Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Loss-Tolerant Quantum Position Verification for Metropolitan Area Networks

Kaushik Chakraborty

kaushik.chakraborty@jpmchase.com

JPMORGANChase https://orcid.org/0000-0002-6425-0418

Wen Yu Kon

JPMorganChase https://orcid.org/0000-0001-8174-6004

Niccolo Bigagli

Qunnect Inc. https://orcid.org/0000-0002-2598-4320

Andrew Conrad

JPMorganChase

Taylor Shields

JPMorganChase https://orcid.org/0000-0002-6225-6541

Fatih Kaleoglu

JPMorganChase https://orcid.org/0009-0003-0565-1566

Ignatius William Primaatmaja

JPMorganChase

Alexander Craddock

Qunnect Inc.

RJ Pisani

Qunnect Inc.

Mael Flament

Qunnect Inc. https://orcid.org/0000-0002-3963-9894

Jude Seeber

JPMorganChase

Omar Amer

JPMorganChase

Charles Lim

National University of Singapore https://orcid.org/0000-0002-2332-4126

Mehdi Namazi

Qunnect Inc.

Rob Otter

JPMorganChase

Xinhua Ling

JPMorganChase

Article

Keywords:

Posted Date: November 25th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10145993/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: Yes there is potential Competing Interest. W.Y.K., I.W.P., C.L., and K.C. are co-inventors on a patent application related to this work (U.S. Patent US-12675596-B2 ``Systems and methods for source-independent quantum position verification''). A.C., T.S., J.S., O.A. are co-inventors on a patent application related to this work (U.S. Patent Application 63/782,777 ``Low-Latency Wireless Communication'').

Loss-Tolerant Quantum Position Verification for Metropolitan Area Networks

Wen Yu Kon,[1,*] Niccolò Bigagli,[2,*] Andrew Conrad,[1,*] Taylor Shields,[1] Fatih Kaleoglu,[1] Ignatius William Primaatmaja,[1] Alexander Craddock,[2] RJ Pisani,[2] Mael Flament,[2] Jude Seeber,[1] Omar Amer,[1] Charles Lim,[1] Xinhua Ling,[1] Rob Otter,[1] Kaushik Chakraborty,[1,†] and Mehdi Namazi[2,‡]

[1] *Global Technology Applied Research, JPMorganChase, New York, NY 10017, USA*
[2] *Qunnect Inc., 141 Flushing Ave, Ste 1110, Brooklyn, NY 11205-1005*

(Dated: November 23, 2026)

A *spacetime seal*, a cryptographic guarantee that a digital event has occurred at an approved location and time, can augment a digital signature with location attestation for legal, financial, and regulatory use cases. In adversarial settings any purely classical realization of such a seal can be spoofed [1, 2]. Quantum position verification (QPV) offers a physics-based solution, exploiting the no-cloning theorem and the no-signaling principle to certify a party's spacetime coordinates [2]. While the feasibility of QPV has been recently shown via entanglement- [3] and coherent light-based protocols [4], achieving channel-loss tolerance for these schemes [5, 6] substantially increases implementation complexity at metropolitan scales. Here, we introduce and experimentally demonstrate a loss-tolerant QPV (LT-QPV) protocol whose security is independent of channel loss and whose distance limit is capped by local loss and storage requirements at the prover node. We prove finite-size security against quantum polynomial-time entangled adversaries in the quantum random oracle model instantiated with cryptographically secure hash functions. Implemented entirely with commercial off-the-shelf components, our system certifies position within 22 minutes of net data collection time against i.i.d. adversaries with no early knowledge of the measurement basis (4-bit challenges), with a projected path to real-time certification (< 1 s) against general attacks with upgraded hardware. Our architecture, requiring only a single quantum verifier node alongside classical infrastructure, is naturally compatible with metropolitan-area quantum networks, establishing the foundations for scalable, physics-backed spacetime certification as a deployable service.

INTRODUCTION

Digital signatures are as ubiquitous in our daily lives as in regulatory settings. While they greatly simplify transactions and agreements, they can bear no verifiable attestation of the location where a signing took place. For a growing set of applications, this missing attribute is of paramount importance. In particular, many digital systems operate in environments where the jurisdiction in which data processing, access, or authorization occurs may be relevant. Data-residency rules and related governance considerations arise in connection with regulatory frameworks such as the EU General Data Protection Regulation (GDPR) [7], financial-market regulations such as MiFID II [8–10], export-control frameworks such as ITAR [11], and healthcare statutes such as HIPAA [12], all bind digital activity to specific jurisdictions. Similarly, sovereign-cloud mandates, sanctions compliance, electronic notarization, and trusted confidential computing (TCC) [13] can benefit from a verifiable, tamper-evident attestation of where a digital event has occurred. Developing trustworthy protocols for location verification is therefore an important technical problem for modern digital service providers.

Within current communication frameworks, time and location metadata accompanying digital signatures can be subverted. For instance, an attacker can redirect traffic via DNS or API-gateway compromise, interfere with sensor paths, mask IP addresses through proxies and VPNs, spoof MAC addresses, or manipulate system clocks. More fundamentally, no purely classical position-verification protocol can be secure against colluding adversaries [1, 2]. These limitations motivate the need to expand current techniques to include beyond-classical capabilities.

A potential approach to provide secure location information is quantum position verification (QPV), a class of protocols that can be used to generate a *spacetime seal*, a certified, publicly verifiable stamp of the time and location of a signing event whose security rests on physical principles rather than on the integrity of any particular network. A powerful technique, QPV can go beyond spacetime certification and support location-based access control, position-based key exchange [2, 14] and treaty and inspection verification.

QPV exploits the no-cloning theorem and the no-signaling principle to certify that a party occupies a claimed position in spacetime. In a QPV protocol, two or more cooperating verifiers challenge a prover to demonstrate that it occupies a claimed position by requiring it to respond correctly to quantum and classical inputs within a

* These authors contributed equally to this work.
† kaushik.chakraborty@jpmchase.com
‡ mehdi@quconn.com

narrow timing window dictated by the speed of light. While unconditional security against adversaries possessing unbounded entanglement is known to be impossible [2, 15], meaningful security can be achieved under physically motivated resource constraints such as limited entanglement [3, 6, 16, 17], computational hardness assumptions [18], or polynomial resources (e.g. query access) in the quantum random oracle model [19]. A central practical obstacle, however, has been channel loss: photons transmitted over realistic quantum channels between the prover and verifier are frequently lost. To manage channel loss, existing protocols have to either exponentially increase the number of measurement bases [6] or employ complex Bell-state measurements [5].

Experimental efforts to realize QPV have accelerated in recent years, with three concurrent demonstrations highlighting both the progress and the remaining challenges. Kanneworff *et al.* [20] reported a partial implementation of a single-photon SWAP-based demonstration, providing a proof of concept but lacking security against entangled adversaries. Kavuri *et al.* [3] proposed and demonstrated a device-independent protocol that removes trust assumptions on the measurement devices at the cost of stringent experimental requirements. Their protocol limits the loss tolerance to 1/3, matching that of Bell tests. Finally, Fan-Yuan *et al.* [4] demonstrated a prepare-and-measure scheme using coherent states, offering some practical simplicity but relying on hollow-core fibers. These specialized fiber optics are more expensive and less widely deployed than standard telecom fiber, presenting practical challenges for large-scale deployment. Furthermore, at the metropolitan regime, partial channel loss-tolerance is achieved with an exponentially growing measurement complexity while full channel loss-tolerance requires a complex Bell state measurement using the scheme in Ref. [5] (assuming speed of light classical communication), which presents further experimental challenges.

Here, we propose and experimentally demonstrate a loss tolerant QPV protocol (LT-QPV) whose security is independent of channel loss. By shifting the duty of preparing and distributing entangled qubits to the prover and by assuming the verifier possesses a trusted measurement device, any no-detection rounds at the latter location can be safely discarded, providing intrinsic tolerance to channel loss. This provides better scaling compared to simple prepare-and-measure QPV that is sufficient for implementation at metropolitan distances, while still not allowing for arbitrary scaling of prover-verifier separation in practical settings where standard optical fibers are used for quantum communication. Due to their limited transmission speed, these fibers require the use of quantum memories at the prover, which in turn couple prover efficiency to distance. With a fiber delay loop, as in our experiment, the storage loss is a factor of 3 smaller than the loss between the verifier and prover. Throughout, we refer to a protocol as "channel-loss tolerant" if its security is independent of the loss on the prover-verifier quantum channel (given basis-independent detection at the trusted verifier). We reserve "fully loss tolerant" for protocols whose security is also independent of prover–verifier separation, i.e. of the channel loss and storage requirements that grow with it. LT-QPV is channel-loss-tolerant, and it becomes loss-tolerant only when classical and quantum signals travel at the speed of light. Channel-loss tolerance is sufficient in many cases, as most practical applications of QPV do not require quantum channels spanning hundreds or thousands of kilometers.

We prove the finite-size security of LT-QPV against quantum polynomial-time (QPT) adversaries in the quantum random oracle model (QROM) [21], covering both independently and identically distributed (i.i.d.) attacks, where an adversary performs the same attack strategy independently for every round (also known as individual attacks) [22, 23], and general coherent attacks under sequential repetition. We further validate the protocol with a short-distance experimental demonstration, certifying the location of an untrusted prover at a distance of ∼60m with our LT-QPV protocol using only standard, commercially-available hardware, as shown in Fig. 1**a**, against an adversary performing i.i.d. attacks with no early knowledge of the measurement basis.

The quantum communication requirements of the LT-QPV framework are naturally compatible with emerging quantum network architectures in which entanglement is distributed and measured at network nodes, and the classical requirements are plausibly realizable at metropolitan scales utilizing cellular towers or other standard wireless communication technologies. While we do not validate our protocol against any of the regulatory standards we previously mentioned, these characteristics open a practical route towards realizing secure spacetime seals as an early application of metro-scale quantum networks and provide a basis for future developments.

THE PROTOCOL

We consider a setting where two verifiers, V_0^Q and V_1^C, cooperate to certify the location of a prover P at a claimed position between them, as illustrated in Fig. 1. One verifier, V_0^Q, is quantum-enabled, i.e. they are able to measure the state

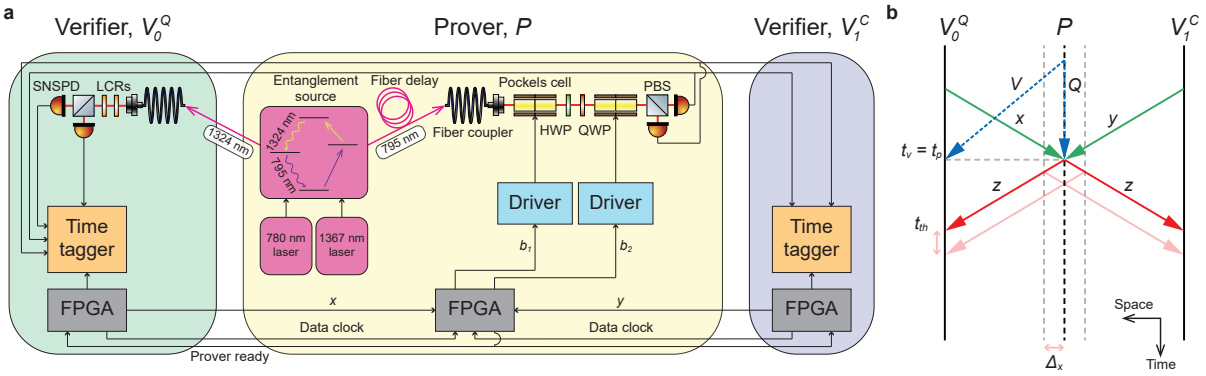


FIG. 1: **a**, **Sketch of the experimental setup.** Our system consists of an untrusted prover P, a quantum verifier V_0^Q, and a classical verifier V_1^C. The prover generates an entangled pair and transmits 1324 nm (Telecom) photon to V_0^Q, then later measures the 795 nm (NIR) photon based on the challenge commands x, y provided by V_0^Q and V_1^C. The measurement result z is transmitted back to both verifiers, which check if the result matches the measurement of the Telecom photon and determine the positional uncertainty based on the transmission times of x, y and the receive times of z. **b**, **Spacetime diagram of the LT-QPV protocol**. The quantum verifier V_0^Q, the quantum prover P, and the classical verifier V_1^C are positioned on a line segment. The blue dotted arrow represents the quantum channel from P to V_0^Q. The green and red lines represent classical channels. While the figure presented shows $t_V = t_P$, this is in general not necessary. More details on the choices of t_V and t_P can be found in Supplementary Section III B 1.

of a qubit, while the other, V_1^C, is fully classical. The LT-QPV protocol is comprised of repeated QPV rounds during which classical and quantum information is exchanged between the three nodes. In each round, the prover generates a Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, where 0 and 1 refer to any orthogonal qubit states (e.g. horizontal and vertical photon polarization, H and V). One qubit (subsystem Q) is retained by the prover, the other (subsystem V) is transmitted through a quantum channel to verifier V_0^Q. Concurrently, verifiers V_0^Q and V_1^C issue randomly chosen classical challenges x and y, timed to arrive at the prover's claimed position simultaneously. A shared public hash function f, such as SHA3 [24], maps the pair of challenges (x, y) to a measurement basis $\alpha = f(x, y)$, selected from m possible bases. Verifier V_0^Q holds a fully characterized measurement device that performs projective measurements in basis α with basis vectors

$$|\psi_0^\alpha\rangle = \cos\left(\frac{\theta_\alpha}{2}\right)|0\rangle + \sin\left(\frac{\theta_\alpha}{2}\right)e^{i\phi_\alpha}|1\rangle, \qquad (.1)$$

and its orthogonal state $|\psi_1^\alpha\rangle$, where θ_α and ϕ_α are the polar and azimuthal angles on the Bloch sphere for basis α. Valid rounds occur when the measurement apparatus at both the prover and V_0^Q is set to the same basis, and V_0^Q detects a qubit. If the prover also detects a qubit, they forward the measurement result, z, to both verifiers. After N valid rounds, the verifiers note the number of rounds when the prover had a detection, N_{det}, the number of error rounds in which the prover's and verifier's outcomes disagree, N_{err}, the number of double-click events at V_0^Q, N_{dc}, and the number of rounds the prover's responses to each verifier are mismatched (i.e. the z values received by V_0^Q and V_1^C are different), N_{mis}. The prover's location is certified by checking that: (1) the prover efficiency (the ratio of valid rounds that are detected by the prover) meets a minimum threshold $\eta = N_{\text{det}}/N \geq \eta_{\text{th}}$, (2) the effective quantum bit error rate (QBER) is below a maximum threshold, $\text{QBER} = (N_{\text{err}} + N_{\text{dc}})/N_{\text{det}} \leq e_{\text{th}}$, and (3) N_{mis} is below a maximum threshold, $N_{\text{mis}}/N \leq p_{\text{mis,th}}$. The protocol is detailed in the methods and Supplementary Information, and a spacetime diagram of a single round is shown in Fig. 1**b**. We note that if the classical and quantum communication speeds, v_{cl} and v_V, are not at the speed of light, c, and the prover's processing time is non-zero, the prover P can only be certified to be within a region. We also note that we do not simply abort the protocol when mismatch is observed since in practice, mismatches caused by timing fluctuations where one value may arrive after the cut-off time or other imperfections such as noise in the classical channel may occur.

LT-QPV can be viewed as a source-independent version of a f-measure QPV protocol [16]. The classical communications in both protocols are identical, and the main difference is in the quantum state preparation and transfer. Standard f-measure QPV has the verifier prepare qubit Q to

be sent to the prover, while we allow the prover to prepare an entangled state and send V to the verifier. As such, the channel loss for f-measure protocols is experienced by the qubit received by the prover, while the channel loss in LT-QPV is experienced by the verifier's qubit V instead. Consequently, excess channel loss in f-measure lowers the honest prover's efficiency and can cause the honest prover to fail, whereas in LT-QPV the same loss does not affect the prover's efficiency, leading to channel-loss tolerance as detailed below. Switching to source-independence also requires a trusted measurement device instead of a trusted source at the verifier, and an additional entanglement source at the prover.

The central theoretical result of our protocol is that LT-QPV security is independent of channel loss between the prover and verifier by having the prover prepare and broadcast the entangled quantum state, assuming that the verifier holds a trusted measurement device. Crucially, the loss tolerance is conditional on this device's detection probability being independent of the measurement basis α. Only then are no-detection rounds uninformative and safely discardable. We note that this does not imply arbitrary separation between the prover and verifier V_0^Q since the distance may indirectly affect the prover-side loss. The loss-tolerance follows from the causal structure of the protocol: under the QROM, the measurement basis α is first revealed at the prover location P at time t_P. Since the detection event at V_0^Q is space-like separated from the basis revelation (see Fig. 1**b**), the verifier's detection decision is independent of α and no-detection rounds can be safely discarded. While our protocol is intrinsically tolerant to channel loss, local losses on the prover side (including source heralding efficiency) can degrade performance, with the tolerated prover efficiency scaling as $\eta \sim \frac{1}{m}$ in the asymptotic regime ($N \to \infty$) for zero QBER and uniform basis choice.

We prove finite-size security against entangled QPT adversaries (adversaries with memory, computational power, entanglement and query access to f bounded by a polynomial in the security parameter n) in the QROM model, establishing that the protocol is ε_{sou}-sound and ε_{com}-complete for both i.i.d. and general attacks. The theorem and proof structure is presented in the Methods and the complete proof is provided in the Supplementary Information. This indicates that an honest prover fails verification with probability at most ε_{com}, while any QPT adversary passes verification with probability at most ε_{sou}. Notably, the security proof requires no assumptions on the prover's source, rendering the protocol source-independent. Multi-photon attacks on V_0^Q's measurement device are handled through universal squashing [25], which treats double-click events as errors, and the monogamy of entanglement [26] ensures that any adversary attempting to correlate with both verifiers simultaneously incurs QBER exceeding the verification threshold.

THE EXPERIMENT

After sketching the contours and the strengths of LT-QPV, we experimentally demonstrate its feasibility. The setup is comprised of quantum and classical layers connecting the prover to the two verifiers. The quantum layer provides and measures the entangled particles used in the protocol; the classical layer handles the selection of measurement bases, the calculation of the uncertainty areas around the verifiers, and the collection, compiling, and analysis of measurement results. Fig. 1**a** shows a diagram of the experimental setup.

The qubits used in our protocol are polarization-entangled photon pairs generated by a warm rubidium entanglement source [27] placed at the prover's location. Each pair is constituted by a photon at 795 nm (near infrared, or NIR) and one at 1324 nm (telecom), emitted in the $|\Phi^+\rangle$ Bell state. The NIR photon is kept at the prover's location, delayed by a 42 m optical fiber delay line, and then coupled into a measurement station capable of measuring in 16 unique bases, a number that ensures no security issues for $\eta \gtrsim 6.25\%$ for zero QBER and uniform basis choice. The telecom photon is coupled into a fiber deployed between the prover and V_0^Q, after which it encounters its own measurement station.

Low-latency communication and control between the verifier and prover nodes are realized using field-programmable gate arrays (FPGAs). For each QPV round, the verifiers' FPGAs transmit random four-bit challenge signals $x, y \in \{0,1\}^4$, which are timed to arrive simultaneously at the prover's claimed location. The prover then selects a measurement basis $\alpha = f(x,y)$ out of the 16 possible measurement basis using a 16×16 randomly-generated lookup table stored in the FPGA's memory. To enact fast basis selection for each measurement we employ two back-to-back high-voltage Pockels cells, each selecting one of 4 unique polarization rotations and capable of nanosecond switching. QPV rounds are repeated at a 200 kHz rate, limited by the cells' drivers and clocked by the FPGAs. The probabilistic nature of the entanglement source makes it impossible to predict whether a classical round will lead to zero, one, or more than one valid rounds. More details on how the quantum and the classical layers cooperate to enact the QPV protocol are presented in

the Methods.

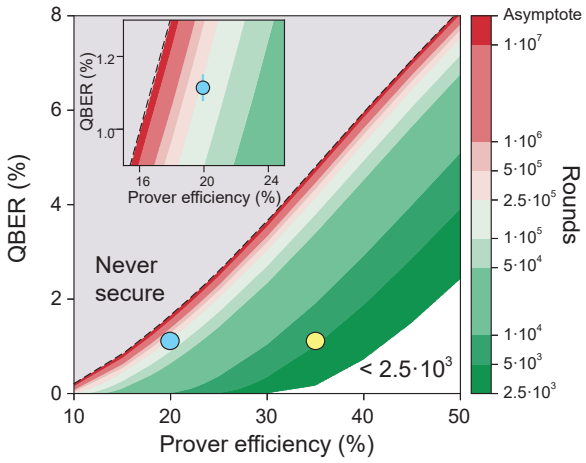


FIG. 2: Performance of the QPV system required to achieve a security of $\varepsilon_{com} = 10^{-2}$ and $\varepsilon_{sou} = 10^{-2}$ against i.i.d. adversary assuming $\varepsilon_{ROM} = 0$ with expected mismatch probability $p_{\text{mis}} = 5.49 \times 10^{-6}$ and double click probability $p_{\text{dc}} = 1.45 \times 10^{-4}$. The dotted line represents the performance requirements in the asymptotic regime and the solid lines represents the performance requirements for N valid rounds. The blue dot denotes the performance of our QPV system implementing the LT-QPV protocol, which requires $\geq 2.55 \times 10^5$ rounds to achieve security. The yellow dot demonstrates how the number of required rounds can be reduced by increasing the prover efficiency.

Prior to the QPV demonstration, we execute a full scale calibration round to characterize hardware performance and calculate the parameters under which the protocol can successfully certify the prover's location. Note that an independent calibration run is necessary to avoid violating the assumption that the performance thresholds and number of valid rounds N are chosen prior to the protocol run, as explained in the Supplementary Information. The calibration round is performed by running the full setup over 47 minutes of net data collection time, equal to 184 minutes of continuous operation. This overhead is due to our data acquisition software and can be shortened as explained in the Methods. During the calibration, we measure an overall QBER of $1.17 \pm 0.05\%$ and a prover's efficiency of $\eta = 20.10 \pm 0.07\%$. As shown in Fig. 2, under an i.i.d. adversary model with no early knowledge of the measurement basis and with security parameters $\varepsilon_{com} = 10^{-2}$ and $\varepsilon_{sou} = 10^{-2}$, a total of $N \geq 2.55 \times 10^5$ rounds is required to certify the prover's position, and the observed performance must stay within the acceptance thresholds $\eta_{\text{th}} = 19.86\%$, $e_{\text{th}} = 1.31\%$, and $p_{\text{mis,th}} = 2.9 \times 10^{-5}$.

With these requirements established, we carry out the full LT-QPV demonstration. In under 22 minutes of net data collection time we complete $N = 2.6 \times 10^5$ rounds and measure an effective QBER of $1.23 \pm 0.05\%$, a prover's efficiency of $\eta = 19.96 \pm 0.08\%$, and only one mismatched response, $p_{\text{mis}} = 3.8 \times 10^{-6}$, clearing the required acceptance checks and certifying the prover's location. To highlight our setup's stability, we point out that our QPV data collection is performed three days after the calibration dataset with minimal intervention between runs. Further repetition of QPV instances can be enacted to establish an empirical pass rate.

The positional uncertainty of the prover is determined by calculating the distance that light in free space could have traveled during the time elapsed between the transmission of the challenge commands and the reception of the result of the quantum measurement. In our QPV instance, the radii for verifiers V_0^Q and V_1^C are found to be $r_0 = 58.1$ m, and $r_1 = 64.6$ m, respectively. We calculate the quantum-advantage ratio compared to classical ranging as the volume of the positional uncertainty region divided by that of a classical ranging protocol with the same configuration of verifiers; this definition was introduced and used in [3]. The quantum advantage values are 2.18 (1-D), 2.44 (2-D), and 2.67 (3-D), using the measured timing and geometry for our LT-QPV demonstration (see calculations in Supplementary Section VIII D). As shown in Fig. 3, our positional uncertainty region does not include the verifiers' locations. In contrast, the equivalent region of any classical position verification protocol always contains the line segment connecting the two verifiers even in the ideal case without any latency. In practice, network latency leads the positional uncertainty region to circumscribe an ellipsoid with foci at the verifiers [3]. This implies that our protocol securely verifies the position of the prover more precisely than any classical protocol, providing an indisputable quantum advantage [1].

DISCUSSION

Thus far we have demonstrated that the LT-QPV can be implemented experimentally using commercially available hardware and standard telecom infrastructure against i.i.d. adversaries with limited query access. Together with finite-size security guarantees against both i.i.d. and general entangled adversaries under the QROM, and a source-independent security proof that places no trust assumptions on the prover's hardware, LT-QPV serves as a potential candi-

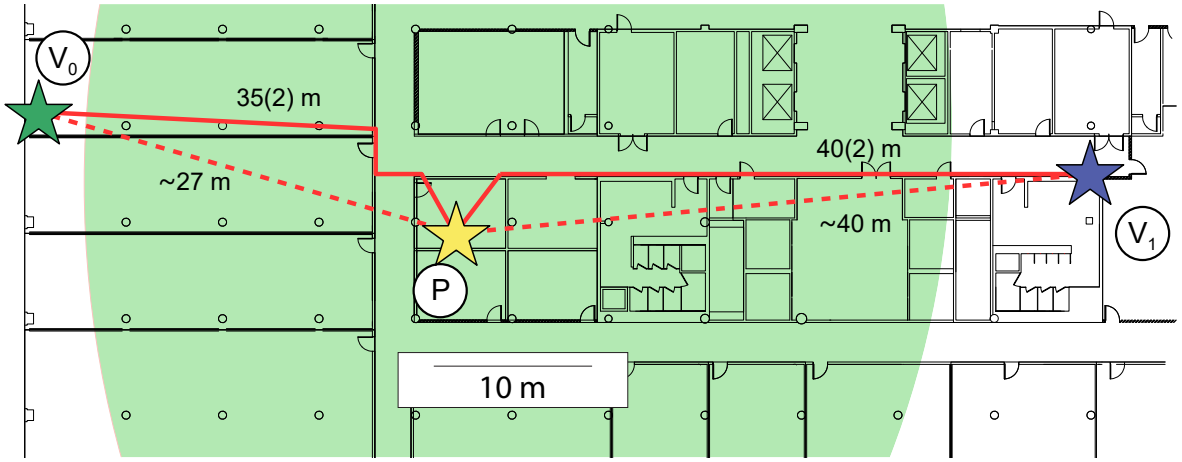


FIG. 3: **Positional uncertainty diagram.** The area in which the prover could be located based on the roundtrip time of the QPV signals is shaded in green and overlaid over a diagram of our experiment, including the real locations of both verifiers and of the prover, the cable paths and the building's floorplan.

date for positional verification at the metropolitan scale.

Our protocol occupies a distinct position within the current QPV experimental landscape. Prior demonstrations have each addressed only a subset of the main deployability challenges, namely security, channel loss tolerance at metropolitan scales, or hardware accessibility [3, 4, 20]. Device-independent approaches [3] offer the strongest security guarantees with minimal assumptions but have low loss tolerance, fundamentally limiting their reach over metropolitan distances. The implementation by Ref. [4] achieves practical simplicity but the underlying protocol [6] does not provide improved loss tolerance with increased number of measurement bases at practical 0.27% QBER with current security analysis (see Supplementary Fig. 12). Combining it with the loss-tolerance scheme proposed in Ref. [5] introduces the use of a Bell state measurement and entanglement source that may not have sufficiently good performance for security when commercial devices are used, and would require additional modifications due to the possibility of post-selection on multi-photon events at arbitrary channel loss. A detailed discussion of the challenges is presented in Supplementary Section VIII A. Relying on hollow-core fiber remains expensive and sparsely deployed relative to standard telecom infrastructure. The single-photon SWAP-based demonstration [20] provides valuable proof-of-concept results but lacks provable security against entangled adversaries.

LT-QPV addresses all these simultaneously by decoupling channel-loss tolerance from measurement complexity through a causal argument rather than a hardware workaround. It provides channel-loss-independent security, with the prover-verifier separation limited by prover-side loss, including quantum memory storage loss, in practical settings, while not being prohibitively challenging to implement with commercial hardware. We note however that scaling to larger separations may still introduce other practical considerations such as higher polarization drift and longer storage times (discussed later) that may translate to additional noise, lower rates and prover-side loss, and whose impact depends on the choice of implementation. The trade-off accepted in this work is that security is proved under QROM and with a computational assumption.

Since QPV cannot be information-theoretically secure [1, 2], some assumption on the adversary is necessary. Prior work assumes bounded shared entanglement [3, 6, 16], while we work in the QROM [19], a standard model in cryptography that allows the adversary polynomial entanglement. As for any QROM proof, instantiating f with a concrete hash function is heuristic (see Supplementary Remark IV.2). The computational assumption on the adversary only has to hold during the short QPV protocol run and do not face the same "harvest-now-decrypt-later" issues that are present in secure key exchange. The QROM is well-precedented in classical [28, 29] and quantum cryptography [19, 21, 30], including in the security proofs of the NIST post-quantum standards. Instantiating the random oracle with a concrete hash function is, however, a heuristic step whose effect cannot be quantified within the QROM. We discuss this in Supplementary Remark IV.2. We also note that classical position verification is insecure even with computational assumptions [1], so our QPV demonstration still presents a genuine advantage over classical schemes. As such, we believe that this is a reasonable tradeoff and assumption to make, but a careful choice of the instantiation

(e.g. SHA3) of the hash function with sufficiently large input size is required for the QROM guarantee to be a meaningful heuristic for the deployed protocol. This suggests that the barriers to QPV deployment at metropolitan distances are not fundamental and that our protocol design choices address the limitations that have constrained prior demonstrations.

A comparison of our protocol and its demonstration with prior QPV implementations is shown in Fig. 4, where the maximum distances are asymptotic limits: they are the separations at which the prover efficiency η reaches the threshold η_{th} as $N \to \infty$, so the required number of valid rounds, and hence the certification time, diverges as the separation approaches them. Kavuri et al.'s implementation [3] is secure above 2/3 end-to-end efficiency and Fan Yuan et al.'s implementation [4] is secure above 50% efficiency for the link between the quantum verifier and the prover in the asymptotic regime with zero QBER. In this setting, their implementation is able to scale to a maximum of 6.0 km and 11.3 km respectively. Our LT-QPV protocol is secure above 16% efficiency for the prover's delay line and measurement station in the asymptotic regime at our current QBER. We compare the performance of our LT-QPV protocol for several configurations: a) system as-is, b) swapping NIR and telecom fibers, c) adding Ultra-Low Loss (ULL) fibers and matching the initial end-to-end efficiency of 81% as Kavuri et al., and d) increasing the source heralding efficiency (HE) from 43% $\to$ 70% (commercially achievable), and adding future low-loss Hollow-Core Fibers (HCF), see Fig. 4. These results indicate that using commercially-available hardware ULL fiber, our LT-QPV protocol can scale to over 100 km, well within the range of metropolitan scale quantum networks.

While LT-QPV addresses many of the outstanding challenges of QPV protocols, it still faces limitations and practical requirements. A key protocol-level requirement is the necessity for the prover to store one qubit of an entangled pair (subsystem Q, see Fig. 5**b**) until the classical challenges arrive and the measurement basis is determined. This storage time is constrained by the need for subsystem V to arrive at the quantum verifier before challenge y hypothetically would, with contributions from: (1) the latency of transmitting y from V_1^C to the prover, $\Delta t_{\text{cl}} = d_{V_1^C P}\left(\frac{1}{v_{\text{cl}}} - \frac{1}{c}\right)$, and (2) the latency for transmitting V from the prover to V_0^Q, $\Delta t_V = d_{V_0^Q P}\left(\frac{1}{v_V} - \frac{1}{c}\right)$, where d_{AB} represents the distances between A and B (see Supplementary Section III B 1 for details). In favorable settings where both the classical communication and the quantum link operate close to c (e.g., free-space or hollow-core-fiber segments), the required storage time can be made arbitrarily small without the need for a quantum memory. By contrast, in a practical setting where quantum transmission is performed over standard optical fiber with $2/3 \cdot c$ transmission speed, the storage time scales linearly with distance. In this regime, depending on the choice of quantum memory, the required storage time couples prover efficiency to the prover–verifier separation. Full loss tolerance, in the sense of arbitrary separation, is therefore retained only when classical and quantum communication travel at the speed of light. Nevertheless, even without long-lived, error-corrected quantum memories, passive optical delay (fiber spools or delay lines), as used in our experiment, or a commercially-available free-space photonic memory [31] can provide sufficient storage for LT-QPV to retain better distance scaling than [4]. For instance, using the same standard fiber in the delay loop with the same attenuation as the quantum channel can allow the loss in the fiber loop to be only 1/3 of the fiber loss in the quantum channel (see Supplementary Section III B 1 for an example), a constant-factor reduction instead of full channel-loss tolerance.

Our current demonstration has two further implementation-specific limitations that we expect can be addressed through hardware improvements achievable with existing or near-term technology. The first is the short length of the challenge signals (4 bits). For such short challenges, the ε_{ROM} term is not meaningfully bounded. The demonstration is therefore secure against i.i.d. adversaries with no early knowledge of the measurement basis, meaning adversaries whose strategy depends on only α, which is learned at the claimed position at time t_P (see Supplementary Remark IV.2). It does not establish security against general query-bounded QPT adversaries or general attacks. The choice of a small 4-bit challenge is due to the short distance of our demonstration, in which the additional latency required to compute f for longer challenges would introduce a timing uncertainty that is too large for our setup. At the metropolitan-scale separations the protocol is designed for, the correspondingly larger timing budget accommodates an extension to a 128- or 256-bit challenge and use of a cryptographic hash function such as SHA3 [24], narrowing the gap with the ideal random oracle, at the cost of additional positional uncertainty and storage time from the hash computation.

The second limitation is that the implementation is only secure against i.i.d. attacks but vulnerable to general ones. This is partly due to the slow switching speed of the verifier's liquid crystal retarders (LCRs), which leads to multiple consecutive valid rounds sharing the same verifier

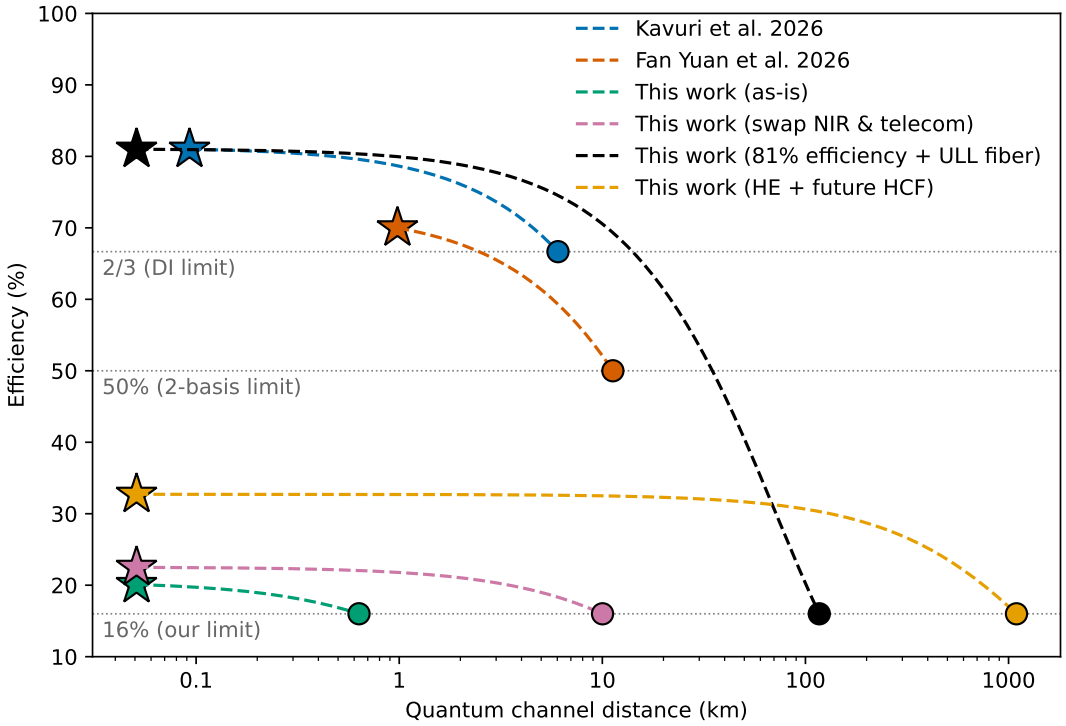


FIG. 4: **Scaling performance of our protocol.** Prior QPV work is secure until the efficiency falls below 2/3 for the Device Independent asymptotic limit (Kavuri et al.), or 50% for the 2-basis limit (Fan Yuan et al.). Our LT-QPV scaling performance is shown for four configurations: a) system as-is, b) swapping Near-Infrared (NIR) and Telecom fibers, c) adding Ultra-Low Loss (ULL) fibers and matching the initial end-to-end efficiency of 81% as the prior work (Kavuri et al.), and d) increasing the source heralding efficiency (HE) from 43% → 70%, and adding future low-loss Hollow-Core Fibers (HCF). Stars denote initial operating point, while end points denote scaling limit.

measurement basis that an adversary may exploit (more details in Supplementary Section V D). Replacing the LCRs with commercial Pockels cells would provide the fast per-round basis switching required for security against general attacks. Even with such fast switching, security against general attacks imposes substantially stronger finite-size requirements. With our current performance, a large number of valid rounds $N \approx 5\times10^8$ (roughly a month of net data collection) would be needed to be secure against general attacks (see Supplementary Section V C for details). We expect that a tighter security analysis against general attacks, which we leave as an open problem, could reduce these requirements, and that performance improvements could further reduce both the finite-size requirements and the time to accumulate the necessary rounds. A separate improvement that can be made is to tighten ε_{sou} to provide a stronger cryptographic guarantee by having a longer net collection time. Selecting $\varepsilon_{\text{sou}} = 2^{-64}$ would require $N = 1.5\times10^6$ valid rounds and a net collection time of 130min while selecting $\varepsilon_{\text{sou}} = 10^{-6}$ would require $N = 5.5\times10^5$ valid rounds and a net collection time of 48min against i.i.d. adversaries, and assuming $\varepsilon_{ROM} = 0$. A smaller overall ε_{sou} and thus ε_{ROM} also requires a longer challenge n. Addressing both limitations, extending the challenge length and replacing the liquid crystals with fast Pockels cells, represents a clear and technically feasible path toward a QPV demonstration that is fully secure against general QPT adversaries.

Besides hardware improvements to address query size and security level, further safeguards are required to address possible side-channel attacks on the measurement device, which LT-QPV assumes to be trusted. This assumption is central since the loss tolerance property relies on basis-independent detection probability for the post-selection on detection rounds. Depending on the implementation of the measurement devices, there are known side-channel attacks on quantum measurement devices [32–34], such as detector blinding [35, 36] and Trojan-horse attacks [37, 38], and various countermeasures have been proposed, such as introducing variable attenuation and photocurrent monitoring [39, 40], random detector efficiency [41], or careful quantification of leakages [42]. In our implementation, the verifier-side transmission is consistent across all 16 bases

(see Supplementary Section VII A). We leave a complete implementation of LT-QPV with suitable protection against side-channel attacks for future work.

LT-QPV is a protocol intended for deployed networks, thus fast operation is an important performance metric limited by the number of required rounds and the hardware repetition rate. The prover efficiency currently limits the number of valid rounds for position verification. The warm-rubidium entanglement source used in our demonstration provides a native heralding efficiency of $\sim 43\%$, which translates into a prover efficiency of $\eta \approx 20\%$ due to losses in the measurement apparatus. The most direct route to improved performance is to swap the NIR and Telecom arms, which improves the end-to-end system efficiency from 20.1% to 22.5%, and reduces the prover's fiber loss from 4 dB/km to 0.35 dB/km. In order to realize swapping NIR and Telecom arms, the prover (verifier) measurement stations would need to update the anti-reflection coating from 795 nm to 1324 nm (1324 nm to 795 nm). This shifts the operating point to higher transmission at comparable QBER, reducing the number of valid rounds required (see Fig. 2).

A further improvement in source heralding efficiency of 70%, which is commercially achievable, can further improve the prover-side efficiency to $> 56\%$, requiring $N < 2500$ rounds against i.i.d. adversaries and $N < 5 \times 10^4$ against general attacks. Further improvement of the prover-side efficiency of LT-QPV to match the end-to-end efficiency of Ref. [3] (81%) reduces the requirement to $N < 5000$ against general attacks. Higher repetition rates are achievable by increasing the switching rate of the prover's Pockels cells. In principle, rates up to 100 MHz are possible, although 1-10 MHz is likely more realistic, giving a 5 to 50 times boost in rate. Switching the verifier's LCR to Pockels cells also allows removing the need for sifting, providing another 16 times boost in rate. With these reasonable updates, a certification time $\lesssim 1$ s is achievable against general attacks.

With a credible path to sub-second certification times, we now present a conceptual design for deploying LT-QPV in metropolitan-area networks. In the most pared-down version of our protocol, only one verifier requires quantum capabilities (a fiber-optic link, single-photon detectors, and photon polarization control). All other verifiers operate purely classically, exchanging challenges and receiving measurement outcomes via wireless or optical links. As illustrated in Fig. 5**a**, in a practical deployment a small number of quantum verifier nodes connected to the coverage area by standard telecom fiber could provide quantum measurements for a much larger number of provers within the network. Multiple classical verifier nodes, each consisting of a time tagger and a synchronized clock, are distributed across the metropolitan area at surveyed positions, providing the geometric diversity required for three-dimensional triangulation from the arrival times of the prover's classical responses. Multiple provers can operate within this shared infrastructure simultaneously, with each carrying an entanglement source and a measurement module. The quantum infrastructure thus reduces to a few nodes serving the entire coverage area. The deployment scales through the addition of inexpensive classical verifiers, components that are mature, commercially available, and already deployed at scale for applications such as 5G network synchronization and financial exchange co-location. For a target metropolitan network distance of 12 km (about half the length of Manhattan island), fiber loss on the quantum link affects only the certification time and not the security, requiring no quantum repeaters or entanglement distillation, provided the prover-side quantum memory required at this distance is supplied. This architecture inverts the usual assumption in quantum position verification that extending coverage requires proportionally scaling the quantum hardware, making city-wide deployment economically viable. A formal security analysis of LT-QPV beyond the one-dimensional (collinear) setting is required for a complete security treatment of such deployments, and we leave this for future work. Moving to a network setting breaks the ideal collinear configuration of QPV, shown in Fig. 5**b**, thereby increasing the necessary quantum storage time to $\Delta t_V \approx d_{V_0^Q P}(\frac{1}{v_V} - \frac{\cos\theta}{c})$ as a necessary condition for security, where θ is the angle the classical verifier makes with the line connecting the quantum verifier to the prover (see Fig. 5**c**). However, since the angle θ scales inversely with the number of classical verifiers k ($\theta \sim \pi/k$), the storage time can in principle be reduced to a level similar to that of the collinear case by a careful choice of verifiers' number and locations (more details in Supplementary Section III B 2).

The QPV protocol and deployment we propose suggests a concrete model for spacetime certification as a service. At the moment of signing a document, certifying a regulatory filing, or authenticating a high-value transaction, a client acting as the prover initiates the LT-QPV protocol: one photon from their entanglement source travels via fiber to a quantum verifier, while classical responses are timed against the surrounding classical verifiers to determine the prover's position. Upon successful verification, the verifiers jointly issue a digitally signed certificate attesting to the prover's position and the time of the event, a spacetime seal anchored to the laws of physics rather than to

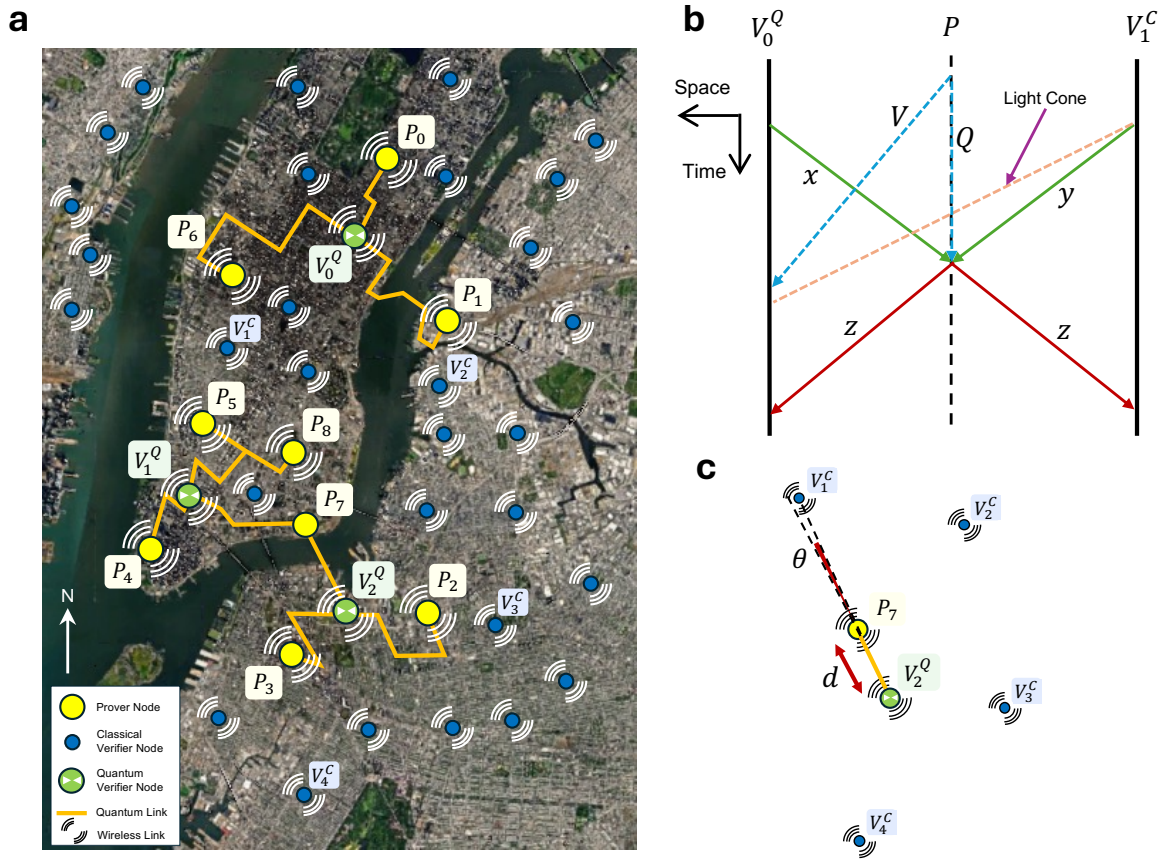


FIG. 5: **a. Conceptual design of LT-QPV deployment architecture on a metropolitan scale.** In a real-life realization of our LT-QPV protocol, multiple verifiers and prover nodes may be scattered around a metropolitan area, New York City as an example. A few quantum verifier nodes (green) with measurement devices will be connected via fibers (black links) to several prover nodes (yellow) each. Classical verifiers (blue) can be scattered around the city. All classical communications can take place wirelessly. **b. Quantum storage time estimation in collinear setting.** Quantum verifier V_0^Q and classical verifier V_1^C certifying the location X_P of a prover P. The timings have to be chosen such that challenge y arrives at V_0^Q after the quantum system V, i.e. the blue arrow must always be above the orange dotted line (future light cone of the event where V_1^C sends out challenge y). **c. Scaling of quantum storage time of the prover.** An example configuration of a prover, a quantum verifier, and a subset of classical verifiers (blue) to be used in the position verification protocol. The storage time $\Delta t_V + \Delta t_{\mathsf{cl}}$ depends on the distance d between the prover and the quantum verifier, as well as the minimum angle θ between the prover, the quantum verifier, and a classical verifier.

the honesty of the signee or to device integrity or self-reported metadata. This certificate can subsequently be verified by any relying party or can serve as the location attestation in TCC. Realizing a spacetime seal service will require systematic protocol design and engineering developments, but this work sketches a concrete path: improving prover efficiency and valid-round rate through higher end-to-end detection efficiency and faster switching; strengthening robustness beyond i.i.d. operating regimes through rapid, per-round basis selection; extending the challenge length to better approximate the random-oracle ideal; and validating kilometer-scale operation over deployed urban fiber with multiple classical verifiers for full three-dimensional triangulation. The LT-QPV architecture integrates naturally with emerging quantum networks in which entanglement is generated at network nodes and distributed for measurement, enabling LT-QPV to provide spacetime-seal certificates as one application running alongside other entanglement-enabled services, such as key distribution and distributed sensing, on the same infrastructure.

METHODS

Protocol Description

We provide an informal description of the LT-QPV protocol here, and the full protocol can be found in Supplementary Section III B. The protocol begins with repeating QPV rounds until there are N valid rounds:

1. **Quantum State Transfer**: The prover prepares a Bell state $|\Phi^+\rangle_{VQ}$. The prover sends quantum system V to V_0^Q and keeps quantum system Q.
2. **Verifier Message**: V_0^Q and V_1^C randomly selects and sends $x \in \{0,1\}^n$ and $y \in \{0,1\}^n$ respectively such that they both arrive at P at time t_P.
3. **Verifier Measurement**: V_0^Q computes basis $\alpha = f(x,y)$ and measures V in basis α with measurement outcome s (which can include double-clicks, $s = dc$). If no photon is detected or if quantum system V fails to arrive by t_V, the round is considered invalid.
4. **Prover Measurement**: After receiving x and y, the prover computes $\alpha = f(x,y)$ and measures Q in basis α, with measurement outcome z. If no photon is detected, the prover sets $z = \perp$. The prover sends z to both verifiers (z_0 to V_0^Q and z_1 to V_1^C).
5. **Timing Check**: The verifiers check if the responses arrive within a threshold t_{th} of the expected arrival time. If any check fails, the protocol aborts immediately.

Of the N valid rounds, let N_{det} be the number of rounds detected by the prover ($z \neq \perp$), N_{dc} be the number of double-click rounds ($s = dc$), N_{err} be the number of error rounds ($s \neq z$), and N_{mis} be the number of rounds with mismatched responses ($z_0 \neq z_1$). The verifiers conclude that the prover is at the claimed location if

1. Prover efficiency is above a certain threshold, $N_{\text{det}}/N \geq \eta_{\mathsf{th}}$
2. Effective QBER is below a certain threshold, $(N_{\text{dc}} + N_{\text{err}})/N_{\text{det}} \leq e_{\mathsf{th}}$
3. Probability of mismatched responses is below a threshold, $N_{\text{mis}}/N \leq p_{\mathsf{mis,th}}$

Completeness

Recall that the completeness error ε_{com} is the probability that an honest prover fails the LT-QPV verification. Consider an honest prover at location X_P and verifiers with imperfect devices that results in transmission η, QBER of e, and double-click probability p_{dc}. Since classical communication is almost error-free, we assume that an honest prover can always provide matching responses and respect the timing constraints. The protocol proceeds in an i.i.d. manner, allowing us to use tight concentration bounds [43] to bound the probability of failing the checks. More formally,

Theorem 1. *Consider an honest implementation with single-round transmission η, QBER e, double-click probability p_{dc}, and mismatch probability p_{mis}. LT-QPV is ε_{com}-complete with completeness error*

$$\begin{aligned}\varepsilon_{\text{com}} =& \Phi\left(-\sqrt{2NH\left(\eta_{\mathsf{th}} + \frac{1}{N}, \eta\right)}\right) \\ &+ 1 - \Phi\left(\sqrt{2N\eta_{\mathsf{th}} H\left(e_{\mathsf{th}} - \frac{1}{N\eta_{\mathsf{th}}}, e'\right)}\right) \\ &+ 1 - \Phi\left(\sqrt{2NH\left(p_{\mathsf{mis,th}} - \frac{1}{N}, p_{\mathsf{mis}}\right)}\right),\end{aligned}$$

where $e' = p_{dc} + (1 - p_{dc})e$, $H(x,p) = x\ln(x/p) + (1-x)\ln[(1-x)/(1-p)]$ is the Kullback-Leibler divergence for a binary distribution, $\Phi(x)$ is the cumulative distribution function of a standard normal distribution, η_{th}, e_{th} and $p_{\mathsf{mis,th}}$ are the threshold values for transmission, QBER, and mismatch probability and are selected such that $\eta_{\mathsf{th}} \leq \eta - \frac{1}{N}$, $e_{\mathsf{th}} \geq e' + \frac{1}{N\eta_{\mathsf{th}}}$ and $p_{\mathsf{mis,th}} \geq p_{\mathsf{mis}} + \frac{1}{N}$.

Proof Sketch. The probability of failing any check is upper bounded by the sum of probability that each check failed. Since the honest party operates in an i.i.d manner, we bound the probability of each check failing using tight concentration bound from Ref. [43]. □

Soundness

Recall that soundness is the probability that an adversary without a presence at the claimed location passes the LT-QPV verification. We prove that the LT-QPV protocol achieves ε_{sou}-soundness under the QROM against both a general QPT adversary and a QPT adversary restricted to i.i.d. attacks. We state the result for i.i.d. attacks below,

Theorem 2. *LT-QPV is ε_{sou}-sound against i.i.d. query-bounded adversaries in the quantum random oracle model, i.e.*

$$\max_{\mathcal{S} \in \mathcal{A}_{QPT,iid}, \mathcal{M}_{\text{prac}}} \Pr[\textit{checks pass}] \leq \varepsilon_{\text{sou}},$$

where the maximum is taken over adversary strategies $\mathcal{S}$ that are in the set of QPT and i.i.d. strategies $\mathcal{A}_{QPT,iid}$,

$$\begin{aligned}\varepsilon_{\text{sou}} =& \varepsilon_{ROM} + \\ &\max\left\{1-\Phi\left(\sqrt{2NH\left(\eta_{\text{th}}-\frac{1}{N},\eta_{\text{b}}\right)}\right),\right. \\ &\Phi\left(-\sqrt{2NH\left(p_{\text{mis,th}}+\frac{1}{N},p_{\text{mis,b}}\right)}\right), \\ &\left.\Phi\left(-\sqrt{2NH\left(e_{\text{th}}+\frac{1}{N},e_{SDP}\right)}\right)\right\}\end{aligned}$$

for any choice of parameters $\eta_{\text{b}} \leq \eta_{\text{th}} - \frac{1}{N}$ and $p_{\text{mis,b}} \geq p_{\text{mis,th}} + \frac{1}{N}$, and where $e_{SDP}(\eta_{\text{b}}, p_{\text{mis,b}})$ is the solution to the SDP in Equation (IV.19)*, with the added condition that $e_{SDP} \geq e_{\text{th}} + \frac{1}{N\eta_{\text{th}}}$.*

The proof of soundness is split into five distinct steps, with the first three steps simplifying the analysis and the final two steps proving directly that the adversary cannot pass the checks.

- **STEP 1:** Apply the universal squashing model [25] to reduce to a scenario where the first verifier's measurement device only accepts single-qubit inputs.
- **STEP 2:** Invoke the QROM and computational assumption to ensure that basis information is only revealed at (t_P, X_P) and to rule out attacks that exploit the structure of function f.
- **STEP 3:** Demonstrate that the soundness is independent of channel loss, allowing the no-detection rounds at V_1 to be safely discarded.
- **STEP 4:** Derive a relationship between the single-round expected QBER, probability of mismatch of responses and transmission for any adversary strategy.
- **STEP 5:** Using statistical methods such as concentration bounds, demonstrate that given the relationship between the expectation values, no adversary can pass the checks except with low probability.

The detailed proof is provided in Supplementary Section IV C.

The security proof extends to general QPT adversaries by the same argument, with two key modifications: (i) the effective QBER check is replaced by $N_{\text{dc}} + N_{\text{err}} \leq N\tilde{e}_{\text{th}}$, and (ii) statistical analysis in Step 5 is carried out using conditional expectation values instead of unconditional ones. The soundness against general adversaries is presented in Supplementary Theorem V.2, and the detailed proof is provided in Supplementary Section V B.

Numerical Analysis

To evaluate the parameter regime where QPV is secure, we numerically simulate the minimum performance that an honest prover has to achieve for a given transmission η. The results are shown in Fig. 2, with security parameters $\varepsilon_{com} = 10^{-2}$ and $\varepsilon_{sou} = 10^{-2}$ for various number of rounds. The completeness budget ε_{com} is distributed with $0.1\varepsilon_{com}$ attributed to the statistical fluctuations of each of η and p_{mis} and $0.8\varepsilon_{com}$ attributed to the statistical fluctuations of QBER (terms of the completeness in Theorem 1). The simulation is carried out by solving the semidefinite program (SDP) in Supplementary Equation (IV.19), where we use ncpol2sdpa [44] and PICOS [45] interface with QICS [46] solver.

Experimental Setup

An overview of our experimental setup is presented in Fig. 1**a**. The setup consists of two trusted verifier nodes and one untrusted prover node connected by a quantum and a classical layer.

The core of the quantum layer is constituted by a warm rubidium entanglement source [27] placed at the prover's location. The source provides entangled photon pairs at 795 nm (near infrared, or NIR) and 1324 nm (telecom) in the $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$ Bell state. The specific requirement of our QPV protocol to maximise the NIR heralding efficiency led us to modify the source with respect to previous work. Enriched ^{85}Rb is used as the medium for the four-wave mixing, and the pumping is enacted by lasers at 780 nm and 1367 nm. The source is operated such that, at the origin, it outputs about 4.2 million NIR photons/s, 5.3 million telecom photons/s, and 2.1 million coincidences/s leading to a 43% heralding efficiency (defined as the rate of coincidences divided by the rate of telecom photons). The effective signal-idler cross-correlation for the coincidence window we use in the experiment is $g_{si} \approx 190$, leading to a minimum achievable QBER of $\text{QBER}_{\text{min}} \approx 0.52\,\%$.

After their generation, the photons from the entanglement source are coupled into optical fibers. The NIR photon is brought via a 42 m delay line to its measurement station comprised of two Pockels cells, a half-wave plate (HWP), a quarter-wave plate (QWP), and a polarizing beam splitter (PBS). The Pockels cells and wave plates are used to set the measurement in one of the 16 bases

used in our protocol. After the PBS, the photons are coupled into optical fibers and routed to superconducting nanowires single photon detectors (SNSPDs).

The telecom photon serves as an agreement by the prover to perform a QPV round and is transmitted from the prover to verifier 0, where it leads to a second measurement station where two liquid crystal retarders (LCRs) at 45° to each other are used to set arbitrary measurement bases and a PBS and another set of SNSPDs are used for projective measurements at the verifier's location.

The classical layer is coordinated by three FPGAs connected by high-speed copper-shielded coaxial air-core plenum cables that can transmit signals at $0.88 \cdot c$ [47], where c is the speed of light. Verifiers V_0 and V_1 transmit classical messages x and y consisting of 4-bit binary numbers that are chosen uniformly at random from $\{0,1\}^4$ to the prover, respectively. The verifiers coordinate the transmission of x, y such that they arrive simultaneously at the prover's claimed location. Upon receiving classical values of x, y the prover selects the measurement basis from a random lookup table with 16 possible measurement bases, and sends the appropriate control signals to fire the Pockels cells. After passing through the Pockels cells and measurement optics, the photon is detected by SNSPDs. The classical measurement result is relayed back to each verifier using high-speed air-core cables. All the signals necessary for the security determination (x and y values, measurement results, synchronization clocks) are logged onto two time taggers at the verifiers. Any rounds with mismatched prover and verifier measurement bases are discarded.

Our data collection system currently takes approximately 22.7 s to collect 5 s of data. This overhead arises from two sources: first, a conservative 15 s settling period allotted for the LCR voltages to stabilize prior to QBER measurement, and second, the remainder from the data transfer method. Neither represents a fundamental limitation. In practice, the LCRs settle within approximately 1 s, and the transfer overhead can be eliminated by utilizing the network features of the Swabian time tagger, such that 5 s of data would require only 6 s in total.

Central to the positional determination of QPV are the operational delays at the prover. Measurement delays including receiving and processing the x and y values, processing latencies in determining the requested measurement basis, firing the Pockels cells, and detecting the projected single photon result, all increase the uncertainty radius around each verifier (specific details are provided in the Supplementary Information). Instead of predicting the sum of these effects, the verifiers have the ability to set the region of interest (ROI) where to accept photon measurements to optimize experimental parameters, namely positional uncertainties and QBER. This allows us to select photons that reach the Pockels cells right after the measurement basis is settled, minimizing delays. To determine the ROI, we perform the measurement shown in Fig. 6, measuring the QBER with varying ROI start time after the prover is ready to receive commands (earlier start times lead to improved positional uncertainties, but at the expense of higher QBER).

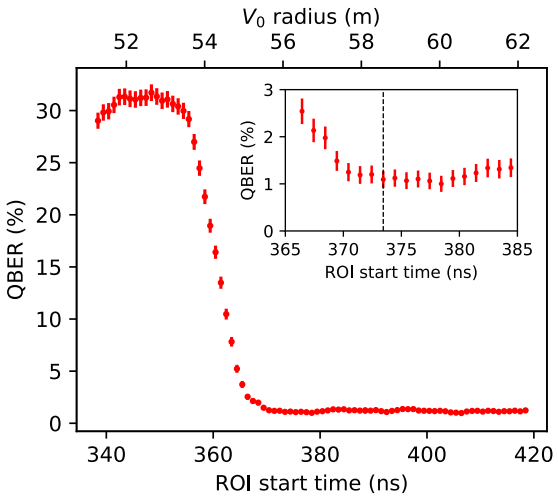


FIG. 6: ROI start time tuning accounts for the delays in the prover's quantum measurement. Specifically, we place the ROI start time (the dashed vertical line in the inset plot) immediately after the Pockels cell has finished settling, which corresponds to low QBER, and reasonably low positional uncertainty. Moving the ROI start time earlier could achieve improved positional uncertainty, but at the expense of higher QBER.

Photon Losses

The quantum signals experience various losses before being measured and converted into electrical signals logged into the time taggers. The NIR losses directly affect the level of security of the protocol. In our setup, the telecom losses only affect the time it takes to certify the positional verification. The cumulative efficiency of the NIR and telecom channels respectively were measured to be 46(5) % and 41(5) %. A full breakdown is provided in the Supplementary information.

[1] Chandran, N., Goyal, V., Moriarty, R. & Ostrovsky, R. Position based cryptography. In Annual International Cryptology Conference, 391–407 (Springer, 2009).

[2] Buhrman, H. et al. Position-based quantum cryptography: Impossibility and constructions. SIAM J. Comput. **43**, 150–178 (2014).

[3] Kavuri, G. A. et al. Quantum position verification with remote untrusted devices. Nature (2026). URL https://doi.org/10.1038/s41586-026-11247-3.

[4] Fan-Yuan, G.-J. et al. Relativistic position verification with coherent states. Nature Physics 1–6 (2026).

[5] Allerstorfer, R. et al. Making existing quantum position verification protocols secure against arbitrary transmission loss. Phys. Rev. Lett. **135**, 260801 (2025).

[6] Escolà-Farràs, L. m. c. & Speelman, F. Single-qubit loss-tolerant quantum position verification protocol secure against entangled attackers. Phys. Rev. Lett. **131**, 140802 (2023).

[7] European Parliament & Council of the European Union. Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation) (text with eea relevance). Official Journal of the European Union, L 119 (2016).

[8] European Parliament and the Council of the European Union. Directive 2014/65/EU on markets in financial instruments (MiFID II). Directive 2014/65/EU (2014).

[9] European Commission. Commission Delegated Regulation (EU) 2017/574 supplementing Directive 2014/65/EU with regard to regulatory technical standards on the level of accuracy of business clocks (RTS 25). Delegated Regulation (EU) 2017/574 (2017).

[10] European Parliament and the Council of the European Union. Regulation (EU) No 600/2014 on markets in financial instruments (MiFIR). Regulation (EU) No 600/2014 (2014).

[11] U.S. Department of State. International Traffic in Arms Regulations (ITAR), 22 C.F.R. Parts 120–130. Code of Federal Regulations.

[12] U.S. Department of Health and Human Services. HIPAA Administrative Simplification Regulations, 45 C.F.R. Parts 160 and 164. Code of Federal Regulations.

[13] Krishnan, R., Smith, N., Lopez, D. & Arfaoui, G. Trusted computing future: Emerging use cases and solutions. Tech. Rep., Trusted Computing Group (2015). URL https://trustedcomputinggroup.org/resource/trusted-computing-future-emerging-use-cases-and-solutions-whitepaper/.

[14] Kon, W. Y., Primaatmaja, I. W., Chakraborty, K. & Lim, C. Quantum secure key exchange with position-based credentials (2025). arXiv: 2506.03549.

[15] Beigi, S. & König, R. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. New J. Phys. **13**, 093036 (2011).

[16] Bluhm, A., Christandl, M. & Speelman, F. A single-qubit position verification protocol that is secure against multi-qubit attacks. Nat. Phys. **18**, 623–626 (2022).

[17] Llorenç Escolà-Farràs & Speelman, F. Quantum position verification in one shot: parallel repetition of the f-bb84 and f-routing protocols (2025). arXiv: 2503.09544.

[18] Asadi, V., Cleve, R., Culf, E. & May, A. Linear gate bounds against natural functions for position-verification. Quantum **9**, 1604 (2025).

[19] Unruh, D. Quantum position verification in the random oracle model. In Garay, J. A. & Gennaro, R. (eds.) Advances in Cryptology – CRYPTO 2014, 1–18 (Springer Berlin Heidelberg, Berlin, Heidelberg, 2014).

[20] Kanneworff, K. et al. Towards experimental demonstration of quantum position verification using single photons. Quantum Science and Technology **10**, 045004 (2025).

[21] Boneh, D. et al. Random oracles in a quantum world. In Lee, D. H. & Wang, X. (eds.) Advances in Cryptology – ASIACRYPT 2011, 41–69 (Springer Berlin Heidelberg, Berlin, Heidelberg, 2011).

[22] Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. Rev. Mod. Phys. **74**, 145–195 (2002).

[23] Scarani, V. et al. The security of practical quantum key distribution (2009). arXiv: 0802.4155.

[24] National Institute of Standards and Technology. Sha-3 standard: Permutation-based hash and extendable-output functions. Tech. Rep. FIPS PUB 202, U.S. Department of Commerce (2015).

[25] Fung, C.-H. F., Chau, H. F. & Lo, H.-K. Universal squash model for optical communications using linear optics and threshold detectors. Phys. Rev. A **84**, 020303 (2011).

[26] Tomamichel, M., Fehr, S., Kaniewski, J. & Wehner, S. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. New Journal of Physics **15**, 103002 (2013).

[27] Craddock, A. N. et al. High-rate subgigahertz-linewidth bichromatic entanglement source for quantum networking. Physical Review Applied **21**, 034012 (2024).

[28] Fiat, A. & Shamir, A. How to prove yourself: Practical solutions to identification and signature problems. In Odlyzko, A. M. (ed.) Advances in Cryptology — CRYPTO' 86, 186–194 (Springer Berlin Heidelberg, Berlin, Heidelberg, 1987).

[29] Bellare, M. & Rogaway, P. The exact security of digital signatures: How to sign with rsa and rabin. In Maurer, U. (ed.) Advances in Cryptology — EUROCRYPT '96, vol. 1070 of Lecture Notes in Computer Science, 399–416 (Springer, Berlin, Heidelberg, 1996).

[30] Chiesa, A., Raghuraman, S., Spooner, N. & Spooner, M. Succinct arguments in the quantum random oracle model. In Malkin, T. (ed.) Advances in Cryptology — CRYPTO 2021, vol.

12827 of Lecture Notes in Computer Science, 1–30 (Springer, 2021).

[31] Arnold, N. T., Lualdi, C. P., Goggin, M. E. & Kwiat, P. G. All-optical quantum memory. In Quantum Computing, Communication, and Simulation IV, vol. 12911, 387–391 (SPIE, 2024).

[32] Jain, N. et al. Attacks on practical quantum key distribution systems (and how to prevent them). Contemporary Physics **57**, 366–387 (2016).

[33] Xu, F., Ma, X., Zhang, Q., Lo, H.-K. & Pan, J.-W. Secure quantum key distribution with realistic devices. Rev. Mod. Phys. **92**, 025002 (2020).

[34] Marquardt, C. et al. Implementation attacks against qkd systems. Tech. Rep. 575, Federal Office for Information Security, Germany (BSI) (2023). URL https://www.bsi.bund.de/EN/Service-Navi/Publikationen/Studien/QKD-Systems/Implementation_Attacks_QKD_Systems_node.html.

[35] Makarov, V. Controlling passively quenched single photon detectors by bright light. New Journal of Physics **11**, 065003 (2009).

[36] Lydersen, L. et al. Hacking commercial quantum cryptography systems by tailored bright illumination. Nature Photonics **4**, 686–689 (2010).

[37] Vakhitov, A., Makarov, V. & Hjelme, D. Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography. Journal of Modern Optics **48**, 2023–2038 (2001).

[38] Gisin, N., Fasel, S., Kraus, B., Zbinden, H. & Ribordy, G. Trojan-horse attacks on quantum-key-distribution systems. Physical Review A **73**, 022320 (2006).

[39] Yuan, Z. L., Dynes, J. F. & Shields, A. J. Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography. Applied Physics Letters **98**, 231104 (2011).

[40] Koehler-Sidki, A. et al. Best-practice criteria for practical security of self-differencing avalanche photodiode detectors in quantum key distribution. Phys. Rev. Appl. **9**, 044027 (2018).

[41] Lim, C. C. W., Walenta, N., Legré, M., Gisin, N. & Zbinden, H. Random variation of detector efficiency: A countermeasure against detector blinding attacks for quantum key distribution. IEEE Journal of Selected Topics in Quantum Electronics **21**, 192–196 (2015).

[42] Pinheiro, P. V. P. et al. Eavesdropping and countermeasures for backflash side channel in quantum cryptography. Opt. Express **26**, 21020–21032 (2018).

[43] Zubkov, A. M. & Serov, A. A. A complete proof of universal inequalities for the distribution function of the binomial law. Theory of Probability & Its Applications **57**, 539–544 (2013).

[44] Peter, W. Algorithm 950: Ncpol2sdpa—sparse semidefinite programming relaxations for polynomial optimization problems of noncommuting variables. ACM T. Math. Software **41**, 21 (2015).

[45] Sagnol, G. & Stahlberg, M. PICOS: A Python interface to conic optimization solvers. Journal of Open Source Software **7**, 3915 (2022).

[46] He, K., Saunderson, J. & Fawzi, H. QICS: Quantum information conic solver (2024). arXiv: 2410.17803.

[47] Gamma Electronics. Rigid aluminum-shielded coaxial air-core plenum cable (model: Pln-al-50r). Datasheet Version 1.6 (2025). URL https://gammaelectronics.net/collections/plenum-cable/products/aluminum-shielded-coaxial-air-core-plenum-cable-500-ft-spool. Document date: 2/25/25.

ACKNOWLEDGMENTS

Special thanks to Giuseppe Di Cera (JPMorganChase) for detailed insights and discussions on quantum position verification and quantum networking technologies, notably their potential commercial applications. We thank Brett Sanford (JPMorganChase) for administrative support for this project. We thank Marco Pistoia for assisting with the internal patent filing approval process for patent IDF-2024-0733 during his tenure at JPMorganChase. C.L. and I.W.P. contributed to this work during their tenure at JPMorganChase. Additionally, a major thank you to Noel Goddard of Qunnect, without whom this collaboration would not have been possible.

COMPETING INTERESTS

W.Y.K., I.W.P., C.L., and K.C. are co-inventors on a patent application related to this work (U.S. Patent US-12675596-B2 “Systems and methods for source-independent quantum position verification”). A.C., T.S., J.S., O.A. are co-inventors on a patent application related to this work (U.S. Patent Application 63/782,777 “Low-Latency Wireless Communication”).

DISCLAIMER

This paper was prepared for informational purposes with contributions from the Global Technology Applied Research center of JPMorgan Chase & Co. This paper is not a product of the Research Department of JPMorgan Chase & Co. or its affiliates. Neither JPMorgan Chase & Co. nor any of its affiliates makes any explicit or implied representation or warranty and none of them accept any liability in connection with this paper, including, without limitation, with respect to the completeness, accuracy, or reliability of the information contained herein and the potential legal, compliance, tax, or accounting effects thereof. This document is not intended as investment research or investment advice, or as a recommendation, offer, or solicitation for the purchase or sale of any security, financial instrument, financial product or

service, or to be used in any way for evaluating the merits of participating in any transaction.

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- JPMCQunnectDemoSupp.pdf