Supplementary Materials for "Loss-Tolerant Quantum Position Verification for Metropolitan Area Networks"

CONTENTS

I. Notation 2

II. Preliminaries 2
A. Quantum Random Oracle Model 2

III. Loss-Tolerant QPV 3
A. Protocol Assumptions 3
B. Protocol Description 3
1. Choice of Timing Parameters 4
2. Timing Parameters in Networks 6

IV. Security of LT-QPV 8
A. Security Definition 8
B. Completeness 9
C. Soundness 10
1. Universal Squashing 10
2. Random Oracle Model 12
3. Channel Loss Independence 14
4. Single-Round Analysis 15
5. Finite-Size Analysis 16
D. Numerical Simulation 18
E. Calibration Rounds 19

V. LT-QPV Secure against General Attacks 19
A. Completeness 19
B. Soundness 20
1. Single-Round Analysis 21
2. Finite-Size Analysis 22
C. Numerical Simulation 23
D. Reuse of Verifier Basis 23

VI. Adversary with Imperfect Devices 24

VII. Experiment 24
A. Quantum layer details 24
B. Quantum Measurement Basis 25
C. Low-Latency Communications System 26
D. Time Synchronization 27
E. Positional Uncertainty 28
F. Look-up Table 30

VIII. Protocol Comparison 30
A. Comparison with QPV_m^{η} protocol with commitment at metropolitan distances 30
B. Comparison with other implementations 32
C. Scaling Performance with System Upgrades 32
D. Quantum-Advantage Ratios: Construction and Calculation 33

References 36

I. NOTATION

We list our notation in Table I. Note that $N_{\max}$ and N are fixed parameters decided before the protocol begins, whereas $N_{\text{det}}, N_{\text{dc}}, N_{\text{err}}, N_{\text{mis}}$ are values observed during the protocol.

$V_0 = V_0^Q, V_1 = V_1^C$	Left (quantum) and right (classical) verifiers
P	Prover
X_0, X_1	The position of V_0, V_1
X_P	Prover's claimed location
x, y	Left and right classical challenges
t_x	Time that classical challenge x is transmitted from V_0
t_y	Time that classical challenge y is transmitted from V_1
α	Basis choice
s	Measurement outcome of V_0
$\left\|\psi_0^\alpha\right\rangle, \left\|\psi_1^\alpha\right\rangle$	Measurement basis for basis choice α and outcome $s = 0, 1$
z	Prover's response
z_0	Prover's response to V_0
z_1	Prover's response to V_1
t_{z_0}	Time that prover's response is received by V_0
t_{z_1}	Time that prover's response is received by V_1
Δ_X^0, Δ_X^1	Positional uncertainty (left and right)
Q	Prover's quantum register
V	V_0's quantum register
t_V	Time of V arriving at V_0
t_P	Time of x, y arriving simultaneously at X_P
$f : \{0,1\}^n \times \{0,1\}^n \to [m]$	Function that computes the measurement basis (Note $[m] = \{0, \cdots, m-1\}$)
η	Prover efficiency
p_{mis}	Mismatch probability
e	QBER
t_{th}	Amount of delay tolerated on time of arrival of z_0
η_{th}	Prover efficiency threshold
e_{th}	QBER threshold conditioned on detection by P (error in N_{det} detection rounds)
$p_{\mathsf{mis,th}}$	Mismatch probability threshold
$N_{\max}$	Maximum number of rounds
N	Target number of valid rounds (rounds with detection by V_0, including double-clicks)
N_{det}	Number of rounds with detection by V_0 and P
N_{dc}	Number of rounds with double-click detection by V_0
N_{err}	Number of rounds with single detection by V_0 with incorrect prover answer ($s \neq z_0$)
N_{mis}	Number of rounds with mismatched responses ($z_0 \neq z_1$).
n	Security parameter
m	Number of measurement bases
d_{AB}	Distance between two parties A and B
c	Speed of light in vacuum
v_{cl} ($\beta_{\mathsf{cl}} = v_{\mathsf{cl}}/c$)	Speed of light in classical communication channel
$\tilde{e}_{\mathsf{th}}$	Amount of error tolerated in all N rounds (unconditioned error)
$\mathcal{S}$	Adversary strategy
$\mathcal{A}_a$	Set of adversary strategies, with restrictions labeled by a

TABLE I: List of notations used. Subscript i denotes the value of a variable during the i-th round with successful detection by V_0 (e.g. x_i), while superscript j denotes the j-th overall round regardless of successful detection (e.g. x^j).

II. PRELIMINARIES

A. Quantum Random Oracle Model

The Quantum Random Oracle Model [1] is an idealized cryptographic security model, in which a function f is assumed to have no white-box leakage of information. In other words, f is indistinguishable from a truly random

function, and the contents of f are only accessible via black-box queries, given by the unitary $U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$. A *query-bounded* algorithm can invoke U_f at most a polynomial number of times in the input length $|x|$. If U_f is queried with quantum state ρ, then the *query weight* on input x is given by $\mathrm{Tr}\left((\langle x| \otimes I_{\mathcal{Y}})\, \rho\, (|x\rangle \otimes I_{\mathcal{Y}})\right)$, where $I_{\mathcal{Y}}$ is the identity operator on the auxiliary register.

We recall the following results from the literature:

Lemma II.1 (Query Extraction from a Random Oracle [2]). *Let $\mathcal{A}$ be an oracle algorithm which makes at most T oracle queries to a function $f : \{0,1\}^m \to \{0,1\}^n$. Define $|\phi_i\rangle$ as the global state after $\mathcal{A}$ makes i queries, and $W_y(|\phi_i\rangle)$ as the sum of squared amplitudes in $|\phi_i\rangle$ of terms in which $\mathcal{A}$ queries f on input y. Let $\epsilon > 0$ and let $F \subseteq \{0,1,\ldots,T-1\} \times \{0,1\}^m$ be a set of time-input pairs such that $\sum_{(i,y)\in F} W_y(|\phi_i\rangle) \leq \epsilon^2/T$.*

For $i \in \{0,1,\ldots,T-1\}$, let f'_i be an oracle obtained by reprogramming f on inputs in $\{y \in \{0,1\}^m : (i,y) \in F\}$ to arbitrary outputs. Let $|\phi'_T\rangle$ be the global state after $\mathcal{A}$ is run with oracle f'_i on the i-th query (instead of f). Then, $\mathsf{TD}\left(|\phi_T\rangle, |\phi'_T\rangle\right) \leq \epsilon/2$.

Lemma II.2 (Simulation of a Random Oracle [3]). *A random oracle $f : \mathcal{X} \to \mathcal{Y}$ is perfectly indistinguishable from a $2q$-wise independent hash function $f' : \mathcal{X} \to \mathcal{Y}$ against a quantum algorithm $\mathcal{A}$ which makes at most q queries.*

III. LOSS-TOLERANT QPV

A. Protocol Assumptions

The goal of QPV is for two verifiers V_0 and V_1, located at X_0 and X_1, to certify the location of a prover P claiming to be at X_P. The verifiers are assumed to have:

- **Secure Communication:** The verifiers share a secure classical communication channel.
- **Measurement Device:** V_0 possesses a trusted measurement device, which can be modeled by Fig. 3(a). The measurement device is assumed to have no side-channels through which the adversary could learn the measurement basis (e.g. via Trojan horse attack) or control the device externally (e.g. via blinding attack). The device is also assumed to have basis-independent and balanced detector loss, and no dark counts.

Only verifier V_0 needs to perform quantum operations, while V_1 is fully classical.

We make the following assumptions regarding the honest prover:

- **Position:** The honest prover's claimed location X_P lies on the line segment connecting the two verifiers.
- **Communication:** The honest prover P has a classical communication link to both verifiers V_0 and V_1 and a quantum channel to verifier V_0.
- **Quantum Source**: The honest prover P has access to a quantum source to generate entangled states such as the Bell state.

We note that while we assume basis-independent and balanced detector loss and no dark counts for simplicity, these can in general be accounted for by artificially balancing the detector loss and by modifications in the security analysis respectively. An imbalance on the verifier device can generally be compensated by artificially introducing loss in the SNSPD arm where there is a higher transmission (changing click to no click in the data with some probability) or for specific basis where there is a higher transmission. To account for the dark count rate, they can be incorporated into the security analysis either by (1) modeling the detector POVMs with the same measurement basis, but with an additional map from no click outcome to click outcome for the detector with probability p_d or (2) upper bounding the number of dark count events and treating them in the most favorable manner (detected, no error, no mismatch).

B. Protocol Description

Before the LT-QPV protocol begins, the verifiers and prover agree on some public parameters. These include the security parameter n and the number of rounds N. The number of bases m and the bases $\{|\psi_0^\alpha\rangle, |\psi_1^\alpha\rangle\}_{\alpha\in[1,m]}$ can be chosen based on the loss in the prover's device, since increasing m improves the loss tolerance of the scheme to prover-side loss. Ideally, the bases should be chosen to be uniformly spread on the Bloch sphere to minimize any overlap between basis states of different bases. They also share a hash function f to compute the basis choice from the

Protocol 1: Loss-Tolerant QPV

Goal. Verifiers V_0 and V_1 (V_0 located at X_0 and V_1 located at X_1) certify that the prover P is at position $X_P \in (X_0, X_1)$.
Public Parameters. Security parameter n. Number of bases m. Target number of valid rounds N. Maximum number of rounds $N_{\max}$. Hash function $f : \{0,1\}^n \times \{0,1\}^n \to [m]$. Effective QBER threshold e_{th}. Time threshold t_{th}. Prover efficiency threshold η_{th}. Mismatch threshold $p_{\mathsf{mis,th}}$.

1. Set $i = 1$ (current valid round) and $j = 1$ (current round). Repeat until N valid rounds are completed or total round limit is reached, i.e. repeat while $i \leq N$ and $j \leq N_{\max}$:

   (a) **Verifier Description**

   i. **Setup**: V_0 randomly selects $x \in \{0,1\}^n$ and $y \in \{0,1\}^n$ and sends y to V_1 using a secure channel. The verifiers communicate with the prover to agree on a time t_V when the quantum system V is expected to arrive at V_0. The verifiers also communicate and agree on a time t_P for x and y signals to arrive at X_P.

   ii. **Verifier Message**: V_0 and V_1 send x and y respectively at $t_P - d_{V_0P}/v_{\mathsf{cl}}$ and $t_P - d_{V_1P}/v_{\mathsf{cl}}$ such that they both arrive at P at time t_P.

   iii. **Verifier Quantum Measurement**: V_0 computes basis $\alpha = f(x, y)$ and measures the received quantum system V in basis α. V_0 records measurement outcome s. If a double-click is detected, the verifier sets $s = dc$. If no photon is detected or if quantum system V fails to arrive by t_V, V_0 sets $s = \perp$.

   (b) **Prover Description**

   i. **Quantum State Transfer**: The prover prepares a Bell state $\left|\Phi^+\right\rangle_{VQ}$. The prover sends quantum system V to the verifier and keeps quantum system Q in a quantum memory.

   ii. **Prover Quantum Measurement**: After receiving x and y, the prover computes $\alpha = f(x, y)$ and measures quantum system Q in the computed basis, and obtains outcome $z \in \{0, 1, \perp\}$, where $z = \perp$ corresponds to the case of no detector click. If a double-click is detected, the prover assigns $z \in \{0, 1\}$ randomly. The prover sends the measurement outcome z to both verifiers at time t_P.

   (c) **Detection Check**: After receiving outcome $z_{0,i}$ at V_0 and $z_{1,i}$ at V_1, if $s = \perp$ (i.e. no detection at verifier), the round is discarded and the round restarts from (a), incrementing $j = j + 1$. If $s \neq \perp$, the verifiers record the round information $(x_i, y_i, z_{0,i}, z_{1,i}, s_i) = (x, y, z_0, z_1, s)$ and proceed to the final step.

   (d) **Timing Check**: V_0 and V_1 record the arrival time of the respective responses z_0 and z_1 as t_{z_0} and t_{z_1}. The verifiers check if the timings are valid, (1) $t_{z_0} - t_P \leq d_{V_0P}/v_{\mathsf{cl}} + t_{\mathsf{th}}$, (2) $t_{z_1} - t_P \leq d_{V_1P}/v_{\mathsf{cl}} + t_{\mathsf{th}}$ for some threshold t_{th}. If any check fails, the protocol aborts immediately. The verifiers also note that a successful detection round has been recorded by incrementing $i = i + 1, j = j + 1$.

2. **Parameter Estimation**: If $i < N$, abort the protocol. The verifiers record the number of detected rounds N_{det} where $z_{0,i} \neq \perp$, the number of double-click rounds N_{dc} where $z_{0,i} \neq \perp$ and $s_i = dc$, the number of error rounds N_{err} where $z_{0,i} \neq \perp$ and $z_{0,i} \neq s_i$, and the number of rounds with mismatched responses N_{mis} where $z_{0,i} \neq z_{1,i}$. The verifiers check if (1) the prover efficiency is above a certain threshold, $N_{\mathrm{det}} \geq N\eta_{\mathsf{th}}$, (2) the effective QBER is below a certain threshold, $N_{\mathrm{dc}} + N_{\mathrm{err}} \leq N_{\mathrm{det}} e_{\mathsf{th}}$, and (3) the rate of mismatched responses is below a threshold, $N_{\mathrm{mis}} \leq N p_{\mathsf{mis,th}}$. If all checks pass, the verifiers conclude that the prover is in the $(X_P \pm \Delta_X)$-region. Otherwise, the protocol aborts.

challenges x and y, which is assumed to have no white-box leakage of information, i.e. the structure of the function should not reveal any information beyond its input-output relation.

The verifiers also decide on suitable threshold values to meet the performance and security requirements of the protocol. The LT-QPV protocol is described in Protocol 1 below.

1. *Choice of Timing Parameters*

There are two key timing parameters to be selected. The first is t_P, the time at which the challenges x and y are expected to arrive at X_P. The second is t_V, the time at which quantum system V is expected to arrive at V_0. The choices of timing parameters t_P and t_V directly impact the storage time of quantum system Q and the region around X_P where we can certify the location of the prover. When the classical or quantum communication between the prover and verifiers are not at the speed of light in vacuum, the required storage times and verification regime increase.

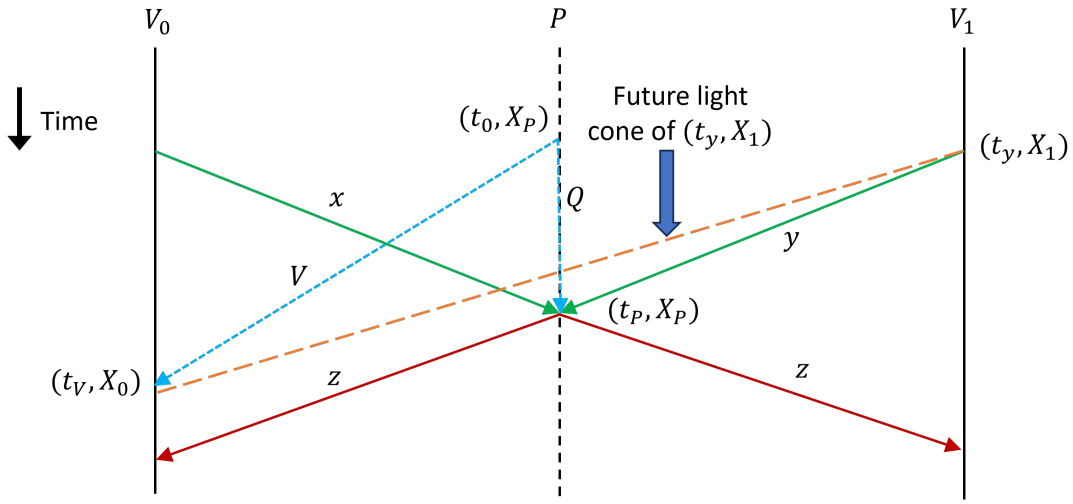


FIG. 1: Communication process between provers and verifiers in the LT-QPV protocol. Verifiers V_0 and V_1 are located at X_0 and X_1, and prover P is located at X_P. t_0 is the time quantum systems VQ is generated, t_y is the time challenge y is sent, t_V is the expected time of arrival of quantum system V and t_P is the expected time of arrival of challenges x and y at X_P. The timings have to be chosen such that y (and in turn the basis α) cannot influence the quantum system V, i.e. at V_0, the blue arrow must always be above the orange dotted line (future light cone of the event where V_1 sends out challenge y).

For a classical communication speed of $v_{\mathsf{cl}} = \beta_{\mathsf{cl}} c$, verifiers V_0 and V_1 send challenges x and y at times $t_x = t_P - \frac{d_{V_0 P}}{c\beta_{\mathsf{cl}}}$ and $t_y = t_P - \frac{d_{V_1 P}}{c\beta_{\mathsf{cl}}}$ respectively. Importantly, the timings need to be chosen such that the spacetime coordinate (t_y, X_1) and (t_V, X_0) are spacelike separated to prevent the basis information α from influencing the preparation of quantum system V since $\alpha = f(x, y)$ requires knowledge of y. This is illustrated in Fig. 1, where the future light cone of (t_y, X_1) does not contain (t_V, X_0). In practice, this means that the storage time of quantum system Q scales linearly with the amount of delay in the communication of system V and challenges x and y relative to the speed of light. More precisely, if the joint quantum system VQ is generated at time t_0 and V travels at speed $\beta_V c$, then the storage time needs to satisfy $t_P - t_0 > \frac{d_{V_0 P}}{c}\left(\frac{1}{\beta_V} - 1\right) + \frac{d_{V_1 P}}{c}\left(\frac{1}{\beta_{\mathsf{cl}}} - 1\right)$. Therefore, for high-speed classical communication and free-space or hollow-core fiber quantum communication ($\beta_{\mathsf{cl}}, \beta_V \approx 1$), the storage time can be arbitrarily small. For quantum communication over standard optical fiber ($\beta_{\mathsf{cl}} \approx 1, \beta_V \approx 2/3$), the storage time scales linearly with distance as $\frac{d_{V_0 P}}{2c}$. The impact of storage time on the prover-side loss depends on the choice of quantum storage medium. Consider a quantum storage with η_i internal storage loss (loss at zero delay) and a delay-dependent loss $\eta(\tau) = 10^{-L\tau}$, where L is the decay rate. The overall prover side loss would thus be $\eta = \eta_i \eta(\tau) \eta'$, where η' is the transmission of the remaining components of the prover-side device excluding the quantum storage. If the quantum storage is implemented using a delay loop with standard optical fiber ($L = 0.2c/10^4$), a loop of distance $\frac{1}{3} d_{V_0 P}$ is required. This allows us to extend the distance between the prover and verifier V_0 by a factor of 3 compared to having the entanglement source at the verifier, providing a constant-factor extension instead of full channel-loss tolerance.

To distinguish channel-loss tolerance from the usual notion of independence from the prover–verifier separation, we define a protocol to be *channel-loss tolerant* if its security is independent of the loss on the quantum channel to the verifier. We call a protocol *fully* channel-loss tolerant if its security is also independent of the prover–verifier separation. As such, LT-QPV is channel-loss tolerant, and it is fully channel-loss tolerant only when classical and quantum signals both travel at the speed of light ($t_P - t_0$ independent on $d_{V_i P}$).

In the ideal scenario where messages are sent at the speed of light and the prover's response to the challenges is instantaneous, the responses are expected to arrive at time $t_{z_0} = t_P + d_{z_0 P}/c$ and $t_{z_1} = t_P + d_{z_1 P}/c$, and we set $t_{\mathsf{th}} = 0$. This allows the verifiers to certify the location of the prover to be at X_P exactly. However, in practice, the classical communication occurs at a lower speed $\beta_{\mathsf{cl}} < 1$ and the honest prover requires some processing time, which is used to set t_{th}. This extends the time between when the messages are sent, t_x and t_y, and the time the messages arrive, t_{z_0} and t_{z_1}. The time extension can be mapped to positional uncertainty via four inequalities: the prover must be able to receive a signal from V_b and respond to $V_{b'}$ in time for $b, b' \in \{0, 1\}$. Because Protocol 1 imposes symmetric timing constraints on both verifiers, it is enough to consider the case $b = b'$, which restricts the location X of the

prover to the intersection of the following two circles:

$$d_{V_0X} \leq \frac{d_{V_0P}}{\beta_{\mathsf{cl}}} + \frac{ct_{\mathsf{th}}}{2}, \quad d_{V_1X} \leq \frac{d_{V_1P}}{\beta_{\mathsf{cl}}} + \frac{ct_{\mathsf{th}}}{2}.$$

The inequalities obtained by the two cases when $b \neq b'$ are redundant due to symmetry. Note that in the general case, they will impose additional constraints as elliptical regions, as discussed in [4].

Consequently, in the case of one dimension (i.e. V_0, P, V_1 are on a line), any party within the region between $X_P - \Delta_X^0$ and $X_P + \Delta_X^1$ can theoretically pass the QPV with fast enough processing time and the ability to receive the challenges at the speed of light, where $\Delta_X^0 = d_{V_1P}\left(\frac{1}{\beta_{\mathsf{cl}}} - 1\right) + \frac{ct_{\mathsf{th}}}{2}$ and $\Delta_X^1 = d_{V_0P}\left(\frac{1}{\beta_{\mathsf{cl}}} - 1\right) + \frac{ct_{\mathsf{th}}}{2}$. As such, the verifiers can only certify that the prover is located within this region, which we term $(X_P \pm \Delta_X)$-region.

2. *Timing Parameters in Networks*

In a real metropolitan setting with classical and quantum networks, the prover and the verifiers are better modeled in two dimensions. In general, when the prover does not lie on a line connecting two verifiers, at least three verifiers will be needed and the measurement basis will need to be split into three messages instead of two.

While we do not formally discuss the security analysis in two dimensions, we discuss how the timing parameters may be set to satisfy the spacelike separation requirement (see Fig. 1) as a necessary condition for security as well as its effect on the positional uncertainty region.

We consider a set of k classical verifiers $V_1, V_2, \ldots, V_k$ and a separate quantum verifier V^Q. We will argue below that the quantum storage time scales linearly with the distance d_{V^QP} between the quantum verifier and the prover. Accordingly, it is generally wise to pick a configuration such that the quantum verifier is as close as possible to the prover. For instance, one may simply pick the nearest quantum verifier node to be used in a protocol with a given prover location X_P.

As before, the quantum state needs to arrive at V^Q at time t_V, and the classical signals $x_1, x_2, \ldots x_k$ are scheduled to arrive at the honest prover's location X_P at time t_P. Suppose the adversary has a party at each verifier's location. For security to hold, the quantum state sent to V^Q cannot depend on all the classical signals, which yields the condition:

$$t_V < \max_{i\in[k]} t_P - \frac{d_{V_iP}}{\beta_{\mathsf{cl}}c} + \frac{d_{V_iV^Q}}{c}.$$

This translates to a lower bound on storage time of P as before. Let t_0 be the time P starts sending the quantum state, then we have

$$t_P - t_0 = (t_P - t_V) + (t_V - t_0) > \min_{i\in[k]} \left(\frac{d_{V_iP}}{\beta_{\mathsf{cl}}c} - \frac{d_{V_iV^Q}}{c}\right) + \frac{d_{V^QP}}{\beta_V c}. \tag{III.1}$$

To see the scaling of the storage time in Eqn. (III.1), suppose the optimal vertex V_i makes an angle θ_i with the line connecting V^Q and P, hence we have

$$\begin{aligned} t_P - t_0 &\approx \frac{d_{V_iP}}{\beta_{\mathsf{cl}}c} - \frac{\sqrt{d_{V_iP}^2 + 2d_{V_iP}d_{V^QP}\cos(\theta_i) + d_{V^QP}^2}}{c} + \frac{d_{V^QP}}{\beta_V c} \\ &\approx \frac{d_{V_iP}}{c}\left(\frac{1}{\beta_{\mathsf{cl}}} - 1\right) + \frac{d_{V^QP}}{c}\left(\frac{1}{\beta_V} - \cos(\theta_i)\right) \end{aligned} \tag{III.2}$$

up to an $O(d_{V^QP}^2/d_{V_iP}c)$ term which is small when[1] $d_{V^QP} \ll d_{V_iP}$. Note that as the angle θ_i tends to 0 this converges to the expression for the one dimensional case. Eqn. (III.2) favors classical verifiers that are closer to P, and those that make smaller angles with the line V^QP.

We depict a possible metropolitan network configuration in Fig. 2. In this configuration, quantum verifier nodes are spread across the area covering possible locations X_P, whereas the classical verifiers are positioned in a way that enables picking k classical verifiers that form a convex polygon containing P and V^Q in the interior. In the $\beta_{\mathsf{cl}} \approx 1$ approximation, the first term in Eqn. (III.2) vanishes and the storage time scales linearly with d_{V^QP}, which

[1] When this is not the case, we have $d_{V_iP} = O(d_{V^QP})$ and the storage time scales linearly with d_{V^QP} as desired.

is proportional to $1/\sqrt{N_Q}$ in a quantum network with N_Q quantum nodes over a fixed metropolitan area, assuming the quantum nodes are placed roughly equidistantly.

There are two scenarios that realize the $\beta_{\text{cl}} \approx 1$ approximation. The first is when classical communication is performed close to the speed of light, e.g. radio or free-space communication. Another way the approximation is valid is by assuming the adversary is limited to the same classical communication constraints as the honest parties in the network. Since β_{cl} is the ratio between honest and malicious communication speeds, effectively this means $\beta_{\text{cl}} \approx 1$. One can imagine an adversary tapping into the classical fiber-optic cables and controlling the transmission over the network, rather than using its own separate communication channel, which may induce overhead and make the attack less effective. The optimal V_i for the storage time will be chosen by the minimal angle θ_i, which depends on the configuration. The angle only affects the constant factor since $1/\beta_V - \cos(\theta_i) \in [1/\beta_V - 1, 1/\beta_V + 1]$. In a random configuration with the constraints above, the angle will satisfy $\theta_i \sim \pi/k$.

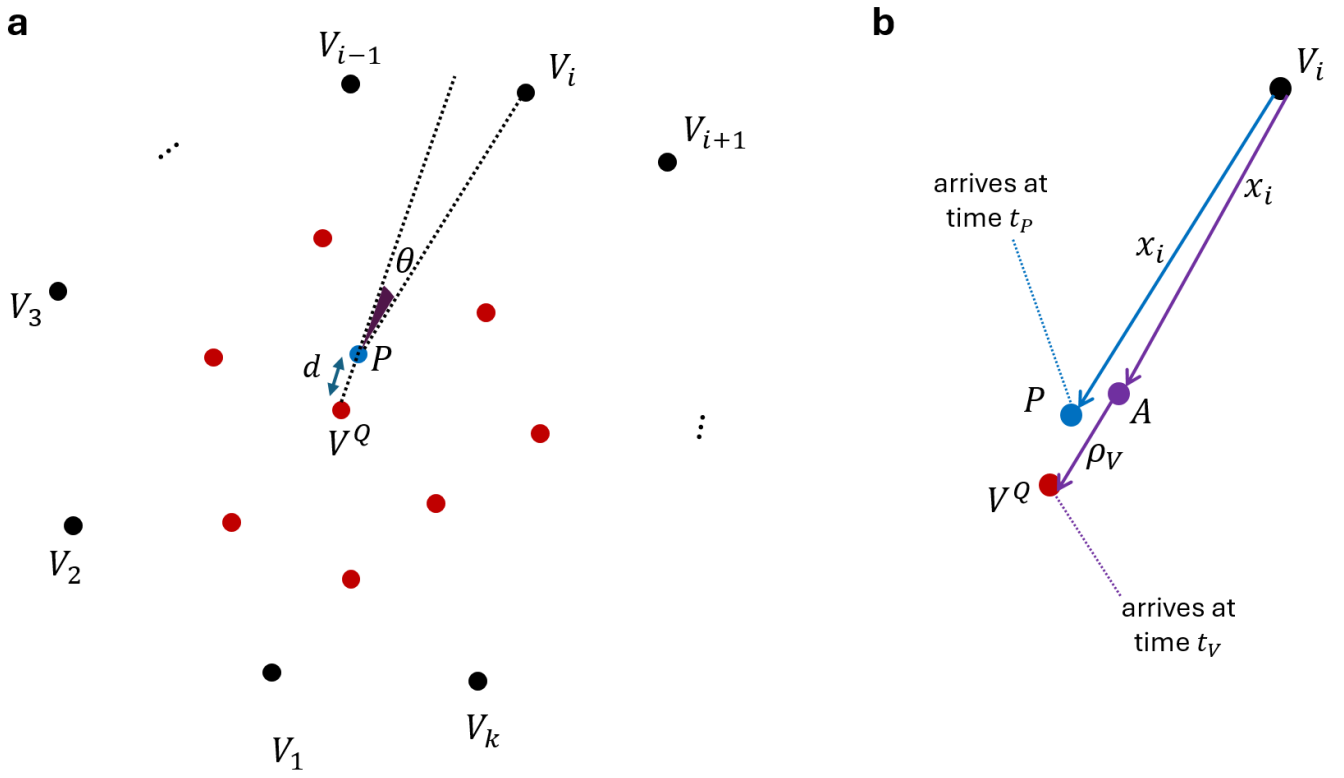


FIG. 2: **Depiction of two-dimensional QPV network. a** The red nodes represent quantum verifiers, and the black nodes represent classical verifiers. The prover P is represented by the blue node. To verify the position of P, the nearest quantum verifier V^Q at distance d is chosen for the protocol. k classical verifiers are used such that they form a k-gon containing P and V^Q. A particular classical verifier V_i makes the minimal angle θ_i with the line connecting V^Q and P. Thanks to the signal sent by V_i the quantum storage time of P scales linearly with d, hence proportional to $1/\sqrt{N_Q}$, where N_Q is the number of quantum verifiers placed in a fixed region. For an average position of P, the optimal angle satisfies $\theta_i \approx \pi/k$. Using more classical verifiers (i.e. a larger value of k) decreases the angle θ and reduces the storage time by a constant factor. **b** Visualization of the timing constraint induced by V_i. A malicious prover A (purple node) must receive classical signal x_i from V_i and send a quantum state ρ_V to V^Q before time t_V, whereas x_i must arrive at P at time t_P.

As for the positional uncertainty region, it is given by the intersection of circles $d_{V_0 X} \leq \frac{d_{V_i P}}{\beta_{\text{cl}}} + \frac{t_{\text{th}}}{2}$ for $i \in [k]$ as in the one dimensional case. The region always contains this intersection, and is equal to it when the time thresholds are symmetrical at each verifier as in Protocol 1.

IV. SECURITY OF LT-QPV

A. Security Definition

Having established the protocol, we now analyze its security. The goal of LT-QPV is to certify the location of an honest prover, and we consider two separate aspects to define security. Firstly, we expect that any honest prover should pass the checks – a secure QPV that fails to certify any honest prover would be of no practical use. This security condition is termed completeness, for which we can define a completeness error ε_{com} as the probability that an honest prover fails the checks in QPV. In general, we expect that any implementation should respect the timing constraints, and we focus on the parameter checks.

Definition IV.1. *Consider an honest prover P at location X_P. Protocol 1 is ε_{com}-complete if it fails the checks with probability at most ε_{com}, i.e.* $\Pr[\textit{checks fail}] \leq \varepsilon_{\text{com}}$.

Secondly, for an adversary not at the correct location, we expect that they should fail the QPV checks. Before defining this condition, let us consider how to model the adversary. Since the verifiers certify the location of the prover within the $(X_P \pm \Delta_X)$-region, the adversary can be considered to be any party (or parties) located outside the region. Without loss of generality, it is sufficient to consider an adversary consisting of two parties, which we term Alice and Bob, with Alice located between V_0 and $X_P - \Delta_X^0$, and Bob located between V_1 and $X_P + \Delta_X^1$. In general, the adversary has access to ideal quantum devices, including quantum computers and entangled states between them. We model such an adversary as holding state ρ_{E_0} at the start of the protocol, then for each round $j \geq 1$:

1. The adversary generates a shared state $\rho_{A^jB^j} = \mathcal{E}^j(\rho_{E^{j-1}})$ between Alice and Bob.

2. When Alice receives x^j and Bob receives y^j, they perform an operation on their component of the state respectively. At the same time, Alice also generates quantum system V^j to be sent to the verifier V_0. Alice and Bob can also split their quantum system into two components, with one component to be kept (labeled with K) and one component to be sent to the other party (labeled with S). The resulting state is $\rho_{V^jA^j_KA^j_SB^j_KB^j_S} = \mathcal{E}^{x^j}_{A^j\to V^jA^j_KA^j_S} \otimes \mathcal{E}^{y^j}_{B^j\to B^j_KB^j_S}[\rho_{A^jB^j}]$. A^j_S and B^j_S are sent to Bob and Alice respectively.

3. After time t^j_P, when Alice receives y^j and Bob receives x^j, Alice performs a measurement on her subsystems $A^j_KB^j_S$ with POVM $A^{x^j,y^j}_{z^j_0}$ while Bob performs a measurement on his subsystems $B^j_KA^j_S$ with POVM $B^{x^j,y^j}_{z^j_1}$. Alice and Bob send z^j_0 and z^j_1 to verifier V_0 and V_1 respectively. The verifier performs the measurement with projective operator $\Pi^{f(x^j,y^j)}_{s^j}$ on subsystem V^j. The resulting statistics are

$$\Pr\left[s^j, z^j_0, z^j_1\right] = \text{Tr}\left[(\Pi^{f(x^j,y^j)}_{s^j} \otimes A^{x^j,y^j}_{z^j_0} \otimes B^{x^j,y^j}_{z^j_1})\rho_{V^jA^j_KB^j_SA^j_SB^j_K}\right].$$

4. The information z^j_0, z^j_1, x^j and y^j, along with the post-measurement state of Alice and Bob form the new adversary state ρ_{E^j}. The information s^j, z^j_0, z^j_1, x^j and y^j are stored for parameter checks (according to protocol requirements).

We label each adversary strategy by the choice of quantum channels and measurement,

$$\mathcal{S} = \{\rho_{E_0}, \mathcal{E}^j, \{\mathcal{E}^{x^j}_{A^j}\}_{x^j}, \{\mathcal{E}^{y^j}_{B^j}\}_{y^j}, \{A^{x^j,y^j}_{z^j_0}\}_{x^j,y^j,z^j_0}, \{B^{x^j,y^j}_{z^j_1}\}_{x^j,y^j,z^j_1}\}.$$

It is known that QPV cannot be unconditionally secure [5, 6], so it is necessary to place additional assumptions on the adversary. Here, we assume that the classical and quantum resources of the adversary, i.e. memory, computational power, and entanglement, are upper-bounded by a polynomial in the security parameter n. We label this set of strategies $\mathcal{A}_{QPT}$. We also label the measurement device of the verifier as $\mathcal{M}_{\text{prac}} = \{\Pi^\alpha_s\}_{\alpha,s}$. We define the second security condition, soundness, with the associated soundness parameter ε_{sou}, as the maximum probability that an adversary passes the QPV checks.

Definition IV.2. *Protocol 1 is defined to be ε_{sou}-sound against a QPT adversary if for any QPT adversary strategy, the QPV checks pass with at most probability ε_{sou}, i.e.*

$$\max_{\mathcal{S}\in\mathcal{A}_{QPT},\mathcal{M}_{\text{prac}}} \Pr[\textit{checks pass}] \leq \varepsilon_{\text{sou}}. \tag{IV.1}$$

B. Completeness

The completeness is determined from an honest implementation (to be discussed in Sec. VII) of the QPV protocol. Recall from the main text

Theorem IV.1. *Consider an honest implementation with single-round prover efficiency η, QBER e, double-click probability p_{dc}, and mismatch probability p_{mis}. Protocol 1 is $\varepsilon_{\mathrm{com}}$-complete with completeness error*

$$\varepsilon_{\mathrm{com}} = \Phi\left(-\sqrt{2NH\left(\eta_{\mathsf{th}}+\frac{1}{N},\eta\right)}\right)+1-\Phi\left(\sqrt{2N\eta_{\mathsf{th}}H\left(e_{\mathsf{th}}-\frac{1}{N\eta_{\mathsf{th}}},e'\right)}\right)+1-\Phi\left(\sqrt{2NH\left(p_{\mathsf{mis,th}}-\frac{1}{N},p_{\mathsf{mis}}\right)}\right), \tag{IV.2}$$

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 prover efficiency, 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. Since the timing constraints are respected, the checks that can fail are the checks for prover efficiency, QBER, and mismatch.

$$\begin{aligned}\Pr[\textit{checks fail}] =& \Pr[\{N_{\mathrm{det}} < N\eta_{\mathsf{th}}\}\vee\{N_{\mathrm{err}}+N_{\mathrm{dc}} > N_{\mathrm{det}}e_{\mathsf{th}}\}\vee\{N_{\mathrm{mis}} > Np_{\mathsf{mis,th}}\}]\\ \leq& \Pr[N_{\mathrm{det}} < N\eta_{\mathsf{th}}]+\Pr[N_{\mathrm{mis}} > Np_{\mathsf{mis,th}}]+\Pr[N_{\mathrm{det}}\geq N\eta_{\mathsf{th}}, N_{\mathrm{err}}+N_{\mathrm{dc}} > N_{\mathrm{det}}e_{\mathsf{th}}],\end{aligned} \tag{IV.3}$$

where the second step uses the union bound and the property that $A\cup B = A\cup(A^c\cap B)$.

Using the tight concentration bound from Ref. [7], we bound the prover efficiency check failure probability by

$$\Pr[N_{\mathrm{det}} < N\eta_{\mathsf{th}}] = \Pr[N_{\mathrm{det}} \leq \lceil N\eta_{\mathsf{th}}\rceil - 1] \leq \Phi\left(-\sqrt{2NH\left(\frac{\lceil N\eta_{\mathsf{th}}\rceil}{N},\eta\right)}\right) \leq \Phi\left(-\sqrt{2NH\left(\eta_{\mathsf{th}}+\frac{1}{N},\eta\right)}\right), \tag{IV.4}$$

where we use the property that $\frac{\partial}{\partial x}\Phi(-\sqrt{2NH(x,p)}) \geq 0$ for $x < p$.

We apply the same concentration bound to the mismatch probability,

$$\begin{aligned}\Pr[N_{\mathrm{mis}} > Np_{\mathsf{mis,th}}] = 1-\Pr[N_{\mathrm{mis}} \leq \lfloor Np_{\mathsf{mis}}\rfloor] &\leq 1-\Phi\left(\sqrt{2NH\left(\frac{\lfloor Np_{\mathsf{mis,th}}\rfloor}{N},p_{\mathsf{mis}}\right)}\right)\\ &\leq 1-\Phi\left(\sqrt{2NH\left(p_{\mathsf{mis,th}}-\frac{1}{N},p_{\mathsf{mis}}\right)}\right),\end{aligned} \tag{IV.5}$$

where we use the property that $\frac{\partial}{\partial x}\Phi(\sqrt{2NH(x,p)}) \geq 0$ if $x \geq p$.

Using the same concentration bound, we similarly bound the error check failure probability,

$$\begin{aligned}&\Pr[N_{\mathrm{det}}\geq N\eta_{\mathsf{th}}, N_{\mathrm{err}}+N_{\mathrm{dc}} > N_{\mathrm{det}}e_{\mathsf{th}}]\\ =&\sum_{N_{\mathrm{det}}\geq N\eta_{\mathsf{th}}}\Pr[N_{\mathrm{det}}]\Pr[N_{\mathrm{err}}+N_{\mathrm{dc}} > N_{\mathrm{det}}e_{\mathsf{th}}|N_{\mathrm{det}}]\\ =&\sum_{N_{\mathrm{det}}\geq N\eta_{\mathsf{th}}}\Pr[N_{\mathrm{det}}](1-\Pr[N_{\mathrm{err}}+N_{\mathrm{dc}} \leq \lfloor N_{\mathrm{det}}e_{\mathsf{th}}\rfloor|N_{\mathrm{det}}])\\ \leq&\sum_{N_{\mathrm{det}}\geq N\eta_{\mathsf{th}}}\Pr[N_{\mathrm{det}}]\left[1-\Phi\left(\sqrt{2N_{\mathrm{det}}H\left(\frac{\lfloor N_{\mathrm{det}}e_{\mathsf{th}}\rfloor}{N_{\mathrm{det}}},e'\right)}\right)\right]\\ \leq&\sum_{N_{\mathrm{det}}\geq N\eta_{\mathsf{th}}}\Pr[N_{\mathrm{det}}]\left[1-\Phi\left(\sqrt{2N_{\mathrm{det}}H\left(e_{\mathsf{th}}-\frac{1}{N_{\mathrm{det}}},e'\right)}\right)\right]\\ \leq&1-\Phi\left(\sqrt{2N\eta_{th}H\left(e_{\mathsf{th}}-\frac{1}{N\eta_{\mathsf{th}}},e'\right)}\right),\end{aligned} \tag{IV.6}$$

where the fourth line applies the tight concentration bound [7]. The fifth line uses the property that $\frac{\partial}{\partial x}\Phi(\sqrt{2NH(x,e')}) \geq 0$ if $x \geq e'$. In the sixth line, we use the property that $\frac{\partial}{\partial N}\Phi(\sqrt{2NH(x-1/N,e')}) \geq 0$ when $x-\frac{1}{N} \geq e'$ and upper bound each term in the summation by the worst case term at $N_{\mathrm{det}} = N\eta_{\mathsf{th}}$. □

C. Soundness

For simplicity, we first prove the soundness of the protocol against a more restricted QPT adversary, which is only allowed to perform independent and identical (i.i.d.) attacks across all rounds. We label the set of strategies available for the adversary as $\mathcal{A}_{QPT,iid}$. We will further extend the proof to establish soundness against general QPT adversaries in Sec. V.

As discussed in the Methods section, the proof can be split into five steps, which are presented in the respective subsections below. The first step of universal squashing reduces the measurement device from the practical model to a lossless qubit measurement device, and restricts the adversary's strategy to one where quantum system V is prepared with no photons or with a single photon (single qubit). We label this set of adversary strategies $\mathcal{A}_q$, and the set of measurements $\mathcal{M}_{\mathrm{q}} = \{|\perp\rangle\langle\perp|, |\psi_0^\alpha\rangle\langle\psi_0^\alpha|, |\psi_1^\alpha\rangle\langle\psi_1^\alpha|\}_\alpha$, where $|\perp\rangle\langle\perp|$ detects the zero-photon event and $|\psi_0^\alpha\rangle$ and $|\psi_1^\alpha\rangle$ are the qubit basis states for measurement basis α. The second step reduces the set of QPT strategies to a set of restricted strategies $\mathcal{A}_{res}$ under the QROM. $\mathcal{A}_{res}$ describes a set of strategies where the adversary prepares a shared state, ρ_{VAB} and measures subsystems A and B independently to generate responses z_0 and z_1. The third step further restricts $\mathcal{A}_{res,q}$ to strategies where the adversary always prepares a single qubit in quantum system V, and we label this set of adversary strategies $\mathcal{A}_{res,nl}$. The fourth step relates single-round quantities of the restricted adversary, showing that at high prover efficiency and low mismatch, the QBER must be high. This relation is then used in the fifth step to prove the soundness against adversaries performing restricted strategies.

Recall from the main text that

Theorem IV.2. *Protocol 1 is $\varepsilon_{\mathrm{sou}}$-sound against i.i.d. query-bounded adversaries in the quantum random oracle model, i.e.*

$$\max_{\mathcal{S}\in\mathcal{A}_{QPT,iid},\mathcal{M}_{\mathrm{prac}}} \Pr[\mathit{checks\,pass}] \leq \varepsilon_{\mathrm{sou}}, \tag{IV.7}$$

where

$$\begin{aligned}\varepsilon_{\mathrm{sou}} = \varepsilon_{ROM} + \max\Bigg\{&1-\Phi\left(\sqrt{2NH\left(\eta_{\mathsf{th}}-\frac{1}{N},\eta_{\mathsf{b}}\right)}\right), \Phi\left(-\sqrt{2NH\left(p_{\mathsf{mis,th}}+\frac{1}{N},p_{\mathsf{mis,b}}\right)}\right),\\ &\Phi\left(-\sqrt{2NH\left(e_{\mathsf{th}}+\frac{1}{N},e_{SDP}\right)}\right)\Bigg\}\end{aligned} \tag{IV.8}$$

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

Proof. It is sufficient to prove that

$$\max_{\mathcal{S}\in\mathcal{A}_{res,iid,nl},\mathcal{M}_{\mathrm{q}}} \Pr[\mathit{checks\,pass}] \leq \varepsilon - \varepsilon_{ROM} \tag{IV.9}$$

since Thms. IV.3 to IV.5 guarantee the $\varepsilon_{\mathrm{sou}}$-soundness.

$$\begin{aligned}&\max_{\mathcal{S}\in\mathcal{A}_{res,iid,nl},\mathcal{M}_{\mathrm{q}}} \Pr[\mathit{checks\,pass}] \leq \varepsilon_{\mathrm{sou}} - \varepsilon_{ROM} \xRightarrow{\textit{Thm. IV.5}} \max_{\mathcal{S}\in\mathcal{A}_{res,iid,q},\mathcal{M}_{\mathrm{q}}} \Pr[\mathit{checks\,pass}] \leq \varepsilon_{\mathrm{sou}} - \varepsilon_{ROM}\\ &\xRightarrow{\textit{Thm. IV.4}} \max_{\mathcal{S}\in\mathcal{A}_{QPT,iid,q},\mathcal{M}_{\mathrm{q}}} \Pr[\mathit{checks\,pass}] \leq \varepsilon_{\mathrm{sou}} \xRightarrow{\textit{Thm. IV.3}} \max_{\mathcal{S}\in\mathcal{A}_{QPT,iid},\mathcal{M}_{\mathrm{prac}}} \Pr[\mathit{checks\,pass}] \leq \varepsilon_{\mathrm{sou}}.\end{aligned} \tag{IV.10}$$

Applying Thm. IV.7 completes the proof. □

We note that the added condition $e_{SDP} \geq e_{\mathsf{th}} + \frac{1}{N\eta_{\mathsf{th}}}$ can be checked when performing numerical analysis, and it is not violated in the regime of study.

1. Universal Squashing

The first reduction concerns the imperfection of the measurement device, which can cause a discrepancy between the ideal qubit measurement described by the protocol and the actual measurement device in the presence of multi-photon events. Multi-photon events are not unique to LT-QPV, and standard prepare-and-measure QPV protocols face similar issues where an imperfect source at the verifier may generate multiple photons. To account for this imperfection,

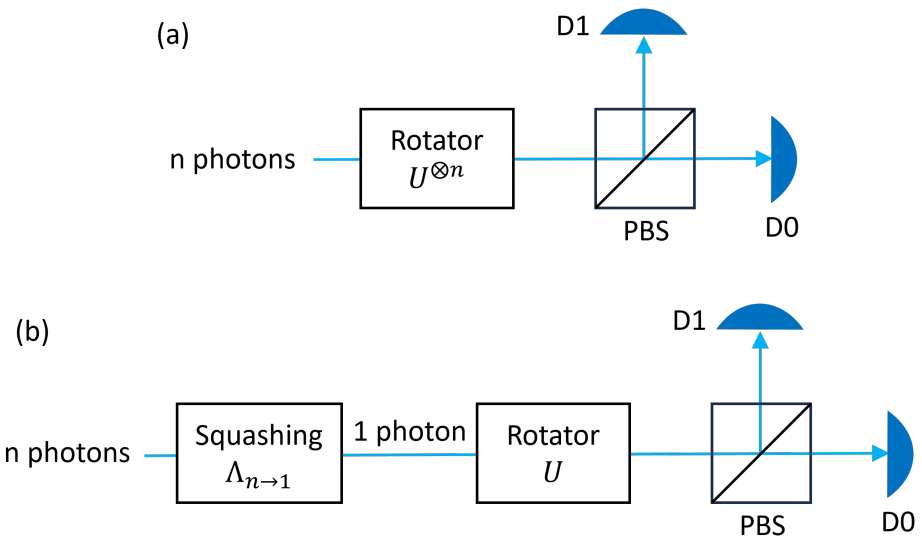


FIG. 3: Comparison between the verifier's (a) practical measurement device and (b) ideal single qubit measurement device with squashing map. In the practical measurement device, the rotation U to the correct measurement basis is applied to all incoming photons. In the ideal measurement device, it accepts only a single (or zero) photon and behaves like an ideal single qubit measurement. This single photon input is enforced by a squashing map $\Lambda_{n\to 1}$, which randomly selects one of the n photons to transmit. $D0$ and $D1$: threshold detectors, PBS: Polarizing beam splitter.

we consider a realistic model for the verifier's imperfect detector shown in Fig. 3a. Ref. [8] demonstrated that using a universal squashing model, one can relate the practical measurement device to an ideal one with a squashing map shown in Fig. 3b. Specifically, the single click events in both models match and double-click events in the practical measurement device can be assigned to the $0/1$ outcomes of the ideal measurement device to obtain a bound on the ideal measurement device statistics. For all other events, such as prover mismatch or no detection by the prover, the verifier's $0/1$ outcome does not impact the assignment.

We summarize this reduction as Thm. IV.3:

Theorem IV.3. *Suppose protocol 1 is ε-sound with an ideal measurement device. Then, protocol 1 is ε-sound with a practical measurement device, i.e. for any set of adversary strategies $\mathcal{A}$,*

$$\max_{\mathcal{S}\in\mathcal{A}_q,\mathcal{M}_{\text{q}}} \Pr[\textit{checks pass}] \leq \varepsilon \implies \max_{\mathcal{S}\in\mathcal{A},\mathcal{M}_{\text{prac}}} \Pr[\textit{checks pass}] \leq \varepsilon, \tag{IV.11}$$

where $\mathcal{A}_q$ is the corresponding set of adversary strategies with channel $\mathcal{E}_{A_i}^{x_i}$ restricted to generate zero or single-photon states in quantum system V_i.

Proof. Since we assume that the loss on the verifier-side is basis-independent and balanced, we can model the measurement device loss as a beam-splitter with transmission η_V placed before a lossless measurement device. We focus on the lossless measurement device model shown in Fig. 3 for the remainder of this proof.

Suppose there exists an adversary strategy $\mathcal{S}$ for the practical measurement device scenario that passes the following checks with probability ε': (1) $N_{\text{det}} \geq N\eta_{\text{th}}$, (2) $N_{\text{dc}} + N_{\text{err}} \leq N_{\text{det}} e_{\text{th}}$ and (3) $z_{0,i} = z_{1,i}, \forall i \in [N]$. Let us consider when the same strategy $\mathcal{S}$ is utilized with the ideal measurement device and squashing map, and let N, N'_{det}, N'_{dc} and N'_{err} be the statistics. By universal squashing [8], the outcomes in the practical measurement device can be matched to outcome assignment in the ideal measurement device, with

1. If neither D0 nor D1 clicks (no photons), then neither would click in the ideal measurement device.
2. If D0 clicks and D1 does not, then D0 clicks and D1 does not in the ideal measurement device.
3. If D1 clicks and D0 does not, then D1 clicks and D0 does not in the ideal measurement device.
4. If both D0 and D1 click (double-click event), then either D0 or D1 clicks in the ideal measurement device.

Since detection events N and N_{det} count events where a click is detected at the measurement device (with differing prover response), the number of such events remains the same in the ideal measurement device, $N' = N$ and $N'_{\text{det}} = N_{\text{det}}$. Since the ideal measurement device only accepts a single-photon after the squashing map, there are no double-click events, $N'_{\text{dc}} = 0$. We note that there can be double-click events when no detection occurs at the prover, $z_{0,i} = \perp$, but in both models, these events are considered to be part of prover loss.

Error events are events where the measurement device outcome does not match the prover's response, $s_i \neq z_{0,i}$ and $z_{0,i}, s_i \neq \perp$. For the idealized model, this includes both the error from single click events, and some contribution from double-click events. Consequently, we bound the number of error events $N_{\text{err}} \leq N'_{\text{err}} \leq N_{\text{err}} + N_{\text{dc}}$ since double-clicks can either be assigned to errors in the worst case or correct responses in the optimistic case. This implies that when $N_{\text{err}} + N_{\text{dc}} \leq N_{\text{det}} e_{\mathsf{th}}$, then $N'_{\text{err}} + N'_{\text{dc}} \leq N_{\text{det}} e_{\mathsf{th}}$. Combining the earlier results, if the strategy $\mathcal{S}$ passes the checks with the practical measurement device with probability ε', then it will also pass the checks with the ideal measurement device and squashing map with probability at least ε'.

Without loss of generality, we consider the squashing map $\Lambda_{n\to 1}$ and the detector loss (η_V beam-splitter) to be implemented by the adversary, i.e. when the adversary generates the state $\rho_{V_i A_K^j A_S^j B_K^j B_S^j}$, it applies the beam-splitter U_{η_V} and $\Lambda_{n\to 1}$ to V_i before sending the state to V_0. The verifier's measurement is the ideal qubit measurement (and zero-photon measurement) $\mathcal{M}_{\text{q}} = \{|\perp\rangle\langle\perp|, |\psi_0^\alpha\rangle\langle\psi_0^\alpha|, |\psi_1^\alpha\rangle\langle\psi_1^\alpha|\}_\alpha$, where $\alpha = f(x,y)$ is the basis choice. We define $\mathcal{A}_q$ as the set of adversary strategies where the channel $\mathcal{E}_{A_i}^{x_i}$ is restricted to generated only single or zero-photon state in quantum system V_i. Since the state that is sent to the ideal qubit measurement can only be a single or zero-photon state (imposed by $\Lambda_{n\to 1}$), any strategy $\mathcal{S} \in \mathcal{A}$ which implements the beam-splitter and squashing map can be mapped to an equivalent strategy in $\mathcal{A}_q$. The earlier discussion implies that for any strategy $\mathcal{S} \in \mathcal{A}$ with verifier measurement $\mathcal{M}_{\text{prac}}$ that can pass the checks with probability ε', there exists a strategy $\mathcal{S}' \in \mathcal{A}_q$ with verifier measurement $\mathcal{M}_{\text{q}}$ can pass the checks with probability at least ε'. If $\varepsilon' > \varepsilon$, it contradicts the presumption that protocol 1 is ε-sound with an ideal measurement device, and thus, there cannot be such a strategy $\mathcal{S} \in \mathcal{A}$ that passes the checks with probability $\varepsilon' > \varepsilon$ with a practical measurement device. As such, protocol 1 is ε-sound with a practical measurement device. □

2. *Random Oracle Model*

The QROM, along with a suitable choice of hash function f, reduces the set of QPT strategies $\mathcal{A}_{QPT}$ to a corresponding set of restricted strategies $\mathcal{A}_{res}$, where channels $\mathcal{E}_{A^j}^{x^j}$ and $\mathcal{E}_{B^j}^{y^j}$ are independent of x^j and y^j, and the POVMs $A_{z_0^j}^{x^j,y^j} = A_{z_0^j}^{\alpha^j}$ and $B_{z_1^j}^{\alpha^j}$ are dependent only on the basis choice α^j. We refer to adversaries in the restricted strategy set $\mathcal{A}_{res}$ as adversaries with no early knowledge of the measurement basis. They learn α^j only at times $t_P^j + d_{V_0 P}/c$ (Alice) and $t_P^j + d_{V_1 P}/c$ (Bob). Since the restricted strategy is independent of x^j and y^j except through α^j, we combine Alice's and Bob's operations with the preparation of $\rho_{A^j B^j}$, and summarize the adversary strategy as

1. The adversary generates a shared state $\rho_{V^j A^j B^j} = \widetilde{\mathcal{E}}^j(\rho_{E^{j-1}})$.
2. When Alice receives y^j and Bob receives x^j, Alice performs a measurement on her subsystem A^j with POVM $A_{z_{0,i}}^{\alpha^j}$ while Bob performs a measurement on his subsystem B^j with POVM $B_{z_1^j}^{\alpha^j}$. Alice and Bob send z_0^j and z_1^j to verifiers V_0 and V_1 respectively.

Formally, we show that

Theorem IV.4. *In the quantum random oracle model, if Protocol 1 is ε-sound against adversaries performing a restricted strategy, then Protocol 1 is $(\varepsilon + \varepsilon_{ROM})$-sound against QPT adversaries, where ε_{ROM} is negligible in the security parameter n, i.e. for any set of QPT adversary strategies $\mathcal{A}_{QPT}$,*

$$\max_{\mathcal{S}\in\mathcal{A}_{res},\mathcal{M}} \Pr[\textit{checks pass}] \leq \varepsilon \implies \max_{\mathcal{S}\in\mathcal{A}_{QPT},\mathcal{M}} \Pr[\textit{checks pass}] \leq \varepsilon + \varepsilon_{ROM}, \tag{IV.12}$$

where $\mathcal{A}_{res}$ is the corresponding set of restricted strategies.

Proof. We will prove this via a sequence of hybrids. We set $\varepsilon_{ROM} = 2qN_{\max}2^{-n} + N_{\max}^2/2^{2n+1}$, where q is an upper bound on the total number of oracle queries that can be performed by an adversary.

- **Hybrid 0:** This is the original QPV soundness experiment, where the adversaries are allowed to perform any QPT strategy in $\mathcal{A}_{QPT}$.
- **Hybrid 1:** This is the same as **Hybrid 0**, except the challenges (x^j, y^j) are sampled such that $(x^j, y^j) \neq (x^k, y^k)$ for $j \neq k$.

- **Hybrid 2.0:** In this hybrid, Alice and Bob are given additional information. In every round j, Alice learns α^j at time $t_P^j + d_{V_0P}/c$ and Bob learns α^j at time $t_P^j + d_{V_1P}/c$.

- **Hybrids 2.1 to 2.$N_{\max}$:** For $j \in [N_{\max}]$, Hybrid j is the same as **Hybrid** $j-1$, except the random oracle f is reprogrammed on input (x^j, y^j) to satisfy $f(x^j, y^j) = u^j$, where $u^j \in [m]$ is a uniformly random number independent from the rest of the protocol.

- **Hybrid 3:** In this hybrid, Alice and Bob only receive α^j at times $(t_P^j + d_{V_0P}/c, t_P^j + d_{V_1P}/c)$ as before, but they do not receive values (x^j, y^j), and there is no random oracle.

Let p_i be the maximum probability of success that an adversary can achieve in **Hybrid** i, i.e. the maximum probability of passing the checks in QPV. We will reach a contradiction through the following sequence of claims:

Claim IV.1. $p_1 \geq p_0 - N_{\max}^2/2^{2n+1}$.

Proof. Conditioned on no collision between pairs (x^j, y^j), the two hybrids are identical. Therefore, for a fixed adversary, the difference between the success probabilities $|p_1 - p_0|$ is upper-bounded by the probability that there exists $j \neq k$ with $(x^j, y^j) = (x^k, y^k)$, which is at most $N_{\max}^2/2^{2n+1}$ by the birthday bound. Note that here we used the total number of rounds $N_{\max}$ as opposed to N because the adversary can affect which rounds are detected by V_0 based on the value x^j. □

Claim IV.2. $p_{2.0} \geq p_1$.

Proof. Since the adversary receives more information, the optimal success probability cannot decrease. □

Claim IV.3. $p_{2.j} \geq p_{2.(j-1)} - 2q2^{-n}$ *for* $j \in [N_{\max}]$.

Proof. Let $j \in [N_{\max}]$ and $(\mathcal{A}, \mathcal{B})$ be an adversary that succeeds in **Hybrid 2.**$(j-1)$ with probability $p_{2.(j-1)}$, with random oracle f^{j-1}. Let f^j be the random oracle in **Hybrid 2.**j, so that $f^j(x^j, y^j) = u^j$ and $f^j(x', y') = f^{j-1}(x', y')$ for $(x', y') \neq (x^j, y^j)$. We will describe a reduction $(\mathcal{A}', \mathcal{B}')$ for **Hybrid 2.**j as follows:

- At times $t < t_P^j + d_{V_0P}/c$, $\mathcal{A}'$ runs $\mathcal{A}$ using f^j as the oracle. Similarly, at times $t < t_P^j + d_{V_1P}/c$, $\mathcal{B}'$ runs $\mathcal{B}$ using f^j as the oracle.

- At times $t \geq t_P^j + d_{V_0P}/c$, $\mathcal{A}'$ can simulate f^{j-1} using (x^j, y^j, f^j) by reprogramming f^j to output α^j on input (x^j, y^j), so $\mathcal{A}'$ can run $\mathcal{A}$ with the correct oracle f^{j-1}. Similarly, $\mathcal{B}'$ can run $\mathcal{B}$ with the correct oracle f^{j-1} at times $t \geq t_P^j + d_{V_1P}/c$.

- $\mathcal{A}'$ (resp. $\mathcal{B}'$) outputs what $\mathcal{A}$ (resp. $\mathcal{B}$) outputs, responding to the same verifier.

Note that the view of $(\mathcal{A}, \mathcal{B})$ as simulated by $(\mathcal{A}', \mathcal{B}')$ differs from **Hybrid 2.**$(j-1)$ at times $(t < t_P^j + d_{V_0P}/c, t < t_P^j + d_{V_1P}/c)$, where the first time is for $\mathcal{A}$ and the second time is for $\mathcal{B}$. Additionally, the oracles only differ on input (x^j, y^j). Recall that the adversary makes at most q total queries to the oracle. Therefore, by Lemma II.1, the total query weight of $(\mathcal{A}, \mathcal{B})$ on input (x^j, y^j) at times $(t < t_P^j + d_{V_0P}/c, t < t_P^j + d_{V_1P}/c)$ is at least $4(p_{2.(j-1)} - p_{2.j})^2/q$. On the other hand, since at these times y^j is information-theoretically hidden from $\mathcal{A}$ and x^j is information-theoretically hidden from $\mathcal{B}$, it implies that the query weight is at most $q2^{-2n}$. Thus, we have $\left|p_{2.(j-1)} - p_{2.j}\right| \leq 2q2^{-n}$ as desired. □

Claim IV.4. $p_3 \geq p_{2.N_{\max}}$.

Proof. Let $(\mathcal{A}, \mathcal{B})$ be an adversary for **Hybrid 2.**$N_{\max}$ that succeeds with probability $p_{2.N_{\max}}$. We give a reduction $(\mathcal{A}', \mathcal{B}')$ that succeeds in **Hybrid 3** with the same probability:

- At time $t = -\infty$ (i.e. before the protocol begins), $\mathcal{A}'$ and $\mathcal{B}'$ sample a $2q$-wise independent hash function f'. In addition, they sample distinct pairs $(x^j, y^j) \in \{0,1\}^n \times \{0,1\}^n$ for $j \in [N_{\max}]$. Then, they reprogram the function f' on inputs (x^j, y^j) so that $f'(x^j, y^j) = \alpha^j$.

- $\mathcal{A}'$ simulates $\mathcal{A}$ and $\mathcal{B}'$ simulates $\mathcal{B}$, using the reprogrammed f' to answer oracle queries and faithfully forwarding any messages output by $(\mathcal{A}, \mathcal{B})$ to the corresponding verifier.

By Lemma II.2, the view of $(\mathcal{A}, \mathcal{B})$ is identical to **Hybrid 2.**$N_{\max}$, hence the checks will pass with probability $p_{2.N_{\max}}$ as desired. □

Note that **Hybrid 0** captures unrestricted strategies and **Hybrid 3** captures the restricted strategies available to the adversary. Therefore, there exists a restricted strategy that succeeds with probability p_3, i.e. $\varepsilon \geq p_3$. Combining with Claims IV.1 to IV.4, we have

$$p_0 \leq p_3 + 2qN_{\max}2^{-n} + N_{\max}^2/2^{2n+1} \leq \varepsilon + \varepsilon_{ROM},$$

which suffices for the proof. □

Remark IV.1 (Deciding the security parameter)**.** *The security parameter (i.e. the hash input length) n should be set according to the computational power of the adversary, measured by the total number of hash function evaluations (q) that the adversary can reasonably perform. It should satisfy $2^n \gg q^2$. If the hash function is picked during the protocol, then the number of queries is estimated based on the protocol duration. If an unkeyed hash function is used, then n should be chosen to be larger to protect against pre-processing attacks.*

Remark IV.2 (Instantiation of the random oracle)**.** *As for any security proof in the (quantum) random oracle model, the guarantee for a concrete instantiation of f, such as SHA3 [9], is heuristic. No efficiently computable function is a random oracle, and there exist artificial constructions that are secure in the random oracle model but insecure under every instantiation. Deviations of a concrete hash function from ideal behavior therefore lie outside the QROM analysis and cannot be quantified in general. Nevertheless, the following can be stated precisely: (i) Theorems IV.2 and V.2 hold against all query-bounded adversaries that access f only through oracle queries. Any adversary doing better must exploit the internal structure of the hash. (ii) The assumption only needs to hold during the protocol run. An online structural attack must also fit within the per-round timing window of below ∼430ns. (iii) No structural attack on full-round SHA3 is known that outperforms generic attacks. (iv) QROM proofs instantiated with SHA3/SHAKE underlie NIST post-quantum standards such as ML-KEM (FIPS 203). A failure of the heuristic for one protocol does not in general transfer to another, but this reflects the confidence placed in SHA3 as an instantiation.*

3. Channel Loss Independence

Consider the restricted adversary model with the restriction that V^j is zero or single-photon, $\mathcal{A}_{res,q}$. When generating $\rho_{V^jA^jB^j}$, the adversary has to make a decision about whether a round is detected (by the choice of preparation of V^j) independent of basis α^j. Intuitively, non-detected rounds provide no advantage to the adversary. As such, it is sufficient to consider an adversary that does not introduce any loss and for a protocol in which exactly N rounds are performed. Let us define the set of adversary strategies with no verifier-side loss as $\mathcal{A}_{res,nl}$, i.e. with the additional imposition that the channel $\widetilde{\mathcal{E}}^j$ generates a qubit V^j (single photon).

Theorem IV.5. *Suppose that Protocol 1 is ε-sound against a restricted adversary that prepares qubit V^j with ideal verifier measurement devices. Then, Protocol 1 is ε-sound against a restricted adversary that prepares a single-photon or vacuum state in V^j with ideal verifier measurement devices, i.e.*

$$\max_{\mathcal{S}\in\mathcal{A}_{res,nl},\mathcal{M}_q} \Pr[\textit{checks pass}] \leq \varepsilon \implies \max_{\mathcal{S}\in\mathcal{A}_{res,q},\mathcal{M}_q} \Pr[\textit{checks pass}] \leq \varepsilon \tag{IV.13}$$

Proof. Consider a restricted adversary with strategy $\mathcal{S} \in \mathcal{A}_{res,q}$ that can pass protocol 1 with probability ε. This adversary prepares the quantum state $\rho_{V^jA^jB^j} = \widetilde{\mathcal{E}}^j(\rho_{E^{j-1}})$, where the adversary is free to decide whether to prepare V^j with a qubit (recall the adversary holds the squashing map) or with no qubit (i.e. no detection). The protocol round then proceeds with the remaining steps, including the measurements of both the adversary and the verifier, which we express as a quantum channel $\mathcal{C}^j$, performed by both the adversary and verifiers. We note that steps in $\mathcal{C}^j$ performed by the verifier, such as the choice of messages x^j and y^j, are independent across rounds and random, thereby allowing for the adversary to simulate these steps internally. Note that the adversary's actions, such as the choice of measurement, can differ between rounds.

In the protocol, the statistics are only generated from the first N rounds where a detection is registered, $s_i \neq \perp$. We summarize the process of the entire protocol as:

1. The adversary prepares ρ_{E_0}.
2. Initialize $i = 1$ and $j = 1$. Repeat until $i = N$:
   (a) The adversary generates $\rho_{V^jA^jB^j} = \widetilde{\mathcal{E}}^j(\rho_{E_{j-1}})$.

(b) The verifiers and adversary proceed with the protocol by applying map $\mathcal{C}^j$ on the prepared state, $\rho_{S^j Z_A^j Z_B^j A^{j'} B^{j'}} = \mathcal{C}^j(\rho_{V^j A^j B^j})$.

(c) The verifiers record S^j, Z_A^j and Z_B^j as the outcome of round i if $S^j \neq \perp$.

(d) Increment $j = j + 1$. If $S^j \neq \perp$, increment i by 1.

Let us consider a modified adversary strategy with a different process:

1. The adversary prepares ρ_{E_0}.

2. Initialize $i = 1$ and $j = 1$. Repeat for N rounds:

(a) The adversary generates $\rho_{V^j A^j B^j} = \widetilde{\mathcal{E}}_i(\rho_{E^{j-1}})$.

(b) The adversary performs a measurement to determine if a qubit is present in quantum system V^j using $\{|\perp\rangle\langle\perp|, |\top\rangle\langle\top|\}$, where $|\top\rangle\langle\top| = |\psi_0^\alpha\rangle\langle\psi_0^\alpha| + |\psi_1^\alpha\rangle\langle\psi_1^\alpha|$ is basis-independent by assumption. Note that the above measurement does not impact the measurement statistics since the measurement operators commute with the verifier's measurement $\{|\perp\rangle\langle\perp|, |\psi_0^\alpha\rangle\langle\psi_0^\alpha|, |\psi_1^\alpha\rangle\langle\psi_1^\alpha|\}$.

(c) If a photon is not detected, the adversary simulates the channel $\mathcal{C}^j$ internally to generate a post-selected state ρ_{E^j}. Increment j by 1 and restart from step (a).

(d) If a photon is present, the verifier and adversary proceed with the protocol, i.e. apply map $\mathcal{C}^j$ on the prepared state to generate statistics S^j, Z_A^j and Z_B^j, and post-selected state ρ_{E^j}.

(e) The verifier record S^j, Z_A^j and Z_B^j as the outcome of round i. Increment i by 1.

By construction, the modified strategy will always give a verifier measurement outcome $S_i = S^j \neq \perp$, and the verifier observes exactly N rounds. The two processes mainly differ in where the decision to add a round into the statistics occurs. In the former, this is performed by the verifier if $S^j \neq \perp$, while in the latter, the adversary chooses to proceed to the next index j if it determines that V^j contains no qubit. Since the processes match, the statistics generated by both processes remain the same, and thus both processes yield an equal probability of passing the checks. Consequently, for any restricted adversary with a strategy that can pass protocol 1 for N detected rounds with probability greater than ε, we can construct a restricted adversary with a strategy for protocol 1 for N rounds with no verifier-side loss that can pass with probability greater than ε. The theorem follows by contradiction. If there exists a strategy $\mathcal{S} \in \mathcal{A}_{res,q}$ that passes protocol 1 with probability exceeding ε, the constructed strategy in $\mathcal{A}_{res,nl}$ would also pass protocol 1 with probability exceeding ε, contradicting the assumption. □

4. *Single-Round Analysis*

Now that we restrict our attention to adversarial strategies in $\mathcal{A}_{res,nl}$, we will switch to indexing rounds by $i \in [N]$ and displaying the round number i as a subscript (see caption of Table I).

Consider the set of restricted adversary strategies $\mathcal{A}_{res,iid,nl}$ with qubit preparation for V_i and i.i.d. attacks. Since the attacks are independent and identical, we can define expectation values for prover efficiency η, probability of mismatched responses ($z_{0,i} \neq z_{1,i}$) p_{mis}, and QBER e, which takes identical values across rounds. We characterize the relation between these three parameters for a single round before proving security.

Theorem IV.6. *Consider a single round of Protocol 1 with an adversary strategy $\mathcal{S} \in \mathcal{A}_{res,iid,nl}$ and ideal verifier measurement $\mathcal{M}_{\mathrm{q}}$. Let η, p_{mis} and e be the prover efficiency, mismatch probability, and QBER of the round respectively. If $\eta \geq \eta_{\mathsf{b}}$ and $p_{\mathsf{mis}} \leq p_{\mathsf{mis,b}}$, then the effective QBER $e \geq e_{SDP}$, where $e_{SDP}(\eta_{\mathsf{b}}, p_{\mathsf{mis,b}})$ is the solution to the SDP in Eqn. (IV.19).*

Proof. For a single round of the restricted adversary strategy, the statistics are given by

$$\Pr[s, z_0, z_1] = \frac{1}{m} \sum_\alpha \mathrm{Tr}\left[(\Pi_s^\alpha \otimes A_{z_0}^\alpha \otimes B_{z_1}^\alpha)\rho_{VAB}\right], \tag{IV.14}$$

where V is a qubit system, and we drop the index i for brevity. Without loss of generality, by state purification and Stinespring's dilation theorem, we can consider a pure strategy with a pure state $|\psi\rangle_{VAB}$ where the purification system can be kept with A to keep $dim(V) = 2$, and projective measurements $\{\tilde{A}_{z_0}^\alpha\}$ and $\{\tilde{B}_{z_1}^\alpha\}$ corresponding to the POVMs. The statistics remain unchanged,

$$\Pr[s, z_0, z_1] = \frac{1}{m} \sum_\alpha \langle\psi|\Pi_s^\alpha \otimes \tilde{A}_{z_0}^\alpha \otimes \tilde{B}_{z_1}^\alpha|\psi\rangle\,. \tag{IV.15}$$

The pure state can be expressed as

$$|\psi\rangle_{VAB} = |0\rangle_V |\phi_0\rangle_{AB} + |1\rangle_V |\phi_1\rangle_{AB}\,, \tag{IV.16}$$

where $|\phi_i\rangle_{AB}$ can be sub-normalized. When ideal qubit measurements are performed by the verifier, the state held by Alice and Bob collapses to one of the sub-normalized states depending on measurement outcomes $s = 0, 1$,

$$\begin{aligned} |\phi_0^\alpha\rangle_{AB} &= \cos\left(\frac{\theta_\alpha}{2}\right)|\phi_0\rangle_{AB} + \sin\left(\frac{\theta_\alpha}{2}\right) e^{-i\phi_\alpha}|\phi_1\rangle_{AB} \\ |\phi_1^\alpha\rangle_{AB} &= \sin\left(\frac{\theta_\alpha}{2}\right)|\phi_0\rangle_{AB} - \cos\left(\frac{\theta_\alpha}{2}\right) e^{-i\phi_\alpha}|\phi_1\rangle_{AB}\,. \end{aligned} \tag{IV.17}$$

The minimum QBER attainable by any adversary $\mathcal{S} \in \mathcal{A}_{res.iid.nl}$ is expressed as an optimization problem

$$\begin{aligned} \min_{|\phi_0\rangle,|\phi_1\rangle,\{\tilde{A}^\alpha_{z_0}\}_{z_0},\{\tilde{B}^\alpha_{z_1}\}_{z_1}} \quad & \frac{1}{m\eta}\sum_{\alpha=1}^{m} \langle\phi_0^\alpha|\tilde{A}_1^\alpha \otimes \mathbb{I}_B|\phi_0^\alpha\rangle + \langle\phi_1^\alpha|\tilde{A}_0^\alpha \otimes \mathbb{I}_B|\phi_1^\alpha\rangle \\ subj.\,to \quad & \frac{1}{m}\sum_{\alpha=1}^{m}\sum_{j=0}^{1} \left\langle\phi_j^\alpha\right|\tilde{A}_\perp^\alpha \otimes \mathbb{I}_B\left|\phi_j^\alpha\right\rangle = 1-\eta \\ & \frac{1}{m}\sum_{\alpha=1}^{m}\sum_{j=0}^{1}\sum_{z_0\neq z_1} \left\langle\phi_j^\alpha\right|\tilde{A}_{z_0}^\alpha \otimes \tilde{B}_{z_1}^\alpha\left|\phi_j^\alpha\right\rangle \leq p_{\mathsf{mis,b}} \\ & \langle\phi_0^\alpha|\phi_0^\alpha\rangle + \langle\phi_1^\alpha|\phi_1^\alpha\rangle = 1,\, \forall\alpha \in \{1,\cdots,m\} \\ & \eta \geq \eta_{\mathsf{b}} \end{aligned} \tag{IV.18}$$

For any strategy with prover efficiency $\eta > \eta_{\mathsf{b}}$, we can construct an equivalent strategy at $\eta_{\mathsf{b}} = \eta$ with the same QBER by randomly setting responses z_0 and z_1 to $\perp$. It is therefore sufficient to optimize at $\eta = \eta_b$. The optimization problem can be relaxed into an SDP following Ref. [10],

$$\begin{aligned} \min_{G\geq 0} \quad & \frac{1}{m\eta_b}\sum_{\alpha=1}^{m} \langle\phi_0^\alpha|\tilde{A}_1^\alpha|\phi_0^\alpha\rangle + \langle\phi_1^\alpha|\tilde{A}_0^\alpha|\phi_1^\alpha\rangle \\ subj.\,to \quad & \frac{1}{m}\sum_{\alpha=1}^{m}\sum_{j=0}^{1} \left\langle\phi_j^\alpha\right|\tilde{A}_\perp^\alpha\left|\phi_j^\alpha\right\rangle = 1-\eta_b \\ & \frac{1}{m}\sum_{\alpha=1}^{m}\sum_{j=0}^{1}\sum_{z_0\neq z_1} \left\langle\phi_j^\alpha\right|\tilde{A}_{z_0}^\alpha\tilde{B}_{z_1}^\alpha\left|\phi_j^\alpha\right\rangle \leq p_{mis,b} \\ & \langle\phi_0|\phi_0\rangle + \langle\phi_1|\phi_1\rangle = 1 \\ & [\tilde{A}_{z_0}^\alpha, \tilde{B}_{z_1}^{\alpha'}] = 0,\, \forall\alpha,\alpha', z_0, z_1, \end{aligned} \tag{IV.19}$$

where G is a Gram matrix with elements $G_{(j,O),(j',O')} = \left\langle\phi_j\right|OO'\left|\phi'_j\right\rangle$, and O refers to operators formed from combinations of $\mathbb{I}$, $\{\tilde{A}^\alpha_{z_0}\}$, and $\{\tilde{B}^\alpha_{z_1}\}$. □

5. *Finite-Size Analysis*

The relation between the single-round expectation values constrains the adversary strategy. Since these expectation values are the same across rounds, we relate them to observed values using concentration bounds. This in turn allows for a comparison between the observed and the threshold values to compute the soundness parameter.

Theorem IV.7. *Protocol 1 with an ideal verifier measurement device is ε-sound against any restricted adversary that prepares V_i as a qubit state, i.e.*

$$\max_{\mathcal{S}\in\mathcal{A}_{res,iid,nl},\mathcal{M}_{\mathrm{q}}} \Pr[checks\,pass] \leq \varepsilon, \tag{IV.20}$$

where

$$\varepsilon = \max\left\{1-\Phi\left(\sqrt{2NH\left(\eta_{\mathsf{th}}-\frac{1}{N},\eta_{\mathsf{b}}\right)}\right), \Phi\left(-\sqrt{2NH\left(p_{\mathsf{mis,th}}+\frac{1}{N},p_{\mathsf{mis,b}}\right)}\right), \Phi\left(-\sqrt{2NH\left(e_{\mathsf{th}}+\frac{1}{N},e_{SDP}\right)}\right)\right\}, \tag{IV.21}$$

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

Proof. To prove security, we show that the adversary cannot simultaneously pass all checks with high probability,

$$\Pr[\textit{checks pass}] \leq \Pr[N_{\mathrm{det}} \geq N\eta_{\mathsf{th}}, N_{\mathrm{err}} \leq Ne_{\mathsf{th}}, N_{\mathrm{mis}} \leq Np_{\mathsf{mis,th}}]. \tag{IV.22}$$

We split the set of adversary strategies $\mathcal{A}_{res,iid,nl}$ into three subsets: (1) $\mathcal{A}^{<\eta_{\mathsf{b}}}_{res,iid,nl}$ where the single-round expected prover efficiency is $\eta < \eta_{\mathsf{b}} < \eta_{\mathsf{th}}$, (2) $\mathcal{A}^{>p_{\mathsf{mis,b}}}_{res,iid,nl}$ where the single-round mismatch probability is high, $p_{\mathsf{mis}} > p_{\mathsf{mis,b}} > 0$, and (3) $\mathcal{A}^{\geq\eta_{\mathsf{b}},\leq p_{\mathsf{mis,b}}}_{res,iid,nl}$ where the single-round expected prover efficiency is high and the mismatch probability is low, $\eta \geq \eta_{\mathsf{b}}$ and $p_{\mathsf{mis}} \leq p_{\mathsf{mis,b}}$.

For the first subset, $\mathcal{A}^{<\eta_{\mathsf{b}}}_{res,iid,nl}$, the prover efficiency check fails with high probability,

$$\begin{aligned}\Pr[\textit{checks pass}] \leq& \Pr[N_{\mathrm{det}} \geq N\eta_{\mathsf{th}}]\\ =& 1-\Pr[N_{det} \leq \lceil N\eta_{th}\rceil - 1]\\ \leq& 1-\Phi\left(\sqrt{2NH\left(\frac{\lceil N\eta_{\mathsf{th}}\rceil - 1}{N},\eta_{\mathsf{b}}\right)}\right)\\ \leq& 1-\Phi\left(\sqrt{2NH\left(\eta_{\mathsf{th}}-\frac{1}{N},\eta_{\mathsf{b}}\right)}\right),\end{aligned} \tag{IV.23}$$

where the third line applies the concentration bound from Ref. [7], and the final line uses the property that $\frac{\partial}{\partial x}\Phi\left(\sqrt{2NH(x,p)}\right) \geq 0$ when $x \geq p$.

For the second subset, $\mathcal{A}^{>p_{\mathsf{mis,b}}}_{res,iid,nl}$, the mismatch check fails with high probability,

$$\begin{aligned}\Pr[\textit{checks pass}] \leq& \Pr[N_{\mathrm{mis}} \leq Np_{\mathsf{mis,th}}]\\ =& \Pr[N_{\mathrm{mis}} \leq \lfloor Np_{\mathsf{mis,th}}\rfloor]\\ \leq& \Phi\left(-\sqrt{2NH\left(\frac{\lfloor Np_{\mathsf{mis,th}}\rfloor + 1}{N},p_{\mathsf{mis,b}}\right)}\right)\\ \leq& \Phi\left(-\sqrt{2NH\left(p_{\mathsf{mis,th}}+\frac{1}{N},p_{\mathsf{mis,b}}\right)}\right),\end{aligned} \tag{IV.24}$$

where the third line applies the concentration bound from Ref. [7], and the final line uses the property that $\frac{\partial}{\partial x}\Phi\left(-\sqrt{2NH(x,p)}\right) \geq 0$ when $x \leq p$.

For the final subset, $\mathcal{A}^{\geq\eta_{\mathsf{b}},\leq p_{\mathsf{mis,b}}}_{res,iid,nl}$, given that $\eta \geq \eta_{\mathsf{b}}$ and $p_{\mathsf{mis}} \leq p_{\mathsf{mis,b}}$, Thm. IV.6 implies that the QBER satisfies $e \geq e_{SDP}(\eta_{\mathsf{b}}, p_{\mathsf{mis,b}})$. Therefore, the QBER check passes with low probability,

$$\begin{aligned}\Pr[\textit{checks pass}] =& \Pr[N_{\mathrm{err}} \leq N_{\mathrm{det}}e_{\mathsf{th}}, N_{\mathrm{det}} \geq N\eta_{\mathsf{th}}]\\ =& \sum_{N_{\mathrm{det}}\geq N\eta_{\mathsf{th}}} \Pr[N_{\mathrm{det}}] \times \Pr[N_{\mathrm{err}} \leq N_{\mathrm{det}}e_{\mathsf{th}}]\\ \leq& \sum_{N_{\mathrm{det}}\geq N\eta_{\mathsf{th}}} \Pr[N_{\mathrm{det}}] \times \Phi\left(-\sqrt{2N_{\mathrm{det}}H\left(e_{\mathsf{th}}+\frac{1}{N_{\mathrm{det}}},e_{SDP}\right)}\right)\\ \leq& \Phi\left(-\sqrt{2N\eta_{\mathsf{th}}H\left(e_{\mathsf{th}}+\frac{1}{N\eta_{\mathsf{th}}},e_{SDP}\right)}\right),\end{aligned} \tag{IV.25}$$

where in the third line, we use the property that $\frac{\partial}{\partial x}\Phi(-\sqrt{2NH(x,p)}) \geq 0$ if $x \leq p$. In the fourth line, we use the fact that $\frac{\partial}{\partial N}\Phi(-\sqrt{2NH(x+\frac{1}{N},p)}) \leq 0$ if $p \geq x + \frac{1}{N}$. The soundness is thus a maximum over the probabilities of passing the checks across the three subsets of strategies. □

D. Numerical Simulation

We study the performance of the LT-QPV protocol by simulating the parameter regime that an honest implementation must satisfy to achieve ε_{com}-completeness and ε_{sou}-soundness. For later comparison with the experimental implementation, we use the characterization of the verifier's measurement device in the implementation. The implementation uses $m = 16$ bases, and the bases listed in Sec. VII B. We note that these basis states are not uniformly distributed over the Bloch sphere due to experimental imperfections, but they are sufficiently well-distributed to demonstrate security in the parameter regime achieved by the experiment.

Consider an honest implementation with prover efficiency η, mismatch probability p_{mis}, and double-click probability p_{dc}. Our goal is to compute the maximum QBER e that an honest implementation must not exceed. At each value of η and p_{mis}, we compute the thresholds η_{th} and $p_{\mathsf{mis,th}}$ from Thm. IV.1 and determine the bounds on adversary prover efficiency η_{b} and mismatch $p_{\mathsf{mis,b}}$ consistent with the soundness condition in Thm. IV.2. By solving the SDP in Eqn. (IV.19), we compute the minimum QBER achievable by the adversary. This allows us to select an appropriate QBER threshold e_{th} to match the soundness condition. From e_{th}, we determine the effective QBER $e' = p_{\mathsf{dc}} + (1-p_{\mathsf{dc}})e$ an honest implementation must achieve to satisfy the completeness requirement.

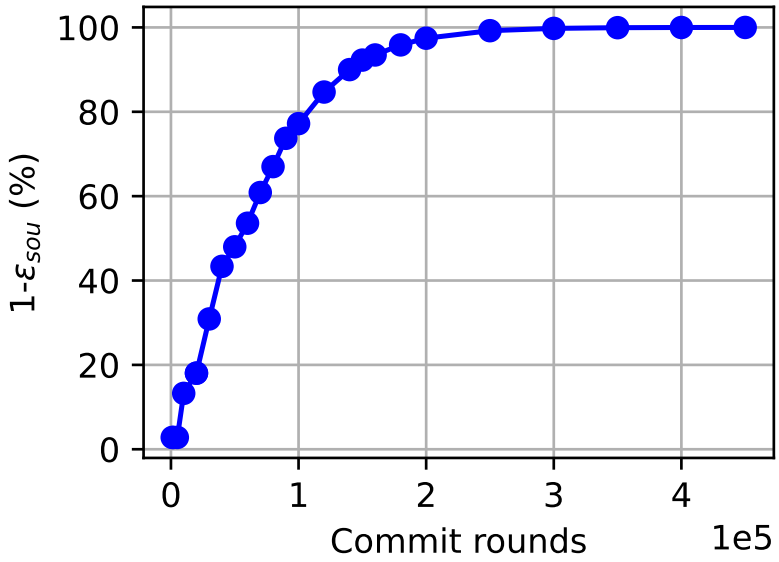


FIG. 4: Confidence of Prover's location (as 1-ϵ_{sou}) vs rounds.

We run the simulation for $\varepsilon_{\text{sou}} = \varepsilon_{\text{com}} = 10^{-2}$ and split the completeness budget as $\varepsilon_{\text{com},\eta} = 0.1\varepsilon_{\text{com}}$, $\varepsilon_{\text{com,mis}} = 0.1\varepsilon_{\text{com}}$, and $\varepsilon_{\text{com,e}} = 0.8\varepsilon_{\text{com}}$,

which we find to perform well in the regime of interest. For simplicity, we assume $\varepsilon_{ROM} = 0$, but the value is generally small for a suitably chosen hash function f and large enough n. We solve the SDP using tools from ncpol2sdpa [11], the PICOS interface [12], and the QICS solver [13] at NPA level $1 + AB$, where the AB operators are restricted only 15 basis combinations: (2,6), (10,14), (1,5), (2,14), (9,13), (1,13), (6,9), (10,11), (11,15), (4,5), (0,4), (2,3), (3,7), (8,9), (14,15). These basis combinations corresponds to verifier basis pairs with the highest overlap $\max\{\left|\left\langle \psi_0^{\alpha} \middle| \psi_1^{\alpha'} \right\rangle\right|^2, \left|\left\langle \psi_0^{\alpha} \middle| \psi_0^{\alpha'} \right\rangle\right|^2\}$, but the choice to retain 15 combinations is heuristic since having more basis combinations would lead to longer SDP solve times while providing tighter QBER bounds. We use the experimentally measured values of $p_{\mathsf{dc}} = 1.45 \times 10^{-4}$ and $p_{\mathsf{mis}} = 5.49 \times 10^{-6}$. We plot maximum tolerable QBER as a function of prover efficiency, which is shown in Main Text Fig. 2. Based on the experimental performance of $\eta = 0.201$, $e = 0.0117$, $p_{\mathsf{mis}} = 5.49 \times 10^{-6}$ and $p_{\mathsf{dc}} = 1.45 \times 10^{-4}$, a run of $N = 2.55 \times 10^5$ is required, with corresponding

threshold $\eta_{\mathsf{th}} = 19.86\%$, $e_{\mathsf{th}} = 1.31\%$ and $p_{\mathsf{mis,th}} = 2.9 \times 10^{-5}$ (equivalent to a check of $N_{\mathrm{mis}} \leq 7$). For the same experimental performance, we also plot the confidence $(1-\varepsilon_{\mathrm{sou}})$ as the number of rounds chosen is increased in Fig. 4.

E. Calibration Rounds

In LT-QPV, there are multiple variables that are required to be set before the protocol is performed. For instance, the number of basis m is chosen based on a rough estimate of the performance of our implementation. Crucially, the number of valid rounds N, and the threshold parameters η_{th}, e_{th}, and $p_{\mathsf{mis,th}}$ have to be carefully chosen to ensure that it remains secure against adversaries (low soundness) while allowing an honest prover's location to be certified (low completeness error). This requires a model characterizing the honest performance of the implementation, which can be obtained through calibration rounds. While calibration rounds are not strictly required to guarantees soundness, having a soundness guarantee alone may not be meaningful. For instance, while setting $\eta_{\mathsf{th}} = 1$, $e_{\mathsf{th}} = 0$, $p_{\mathsf{mis,th}} = 0$ and $N = 10^{10}$ can ensure strong soundness guarantees, the stringent requirements makes it almost impossible for any honest prover to be certified. Therefore, the calibration rounds are necessary to ensure good choice of threshold parameters and have completeness guarantees.

In our protocol, we do not explicitly include the calibration rounds and they are performed prior to the actual QPV run. We note that it is in general possible to have the calibration rounds right before the protocol run [4], but the parameters of the protocol (derived from the calibration) must be selected before the protocol begins. In practice, an adversary can compromise the calibration rounds, but that does not compromise the soundness of the protocol. A fixed choice of parameters N, η_{th}, e_{th} and $p_{\mathsf{mis,th}}$ will guarantee the soundness that can be computed from Theorem IV.2. For a fixed soundness parameter $\varepsilon_{\mathrm{sou}}$, an adversary that has influence over the calibration round can influence the choice of the parameters, but any choice of the parameters will either: (1) guarantee a soundness of $\varepsilon_{\mathrm{sou}}$ or (2) trigger the conclusion that the performance of the implemented system cannot guarantee the required soundness, i.e. the actual QPV run will not be performed since soundness cannot be guaranteed.

We stress that in the protocol and security analysis, the parameters are assumed to be chosen prior to the protocol run. As such, one cannot use the calibration data (or part of it) to demonstrate a secure QPV run. For example, taking the data of the first half of a calibration round as the QPV run would imply that during and after the QPV protocol, the parameters N, η_{th}, e_{th}, and $p_{\mathsf{mis,th}}$ are variables that can change both during and after the protocol run. This opens up an attack that after the first half of the calibration round (data used for QPV run), the adversary can still alter the thresholds in the second half of the calibration, providing the adversary with an advantage that is not considered in the security analysis. Moreover, using the same data for both calibration of the thresholds and protocol run would imply that the thresholds and protocol run data are correlated random variables. For instance, N_{det}, N and η_{th} are random variables that are strongly correlated through a complex relation that depends on how η_{th} is computed from the data. As such, statistical bounds used in the security analysis where fixed thresholds are assumed, such as the concentration bound from Ref. [7] for i.i.d. attacks and from Ref. [14] for general attacks, would no longer apply.

V. LT-QPV SECURE AGAINST GENERAL ATTACKS

We extend the security of LT-QPV and demonstrate that LT-QPV remains sound against general QPT adversaries. More precisely, we prove the security for an LT-QPV protocol where the error check (in parameter estimation) is $N_{\mathrm{dc}} + N_{\mathrm{err}} \leq N\tilde{e}_{\mathsf{th}}$. We term this LT-QPV protocol with unconditioned error check. We term $\tilde{e}$ the unconditioned error, which is not conditioned on detection at V_0, to distinguish it from the QBER e.

A. Completeness

The completeness analysis is slightly modified from that of Protocol 1 due to the change in error check.

Theorem V.1. *Consider an honest prover at X_P, with single-round prover efficiency η, QBER e, double-click probability p_{dc}, and mismatch probability p_{mis}. LT-QPV protocol with unconditioned error check is $\varepsilon_{\mathrm{com}}$-complete with completeness error*

$$\varepsilon_{\mathrm{com}} = \Phi\left(-\sqrt{2NH\left(\eta_{\mathsf{th}} + \frac{1}{N}, \eta\right)}\right) + 1 - \Phi\left(\sqrt{2NH\left(\tilde{e}_{\mathsf{th}} - \frac{1}{N}, \tilde{e}'\right)}\right) + 1 - \Phi\left(\sqrt{2NH\left(p_{\mathsf{mis,th}} - \frac{1}{N}, p_{\mathsf{mis}}\right)}\right), \quad \text{(V.1)}$$

where $e' = p_{dc} + (1-p_{dc})e$, $\tilde{e}' = e'\eta$, $H(x,p) = x\ln(x/p) + (1-x)\ln[(1-x)/(1-p)]$, $\Phi(x)$ *is the cumulative distribution function of a standard normal distribution,* η_{th}, $\tilde{e}_{\mathsf{th}}$, *and* $p_{\mathsf{mis,th}}$ *are the threshold values for prover efficiency, unconditioned error and mismatch probability and are selected such that* $\eta_{\mathsf{th}} \leq \eta - \frac{1}{N}$, $\tilde{e}_{\mathsf{th}} \geq \tilde{e}' + \frac{1}{N\eta_{\mathsf{th}}}$ *and* $p_{\mathsf{mis,th}} \geq p_{\mathsf{mis}} + \frac{1}{N}$.

Proof. We follow the proof of Thm. IV.1, except for the error check. We bound the error check failure probability,

$$\begin{aligned}\Pr[N_{\mathrm{err}} + N_{\mathrm{dc}} > N\tilde{e}_{\mathsf{th}}] \leq & \Pr[N_{\mathrm{err}} + N_{\mathrm{dc}} > \lfloor N\tilde{e}_{\mathsf{th}} \rfloor] \\ = & 1 - \Pr[N_{\mathrm{err}} + N_{\mathrm{dc}} \leq \lfloor N\tilde{e}_{\mathsf{th}} \rfloor] \\ \leq & 1 - \Phi\left(\sqrt{2NH\left(\frac{\lfloor N\tilde{e}_{\mathsf{th}} \rfloor}{N}, \tilde{e}'\right)}\right) \\ \leq & 1 - \Phi\left(\sqrt{2NH\left(\tilde{e}_{\mathsf{th}} - \frac{1}{N}, \tilde{e}'\right)}\right),\end{aligned} \tag{V.2}$$

where the third line applies the tight concentration bound [7] and the fourth line uses the property that $\frac{\partial}{\partial x}\Phi(\sqrt{2NH(x,\tilde{e}')}) \geq 0$ if $x \geq \tilde{e}'$. □

B. Soundness

The proof of soundness is similar to the i.i.d. analysis, except for the single-round analysis and finite-size analysis step. The first three steps of universal squashing, random oracle model, and channel loss independence are agnostic to whether the attack is general or i.i.d., and can therefore apply directly to the soundness proof against general QPT adversaries. The single-round analysis follows similarly, where we seek the minimum unconditioned error $\tilde{e}$ instead of the minimum QBER e conditioned on detection, and use the dual variables of the SDP to demonstrate a linear relation between $\tilde{e}$, p_{mis}, and η. The finite-size analysis then applies a bound from Ref. [14], noting that the linear relation derived from single-round analysis holds even when conditioned on past rounds.

Theorem V.2. *LT-QPV protocol with unconditioned error check is* $\varepsilon_{\mathrm{sou}}$*-sound against general QPT adversaries in the quantum random oracle model, i.e.*

$$\max_{\mathcal{S}\in\mathcal{A}_{QPT},\mathcal{M}_{\mathrm{prac}}} \Pr[\textit{checks pass}] \leq \varepsilon_{\mathrm{sou}}, \tag{V.3}$$

where $\varepsilon_{\mathrm{sou}} = \varepsilon'_{\mathrm{sou}} + \varepsilon_{ROM}$,

$$\nu + \beta(1-\eta_{\mathsf{th}}) - \tilde{e}_{\mathsf{th}} + \gamma p_{\mathsf{mis,th}} = \sqrt{2V}\sqrt{\frac{\log_2(1/\varepsilon'_{\mathrm{sou}})}{N}} + \frac{\nu}{3}\frac{\log_2(1/\varepsilon'_{\mathrm{sou}})}{N}, \tag{V.4}$$

for any choice of dual variables $\beta, \gamma \leq 0$ *and* $\{\varphi_i\}_i$, *and* $\nu(\beta,\gamma,\{\varphi_i\}_i)$ *is a function of dual variables of the SDP in Eqn. (V.9) and* V *is chosen such that* $V = \max\{\nu^2, (\nu + \min\{\beta,-1\} + \gamma)^2\}$.

Proof. It is sufficient to prove that

$$\max_{\mathcal{S}\in\mathcal{A}_{res,nl},\mathcal{M}_{\mathrm{q}}} \Pr[\textit{checks pass}] \leq \varepsilon - \varepsilon_{ROM} \tag{V.5}$$

since Thms. IV.3 to IV.5 guarantee the $\varepsilon_{\mathrm{sou}}$-soundness.

$$\begin{aligned}&\max_{\mathcal{S}\in\mathcal{A}_{res,nl},\mathcal{M}_{\mathrm{q}}} \Pr[\textit{checks pass}] \leq \varepsilon_{\mathrm{sou}} - \varepsilon_{ROM} \xRightarrow{\textit{Thm. IV.5}} \max_{\mathcal{S}\in\mathcal{A}_{res,q},\mathcal{M}_{\mathrm{q}}} \Pr[\textit{checks pass}] \leq \varepsilon_{\mathrm{sou}} - \varepsilon_{ROM} \\ &\xRightarrow{\textit{Thm. IV.4}} \max_{\mathcal{S}\in\mathcal{A}_{QPT,q},\mathcal{M}_{\mathrm{q}}} \Pr[\textit{checks pass}] \leq \varepsilon_{\mathrm{sou}} \xRightarrow{\textit{Thm. IV.3}} \max_{\mathcal{S}\in\mathcal{A}_{QPT},\mathcal{M}_{\mathrm{prac}}} \Pr[\textit{checks pass}] \leq \varepsilon_{\mathrm{sou}}.\end{aligned} \tag{V.6}$$

Applying Thm. V.4 completes the proof. □

1. Single-Round Analysis

We present the single-round analysis to link $\tilde{e}$, p_{mis} and η, noting that any double-click events have been assigned to error outcomes in the ideal verifier measurement $\mathcal{M}_{\mathrm{q}}$ via universal squashing (see Theorem IV.3).

Theorem V.3. *Consider a single round of LT-QPV protocol with unconditioned error check with restricted adversary strategy $\mathcal{A}_{res,nl}$ and ideal verifier measurement $\mathcal{M}_{\mathrm{q}}$. Let η_i, $p_{\mathsf{mis},i}$ and $\tilde{e}_i$ be the prover efficiency, mismatch probability and unconditioned error of the i-th round respectively. For any choice of dual variables $\beta, \gamma \leq 0$ and $\{\varphi_i\}_i$, the single-round quantities satisfy the tradeoff*

$$\tilde{e}_i \geq \nu + \beta(1-\eta_i) + \gamma p_{\mathsf{mis},i}, \tag{V.7}$$

where $\nu(\beta, \gamma, \{\varphi_i\}_i)$ is a function of dual variables of the SDP in Eqn. (V.9).

Proof. We follow the argument of Thm. IV.6, in which we minimize the unconditioned error $\tilde{e}_i$, which can be expressed as

$$\begin{aligned} \min_{|\phi_0\rangle, |\phi_1\rangle, \{\tilde{A}^\alpha_{z_0}\}_{z_0}, \{\tilde{B}^\alpha_{z_1}\}_{z_1}} \quad & \frac{1}{m}\sum_{\alpha=1}^{m} \langle\phi_0^\alpha|\tilde{A}_1^\alpha \otimes \mathbb{I}_B|\phi_0^\alpha\rangle + \langle\phi_1^\alpha|\tilde{A}_0^\alpha \otimes \mathbb{I}_B|\phi_1^\alpha\rangle \\ subj.\,to \quad & \frac{1}{m}\sum_{\alpha=1}^{m}\sum_{j=0}^{1} \left\langle\phi_j^\alpha\right|\tilde{A}_\perp^\alpha \otimes \mathbb{I}_B\left|\phi_j^\alpha\right\rangle \leq 1-\eta_i \\ & \frac{1}{m}\sum_{\alpha=1}^{m}\sum_{j=0}^{1}\sum_{z_0\neq z_1} \left\langle\phi_j^\alpha\right|\tilde{A}_{z_0}^\alpha \otimes \tilde{B}_{z_1}^\alpha\left|\phi_j^\alpha\right\rangle \leq p_{\mathsf{mis},i} \\ & \langle\phi_0^\alpha|\phi_0^\alpha\rangle + \langle\phi_1^\alpha|\phi_1^\alpha\rangle = 1,\ \forall\alpha \in \{1,\cdots,m\} \end{aligned} \tag{V.8}$$

Since $\tilde{e}_i$ is not conditioned on detection, the objective function differs by a factor of η from that in Thm. IV.6. We use the same method [10] to relax the optimization problem into an SDP,

$$\begin{aligned} \min_{G\geq 0} \quad & \frac{1}{m}\sum_{\alpha=1}^{m} \langle\phi_0^\alpha|\tilde{A}_1^\alpha|\phi_0^\alpha\rangle + \langle\phi_1^\alpha|\tilde{A}_0^\alpha|\phi_1^\alpha\rangle \\ subj.\,to \quad & \frac{1}{m}\sum_{\alpha=1}^{m}\sum_{j=0}^{1} \left\langle\phi_j^\alpha\right|\tilde{A}_\perp^\alpha\left|\phi_j^\alpha\right\rangle \leq 1-\eta_i \\ & \frac{1}{m}\sum_{\alpha=1}^{m}\sum_{j=0}^{1}\sum_{z_0\neq z_1} \left\langle\phi_j^\alpha\right|\tilde{A}_{z_0}^\alpha\tilde{B}_{z_1}^\alpha\left|\phi_j^\alpha\right\rangle \leq p_{\mathsf{mis},i} \\ & \langle\phi_0|\phi_0\rangle + \langle\phi_1|\phi_1\rangle = 1 \\ & [\tilde{A}_{z_0}^\alpha, \tilde{B}_{z_1}^{\alpha'}] = 0,\ \forall\alpha,\alpha', z_0, z_1 \end{aligned} \tag{V.9}$$

We now use the SDP to construct a relation between the single-round quantities. Let F_η, F_{mis}, and F_{obj} be matrices representing the prover efficiency constraint, mismatch constraint, and objective function respectively, such that $\mathrm{Tr}[F_\eta G] \leq 1-\eta_i$, $\mathrm{Tr}[F_{\mathrm{mis}}G] \leq p_{\mathsf{mis},i}$, and $\mathrm{Tr}[F_{\mathrm{obj}}G]$. Let F_j and c_j be the matrix and constant of the remaining constraints that are expressed as $\mathrm{Tr}[F_j G] = c_j$. We define a Lagrangian with dual variables β', γ', and $\{\varphi_j\}_j$,

$$L(\beta', \gamma', \{\varphi_j\}_j, G) = \mathrm{Tr}[F_{\mathrm{obj}}G] + \beta'(\mathrm{Tr}[F_\eta G] - 1 + \eta_i) + \gamma'(\mathrm{Tr}[F_{\mathrm{mis}}G] - p_{\mathsf{mis},i}) + \sum_j \varphi_j(\mathrm{Tr}[F_j G] - c_j) \tag{V.10}$$

and construct the Lagrangian dual function,

$$\begin{aligned} g(\beta', \gamma', \{\varphi_j\}_j) &= \inf_{G\geq 0} \mathrm{Tr}\left[\left(F_{\mathrm{obj}} + \beta' F_\eta + \gamma' F_{\mathrm{mis}} + \sum_j \varphi_j F_j\right) G\right] - \beta'(1-\eta_i) - \gamma' p_{\mathsf{mis},i} - \sum_j \varphi_j c_j \\ &= \nu(\{\varphi_j\}_j, \beta', \gamma') - \beta'(1-\eta_i) - \gamma' p_{\mathsf{mis},i}, \end{aligned} \tag{V.11}$$

where $\nu = \inf_{G\geq 0} \mathrm{Tr}\Big[(F_{obj} + \beta' F_\eta + \gamma' F_{\mathrm{mis}} + \sum_j \varphi_j F_j)G\Big] - \sum_j \varphi_j c_j$. Since the SDP is a convex optimization problem, the dual function lower bounds the solution to the SDP for any choice of φ and $\beta', \gamma' \geq 0$ [15], i.e.

$$\tilde{e}_i \geq \tilde{e}_{SDP} \geq \nu - \beta'(1-\eta_i) - \gamma' p_{\mathsf{mis},i}. \tag{V.12}$$

A simple redefinition of $\beta = -\beta'$ and $\gamma = -\gamma'$ completes the proof. □

2. Finite-Size Analysis

Theorem V.4. *LT-QPV protocol with unconditioned error check with an ideal verifier measurement device is ε-sound against any restricted adversary that prepares a qubit state in V_i, i.e.*

$$\max_{\mathcal{S}\in\mathcal{A}_{res,nl},\mathcal{M}_{\mathrm{q}}} \Pr[\textit{checks pass}] \leq \varepsilon, \tag{V.13}$$

where

$$\nu + \beta(1-\eta_{\mathsf{th}}) - \tilde{e}_{\mathsf{th}} + \gamma p_{\mathsf{mis,th}} = \sqrt{2V}\sqrt{\frac{\log_2(1/\varepsilon)}{N}} + \frac{\nu}{3}\frac{\log_2(1/\varepsilon)}{N}, \tag{V.14}$$

for any choice of dual variables $\beta,\gamma \leq 0$ and $\{\varphi_i\}_i$, and $\nu(\beta,\gamma,\{\varphi_i\}_i)$ is a function of dual variables in Eqn. (V.9) and V is chosen such that $V = \max\{\nu^2, (\nu+\min\{\beta,-1\}+\gamma)^2\}$.

Proof. Before we begin the analysis, it is convenient to define the random variables

$$C_i = \begin{cases} \beta, & z_{0,i} = \perp \\ 0, & z_{0,i} \neq \perp, z_{0,i} = s_i \\ -1, & z_{0,i} \neq \perp, z_{0,i} \neq s_i \end{cases} \tag{V.15}$$

and

$$T_i = \begin{cases} 0, & z_{0,i} = z_{1,i} \\ \gamma, & z_{0,i} \neq z_{1,i} \end{cases} \tag{V.16}$$

and

$$Y_i = \nu + C_i + T_i. \tag{V.17}$$

By the single-round tradeoff in Thm. V.3, the expectation value $\mathbb{E}[Y_i]$ is given by

$$\mathbb{E}[Y_i] = \nu + \beta(1-\eta_i) - \tilde{e}_i + \gamma p_{\mathsf{mis},i} \leq 0. \tag{V.18}$$

Since the tradeoff has to be obeyed by any adversary strategy in set $\mathcal{A}_{res,nl}$, this bound holds even when conditioned on past histories. This implies that $\mathbb{E}[Y_i|Y^{i-1}] \leq 0$. Proposition 11 of Ref. [14] states that when $\mathbb{E}[Y_i|Y^{i-1}] \leq 0$ for all $i \in \{1,\cdots,N\}$,

$$\Pr\left[\sum_i Y_i \geq N\delta\right] \leq \varepsilon \tag{V.19}$$

where

$$\delta = \sqrt{2V}\sqrt{\frac{\log_2(1/\varepsilon)}{N}} + \frac{Y_{max}\log_2(1/\varepsilon)}{3N} \tag{V.20}$$

and V is chosen such that $\mathbb{E}[(Y_i)^2|Y^{i-1}] \leq V$ and $Y_{max} = \max_i Y_i = \nu$, since $\beta,\gamma \leq 0$.

We expand the summation as

$$\sum_i Y_i = N\nu + \beta(N - N_{\mathrm{det}}) + \gamma N_{\mathrm{mis}} - N_{\mathrm{err}}. \tag{V.21}$$

Since the checks pass when $N_{\mathrm{mis}} \leq N p_{\mathsf{mis,th}}$, $N_{\mathrm{err}} \leq N e_{\mathsf{th}}$ and $N_{\mathrm{det}} \geq N\eta_{\mathsf{th}}$, we set

$$\delta = \nu + \beta(1-\eta_{\mathsf{th}}) - \tilde{e}_{\mathsf{th}} + \gamma p_{\mathsf{mis,th}} \tag{V.22}$$

to give

$$\Pr[-\beta N_{\mathrm{det}} + \gamma N_{\mathrm{mis}} - N_{\mathrm{err}} \geq -\beta N\eta_{\mathsf{th}} - N e_{\mathsf{th}} + \gamma N p_{\mathsf{mis,th}}] \leq \varepsilon. \tag{V.23}$$

Since passing all checks implies $\sum_{i=1}^N Y_i \geq N\delta$, we conclude that

$$\Pr[\textit{checks pass}] \leq \Pr\left[\sum_{i=1}^N Y_i \geq N\delta\right] \leq \varepsilon. \tag{V.24}$$

To choose V, we notice that $Y_i \in [\nu+\min\{\beta,-1\}+\gamma, \nu]$, since $\beta,\gamma \leq 0$. Therefore, $Y_i^2 \leq \max\{\nu^2, (\nu+\min\{\beta,-1\}+\gamma)^2\}$. As such, $\mathbb{E}[Y_i^2|Y^{i-1}] \leq \max\{\nu^2,(\nu+\min\{\beta,-1\}+\gamma)^2\}$ and it suffices to choose the RHS term as V. □

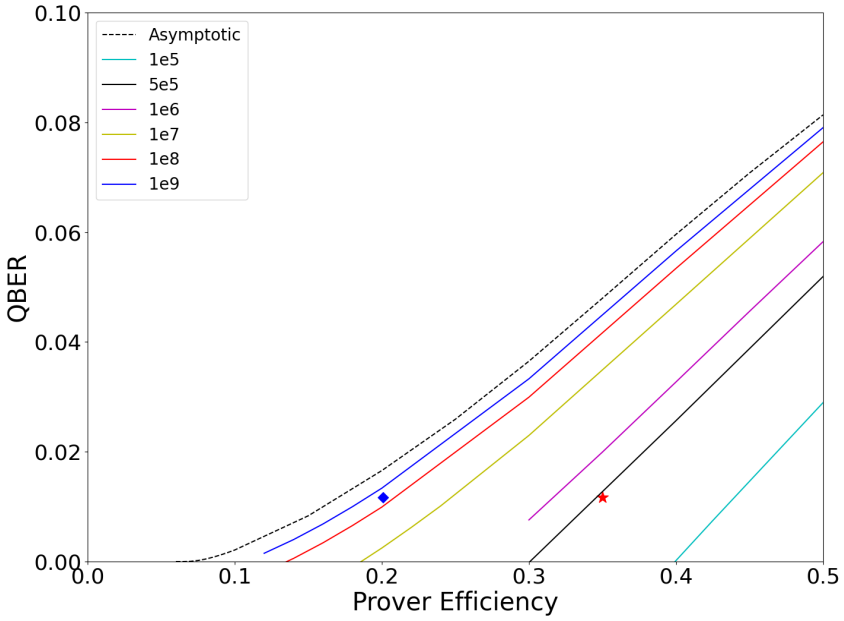


FIG. 5: Plot of QBER and prover efficiency regime secure against general QPV adversaries for $N = 10^5$ to $N = 10^9$ (represented by different colored lines) and in the asymptotic regime (dotted black line). The blue diamond represents the experimental performance and the red star represents the expected performance with improved end-to-end efficiency.

C. Numerical Simulation

We simulate the performance of the LT-QPV protocol against a general QPT adversary using the same set of parameters as the i.i.d. case in Sec. IV D. We run the simulation for $\varepsilon_{\text{sou}} = \varepsilon_{\text{com}} = 10^{-2}$ and split the completeness budget as $\varepsilon_{\text{com},\eta} = 0.1\varepsilon_{\text{com}}$, $\varepsilon_{\text{com,mis}} = 0.1\varepsilon_{\text{com}}$ and $\varepsilon_{\text{com,e}} = 0.8\varepsilon_{\text{com}}$.

The numerical simulation is performed in a similar manner to that described in Sec. IV D, where we seek to determine the QBER e that an honest implementation requires. We also use the same numerical tools as in Sec. IV D. At each η and p_{mis}, we compute η_{th} and $p_{\text{mis,th}}$ using the completeness bound in Thm. V.1. These can then be used to compute $\tilde{e}_{\text{th}}$, though the method of computing $\tilde{e}_{\text{th}}$ from η_{th} and $p_{\text{mis,th}}$ differs between the two soundness proofs. From $\tilde{e}_{\text{th}}$, we determine the effective error $e' = p_{\text{dc}} + (1 - p_{\text{dc}})e$ an honest implementation must achieve based on the completeness.

We compute e_{th} from Eqn. (V.4). We maximize e_{th} by optimizing the choice of dual variables, where different dual variable combinations are obtained by solving the SDP in Eqn. (V.9) at different $p_{\text{mis},i}$ and η_i. A larger e_{th} corresponds to a less stringent requirement on the honest prover.

The simulation results are shown in Fig. 5, with the SDP solved at NPA level $1 + AB$, where the AB operators are restricted to the 15 basis combinations corresponding to the closest bases. The number of rounds necessary to guarantee the same level of security is increased due to the generalization of the adversary. For the same experimental implementation, a run of the order of $N = 5 \times 10^8$ is required, compared to $N = 2.55 \times 10^5$ against an iid adversary. Improving the end-to-end efficiency to obtain an overall efficiency of 35% can significantly reduce the number of rounds by almost 3 orders of magnitude to $N = 5 \times 10^5$.

D. Reuse of Verifier Basis

In the experimental implementation, the verifier basis is reused across multiple rounds due to the slow rate of LCR. In general, this would be insecure against general adversaries which may capitalize on this basis correlation to gain an advantage. Consider the extreme example that only 16 blocks of bases (LCR only switches 16 times) are utilized. An adversary strategy where two colluding parties E_1 and E_2 located at V_0 and V_1 respectively first guess the basis

of each block, and has E_1 prepare quantum states V in that guessed basis and with bit value drawn from a shared random string with E_2, can spoof the prover's location if all basis guesses are correct. This implies that soundness against a general adversary is at least $(1/16)^{16}$, and cannot be reduced further for instance to be below 2^{-128}. There may be more sophisticated strategies that may impact the security analysis.

The key part of the analysis where basis reuse fails is the finite size analysis, where we argue that $\mathbb{E}[Y_i] \leq 0$ holds when conditioned on any past histories. This assumes that the basis is freshly chosen in the i-th round of the protocol and not correlated to the previous rounds. If the basis is reused between the $(i-1)$-th and i-th rounds, consider the described strategy where an adversary makes a guess of the basis in the $(i-1)$-th round, and use the same basis guess in the i-th round. The specific history where the $(i-1)$-th round basis guess is correct would imply that the i-th round basis guess is correct as well, and $\mathbb{E}[Y_i] > 0$ since the responses with be correct and without mismatch. If the verifier instead switches to independent per-round switching by using Pockels cell, the basis for every round is now independently chosen, and this recovers the finite-size analysis argument.

VI. ADVERSARY WITH IMPERFECT DEVICES

In our security analysis, the adversary is assumed to possess perfect quantum devices. However, in practice, they remain subjected to limitations on device performance. This introduces additional challenges for an adversary, potentially restricting the set of available strategies.

In LT-QPV, a key challenge for the adversary is to coordinate responses to both verifiers while maintaining a mismatch p_{mis} below the protocol threshold $p_{\mathsf{mis,th}}$. An honest prover can utilize classical communication which has minimal errors to satisfy the mismatch condition, while an adversary has to coordinate the responses from Alice and Bob. Consider the set of adversary strategies $\mathcal{A}_{res}$, in which Alice and Bob independently measure their respective quantum systems to generate responses z_0 and z_1. If the measurement devices have detection efficiency $\eta_{det} < 1$, each device produces a no-detection outcome $z_0 = \perp$ and $z_1 = \perp$ with probability $1 - \eta_{det}$. The independent losses on both sides directly contribute to mismatch. Even at a detector loss of 1%, the induced mismatch of approximately 2% significantly exceeds the typical $p_{\mathsf{mis,th}}$. Comparable effects may arise from other imperfections, such as imperfect state generation, and the extent of such deviations is strongly dependent on the adversary's implementation platform.

Consider an adversary that has access to detectors with $\eta_{det} < 1$ with no mismatch tolerance, $p_{\mathsf{mis,th}} = 0$. The resulting mismatch forces the adversary to forgo quantum measurements entirely and rely solely on classical communication. This reduces the set of adversary strategies to $\mathcal{A}_{cl}$, the set of classical strategies. Here, an adversary prepares a classical-quantum state $\rho_{VQ} = \sum_q p_q \left|q\right\rangle\!\left\langle q\right|_Q \otimes \rho_V^q$, where q is shared between Alice and Bob and V is a single qubit. The responses z_0 and z_1 are determined by Alice and Bob classically $z_0 = z_1 = g(q, \alpha)$ using the shared information q and the basis α.

This reduction raises a natural question: What parameter regimes, if any, does a gap exist between the set of restricted strategies $\mathcal{A}_{res}$ and the set of classical strategies $\mathcal{A}_{cl}$? Where such a gap exists, improved QPV performance can be established under a reasonable assumption that the adversary's devices are imperfect. In the parameter regimes where none exists, the computation of error tolerance can be significantly simplified. Since the classical strategy is fully described by the choice of qubit state ρ_V, the optimal error threshold can be computed by optimizing over ρ_V. We leave such an exploration for future work.

VII. EXPERIMENT

A. Quantum layer details

Before implementing the LT-QPV protocol, we thoroughly characterized the quantum layer of our experiment. Tables II and III show the efficiency of the transmission of the telecom and NIR transmission and detection apparatus. The SNSPDs used which have very low dark counts (< 5000 counts/s) and only dark counts falling within the 1.2ns coincidence/ROI window can affect a protocol round, giving a per-detector dark count probability of approximately $p_d < 6 \times 10^{-6}$. We also report the efficiency mismatch between the horizontal and vertical polarization channels in Table IV. The verifier-side (telecom) detector shows only a minimal difference between the two channels, which is fairly consistent with the detector model's assumption of balanced detection efficiency. We also note that this mismatch and the total transmission is consistent across all 16 basis since transmission through the Liquid Crystal does not depend on the basis choice. We note that in general, any imbalance on the verifier device between the detection efficiencies can be compensated by either artificially introducing loss in the SNSPD arm with higher transmission or randomly performing a 180 degree rotation of the basis to average out the mismatch in detection efficiencies.

TABLE II: Telecom efficiencies

Location	Step efficiency	Cumulative efficiency
After deployed fiber	0.81(4)	0.81(4)
After LCRs	0.87(5)	0.70(5)
After PBS	0.97(6)	0.68(5)
After SNSPD fiber	0.75(7)	0.51(6)
SNSPD quantum efficiency	0.805(5)	0.41(5)

TABLE III: NIR efficiencies

Location	Step efficiency	Cumulative efficiency
After delay line	0.93(5)	0.93(5)
After Pockels cell 1	0.97(6)	0.90(5)
After Pockels cell 2	0.98(6)	0.88(5)
After PBS	0.93(6)	0.82(5)
After SNSPD fiber	0.82(7)	0.67(6)
SNSPD quantum efficiency	0.765(5)	0.52(5)

B. Quantum Measurement Basis

The LT-QPV protocol requires that the prover and verifier measure half of an entangled photon pair. The prover performs a polarization measurement in the commanded basis, depending on the values x and y, out of 16 possible bases. The verifier also performs a polarization measurement on the other half of the entangled pair. To keep the positional uncertainty at a minimum, the prover must be able to change measurement basis rapidly. The speed constraints at the verifier are much less stringent. The optical design for the verifier polarization measurement is presented in Fig. 6, and consists of two back-to-back full-wave liquid crystal retarders (LCR). One is oriented with the slow axis at 0°, and the other at 45°. This configuration gives us the ability to explore the whole Poincaré sphere and thus produce all LT-QPV target states.

The optical design for the prover's measurement station is presented in Fig. 7. We meet the protocol's speed requirements by using fast-switching Pockels cells (RTP 4 mm, Leysop), controlled by a Field Programmable Gate Array (FPGA). The electronic driver (PCD-DPP, BME Bergmann) for each Pockels cell supports 4 input voltages, enabling 16 total basis combinations for our back-to-back Pockels cells. The Pockels cell slow axis is fixed at 45°, and by using a half-wave plate (HWP) and a quarter-wave plate (QWP), we are able to achieve all target states.

We characterize the prover's optical stack using a classical polarization tomography. The theoretical target states are presented in Fig. 8a, and our measured target states for the prover are presented in Fig. 8b. The optical fiber between the prover and the verifier introduces a unitary transformation to the transmitted telecom photons. Thus, we separately calibrate the LCR voltages that match each of the prover bases after the fiber rotation and confirm the shape of the bases constellation via state tomography. The exact basis vectors as observed by the verifier are shown in Fig. 8c, with the detailed list in Table V. The typical RMS Error of the tomography is 0.0055.

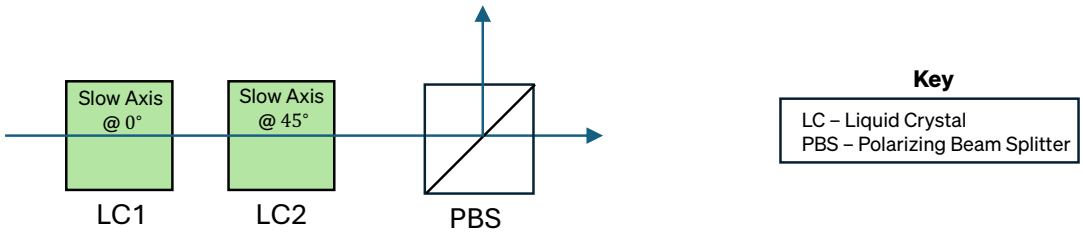


FIG. 6: Verifier Polarization Measurement Station consists of two Liquid Crystal (LC) rotators and a Polarizing Beam Splitter (PBS).

TABLE IV: Horizontal/Vertical mismatch

NIR	
Horizontal efficiency	0.61(5)
Vertical efficiency	0.64(5)
Telecom	
Horizontal efficiency	0.61(5)
Vertical efficiency	0.60(5)

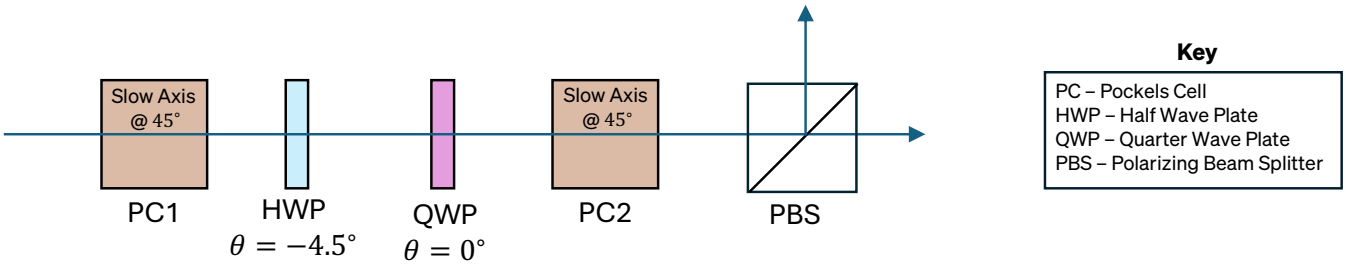
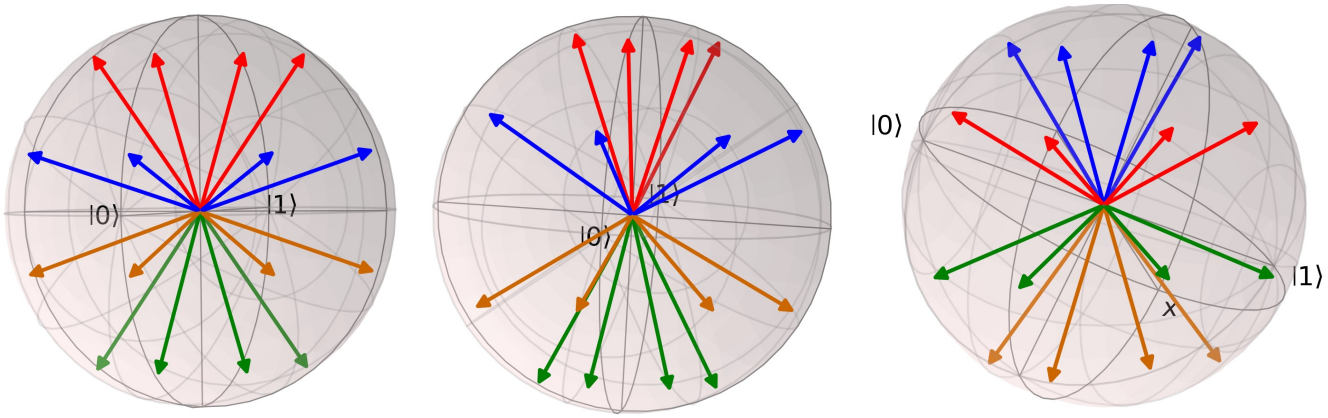


FIG. 7: Prover Polarization Measurement Station consists of two Pockels cells (PC) fast rotators, Half-Wave Plate (HWP), Quarter-Wave Plate (QWP), and Polarizing Beam Splitter (PBS).

C. Low-Latency Communications System

In order to successfully implement our LT-QPV protocol, we designed a custom low-latency communications link driven by FPGA devices over coaxial RF cables with high-propagation velocity (e.g., approximately 88% speed of light). For the LT-QPV protocol, the prover is connected to each verifier V_0 and V_1 with a custom low-latency communications link driven by AMD Zynq RFSoC FPGA's separated by approximately 35(2) m and 40(2) m, respectively.

The round-trip-time of a communication system depends on the transmission latency combined with the processing latency. The processing latency of each node is dependent on the signal routing within the FPGA fabric. For our protocol, we use the programmable logic firmware as the central control system for the low-latency link. To reduce processing latency, modulated electrical signals were generated and received using the high-performance general-purpose input/output (HP-GPIO) pins available at each node. Various dedicated hardware peripherals were tested for lowest latency performance with the GPIO 'bit banging' software-driven process offering the highest performance. Minimizing the processing latency is critical for executing the LT-QPV protocol without suffering unwanted delays which result in increased positional uncertainty. This low-latency HP-GPIO is used to transmit and receive the random challenges messages $x, y \in \{0,1\}^4$ using a hardware random number generator in the FPGA's programmable logic (PL) [16].



(a) (b) (c)

FIG. 8: State Constellation: (a) Ideal States, (b) Pockels Cell States, (c) Verifier States.

#	Prover basis	Verifier basis	Target basis
0	$0.8188\,\|H\rangle + (0.3711 + 0.4381i)\,\|V\rangle$ $0.5741\,\|H\rangle + (-0.5292 - 0.6247i)\,\|V\rangle$	$0.6429\,\|H\rangle + (0.7659 + 0.0099i)\,\|V\rangle$ $0.7660\,\|H\rangle + (-0.6428 - 0.0083i)\,\|V\rangle$	$0.7071\,\|H\rangle + (0.5721 + 0.4156i)\,\|V\rangle$ $0.7071\,\|H\rangle + (-0.5721 - 0.4156i)\,\|V\rangle$
1	$0.8343\,\|H\rangle + (0.0494 + 0.5492i)\,\|V\rangle$ $0.5514\,\|H\rangle + (-0.0747 - 0.8309i)\,\|V\rangle$	$0.6271\,\|H\rangle + (0.6339 - 0.4527i)\,\|V\rangle$ $0.7790\,\|H\rangle + (-0.5103 + 0.3644i)\,\|V\rangle$	$0.7071\,\|H\rangle + (0.2185 + 0.6725i)\,\|V\rangle$ $0.7071\,\|H\rangle + (-0.2185 - 0.6725i)\,\|V\rangle$
2	$0.8145\,\|H\rangle + (-0.3674 + 0.4490i)\,\|V\rangle$ $0.5802\,\|H\rangle + (0.5158 - 0.6303i)\,\|V\rangle$	$0.7405\,\|H\rangle + (0.1421 + 0.6569i)\,\|V\rangle$ $0.6721\,\|H\rangle + (-0.1566 - 0.7237i)\,\|V\rangle$	$0.7071\,\|H\rangle + (-0.2185 + 0.6725i)\,\|V\rangle$ $0.7071\,\|H\rangle + (0.2185 - 0.6725i)\,\|V\rangle$
3	$0.7849\,\|H\rangle + (-0.5693 + 0.2446i)\,\|V\rangle$ $0.6196\,\|H\rangle + (0.7212 - 0.3098i)\,\|V\rangle$	$0.7017\,\|H\rangle + (0.5001 + 0.5075i)\,\|V\rangle$ $0.7125\,\|H\rangle + (-0.4925 - 0.4998i)\,\|V\rangle$	$0.7071\,\|H\rangle + (-0.5721 + 0.4156i)\,\|V\rangle$ $0.7071\,\|H\rangle + (0.5721 - 0.4156i)\,\|V\rangle$
4	$0.8833\,\|H\rangle + (0.3454 + 0.3170i)\,\|V\rangle$ $0.4688\,\|H\rangle + (-0.6508 - 0.5972i)\,\|V\rangle$	$0.3929\,\|H\rangle + (0.9187 - 0.0397i)\,\|V\rangle$ $0.9196\,\|H\rangle + (-0.3926 + 0.0169i)\,\|V\rangle$	$0.8413\,\|H\rangle + (0.4808 + 0.2470i)\,\|V\rangle$ $0.5405\,\|H\rangle + (-0.7483 - 0.3845i)\,\|V\rangle$
5	$0.9317\,\|H\rangle + (0.0518 + 0.3594i)\,\|V\rangle$ $0.3632\,\|H\rangle + (-0.1328 - 0.9222i)\,\|V\rangle$	$0.4554\,\|H\rangle + (0.7012 - 0.5486i)\,\|V\rangle$ $0.8903\,\|H\rangle + (-0.3587 + 0.2806i)\,\|V\rangle$	$0.9145\,\|H\rangle + (0.1690 + 0.3677i)\,\|V\rangle$ $0.4047\,\|H\rangle + (-0.3818 - 0.8309i)\,\|V\rangle$
6	$0.9133\,\|H\rangle + (-0.2888 + 0.2872i)\,\|V\rangle$ $0.4073\,\|H\rangle + (0.6476 - 0.6440i)\,\|V\rangle$	$0.6653\,\|H\rangle + (-0.0088 + 0.7466i)\,\|V\rangle$ $0.7466\,\|H\rangle + (0.0078 - 0.6652i)\,\|V\rangle$	$0.9145\,\|H\rangle + (-0.1690 + 0.3677i)\,\|V\rangle$ $0.4047\,\|H\rangle + (0.3818 - 0.8309i)\,\|V\rangle$
7	$0.8567\,\|H\rangle + (-0.4840 + 0.1786i)\,\|V\rangle$ $0.5159\,\|H\rangle + (0.8037 - 0.2965i)\,\|V\rangle$	$0.5010\,\|H\rangle + (0.4064 + 0.7641i)\,\|V\rangle$ $0.8655\,\|H\rangle + (-0.2353 - 0.4423i)\,\|V\rangle$	$0.8413\,\|H\rangle + (-0.4808 + 0.2470i)\,\|V\rangle$ $0.5405\,\|H\rangle + (0.7483 - 0.3845i)\,\|V\rangle$
8	$0.9141\,\|H\rangle + (0.3849 + 0.1276i)\,\|V\rangle$ $0.4055\,\|H\rangle + (-0.8677 - 0.2876i)\,\|V\rangle$	$0.9570\,\|H\rangle + (0.1423 - 0.2528i)\,\|V\rangle$ $0.2901\,\|H\rangle + (-0.4693 + 0.8340i)\,\|V\rangle$	$0.8910\,\|H\rangle + (0.4540 - 0.0000i)\,\|V\rangle$ $0.4540\,\|H\rangle + (-0.8910 + 0.0000i)\,\|V\rangle$
9	$0.9939\,\|H\rangle + (0.0616 + 0.0912i)\,\|V\rangle$ $0.1100\,\|H\rangle + (-0.5562 - 0.8237i)\,\|V\rangle$	$0.8360\,\|H\rangle + (0.2026 - 0.5099i)\,\|V\rangle$ $0.5487\,\|H\rangle + (-0.3087 + 0.7770i)\,\|V\rangle$	$0.9877\,\|H\rangle + (0.1564 - 0.0000i)\,\|V\rangle$ $0.1564\,\|H\rangle + (-0.9877 + 0.0000i)\,\|V\rangle$
10	$0.9571\,\|H\rangle + (-0.2858 + 0.0479i)\,\|V\rangle$ $0.2898\,\|H\rangle + (0.9439 - 0.1581i)\,\|V\rangle$	$0.9219\,\|H\rangle + (-0.0351 + 0.3858i)\,\|V\rangle$ $0.3874\,\|H\rangle + (0.0835 - 0.9181i)\,\|V\rangle$	$0.9877\,\|H\rangle + (-0.1564 + 0.0000i)\,\|V\rangle$ $0.1564\,\|H\rangle + (0.9877 - 0.0000i)\,\|V\rangle$
11	$0.8884\,\|H\rangle + (-0.4566 + 0.0474i)\,\|V\rangle$ $0.4590\,\|H\rangle + (0.8837 - 0.0917i)\,\|V\rangle$	$0.9814\,\|H\rangle + (0.0595 + 0.1827i)\,\|V\rangle$ $0.1922\,\|H\rangle + (-0.3039 - 0.9331i)\,\|V\rangle$	$0.8910\,\|H\rangle + (-0.4540 + 0.0000i)\,\|V\rangle$ $0.4540\,\|H\rangle + (0.8910 - 0.0000i)\,\|V\rangle$
12	$0.8805\,\|H\rangle + (0.4627 - 0.1031i)\,\|V\rangle$ $0.4740\,\|H\rangle + (-0.8594 + 0.1916i)\,\|V\rangle$	$0.8777\,\|H\rangle + (0.4632 - 0.1230i)\,\|V\rangle$ $0.4793\,\|H\rangle + (-0.8483 + 0.2252i)\,\|V\rangle$	$0.8413\,\|H\rangle + (0.4808 - 0.2470i)\,\|V\rangle$ $0.5405\,\|H\rangle + (-0.7483 + 0.3845i)\,\|V\rangle$
13	$0.9510\,\|H\rangle + (0.0521 - 0.3047i)\,\|V\rangle$ $0.3091\,\|H\rangle + (-0.1604 + 0.9374i)\,\|V\rangle$	$0.7780\,\|H\rangle + (0.4330 - 0.4552i)\,\|V\rangle$ $0.6283\,\|H\rangle + (-0.5362 + 0.5637i)\,\|V\rangle$	$0.9145\,\|H\rangle + (0.1690 - 0.3677i)\,\|V\rangle$ $0.4047\,\|H\rangle + (-0.3818 + 0.8309i)\,\|V\rangle$
14	$0.9113\,\|H\rangle + (-0.3195 - 0.2597i)\,\|V\rangle$ $0.4117\,\|H\rangle + (0.7072 + 0.5747i)\,\|V\rangle$	$0.8563\,\|H\rangle + (0.1095 + 0.5047i)\,\|V\rangle$ $0.5165\,\|H\rangle + (-0.1816 - 0.8368i)\,\|V\rangle$	$0.9145\,\|H\rangle + (-0.1690 - 0.3677i)\,\|V\rangle$ $0.4047\,\|H\rangle + (0.3818 + 0.8309i)\,\|V\rangle$
15	$0.8706\,\|H\rangle + (-0.4783 - 0.1154i)\,\|V\rangle$ $0.4920\,\|H\rangle + (0.8463 + 0.2042i)\,\|V\rangle$	$0.9238\,\|H\rangle + (0.2814 + 0.2598i)\,\|V\rangle$ $0.3830\,\|H\rangle + (-0.6787 - 0.6267i)\,\|V\rangle$	$0.8413\,\|H\rangle + (-0.4808 - 0.2470i)\,\|V\rangle$ $0.5405\,\|H\rangle + (0.7483 + 0.3845i)\,\|V\rangle$

TABLE V: Basis states used in the experiment by the prover and verifier, and the ideal target basis. Each cell shows the two states in the basis. We note that the prover basis appears rotated relative to the verifier basis to compensate for rotations in the quantum channel.

Existing communication approaches, such as fiber-optic cable or coaxial cable, provide communication speeds slightly slower than the speed of light and cables often do not follow straight lines, both of which can add unacceptable latency. Future improvements to this link will involve utilizing the RFSoC's integrated Radio Frequency (RF) transceivers which can support classical radio signals to travel approximately at the speed of light through air and potentially in a direct line of sight. Current commercially available point-to-point radio links, however, have transmission and reception latencies that are too high to be of practical value for QPV.

D. Time Synchronization

We develop a custom time synchronization solution which combines low-latency communication and control that does not require access to additional dedicated hardware solutions such as White Rabbit [17]. Our approach starts with the Prover transmitting a ready message to each verifier indicating that they are ready to begin the next round. Upon receiving this message, the verifiers wait a custom time delay Δt_x and Δt_y and then transmit the challenge commands (x, y) to the Prover. Upon receiving the challenge commands, the prover immediately determines the basis and performs the measurement.

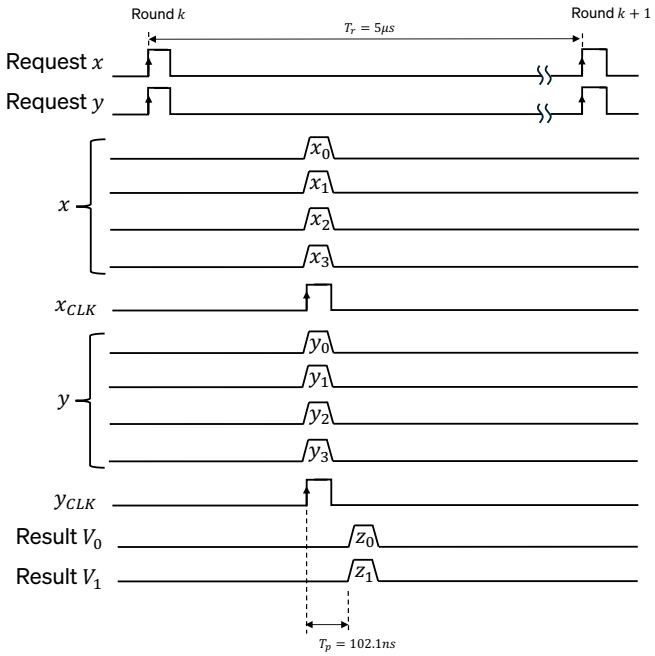


FIG. 9: Prover Timing Diagram. The prover begins each round by transmitting a request for challenge values x and y from Verifier 0, and 1, respectively. The verifiers transmit a 4-bit message for x and a 4-bit message for y along with data clock signals which are timed to arrive simultaneous at the prover's location. Upon, receiving x and y the prover uses a local i.i.d. table to determine the requested basis and perform the measurement. The measurement result is transmitted back to each verifier. The duration of time for the prover to perform the measurement is approximately 102.1 ns.

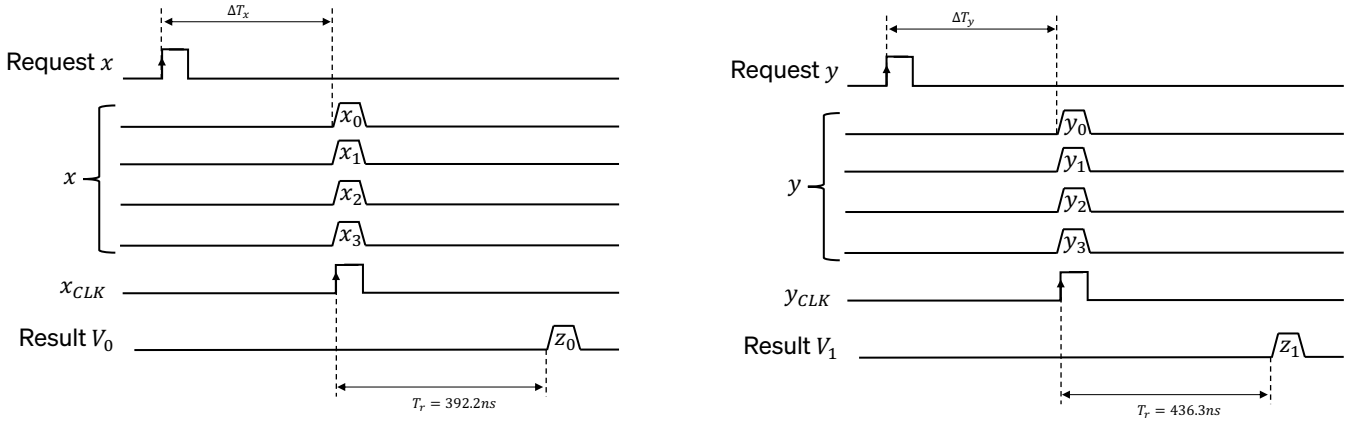


FIG. 10: Verifier Timing Diagram. After receiving the request for challenge messages x, y each verifier waits a predetermined time ΔT_x and ΔT_y before transmitting challenge messages x, y to the prover. The round-trip time between transmitting the challenge commands and receiving the measurement result is used to determine the positional uncertainty.

E. Positional Uncertainty

The final positional uncertainty of the prover depends on the round trip time from transmitting basis commands to the prover until each verifier receives a valid measurement response. This round trip time depends on the communication latencies and measurement latencies of the system. Specifically, each verifier can bound the prover's location within a radius from each verifier's location. Such radius is defined as $r_{V_0} = c \cdot (t_{z_0} - t_x)/2$, where t_x is the time Verifier 0 transmits basis commands and t_{z_0} is the time receiving an answer from the prover.

We measure the total round-trip delay time for V_0 to be 387.4 ns, and V_1 to be 431.3 ns, which corresponds to

a positional uncertainty of 58.1 m and 64.6 m, respectively. A latency budget for both V_0 and V_1 is presented in Tables VI and VII, respectively. We measure the RF cable delays by transmitting a signal down to the prover and measuring the response. The Region of Interest (ROI) is a user setting, which we select as 10 ns. The measured FPGA processing delay includes receiving the 4-bit value x and the 4-bit value y, clock signals X_{CLK} and Y_{CLK}, looking up the appropriate basis setting from the lookup table and transmitting the correct Pockels cells control sequence. The FPGA uses 1.8V logic; however, the Pockels cells requires 3.3V logic, which is implemented using external level shifters. The propagation delay time of the level shifters is measured to be 2.9ns. The Pockels cells driver delay and Pockels cells rise time are determined based on datasheet values. The SNSPD delay is measured to be 20 ns. Electrical patch cables interface with the high-propagation speed RF cables and the FPGA as well as the SNSPD to the high-propagation RF cables. Optical patch cables connect the free-space setup to the SNSPD, and the propagation delays represent the free-space photon transmission on the optical table as it passes through the Pockels cells and optical setup. We estimate the total measurement latency for V_0 (V_1) to be approximately 390 ns (432 ns), which corresponds to an estimated positional uncertainty of 58.4 m (64.8 m). This estimate is very close to our measured round-trip delay for V_0 (V_1) of 387.4 ns (431.3 ns), which corresponds to a measured positional uncertainty of 58.1 m (64.6 m).

Furthermore, we have verified the space-like separation between detection event at V_0 and the basis revelation. The quantum subsystem V is received by V_0 137 ns after y is sent by V_1, but that does not provide sufficient time for y to traverse the 66.5 m straight-line distance between V_0 and V_1, i.e. V is received before challenge y can arrive at V_0.

TABLE VI: LT-QPV Measurement Latency Budget (Verifier 0)

Node	Component	V_0 Latency (ns)	V_0 Positional Uncertainty (m)
Verifier 0	RF Cable Delays	277.5	41.6
Verifier 0	Region of Interest	10	1.5
Prover	FPGA Processing Delay	11.4	1.7
Prover	Level Shifter Delay	2.9	0.4
Prover	Pockels Cell Driver Delay†	30	4.5
Prover	Pockels Cell Rise Time†	1.5	0.2
Prover	SNSPD Delay	20	3.0
Prover	Misc. Electrical Cable Delays	22.2	3.3
Prover	Misc. Optical Patch Cable Delays	10.1	1.5
Prover	Misc. Optical Propagation Delays	4	0.6
Estimated Total Delay (V_0)		389.6	58.4
Measured Total Delay (V_0)		387.4	58.1

†Determined by datasheet.

TABLE VII: LT-QPV Measurement Latency Budget (Verifier 1)

Node	Component	V_1 Latency (ns)	V_1 Positional Uncertainty (m)
Verifier 1	RF Cable Delays	320.1	48.0
Verifier 1	Region of Interest	10	1.5
Prover	FPGA Processing Delay	11.4	1.7
Prover	Level Shifter Delay	2.9	0.4
Prover	Pockels Cell Driver Delay†	30	4.5
Prover	Pockels Cell Rise Time†	1.5	0.2
Prover	SNSPD Delay	20	3.0
Prover	Misc. Electrical Cable Delays	22.2	3.3
Prover	Misc. Optical Patch Cable Delays	10.1	1.5
Prover	Misc. Optical Propagation Delays	4	0.6
Estimated Total Delay (V_1)		432.2	64.8
Measured Total Delay (V_1)		431.3	64.6

†Determined by datasheet.

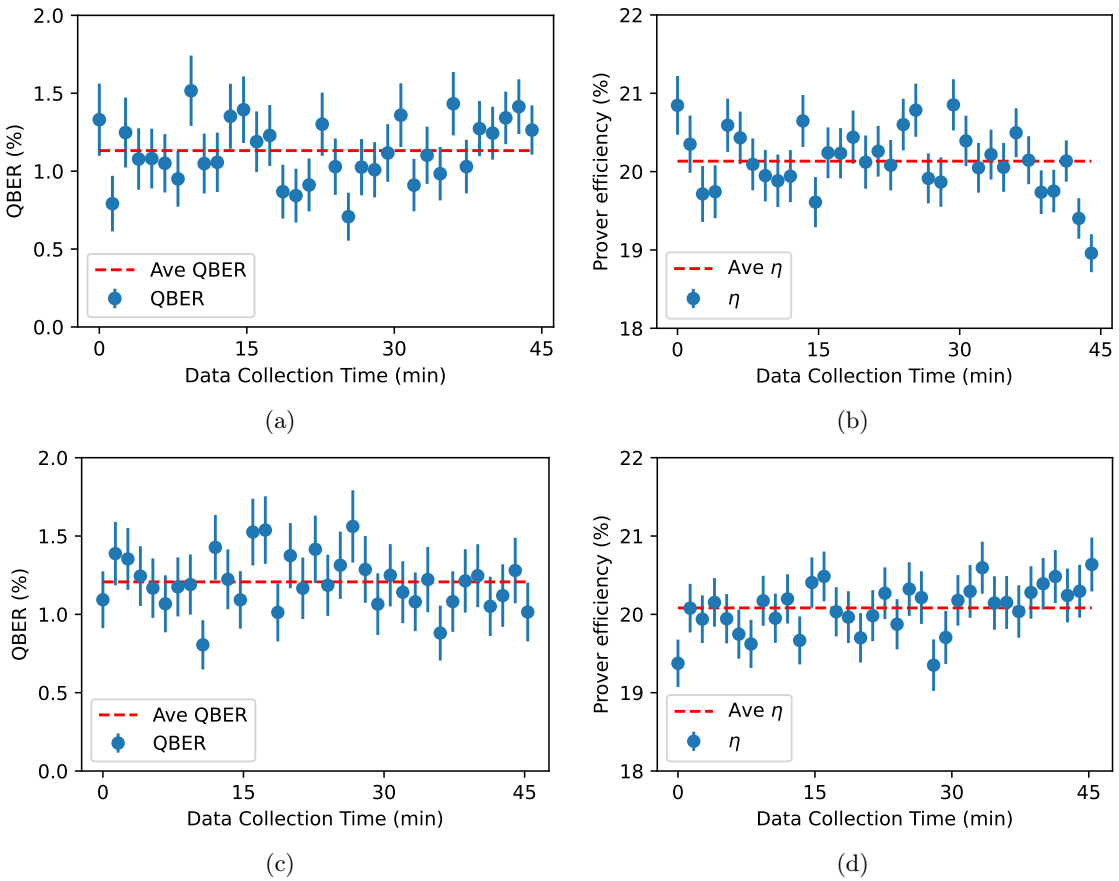


FIG. 11: System Performance: (a) QBER (Calibration), (b) Prover's local Efficiency (Calibration), (c) QBER (QPV Data Run), (d) Prover's local Efficiency (QPV Data Run).

F. Look-up Table

We have provided the full iid look-up table in Table VIII. We note that the look-up table is a randomly generated function used as an instantiation of the random oracle. Provided the adversary treats it as a black box, it behaves as a random function, and the non-uniform basis counts visible in the table are the statistical fluctuations expected of such a function. However, with $n = 4$, the domain has only 256 inputs and can be fully tabulated with a small number of queries, so the ϵ_{ROM} term is not meaningful for this instantiation. Guidance on choosing an appropriate instantiation and security parameter for deployment is given in Sec. IV C 2.

VIII. PROTOCOL COMPARISON

A. Comparison with QPV_m^η protocol with commitment at metropolitan distances

Of the previous implementations and loss tolerance proposals, the implementation by Fan Yuan et. al. [20], of the QPV_m^η protocol in Ref. [18] (a loss-tolerant version of the f-measure protocol [21] with slow quantum information), and whose channel loss tolerance can be provided through a commitment scheme [22] is a promising candidate for metropolitan area deployment. However, there remains two challenges in the near-term to such an implementation using only commercially available hardware. The first is that the current performance of the protocol scales poorly with increased number of basis. Fig. 12 shows that while loss tolerance can improve by increasing the number of bases, at realistic QBER of 0.27% [20], the protocol is insecure for transmission below 50%. We stress that this poor scaling is a consequence of the current security analysis and not an inherent property of the protocol itself. Recent security analysis results shows that the error tolerance of QPV_m^η can be improved significantly at zero loss [23], but it is not straightforwardly clear if this improvement extends to the lossy scenario. Analyzing the protocol using other methods

TABLE VIII: Prover Lookup i.i.d. Table

	Y-Value															
X-Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	6	3	12	14	10	7	12	4	6	9	2	6	10	10	7	4
1	3	7	7	2	5	4	1	7	11	13	5	1	15	11	4	0
2	11	9	5	12	11	8	0	10	10	14	9	15	11	11	15	14
3	13	13	14	13	2	11	6	3	15	8	2	4	2	6	4	8
4	6	1	3	8	11	13	1	9	8	9	4	1	3	11	14	11
5	6	11	12	7	14	2	13	0	3	1	7	3	1	13	5	5
6	9	3	5	12	14	1	9	11	1	9	13	3	13	14	15	14
7	7	13	6	11	8	13	7	4	15	12	1	14	4	7	9	8
8	11	11	11	12	8	12	14	12	0	8	6	8	7	0	11	7
9	7	14	10	2	0	7	2	2	0	10	4	9	6	9	8	11
10	6	8	7	11	1	0	15	6	6	13	7	4	2	11	7	5
11	10	2	0	2	4	14	13	2	0	4	9	6	14	13	6	10
12	8	14	14	9	9	11	12	2	14	15	6	0	3	12	15	3
13	13	4	6	6	12	14	10	12	3	12	15	6	10	2	5	11
14	1	9	12	13	8	4	5	11	11	11	11	3	13	13	10	15
15	9	6	11	8	6	13	0	0	8	10	13	8	3	12	8	2

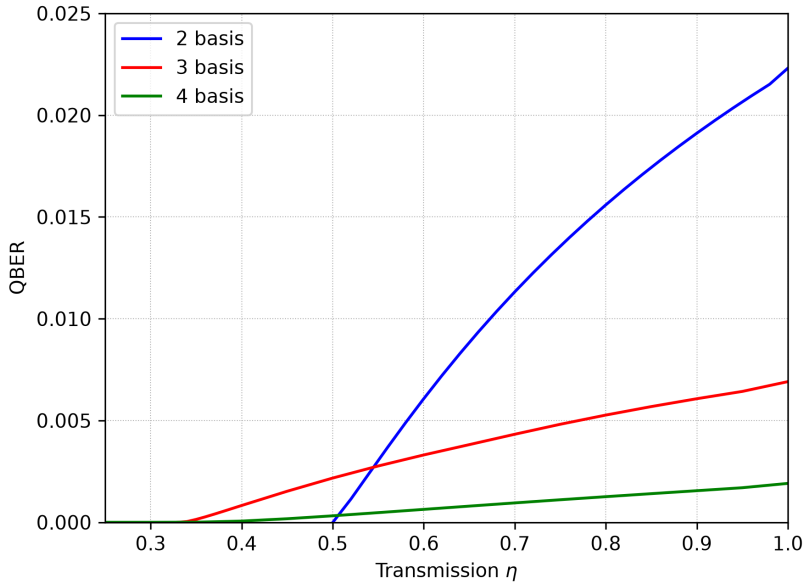


FIG. 12: **Asymptotic Performance of QPV_m^η [18].** Performance of QPV_m^η protocol [18] in the asymptotic regime, using the tighter bounds presented in Ref. [19] at NPA level 1+AB (2/3 basis) and level 1 (4 basis). While the protocol can achieve loss tolerance of $\eta \sim 1/m$ in principle at zero QBER, at the current QBER in Fan Yuan et. al.'s implementation [20] of 0.27%, which uses coherent states instead of the ideal qubit state, the transmission η required still exceeds 50%.

such as under QROM [24] may also significantly increase the performance. The second challenge is the implementation of the commitment scheme proposed in Ref. [22], where a quantum non-demolition measurement is performed by the prover to commit to whether a qubit has been received before the basis is received. In practice, this is implemented via a quantum teleportation or entanglement swapping scheme, where the prover uses an entanglement source and Bell state measurement to teleport the received quantum state, and a Bell state measurement success would indicate the receipt of a qubit. Such an implementation presents four potential issues. Firstly, having a Bell state measurement can introduce a larger QBER that may be beyond the current performance requirements of QPV_m^η or require high transmission to remain secure. Secondly, the heralding efficiency of a commercially available entanglement source and detection efficiency at the prover side may result in a low prover-side efficiency (e.g. at 20% if our system is

used) that is below the current performance requirements of QPV_m^η. Thirdly, the use of coherent states may not be directly compatible with the proposed commitment scheme to achieve full loss-tolerance due to photon-number splitting attack. By post-selecting and committing only on multi-photon events, QPV_m^η is no longer secure since the adversaries have access to more than one copy of the same state. Limits on the channel loss or other techniques such as decoy-state [25] may have to be introduced to combine the commitment scheme with a coherent state implementation. Lastly, if classical communication does not occur at the speed of light (e.g. if coaxial cables are used), the scheme loses its fully channel loss-tolerance property since the qubit from the entanglement source at the prover have to be stored for a duration that scales linearly with the prover-verifier separation – a challenge that our protocol also faces. We note that classical information is easier to transmit at close to the speed of light than quantum information, so achieving full channel-loss tolerance with our protocol, which requires both classical and quantum communication to be at the speed of light, is more challenging in this respect. While an implementation of loss-tolerant version of this proposal is challenging with current hardware, future advances in theoretical analysis and better commercial hardware makes this a promising candidate for loss-tolerant QPV.

In comparison, while our proposal is fully channel-loss tolerant only when classical and quantum communication travel at the speed of light, it is channel-loss tolerant in the sense of Sec. IV C 3 and provides a sufficient level of reach relative to QPV_m^η [18] and Fan Yuan et. al.'s demonstration [20], while at the same time being simpler to implement than the commitment scheme. While the use of a QROM model in our security analysis adds computational assumptions to the protocol, it provides better performance requirements, allowing the protocol to be scaled to 16 basis while maintaining reasonable requirements on error tolerance. This eases the implementation with commercial hardware. To provide further loss-tolerance, our scheme requires the prover prepare an entangled state, and the verifier's measurement serves as a commitment indicating that a qubit has been received through the channel, serving a similar role as the commitment scheme in Ref. [22] where the commitment is performed on the prover side. Compared to Ref. [22], our proposal removes the requirement of a Bell-state measurement, which can raise QBER significantly and is more challenging to implement and achieve security especially when prover-side efficiency is not high. As such, our scheme serves as a good in-between, trading off the level of channel-loss tolerance guarantee of Ref. [22] for the ease of implementation.

B. Comparison with other implementations

Table IX compares the experimental implementation and theoretical guarantees of our protocol and Ref. [4, 20, 26].

C. Scaling Performance with System Upgrades

Table X summarizes the scaling performance for our current system and several potential system upgrades. The starting end-to-end efficiency takes into account all system efficiencies including the entanglement source heralding efficiency, coupling optics efficiency, storage fiber transmission efficiency, and detector efficiencies, etc.

TABLE IX: Comparison of our proposal with recent experimental implementations. For Ref. [4, 20], we present the loss tolerance assuming zero QBER / perfect fidelity of state preparation.

	Kavuri et al. [4] [a]	**Fan-Yuan et al. [20]**	**Kanneworff et al. [26]**	**Our Proposal**
Adversary Model	Small amount of shared entanglement	Linear amount of shared entanglement	No shared entanglement	Polynomial amount of resource (including entanglement)
Trust (Quantum Device)	Not required	State preparation	State preparation	Measurement
Efficiency Requirement (Asymptotic)	Transmission $> 66\%$	Transmission $> 50\%$	Fully loss-tolerant	Prover-side transmission $> 16\%$
Verifier Resource	Pockels Cell + SNSPD	Coherent state source + Modulators	Quantum Dot Source + Modulator	Pockels Cell + SNSPD
Challenge Length	1 bit each (2 basis)	20 bits each (2 basis)	NA (quantum challenge)	4 bits each (16 basis)
End-to-End Efficiency	$> 81\%$	$\sim 70\%$	7.2–12.4%	$\sim 20\%$ (prover-side)
Classical Channel	Coaxial Cable (~ 0.85–$0.87\,c$)	Hollow-core fiber (near c)	Not implemented	Coaxial Cable ($\sim 0.88\,c$)
Prover–verifier separation	$\sim$100 m	0.98 km	200 m	35–40 m
Localization Metric	Area uncertainty $\sim 1/4\times$ of classical, Position uncertainty $\sim$ 116–157 m	Position uncertainty $\sim$ 75 m	NA	Position uncertainty $\sim$ 60 m
Soundness Parameter ε_{sou}	2^{-64}	5×10^{-10}	NA (insecure)	10^{-2} (iid adversary)
Acquisition Time	2 min	5 s	NA (insecure)	22 min (iid adversary)

[a] A commitment extension of this protocol was proposed in a later version of the manuscript, but it is not part of the demonstrated implementation.

TABLE X: Scaling performance of the current system and potential upgrades. Abbreviations: Near Infrared (NIR), Ultra-Low Loss (ULL), Heralding Efficiency (HE), and Hollow Core Fiber (HCF).

Configuration	Starting End-to-End Efficiency (%)	Prover Storage Fiber Loss (dB/km)	Quantum Propagation Speed	Classical Propagation Speed	Max Distance (km)
Current system as-is	20.1%	4	$(2/3)\cdot c$	$0.88\cdot c$	0.6 km
Upgrade: Swap NIR and Telecom Fibers	22.5%	0.35	$(2/3)\cdot c$	$0.88\cdot c$	10.0 km
Upgrade: 81% Efficiency and ULL fiber	81%	0.142	$(2/3)\cdot c$	$0.88\cdot c$	117 km
Upgrade: 70% HE and use Future HCF	32.7%	0.142	$0.99\cdot c$	$0.99\cdot c$	1,094 km

D. Quantum-Advantage Ratios: Construction and Calculation

This subsection (illustrated in Fig. 13) gives the geometric construction behind the quantum-advantage ratios quoted in the main text (2.18, 2.44 and 2.67 in one, two and three spatial dimensions), the definition of the matched classical comparison, and the calculation of each ratio. All inputs are taken from the measurements of the present apparatus.

a. Inputs. Verifiers V_0 and V_1 are separated by $L = 66.5$ m along a straight line, which we take as the x-axis with V_0 at $x = 0$ and V_1 at $x = L$. The measured round-trip times between transmitting the challenge and receiving the response are $T_0 = 387.4$ ns and $T_1 = 431.3$ ns (Tables VI and VII). A prover that answers verifier V_i within T_i must lie within distance

$$r_i = \frac{c\,T_i}{2} \tag{VIII.1}$$

of V_i, which gives $r_0 = 58.1$ m and $r_1 = 64.6$ m. Here c is the speed of light in free space, so r_i is the largest distance

consistent with causality and is independent of the cable velocity factor.

b. Quantum (LT-QPV) region. A prover that passes the protocol must satisfy the timing constraints of both verifiers. Its location is therefore confined to the intersection of two balls,

$$Q \;=\; B(V_0, r_0) \,\cap\, B(V_1, r_1). \tag{VIII.2}$$

Since $|r_0 - r_1| < L < r_0 + r_1$, the region Q is a lens. It does not contain either verifier. Its boundary spheres meet in a circle in the plane

$$x_0 = \frac{L^2 + r_0^2 - r_1^2}{2L} = 27.3 \text{ m}, \tag{VIII.3}$$

of radius $h = \sqrt{r_0^2 - x_0^2} = 51.3$ m. Along the verifier axis, Q spans $x \in [L - r_1,\, r_0] = [1.9,\, 58.1]$ m.

c. Matched classical region. The classical comparison is a classical position-verification protocol in which the verifiers use the same challenge and response times and the same latencies, so the timing windows T_0 and T_1 are identical to those of the quantum protocol. Such a protocol is vulnerable to two colluding adversaries, each of whom holds one of the challenges and forwards it to the other. The adversaries succeed from any location from which a challenge sent by one verifier can be received, processed and returned to the other verifier within the same time budget. Let s_0 and s_1 be the times at which V_0 and V_1 send their challenges, and let $D = c\,(s_1 - s_0)$. Following [4], the set of such locations is

$$C \;=\; \big(B(V_0, r_0) \cap E_3\big) \;\cup\; \big(B(V_1, r_1) \cap E_4\big), \tag{VIII.4}$$

where E_3 and E_4 are the prolate spheroids with foci at V_0 and V_1,

$$E_3 = \big\{X :\; |XV_0| + |XV_1| \le 2r_0 - D\big\}, \qquad E_4 = \big\{X :\; |XV_0| + |XV_1| \le 2r_1 + D\big\}. \tag{VIII.5}$$

The first (second) term is the set of positions from which an adversary can answer V_0 (V_1) in time, using the challenge forwarded by the other verifier's nearby adversary. In the present apparatus the challenges are timed to arrive simultaneously at the prover, so $D = (d_{V_0P} - d_{V_1P})/\beta_{\rm cl} = (35 - 40)/0.88 \approx -5.7$ m, where d_{V_iP} are the cable lengths from V_i to the prover and $\beta_{\rm cl}$ is the velocity factor. Along the verifier axis, C spans $x \in [-27.7,\, 95.0]$ m, a length of $r_0 + r_1 = 122.7$ m. Unlike Q, the region C always contains the segment V_0V_1 and both verifier locations. This is the sense in which a classical protocol cannot localize a prover remotely, and it holds even if the latencies are zero [4]. For this timing the quantum target region of [4], $B(V_0, r_0) \cap B(V_1, r_1) \cap E_3 \cap E_4$, coincides with the lens Q of eqn. (VIII.2), because E_3 and E_4 contain the lens.

d. Definition of the ratio. Following [4], the quantum-advantage ratio in d dimensions is

$$\mathrm{QA}_d = \frac{\mathrm{size}_d(C)}{\mathrm{size}_d(Q)}, \tag{VIII.6}$$

where size_d is length ($d = 1$), area ($d = 2$) or volume ($d = 3$). The ideal classical protocol with zero latency has $C = V_0V_1$ (length L). The comparison of Eqn. (VIII.6) is instead against a classical protocol with the *same* latencies as the implemented quantum protocol.

e. Calculation. In $d = 1$ the regions are intervals on the verifier axis,

$$\mathrm{size}_1(Q) = r_0 + r_1 - L = 56.2 \text{ m}, \qquad \mathrm{size}_1(C) = r_0 + r_1 = 122.7 \text{ m}. \tag{VIII.7}$$

In $d = 2$ we restrict to a plane that contains the verifier axis. The region Q is a lens formed by two overlapping disks, with area

$$\begin{aligned} A_Q = {} & r_0^2 \arccos\frac{L^2 + r_0^2 - r_1^2}{2Lr_0} + r_1^2 \arccos\frac{L^2 + r_1^2 - r_0^2}{2Lr_1} \\ & - \tfrac{1}{2}\sqrt{(-L + r_1 + r_0)(L + r_1 - r_0)(L - r_1 + r_0)(L + r_1 + r_0)}, \end{aligned} \tag{VIII.8}$$

and the area of C is evaluated numerically from eqn. (VIII.4). In $d = 3$ the region Q is the lens formed by two overlapping balls, with volume

$$V_Q = \frac{\pi\,(r_0 + r_1 - L)^2\,\big(L^2 + 2Lr_1 - 3r_1^2 + 2Lr_0 + 6r_0r_1 - 3r_0^2\big)}{12\,L}, \tag{VIII.9}$$

and the volume of C is the volume of revolution of the two-dimensional region about the verifier axis, also evaluated numerically (grid integration, converged to better than 0.1%). Table XI lists the resulting sizes and ratios.

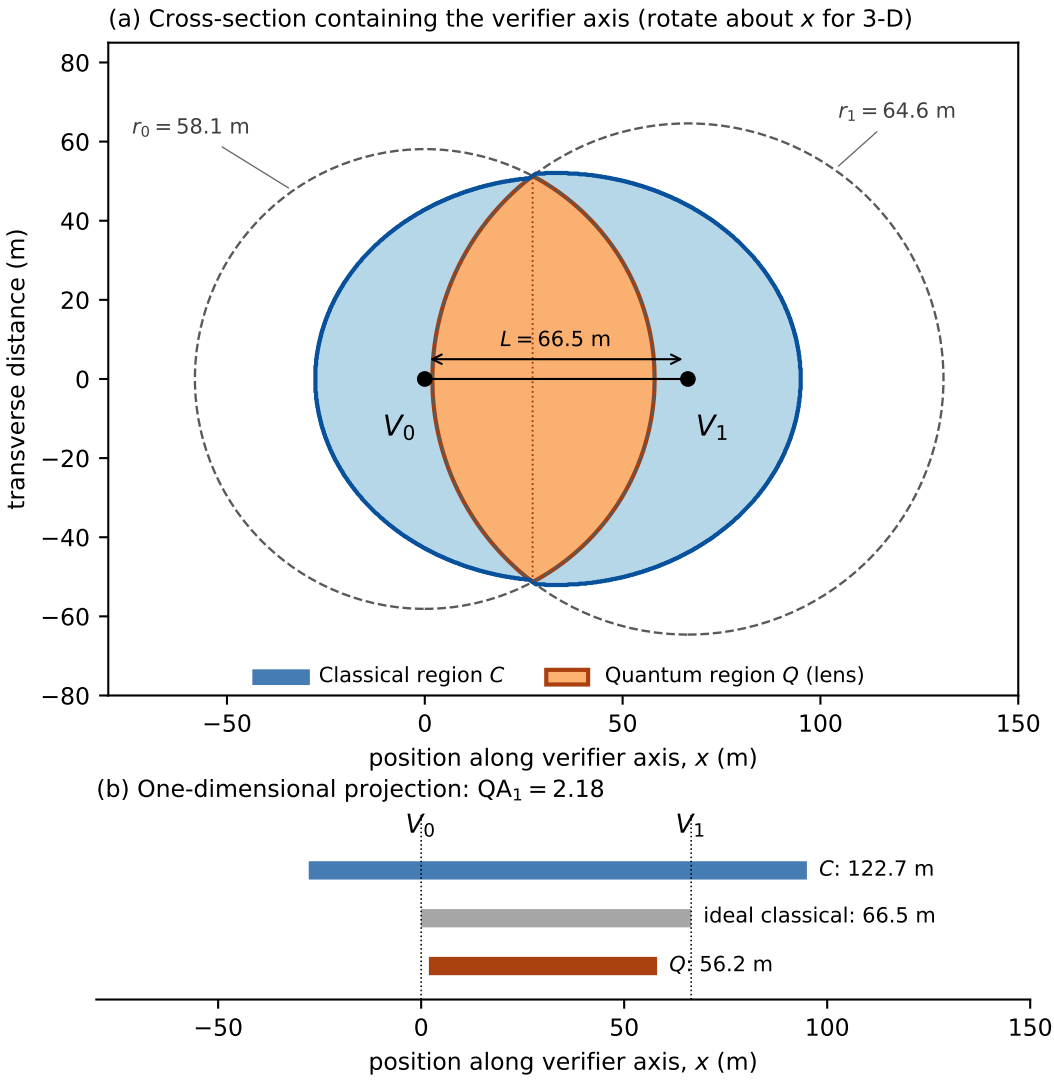


FIG. 13: Construction of the quantum-advantage ratios for the measured geometry ($L = 66.5$ m, $r_0 = 58.1$ m, $r_1 = 64.6$ m). (a) Cross-section in a plane containing the verifier axis. The quantum region Q (orange) is the intersection of the two balls of radii r_0 and r_1 about V_0 and V_1 (dashed circles), and does not contain the verifiers. The matched-latency classical region C (blue) is the union of the two sphere–spheroid intersections of eqn. (VIII.4), and contains both verifiers. Rotating the cross-section about the verifier axis gives the three-dimensional regions. (b) Projection onto the verifier axis, with Q of length 56.2 m, C of length 122.7 m, and the ideal zero-latency classical region (the segment V_0V_1) shown for reference. Figure drawn to scale.

f. What is measured and what is derived. The inputs L, T_0 and T_1 (and hence r_0 and r_1) are measured on the present apparatus. The one-dimensional ratio is evaluated along the verifier axis, which is the configuration in which the experiment was operated and for which the security analysis is given. The two- and three-dimensional ratios are geometric extensions: they assume that the same measured timing bounds apply in the directions transverse to the verifier axis, so that Q and C are the figures of revolution of the one-dimensional construction about that axis. We did not perform a measurement with verifiers or a prover displaced from the axis, and we do not claim a security proof in two or three dimensions here. These ratios therefore characterize the localization permitted by the measured timing and geometry, and they should not be read as separately demonstrated advantages. The ratios also depend only on

TABLE XI: Quantum-advantage ratios for the measured geometry ($L = 66.5$ m, $r_0 = 58.1$ m, $r_1 = 64.6$ m). The classical region is the matched-latency region of Eqn. (VIII.4) with $D = -5.7$ m; the quantum region is the lens of Eqn. (VIII.2).

Dimension	Quantum region Q	Classical region C	QA_d
1-D (length)	56.2 m	122.7 m	2.18
2-D (area)	4.07×10^3 m^2	9.95×10^3 m^2	2.44
3-D (volume)	2.56×10^5 m^3	6.85×10^5 m^3	2.67

L, r_0 and r_1, so they improve as the round-trip latencies are reduced.

[1] 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).

[2] Bennett, C. H., Bernstein, E., Brassard, G. & Vazirani, U. Strengths and weaknesses of quantum computing. *SIAM journal on Computing* **26**, 1510–1523 (1997).

[3] Zhandry, M. Secure identity-based encryption in the quantum random oracle model. *International Journal of Quantum Information* **13**, 1550014 (2015).

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

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

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

[7] 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).

[8] 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).

[9] 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).

[10] Wang, Y., Primaatmaja, I. W., Lavie, E., Varvitsiotis, A. & Lim, C. C. W. Characterising the correlations of prepare-and-measure quantum networks. *npj Quantum Inf.* **5**, 17 (2019).

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

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

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

[14] Himbeeck, T. V. & Pironio, S. Correlations and randomness generation based on energy constraints (2019). arXiv: 1905.09117.

[15] Boyd, S. & Vandenberghe, L. *Convex Optimization* (Cambridge University Press, 2004).

[16] Rosales, D. E. S. *Design and Development of a Quantum Key Distribution System for Highly Mobile Platforms and Its Implementation on Drones and Cars* (The Ohio State University, 2024).

[17] Lipiński, M., Włostowski, T., Serrano, J. & Alvarez, P. White rabbit: A ptp application for robust sub-nanosecond synchronization. In *2011 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication*, 25–30 (IEEE, 2011).

[18] 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).

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

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

[21] 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).

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

[23] 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.

[24] 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).

[25] Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).

[26] Kanneworff, K. *et al.* Towards experimental demonstration of quantum position verification using single photons. *Quantum*

953 *Science and Technology* **10**, 045004 (2025).