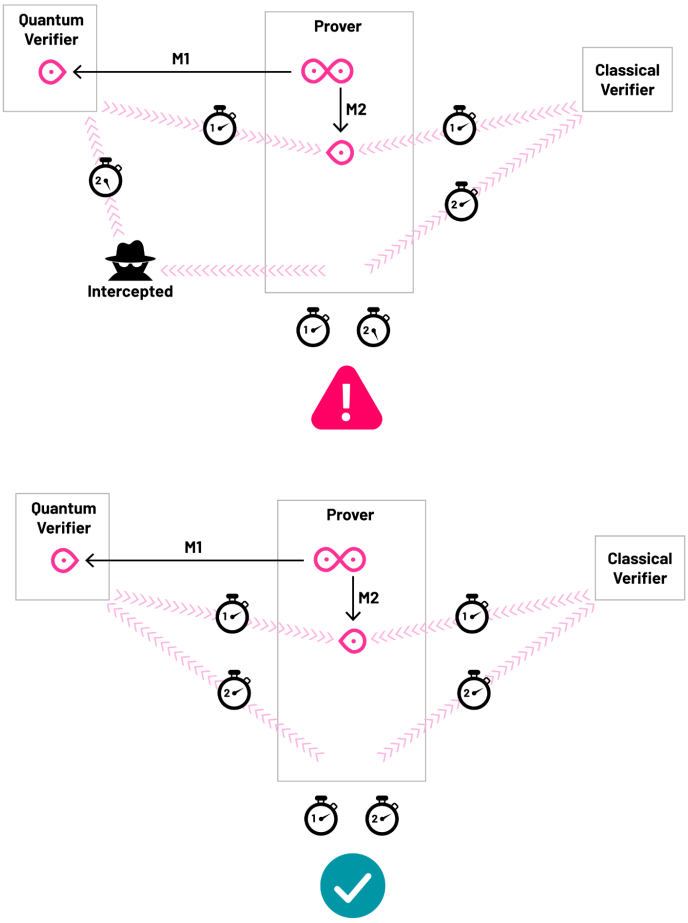


FIGURE 3 • Schematic of Quantum Position Verification: *The Prover generates an entangled photon pair (pink infinity sign) and sends half to Verifier 1 who measures it (M1). The other half is measured by the Prover based on instructions received from the two Verifiers (M2). The time to traverse the path between the Verifiers and Provers is clocked with high precision (stopwatches 1 & 2) providing a precise location. If an eavesdropper is present on the line, the times will not match, triggering an alarm.*

2.4. Summary of Quantum Physical Guarantees

Mapping threats to guarantees

Threat Vector	Classical Defensive Flaw	Quantum Physical Guarantee
Synthetic identity and impersonation at scale	Credentials, biometrics, and behavioral signals can be synthesized by AI models.	**QFA:** identity bound to unclonable hardware, verified by quantum correlation
Machine learning attacks on PUFs	Classical hardware fingerprints are learnable from observed challenge-response pairs.	**QFA:** responses hidden inside locally indistinguishable quantum states
Harvest now, decrypt later	Intercepted ciphertext is archived today and decrypted once quantum computers mature.	**QCP:** interception detected at the moment it occurs, not in hindsight
Automated fiber tapping and rerouting	Power levels and OTDR heuristics are easily bypassed by low-power passive clip-on taps.	**QCP:** quantum-level tap and reroute detection at centimeter scale
Spoofed location, time, and jurisdiction	IP geolocation, GPS signals, and system clocks are routinely spoofed via proxies or VPNs.	**QPV:** spacetime seal secure against classical and quantum adversaries
Rogue Agent-to-Agent transactions	Autonomous software acts at machine velocity with zero human intuition in the execution loop.	**All three:** machine-verifiable provenance covering identity, path, and moment

Key Takeaway

*Entanglement-enhanced security is a true example of **quantum advantage**: each use-case performs an operation that is not possible without quantum technology, and has significant value. This further demonstrates that quantum computing alone is not required to demonstrate quantum advantage, and businesses can take advantage today.*

3. Enterprise Readiness: Qunnect's Progress to Real-World Deployment

A security architecture that requires dedicated, specialized fiber or cryogenic facilities is a laboratory research program, not an enterprise product. Qunnect has built a foundation that allows these novel security protocols to operate directly over deployed, commercial optical networks without requiring infrastructure overhauls or "rip-and-replace" capital expenditure.

Field-Proven Production Benchmarks

The underlying physical layer for these advances in security has been validated by Qunnect across diverse real-world operating environments, proving performance under thermal fluctuations, physical cable strain, and co-propagating classical noise:

Network Name	Host	Uptime	Fidelity	Length	Operating Conditions
MD Aerial Fiber	NIST/UMD <> Qunnect	92.8%	>98%	62 km	Validated over exposed aerial fiber subject to wind, temperature variations, and mechanical vibration. The system preserved entanglement across 24 hours.[14]
GothamQ (New York City)	Qunnect	99.84%	~99%	34 km	Demonstrated 15 consecutive days of uninterrupted entanglement distribution on metropolitan fiber.[15]
BearlinQ (Berlin)	Deutsche Telekom <> Qunnect	>98.5%	85-99% path dependent	15-100 km	Demonstrated 17 consecutive days of uninterrupted entanglement distribution in the presence of digital data traffic (C-band).[16]

Operational Integration

For CISOs and infrastructure architects, quantum entanglement-enhanced security integrates into existing network operations through three key operational design choices:

1. **Standard Rack Form Factor:** Chassis hardware mounts directly into standard 19-inch server racks in central offices or data center environments.
2. **Ambient Temperature Operation:** Requires no liquid helium, dilution refrigerators, or specialized cooling infrastructure.
3. **In-Band Co-existence:** Operates at telecommunications wavelengths, allowing quantum authentication and path integrity signals to co-exist with existing enterprise traffic on leased dark or lit fiber.

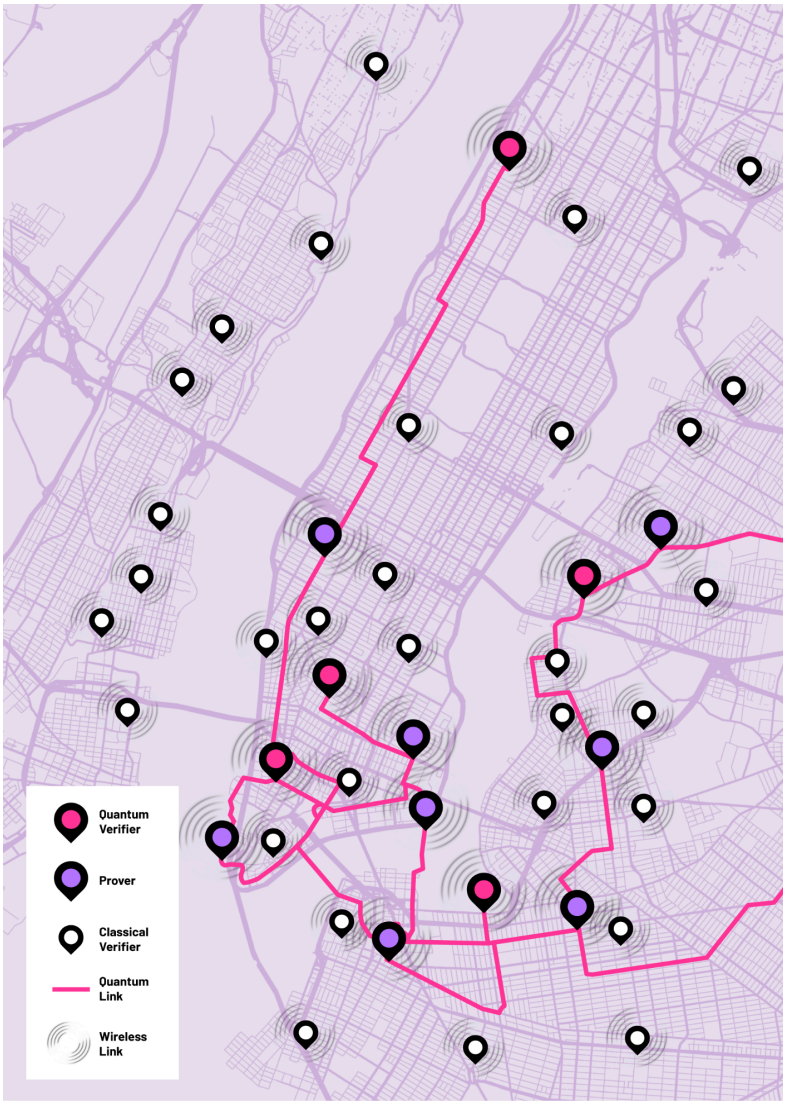
Progress Towards Physical Entanglement Security Deployment

Quantum Device Authentication:

In May 2026, a Sorbonne, CNRS, and Edinburgh collaboration reported the first experimental realization of hybrid hardware-based Quantum Device Authentication scheme: a fully information-theoretically secure authenticated entanglement-enhanced key distribution protocol requiring no pre-shared secret at any stage, at telecom wavelength, sustaining operation across 50 dB of channel attenuation with a quantum bit error rate below 0.6 percent.[17] Qunnect is implementing this protocol family with Deutsche Telekom on the BearlinQ network in Berlin.

Quantum Channel Protection:

In 2026, Qunnect demonstrated its Quantum Channel Protection capability on GothamQ: a physical-layer security system that co-propagates 2.5 GB/s classical data with a 1324 nm entangled-photon monitoring signal. By continuously measuring quantum correlations, timing, polarization, loss, and noise against a calibrated baseline, QCP detects fiber tapping, splitting, path modification, jamming, and other physical interference with sensitivity beyond conventional networking and optical-monitoring tools. Crucially, because Quantum Channel Protection relies on entanglement correlations that cannot be copied or recreated by an adversary, the monitoring signal is fundamentally unspoofable. Qunnect demonstrated the system to members of the U.S. Intelligence Community on its New York City GothamQ network in April and September 2026, showing that this new security layer can be deployed directly over existing fiber infrastructure.

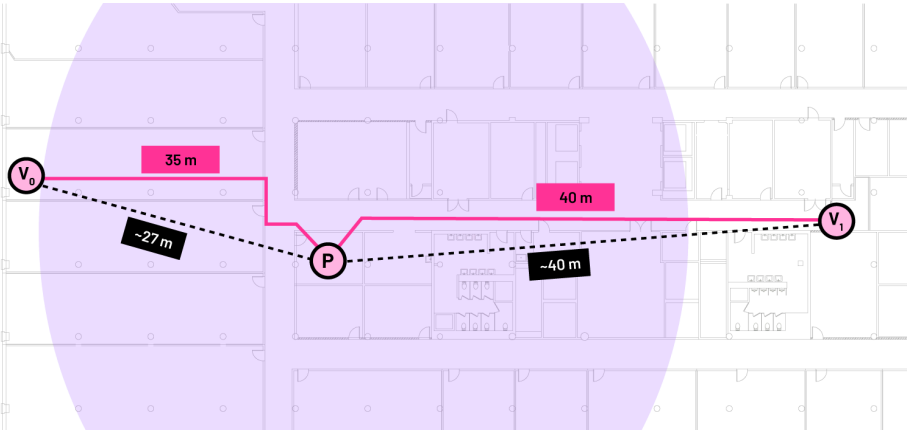


Quantum Position Verification:

Working with a financial partner, Qunnect demonstrated a loss-tolerant Quantum Position Verification protocol whose security does not degrade with channel loss, allowing it to scale in distance without protocol changes.

← ***FIGURE 4 • Scaling QPV in a Metropolitan Network:*** *An exemplary map of New York City where the expensive quantum resources are concentrated in a backbone (pink and purple dots) with numerous inexpensive classical resources (white dots) are able to access the quantum backbone. Any combination of pink, purple and white can certify a transaction with QPV.*

→ ***FIGURE 5 • Demonstration of QPV:*** *Conducted at the Qunnect Headquarters on the 11th floor of a building in the Brooklyn Navy Yard. The Quantum Verifier is connected to the prover by 35m of RF cable and optical fiber. The Classical Verifier is connected by 40m of RF cable and optical fiber. The position of the Prover is verified within the purple shaded area.*



The implementation used commercial off-the-shelf components, achieved position certainty on the order of tens of meters, proved finite-size security against quantum polynomial-time adversaries, and requires only a single quantum verifier node alongside classical infrastructure, which makes it naturally compatible with metropolitan-area quantum networks.[13]

4. Conclusion: A Pragmatic Shift to Security by Entanglement

Entanglement-enhanced security (EES) is a new paradigm shift in digital infrastructure resilience that is grounded in the physical laws of quantum mechanics, enabling engineers to provide a stronger guarantee for security outcomes. EES is further designed to integrate with existing cybersecurity protocols, enhancing them without replacing them. As we talk about EES, it is vital to distinguish it from QKD: EES provides a broader, physics-based authentication layer that bypasses the specific limitations and pre-shared secret requirements inherent in QKD deployments.

A common misconception persists that EES requires the presence of quantum computers. These protocols operate natively using entangled photons distributed over existing commercial telecom fiber without the necessity of operational quantum computing hardware.

The pressure AI and quantum capabilities will exert on digital infrastructure simultaneously erodes the core assumptions that classical security has depended on for decades: 1. that math problems stay hard, 2. that hardware behavior stays unpredictable, and 3. that human intuition can spot an impersonator. By providing deterministic answers to who is communicating, what path the data took, and where and when the event occurred, EES delivers machine-verifiable security for an automated world, deployed directly on the optical fiber already in the ground.

Qunnect

Qunnect is advancing these capabilities for near-term commercial availability, allowing for immediate deployment in standard enterprise environments without the need for cryogenic facilities or quantum processing infrastructure.

Hardware, not hype.

References

1. "Artificial Intelligence." *Cybersecurity and Infrastructure Security Agency*, U.S. Department of Homeland Security, www.cisa.gov/ai. Accessed 17 Sept. 2026.

2. Executive Office of the President, "Securing the Nation Against Advanced Cryptographic Attacks," Executive Order 14412, June 22, 2026, https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks/.

3. Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). Report on Post-Quantum Cryptography. National Institute of Standards and Technology. https://doi.org/10.6028/nist.ir.8105

4. K. Chakraborty, M. Doosti, Y. Ma, C. Wadhwa, M. Arapinis, and E. Kashefi. Quantum Lock: A Provable Quantum Communication Advantage. Quantum 7, 1014, 2023. Reviews the machine learning vulnerability of classical PUFs identified in Gao et al., Nature Electronics, 2020.

5. Rührmair, U., Sehnke, F., Sölter, J., Dror, G., Devadas, S., & Schmidhuber, J. (2010). Modeling attacks on physical unclonable functions. Proceedings of the 17th ACM conference on Computer and communications security, 237–249. https://doi.org/10.1145/1866307.1866335

6. Rose, Scott, Oliver Borchert, Stu Mitchell, and Sean Connelly. Zero Trust Architecture. NIST Special Publication 800-207. Gaithersburg, MD: National Institute of Standards and Technology, 2020. https://doi.org/10.6028/NIST.SP.800-207.

7. Tao, Ke, J. Li, and Srinivas Sampalli. "WISE GUARD - MAC Address Spoofing Detection System for Wireless LANs." In Proceedings of the Second International Conference on Security and Cryptography, 140–147. Setúbal, Portugal: SciTePress, 2007. https://doi.org/10.5220/0002123601400147.

8. Iqbal, M. Z., Fathallah, H., & Belhadj, N. (2011, December). Optical fiber tapping: Methods and precautions. In *High Capacity Optical Networks and Enabling Technologies (HONET)*. IEEE. https://www.researchgate.net/publication/259761851_Optical_Fiber_Tapping_Methods_and_Precautions

9. Center for Strategic and International Studies. "Beyond Autonomous Attacks: The Reality of AI-Enabled Cyber Threats." CSIS Strategic Technologies Blog, April 29, 2026. https://www.csis.org/blogs/strategic-technologies-blog/beyond-autonomous-attacks-reality-ai-enabled-cyber-threats.

10. National Security Agency. "Quantum Key Distribution (QKD) and Quantum Cryptography (QC)." NSA Cybersecurity Advisory. October 26, 2020. https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/.

11. Zhang, W., van Leent, T., Redeker, K., et al. (2022). A device-independent quantum key distribution system for distant users. Nature, 607, 687–691. https://doi.org/10.1038/s41586-022-04891-y

12. S. Goswami, M. Doosti, and E. Kashefi. Hybrid Authentication Protocols for Advanced Quantum Networks. arXiv:2504.11552v2, February 2026.

13. Kon, W. Y., Bigagli, N., Conrad, A., et al. (2026). *Loss-tolerant quantum position verification for metropolitan area networks*. arXiv:2609.23234, September 2026.

14. Y.Shi, J.Su, A.Rahmouni, P.Shrestha, M.Merzouki, G.Bello Portmann, A.Lazenby, M.Flament, M.Namazi, A.Battou, O.Slattery, and T.Gerrits, "Entanglement distribution over a polarization-stabilized aerial fiber," JOCN 18, 813-819 (2026)

15. A.N.Craddock, A.Lazenby, G.Bello Portmann, R.Sekelsky, M.Flament, M.Namazi. Automated Distribution of Polarization-Entangled Photons Using Deployed New York City Fibers. PRX Quantum 5, 030330, 2024

16. M.Sena, M.Flament, S.Andrewski, I.Caltzidis, N.Bigagli, T.Rieser, G.Bello Portmann, R.Sekelsky, R-P.Braun, A.N.Craddock, M.Schulz, K.D. Jöns, M.Ritter, M.Geitz, O.Holschke, and M.Namazi, "High-fidelity quantum entanglement distribution in metropolitan fiber networks with co-propagating classical traffic," J. Opt. Commun. Netw. 17, 1072-1081 (2025)

17. Sorbonne, CNRS, & Edinburgh collaboration. Experimental realization of hybrid hardware-based authentication protocol across 50 dB channel attenuation. May 2026.