UNIVERSITY OF AMSTERDAM

UvA-DARE (Digital Academic Repository)

Making Existing Quantum Position Verification Protocols Secure Against Arbitrary Transmission Loss

Allerstorfer, Rene; Bluhm, Andreas; Buhrman, Harry; Christandl, Matthias; Escolà-Farràs, Llorenç; Speelman, Florian; Verduyn Lunel, Philip

DOI
10.1103/szwj-s7r6

Publication date
2025

Document Version
Final published version

Published in
Physical Review Letters

License
CC BY

Link to publication

Citation for published version (APA):
Allerstorfer, R., Bluhm, A., Buhrman, H., Christandl, M., Escolà-Farràs, L., Speelman, F., & Verduyn Lunel, P. (2025). Making Existing Quantum Position Verification Protocols Secure Against Arbitrary Transmission Loss. *Physical Review Letters*, *135*(26), Article 260801. https://doi.org/10.1103/szwj-s7r6

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, P.O. Box 19185, 1000 GD Amsterdam, The Netherlands. You will be contacted as soon as possible.
UvA-DARE is a service provided by the library of the University of Amsterdam (https://dare.uva.nl)

Download date:05 Sept 2026

Making Existing Quantum Position Verification Protocols Secure Against Arbitrary Transmission Loss

Rene Allerstorfer,[1,2,*] Andreas Bluhm,[3,†] Harry Buhrman,[2,4,5,‡] Matthias Christandl,[6,§] Llorenç Escolà-Farràs,[2,5,‖] Florian Speelman,[2,5,¶] and Philip Verduyn Lunel[1,2,7,**]

[1]*CWI Amsterdam, CWI, Amsterdam, The Netherlands*
[2]*QuSoft, Amsterdam, The Netherlands*
[3]*Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG, Grenoble, France*
[4]*Quantinuum, Partnership House, Carlisle Place, London, United Kingdom*
[5]*University of Amsterdam, Amsterdam, The Netherlands*
[6]*University of Copenhagen, Copenhagen, Denmark*
[7]*Sorbonne Université, CNRS, LIP6, Paris, France*

(Received 2 February 2024; revised 22 July 2025; accepted 13 November 2025; published 22 December 2025)

Signal loss threatens the security of quantum cryptography, especially in quantum position verification (QPV) protocols, where even small losses can compromise security. This Letter modifies traditional QPV to make high transmission loss between verifiers and the prover irrelevant for a class of protocols, including a practically interesting one based on BB84 states ($\mathrm{QPV}^{f}_{\mathrm{BB84}}$). Using photon presence detection and a small time delay, as well as a commitment before proceeding, the protocol's relevant loss rate is reduced to only that of the prover's lab, and the modified protocol has essentially the same security guarantees as the original one. The adapted protocol $\mathsf{c}\text{-}\mathrm{QPV}^{f}_{\mathrm{BB84}}$ thus offers strong security guarantees and feasibility over longer distances. We also discuss the practical implementation of the protocol and parameter estimates.

DOI: 10.1103/szwj-s7r6

Introduction—Imagine the following situation: you are sitting in front of your computer screen, and you see an image or a video online. One way to verify that it is authentic, rather than fake or created by powerful AI, would be to unambiguously verify *where* it was created. Or, as recently reported [1], fraudsters could deepfake some of your business partners in a video call, including their offices in the background, in order to trick you into transferring money to them. This, for example, could be prevented if each participant in the call (later on referred to as *prover*) had a secure and verified location tag, as it should be difficult to enter the company's offices without permission. To create such a tag (with the help of trusted verifier nodes), each participant could use quantum position verification (QPV), certifying that the data that their video consists of was created at the claimed location. QPV could also be used as a tool to create position-based quantum-secure keys [2].

Securely verifying the position of a party—where a coalition of trusted verifiers aims to verify the claimed location of an untrusted party—is unachievable using fully classical protocols, even under computational assumptions, due to the existence of a general attack based on copying the classical information [3]. The no-cloning theorem for quantum states [4] bypasses the general classical attack if quantum information is used instead, motivating the study of quantum position verification [5–8]. A general quantum attack exists [2,9]—when adversaries not at the claimed location are accepted—but consumes an exponential amount of entanglement in the resources required for an honest implementation. The extraordinarily large amount of entanglement required for this attack raises hope for the existence of protocols that are secure against realistically bounded attacks. Indeed, there has been much work on attacks for specific protocols [6,10–23] and security analysis with extra cryptographic assumptions [24,25] or in the random oracle model [26], as well as the first experimental demonstration in [27].

QPV protocols rely on both relativistic constraints and the laws of quantum mechanics. A generic QPV protocol, for simplicity in one dimension (1D) is described in the following way: two trusted verifiers V_0 and V_1, placed on the left and right of an untrusted prover P, respectively, send quantum or classical messages to her at the speed of

*Contact author: rene.allerstorfer@icloud.com
†Contact author: Andreas.Bluhm@univ-grenoble-alpes.fr
‡Contact author: h.m.buhrman@uva.nl
§Contact author: christandl@math.ku.dk
‖Contact author: llorensescola@gmail.com
¶Contact author: f.speelman@uva.nl
**Contact author: Philip.Verduyn-Lunel@lip6.fr

Published by the American Physical Society under the terms of the Creative Commons Attribution 4.0 International license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

light. The prover has to complete a task using the received information and reply correctly to the verifiers at the speed of light as well. The verifiers accept if the prover's response to the task is correct and the timing corresponds to the time it would have taken for signals to travel back from the honest prover; see Fig. 1(a) for a schematic representation of the $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ protocol, described below. These ideas extend to the 3D setup [10], and geometric constraints can be overcome by adding more verifier stations [10,26].

The three properties that are crucial for a QPV protocol to be feasible are security against bounded attackers, security with slow quantum information, and resistance to signal loss. The first property concerns security against attackers who share a limited amount of entanglement, since complete security is impossible if the amount of preshared entanglement is unbounded, even under perfect execution of the protocols. The latter two problems, by contrast, arise from current experimental constraints. Whereas the transmission of classical information at the speed of light is technologically feasible in an almost lossless fashion, e.g., via radio waves, the quantum counterpart faces obstacles. First, most QPV protocols require quantum information to be transmitted at the speed of light in vacuum, but for practical applications this is often unattainable. The speed of light in optical fibers is significantly lower than in vacuum. Moreover, in a future quantum network with fibers, it may often be the case that there is no straight point-to-point connection between the verifiers and the prover, delaying transmission compared to a straight-line path. This opens up a possible attack where there is enough time for attackers to communicate. Second, a sizable fraction of photons will be lost in transmission in practice. In optical fibers, this loss grows exponentially with the distance. This, in turn, would allow attackers to apply loss-dependent attacks, which can completely break a protocol [28].

None of the previously studied QPV protocols possess all three of these properties simultaneously at a useful scale. Any protocol that was able to solve one or two of the mentioned issues had shortcomings regarding the other(s). The $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ protocol that we discuss below satisfies all of them, but only for relatively small distances [29]. If one wants to implement QPV in a future quantum internet, the goal would be for QPV to work over essentially arbitrarily long distances. In this Letter, we present a solution to this problem, and we show that, by slightly modifying the structure of $\mathrm{QPV}^{f}_{\mathrm{BB84}}$, one obtains a protocol that is fully loss tolerant, therefore satisfying all three properties simultaneously. In addition, this modification applies to a broader class of QPV protocols; see SM [30] for further details. Finally, we analyze possible experimental implementations, showing the practical feasibility of our results.

The $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ *protocol*—Let f be a publicly known Boolean function. A round of $\mathrm{QPV}^{f}_{\mathrm{BB84}}$, introduced in [6] and studied in [18,29,39], consists of the verifiers encoding a random bit v in a BB84 state, sending this qubit and

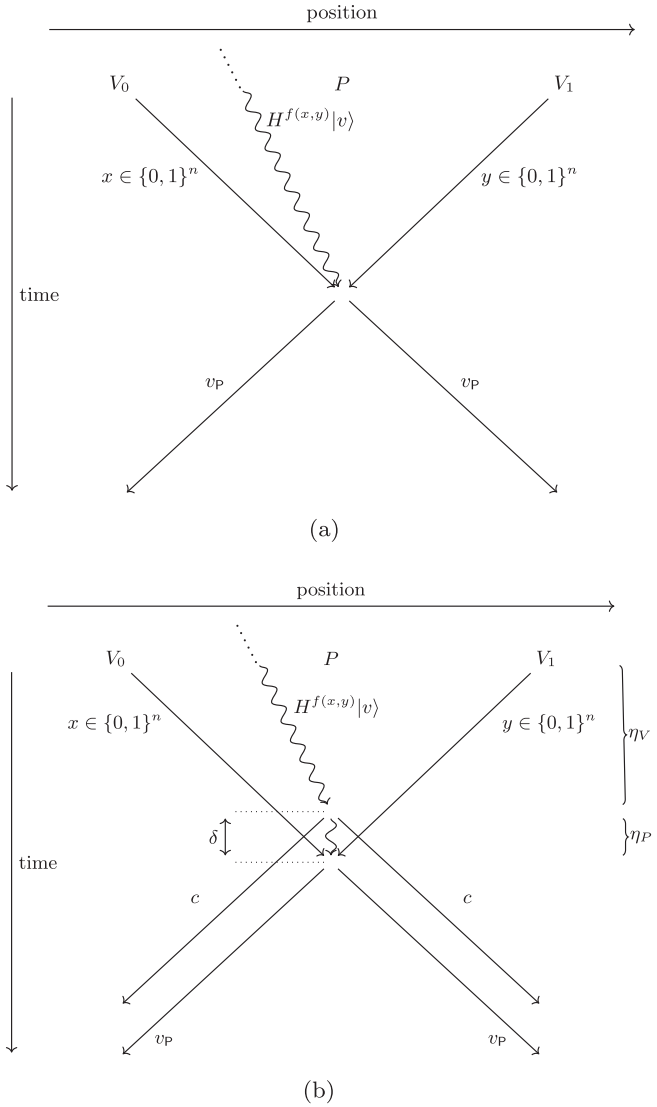

FIG. 1. Schematic representation of (a) $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ and its committing version (b) $\mathsf{c}\text{-}\mathrm{QPV}^{f}_{\mathrm{BB84}}$. In $\mathrm{QPV}^{f}_{\mathrm{BB84}}$, (i) V_0 and V_1 pick $x, y \in \{0,1\}^n$ and $v \in \{0,1\}$ uniformly at random, (ii) V_0 prepares and sends the BB84 qubit state $H^{f(x,y)}|v\rangle$—encoding v—as well as x to P, and V_1 sends y to P such that all information arrives at the same time at P. Only the classical information is required to travel at the speed of light, whereas the quantum information can travel arbitrarily slowly. (iii) The prover computes $f(x,y)$, and depending on the value, she measures the received qubit in the computational [if $f(x,y)=0$] or Hadamard [if $f(x,y)=1$] basis. Then, she broadcasts the outcome v_{P} to the verifiers at the speed of light. (iv) In the end, the verifiers check whether the response arrived at the expected time and corresponds correctly to the encoded bit in the input state. $\mathsf{c}\text{-}\mathrm{QPV}^{f}_{\mathrm{BB84}}$ consists of a modified structural version of $\mathrm{QPV}^{f}_{\mathrm{BB84}}$, where the verifiers send the qubit $H^{f(x,y)}|v\rangle$ at a time δ before they would in $\mathrm{QPV}^{f}_{\mathrm{BB84}}$, and the prover commits $c=1$ upon receiving the qubit, and $c=0$ otherwise. If $c=1$, the protocol proceeds as in $\mathrm{QPV}^{f}_{\mathrm{BB84}}$. In both (a) and (b), the qubit $H^{f(x,y)}|v\rangle$ is originated by V_0 in the past, and undulated and straight lines represent quantum and classical information, respectively.

classical information that has to be evaluated through f, whose output determines the basis in which to measure the received qubit, and the prover broadcasts her outcome measurement v_{P}; see Fig. 1(a). In order to *accept* or *reject* the location, the verifiers execute the protocol sequentially r times. In the idealized case, the verifiers *accept* if all of the answers are correct, i.e., $v = v_{\mathsf{P}}$ in all rounds; otherwise, they reject—other nonidealized cases have been studied when errors and/or loss are included [18,29,39]. In [18], the authors showed that any attackers who preshare $\Omega(n)$ qubits—we denote this attack model by $\mathcal{M}$—cannot answer correctly in a round with probability arbitrarily close to 1, and by executing the protocol sequentially, attackers will be rejected with exponentially high probability in r.

However, if non-negligible loss of the qubits is considered, the security of $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ established in [18] no longer applies. A simple way to see that loss compromises security can be seen from the following attack on $\mathrm{QPV}^{f}_{\mathrm{BB84}}$. Let η_V be the transmission rate between V_0 and P, and place an adversary between V_0 and P (Alice) and between V_1 and P (Bob). Alice intercepts x and the qubit and measures it in the computational or Hadamard basis, selected at random. Then she broadcasts the choice of basis as well as the measurement outcome and x. Bob intercepts and broadcasts y to his fellow attacker. After the communication round, they both compute $f(x, y)$ and know if the selected basis was correct or not. If yes, each of them responds to the verifier closest to them, knowing that the answer is correct. Otherwise, they claim that the qubit was lost, which, throughout this Letter, we denote by the symbol $\perp$. As long as η_V is 50% or below, this simple attack will be successful, as this situation is indistinguishable from an honest prover answering loss with probability $1 - \eta_V$. Hypothetically, if C-band telecom wavelength ($\sim$1550 nm) single-photon sources were used and the photons were sent through optical fibers with a loss of 0.15 dB/km [40], that would translate to a distance of at most 20 km (further reduced by equipment and detector efficiencies). Security for $\eta_V > 1/2$ was proven in [29], and, by encoding the bit v in more than two different bases, security guarantees can be extended for larger loss rates. However, this only provides security for overall constant loss rates, whereas loss in optical fibers decays exponentially with the distance.

QPV with a commitment step—To overcome these roadblocks, we introduce a slight modification in the structure of $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ that makes the transmission loss from the verifiers to the prover η_V irrelevant for security and therefore bridges the gap that prevents QPV from being feasible with current technology. More precisely, we add an extra step that we call the *commitment step*. The modification consists of sending the BB84 qubit employed in $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ in such a way that it arrives at a time $\delta > 0$ before the classical information x and y. Upon receiving the quantum information, the prover sends a *commitment* $c = 1$, confirming that she has received it. After the time δ, she receives the classical information, executes the original protocol $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ as she has all necessary information now, and answers to the verifiers; see Fig. 1(b). If the quantum information has not arrived at the prover, she sends $c = 0$, and no further answers have to be sent. Since the commitment is a classical bit broadcast by a single prover, in the honest case, the verifiers abort the protocol if they receive different commitments.

This extra commitment step prevents the aforementioned guessing attack, intuitively because the earliest point in spacetime at which all quantum and classical input information is available exists only *after* the commitment c needs to be sent. Hence, attackers necessarily will end up with rounds for which they have committed to play, but their guess of the measurement basis turned out to be wrong afterward. They cannot fully mask wrong guesses in $\perp$ responses anymore because they both are required to commit equally, but do not have enough time to coordinate. However, we need to prove that adding the commitment step does not open up new avenues for attacks. Using the fact that the commitment bits cannot rely on all of the classical information, we prove that, for the security of this protocol, the transmission rate η_V between the verifiers and the prover becomes irrelevant. This rate includes all of the losses before the prover commits: in V_0's laboratory, the quantum channel connecting V_0 and P, and the photon detector's efficiency. The transmission rate (in the prover's laboratory) after committing and receiving the classical information will be denoted as η_P, including loss of the photon while waiting for the classical strings x, y.

Security—The most general attack to $\mathtt{c}$-$\mathrm{QPV}^{f}_{\mathrm{BB84}}$ consists of placing an adversary Alice between V_0 and P and an adversary Bob between P and V_1. See Fig. 2 for a schematic representation. Then, (i) the attackers prepare a joint (possibly entangled) quantum state. (ii) Alice intercepts the slow quantum information sent by V_0, performs an arbitrary quantum channel on all of the quantum information that she holds, and then sends a part of it to Bob. Let us denote by ρ^{v} their joint state at this stage (before communication and receiving x, y). (iii) Alice and Bob intercept x and y, make a copy, and send it to the other attacker, respectively. Because of the relativistic constraints, the attackers have to commit before they receive the classical information from the other party; thus their commitment can only depend on x or y, respectively. The most general operation that they can perform is to use local quantum instruments $\{\mathcal{I}^{A}_{c_A|x}\}_{c_A\in\{0,1\}}$ and $\{\mathcal{I}^{B}_{c_B|y}\}_{c_B\in\{0,1\}}$ on their registers of ρ^{v} to determine the commitments c_A and c_B, respectively. They send the commitments c_A, c_B to the verifier closest to them at the appropriate time. If $c_A = c_B = 0$ or $c_A \neq c_B$, no further action is required since, in the first case, the verifiers do not expect any more answers and, in the second case, the protocol is aborted. For $c_A = 1$ and $c_B = 1$, which will be the case that we consider from now on, Alice and Bob will use the postselected state $\tilde{\mathcal{I}}^{xy}_{1}(\rho^{v}) = \mathcal{I}^{xy}_{1}(\rho^{v})/\mathrm{Tr}[\mathcal{I}^{xy}_{1}(\rho^{v})]$, where $\mathcal{I}^{xy}_{1} = \mathcal{I}^{A}_{1|x} \otimes \mathcal{I}^{B}_{1|y}$,

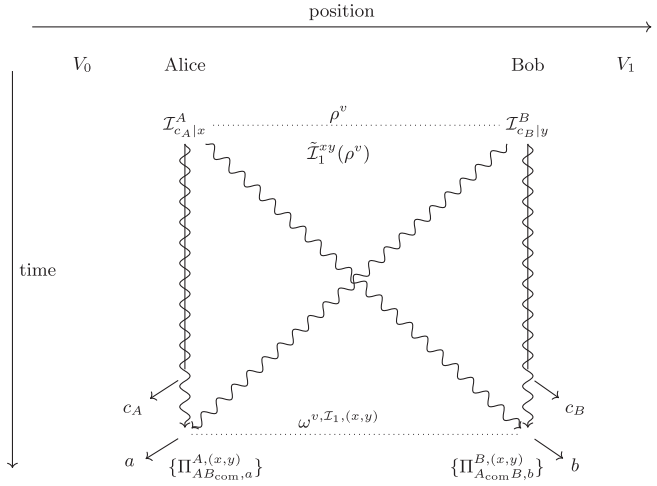

FIG. 2. Schematic representation of a general attack to c-$\mathrm{QPV}^f_{\mathrm{BB84}}$. Undulated lines represent quantum information, whereas straight lines represent classical information.

and we fix a partition into registers $AA_{\mathrm{com}}BB_{\mathrm{com}}$, where Alice possesses registers AA_{com} and Bob possesses BB_{com}, with "com" denoting the subsystems that will be communicated. Alice sends register A_{com} to Bob, and Bob sends register B_{com} to Alice. (iv) Denote by $\omega^{v,\mathcal{I}_1,(x,y)}_{AB_{\mathrm{com}}BA_{\mathrm{com}}}$ the quantum state after communication. Each party performs a POVM on their local register of $\omega^{v,\mathcal{I}_1,(x,y)}_{AB_{\mathrm{com}}BA_{\mathrm{com}}}$, depending on both x and y, and they obtain answers $a, b \in \{0, 1, \perp\}$, respectively. We can write the attackers' POVMs as $\{\Pi^{A,(x,y)}_{AB_{\mathrm{com}},a}\}_a$ and $\{\Pi^{B,(x,y)}_{A_{\mathrm{com}}B,b}\}_b$. Then, given x, y and that $c_A = c_B = 1$, the probability that the attackers output the correct answer v is given by

$$p^{xy}_{\mathrm{corr}} = \mathrm{Tr}\left[\left(\Pi^{A,(x,y)}_{AB_{\mathrm{com}},v} \otimes \Pi^{B,(x,y)}_{BA_{\mathrm{com}},v}\right)\omega^{v,\mathcal{I}_1,(x,y)}_{AA_{\mathrm{com}}BB_{\mathrm{com}}}\right],$$

with average over x, y given by $p_{\mathrm{corr}} = (1/2^{2n})\sum_{x,y} p^{xy}_{\mathrm{corr}}$.

Consistency of the no-photon answers for the transmission rate η_P at the prover's laboratory is given by

$$\frac{1}{2^{2n}}\sum_{x,y}\mathrm{Tr}\left[\left(\Pi^{A,(x,y)}_{AB_{\mathrm{com}},\perp} \otimes \Pi^{B,(x,y)}_{BA_{\mathrm{com}},\perp}\right)\omega^{v,\mathcal{I}_1,(x,y)}\right] = 1 - \eta_P.$$

The most general attack on the noncommitting version $\mathrm{QPV}^f_{\mathrm{BB84}}$ can be obtained by modifying the attack described above, specifically by replacing step (iii) with the following: instead of applying quantum instruments, Alice and Bob apply quantum channels depending on x and y to their local registers, respectively, transforming ρ^v to $\omega^{v,(x,y)}_{AA_{\mathrm{com}}BB_{\mathrm{com}}}$. Then, they act analogously with $\omega^{v,(x,y)}$ taking the role of $\omega^{v,\mathcal{I}_1,(x,y)}$.

Here, we consider a class of attack models on $\mathrm{QPV}^f_{\mathrm{BB84}}$, which we refer to as the *preshared bounded models*, for which one can find an upper bound on the probability of answering correct for any state ρ^v in step (ii) belonging to a given fixed set. We denote the optimal probability that attackers answer correct in a round of $\mathrm{QPV}^{f,\eta_V}_{\mathrm{BB84}}$ and c-$\mathrm{QPV}^{f,\eta_V,\eta_P}_{\mathrm{BB84}}$ divided by η_V and η_P, respectively, by

$$P(\text{attack QPV}^{f,\eta_V}_{\mathrm{BB84}}) \quad \text{and} \quad P(\text{attack c-QPV}^{f,\eta_V,\eta_P}_{\mathrm{BB84}}), \quad (1)$$

where the latter is conditioned on $c_A = c_B = 1$. Dividing by η_P conditions on the event that the attackers actually answer (i.e., do not output $\perp$), allows us to compare this quantity directly with the correctness rate of an honest prover. For instance, in the attack model $\mathcal{M}$, where the set of states consists of those whose number of qubits is linear in n, upper bounds below 1 for $P(\text{attack QPV}^{f,\eta_V}_{\mathrm{BB84}})$ have been established [18,22,29,39].

In Theorem 1, we relate both quantities, showing that attackers cannot take advantage of photon loss η_V and that the only transmission that is relevant for security is η_P (in the time δ). The high level idea is as follows. In a perfect setting (see below for robustness analysis), both attackers should always commit the same bit, i.e., with probability 1, $c_A = c_B$. Without loss of generality, as Alice and Bob act on separate registers, we may assume that Alice applies her quantum instrument $\{\mathcal{I}^A_{c_A|x}\}_{c_A\in\{0,1\}}$ first. But then her commitment c_A completely fixes Bob's c_B, which he obtains by applying his instrument $\{\mathcal{I}^B_{c_B|y}\}_{c_B\in\{0,1\}}$, for any y. We use the gentle measurement lemma [41] together with the fact that any quantum instrument can be decomposed into a measurement followed by a quantum channel (see, e.g., Theorem 7.2 in [42]) to show that the probability of attacking the protocol successfully remains invariant if one replaces the postmeasurement state $\tilde{\mathcal{I}}_1^{xy}(\rho^v)$ by ρ^v. Therefore, we have a postmeasurement state that is independent of x and y. From this, after the commitment, the attackers find themselves in the same situation as in attacking the underlying protocol $\mathrm{QPV}^f_{\mathrm{BB84}}$.

In the setting of perfect attacks, the security of c-$\mathrm{QPV}^f_{\mathrm{BB84}}$ reduces exactly to the security of $\mathrm{QPV}^f_{\mathrm{BB84}}$, but we also consider a robust setting where we allow Alice and Bob to perform an attack that has a nonzero probability to commit differently. We consider this because the verifiers can only run a finite number of rounds, and therefore answering differently with a low probability on some subset of inputs can remain undetected with high probability but could help attackers in principle. In QPV, the prover must respond to each challenge as it arrives, so adversarial operations act per round; our security proof explicitly covers adaptive attackers who may choose their strategy based on the actions in previous rounds, which captures the strongest permitted attack when restricting to sequential repetition. As we show in Sec. B of Supplemental Material (SM) [30], we prove that even in this robust setting only a negligible overhead is added to the

attack success probability of the underlying protocol without the commitment step, where the effective protocol transmission rate is η_P instead of $\eta_V\eta_P$. Furthermore, we can make this overhead as small as we want through sequential repetition of the protocol, where we assume the same model constraints apply in each round.

Theorem 1—Let $k \geq 2$ be a security parameter and suppose $\mathsf{c\text{-}QPV}^{f}_{\mathrm{BB84}}$ is executed sequentially until we have $640k/\tilde{c}^3 = O(k^7)$ rounds in which both attackers commit, where $\tilde{c} = [1/k^2(4 + 3g(\eta_P))^2]$, with $g(\eta_P) \coloneqq \max\{(1/\sqrt{\eta_P}), [1/(1-\eta_P)]\}$. This takes an expected number of rounds $O(k^7)/p_{\mathrm{commit}}$. Then, either the attackers are detected with probability bigger than $1\text{–}3 \times 10^{-9}$ by means of a different commitment, or there is a set $\mathcal{R}$ of size $1 - 1/k$ times the number of rounds such that, for all $i \in \mathcal{R}$, for every preshared bounded model,

$$P(\text{attack } \mathsf{c\text{-}QPV}^{f,\eta_V,\eta_P}_{\mathrm{BB84}}) \leq P(\text{attack } \mathrm{QPV}^{f,\eta_P}_{\mathrm{BB84}}) + \frac{1}{k}.$$

Therefore, by Theorem 1, having a bound on the probability of attacking $\mathrm{QPV}^{f,\eta_P}_{\mathrm{BB84}}$ implies that essentially the same bound applies for its committing version without the loss $1 - \eta_V$. We highlight that Theorem 1 holds for a more general class of QPV protocols and refer the reader to the SM (Sec. B) [30] for more details. In addition, generalizing techniques from [29] and utilizing Azuma's inequality [43], we show that after r sequential repetitions, with $\eta_P < 1$ and a qubit error rate $p_{\mathrm{err}} > 0$, an honest party's claimed location will be accepted with high probability (*completeness*), whereas any attackers in a preshared bounded model, and thus bounded $P(\text{attack } \mathrm{QPV}^{f,\eta_P}_{\mathrm{BB84}})$, will be rejected with exponentially high probability in r (*soundness*), thus implying *security*; see SM (Sec. C) [30].

Possible experimental realization of QPV with commitment—For the commitment, we present a simplified, probabilistic quantum nondemolition measurement (QND), which is feasible with current technology. We do not require a full deterministic QND, and the failure probability will turn out to be irrelevant for security (but relevant for the protocol rate). Additionally, for the prover, it is relatively straightforward to implement the short time delay by storing the received qubit from V_0 in a fixed-length delay loop (no on-demand quantum memory is required). Consider a QND with a detection efficiency of $\eta^{\mathrm{QND}}_{\mathrm{det}}$ and a dark count rate of $p^{\mathrm{QND}}_{\mathrm{dc}}$.

Using photonic qubits and linear optics, our proposal consists of the prover teleporting the quantum input to herself in her laboratory as a simplified means to perform the QND. This can be achieved, for example, through the well-known linear-optical partial Bell state measurement (BSM); see SM D.2 [30] for completeness. The prover has to generate an EPR pair and feed one qubit of it into one input port of the beam splitter (BS). The input quantum state is supposed to enter BS from the other input port. A successful click pattern then indicates the presence of the input state along with a teleportation of it to the remaining EPR qubit that the prover briefly stored. This qubit is subsequently measured in the basis $f(x, y)$.

Since the input states of $\mathsf{c\text{-}QPV}^{f}_{\mathrm{BB84}}$ are BB84 states, in the simplest case, no active feedforwarding of the teleportation corrections is necessary. The corrections predictably change the measurement outcome, and the prover has all of the information to classically error-correct after the final measurement. See SM Sec. D [30] for an analysis of experimental parameters and estimations with current technology in imperfect laboratory setups.

We highlight that high efficiency of the BSM is not required since it effectively just adds to the transmission loss between the verifiers and the prover, which, by Theorem 1 is irrelevant for the security of $\mathsf{c\text{-}QPV}^{f}_{\mathrm{BB84}}$. The same holds for the EPR state generation of the honest prover. If for example the EPR state generation was unsuccessful due to photon loss, it will lead to a "no-detection" round, and such rounds get discarded. In practice, what matters is any process that contributes false positives—one example being detector dark counts—and subsequently introduces errors in the prover's final measurement.

An imperfect QND ultimately limits the maximal distance between the verifiers and the prover, albeit to much larger distances than previously possible in QPV. In SM (Sec. D) [30], we estimate that QPV on distances around 100 km could be possible with near-term technology. At that distance, we loosely estimate a successful and secure position verification rate on the order of 0.1 Hz to be possible if errors other than loss can be kept low. Such a rate may be enough in practical scenarios since realistically speaking an object cannot move far in a few seconds.

Moreover, the verifiers need to be able to generate and modulate single photon states (e.g., polarization) with high frequency.

Discussion—So far, bounds on $P(\text{attack } \mathrm{QPV}^{f,\eta_P}_{\mathrm{BB84}})$ are known in the case where the attackers preshare a linear number of qubits, and these bounds directly carry over to the committing version. Moreover, if super-linear bounds were established for $\mathrm{QPV}^{f}_{\mathrm{BB84}}$, Theorem 1 ensures that they would also apply to the committing version.

Our proof covers sequential repetition; it would be desirable to have a security proof even if protocol rounds are repeated in parallel and thus require only a single execution. For example, proving security for the commitment version of the parallel repetition of $\mathrm{QPV}^{f}_{\mathrm{BB84}}$, whose security was recently proved [39], remains an open problem.

We give rough estimates of experimental parameters since the achievable values will highly depend on the actual equipment used. As our proposal paves the way for a first demonstration of quantum position verification with all of the desired properties, the next step would be to conceptualize a full experiment and see which parameters and rates are achievable given that setup.

See SM [30] for comprehensive details, extensive results, complete proofs, and additional Refs. [42,44–57].

Acknowledgments—We thank Adrian Kent for an interesting initial discussion pointing out photon presence detection to us. We further thank Wolfgang Löffler and Kirsten Kanneworff for helpful discussions. R. A. and H. B. were supported by the Dutch Research Council (NWO/OCW), as part of the Quantum Software Consortium program (Project No. 024.003.037). A. B. is supported by the French National Research Agency in the framework of the "France 2030" program (ANR-11-LABX-0025-01) for the LabEx PERSYVAL. M. C. acknowledges financial support from the Novo Nordisk Foundation (Grant No. NNF20OC0059939 "Quantum for Life"), the European Research Council (ERC Grant Agreement No. 81876), and VILLUM FONDEN via the QMATH Centre of Excellence (Grant No. 10059). This research was conducted when R. A. and P. V. L. were affiliated with CWI Amsterdam and QuSoft. P. V. L. and H. B. were supported by the Dutch Research Council (NWO/OCW), as part of the NWO Gravitation Programme Networks (Project No. 024.002.003). P. V. L. is also supported by France 2030 under the French National Research Agency Award No. ANR-22-PETQ-0007. L. E. F. and F. S. were supported by the Dutch Ministry of Economic Affairs and Climate Policy (EZK), as part of the Quantum Delta NL program. Part of this work was completed while MC was Turing Chair for Quantum Software, associated with the QuSoft research center in Amsterdam, acknowledging financial support by the Dutch National Growth Fund (NGF), as part of the Quantum Delta NL visitor program.

[1] CNN News, Finance worker pays out $25 million after video call with deepfake "chief financial officer" (2024) [accessed: March 22, 2024].
[2] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner, SIAM J. Comput. **43**, 150 (2014).
[3] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky, in *Advances in Cryptology—CRYPTO 2009* (Springer, Berlin, Heidelberg, 2009), pp. 391–407.
[4] W. K. Wootters and W. Zurek, Nature (London) **299**, 802 (1982).
[5] R. G. Beausoleil, A. Kent, W. J. Munro, and T. P. Spiller, Tagging systems, U.S. Patent No. 70 75 438 (2006).
[6] A. Kent, W. J. Munro, and T. P. Spiller, Phys. Rev. A **84**, 012326 (2011).
[7] R. A. Malaney, Phys. Rev. A **81**, 042319 (2010).
[8] R. A. Malaney, in *IEEE Global Telecommunications Conference GLOBECOM 2010* (IEEE, Miami, Florida, USA, 2010), pp. 1–6.
[9] S. Beigi and R. König, New J. Phys. **13**, 093036 (2011).
[10] H. K. Lau and H. K. Lo, Phys. Rev. A **83**, 012322 (2011).
[11] C. C. W. Lim, F. Xu, G. Siopsis, E. Chitambar, P. G. Evans, and B. Qi, Phys. Rev. A **94**, 032315 (2016).
[12] F. Speelman, in *Proceedings of the 11th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2016)*, Leibniz International Proceedings in Informatics (LIPIcs) ol. 61 (Schloss Dagstuhl–Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 2016), pp. 9:1–9:24.
[13] K. Dolev, arXiv:1909.05403.
[14] A. Gonzales and E. Chitambar, IEEE Trans. Inf. Theory **66**, 2951 (2020).
[15] M. Junge, A. M. Kubicki, C. Palazuelos, and D. Pérez-García, Commun. Math. Phys. **394**, 625 (2022).
[16] R. Allerstorfer, H. Buhrman, F. Speelman, and P. Verduyn Lunel, arXiv:2208.04341.
[17] K. Dolev and S. Cree, arXiv:2203.10106.
[18] A. Bluhm, M. Christandl, and F. Speelman, Nat. Phys. **18**, 623 (2022).
[19] J. Cree and A. May, Quantum **7**, 1079 (2023).
[20] R. Allerstorfer, H. Buhrman, A. May, F. Speelman, and P. Verduyn Lunel, Quantum **8**, 1387 (2024).
[21] A. Bluhm, S. Höfer, A. May, M. Stasiuk, P. Verduyn Lunel, and H. Yuen, arXiv:2505.23893.
[22] V. Asadi, R. Cleve, E. Culf, and A. May, Quantum **9**, 1604 (2025).
[23] V. Asadi, E. Culf, and A. May, arXiv:2402.18647.
[24] F. Gao, B. Liu, and Q. Wen, Sci. China Phys. Mech. Astron. **59**, 1 (2016).
[25] J. Liu, Q. Liu, and L. Qian, in *Proceedings of the 13th Innovations in Theoretical Computer Science Conference (ITCS 2022)* (Schloss Dagstuhl–Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 2022).
[26] D. Unruh, in Advances in Cryptology—CRYPTO 2014 (Springer, Berlin, Germany, 2014), pp. 1–18.
[27] K. Kanneworff, M. Poortvliet, D. Bouwmeester, R. Allerstorfer, P. Verduyn Lunel, F. Speelman, H. Buhrman, P. Steindl, and W. Löffler, arXiv:2502.04125.
[28] B. Qi and G. Siopsis, Phys. Rev. A **91**, 042337 (2015).
[29] L. Escolà-Farràs and F. Speelman, Phys. Rev. Lett. **131**, 140802 (2023).
[30] See Supplemental Material at http://link.aps.org/supplemental/10.1103/szwj-s7r6 for the proofs and derivations, which includes Refs. [31–38].
[31] M. J. Bayerbach, S. E. D'Aurelio, P. van Loock, and S. Barz, Sci. Adv. **9**, eadf4080 (2023).
[32] J. Calsamiglia and N. Lütkenhaus, Appl. Phys. B **72**, 67 (2001).
[33] F. Ewert and P. van Loock, Phys. Rev. Lett. **113**, 140403 (2014).
[34] R. H. Hadfield, Nat. Photonics **3**, 696 (2009).
[35] W. Hoeffding, J. Am. Stat. Assoc. **58**, 13 (1963).
[36] M. Michler, K. Mattle, H. Weinfurter, and A. Zeilinger, Phys. Rev. A **53**, R1209 (1996).
[37] D. Niemietz, P. Farrera, S. Langenfeld, and G. Rempe, Nature (London) **591**, 570 (2021).
[38] M. Petrovich, E. Numkam Fokoua, Y. Chen, H. Sakr, A. I. Adamu, R. Hassan, D. Wu, R. Fatobene Ando, A. Papadimopoulos, S. R. Sandoghchi *et al.*, Nat. Photonics **19**, 1203 (2025).
[39] L. Escolà-Farràs and F. Speelman, arXiv:2503.09544.
[40] X. Cao, M. Zopf, and F. Ding, J. Semicond. **40**, 071901 (2019).

[41] A. Winter, Coding theorems of quantum information theory, Ph.D. thesis, Bielefeld University, 1999.
[42] M. Hayashi, *Quantum Information Theory* (Springer, New York, 2016).
[43] K. Azuma, Tohoku Math. J. **19**, 357 (1967).
[44] A. Anwar, C. Perumangatt, F. Steinlechner, T. Jennewein, and A. Ling, Rev. Sci. Instrum. **92**, 041101 (2021).
[45] S. L. Braunstein and A. Mann, Phys. Rev. A **51**, R1727 (1995).
[46] H. Chernoff, Ann. Math. Stat. **23**, 493 (1952).
[47] Z. Chai, X. Hu, F. Wang, X. Niu, J. Xie, and Q. Gong, Adv. Opt. Mater. **5**, 1600665 (2017).
[48] T. Hasegawa, Y. Tamura, H. Sakuma, Y. Kawaguchi, Y. Yamamoto, and Y. Koyano, SEI Tech. Rev. **86**, 18 (2018), https://global-sei.com/technology/tr/bn86/pdf/86-04.pdf.
[49] K. Kraus, Ann. Phys. (N.Y.) **64**, 311 (1971).
[50] Y. Li, Y.-H. Li, H.-B. Xie, Z.-P. Li, X. Jiang, W.-Q. Cai, J.-G. Ren, J. Yin, S.-K. Liao, and C.-Z. Peng, Opt. Lett. **44**, 5262 (2019).
[51] A. Lohrmann, A. Villar, A. Stolk, and A. Ling, Appl. Phys. Lett. **113**, 171109 (2018).
[52] E. Meyer-Scott, C. Silberhorn, and A. Migdall, Rev. Sci. Instrum. **91**, 041101 (2020).
[53] D. V. Reddy, R. R. Nerem, S. W. Nam, R. P. Mirin, and V. B. Verma, Optica **7**, 1649 (2020).
[54] J. M. Senior and M. Y. Jamro, *Optical Fiber Communications: Principles and Practice* (Pearson Education, Harlow, England, 2009).
[55] J. Watrous, *The Theory of Quantum Information* (Cambridge University Press, Cambridge, England, 2018).
[56] H. Weinfurter, Europhys. Lett. **25**, 559 (1994).
[57] D. Williams, *Probability with Martingales* (Cambridge University Press, Cambridge, England, 1991).