Quantum Science and
Technology

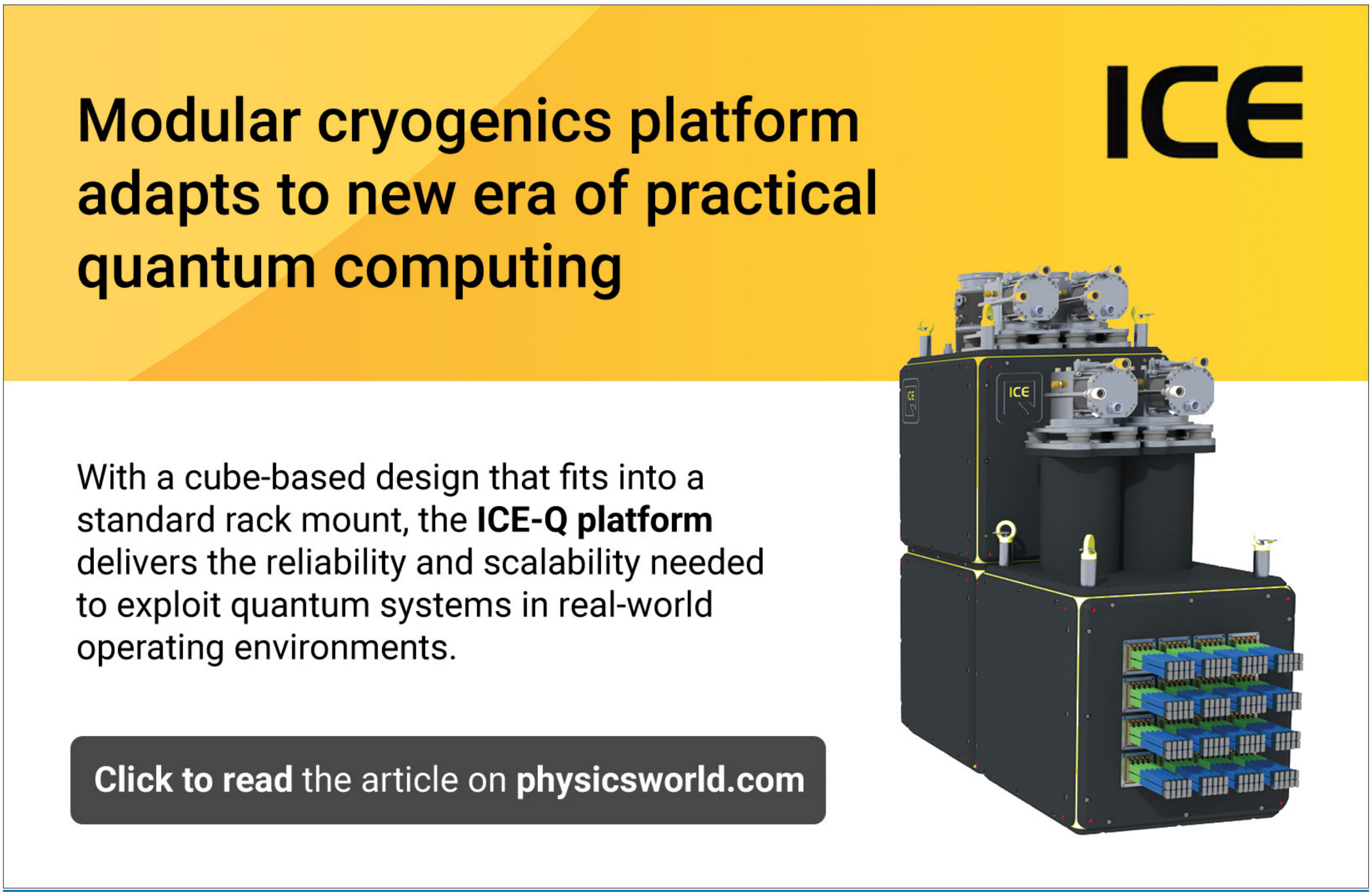
Celebrating the 10th anniversary of Quantum Science and Technology

International Year of Quantum Science and Technology

PURPOSE-LED PUBLISHING™

Towards experimental demonstration of quantum position verification using single photons

To cite this article: Kirsten Kanneworff *et al* 2025 *Quantum Sci. Technol.* **10** 045004



Quantum Science and Technology

OPEN ACCESS

RECEIVED
28 April 2025

REVISED
11 July 2025

ACCEPTED FOR PUBLICATION
22 July 2025

PUBLISHED
1 August 2025

PAPER

Towards experimental demonstration of quantum position verification using single photons

Kirsten Kanneworff[1,*], Mio Poortvliet[1], Dirk Bouwmeester[1,2], Rene Allerstorfer[3,4], Philip Verduyn Lunel[3,4,5], Florian Speelman[3,6], Harry Buhrman[3,6,7], Petr Steindl[1] and Wolfgang Löffler[1,*]

[1] Leiden Institute of Physics, Leiden, The Netherlands
[2] Department of Physics, University of California, Santa Barbara, CA, United States of America
[3] QuSoft, Amsterdam, The Netherlands
[4] CWI, Amsterdam, The Netherlands
[5] Sorbonne Université, CNRS, LIP6, Paris, France
[6] University of Amsterdam, Amsterdam, The Netherlands
[7] Quantinuum, London, United Kingdom
[*] Authors to whom any correspondence should be addressed.

E-mail: kanneworff@physics.leidenuniv.nl and loeffler@physics.leidenuniv.nl

Keywords: quantum position verification, position-based cryptography, single photon sources, quantum dots, quantum networks, quantum cryptography

Supplementary material for this article is available online

Abstract

The geographical position can be a good credential for authentication of a party. This is the basis of position-based cryptography—but classically this cannot be done securely without physical exchange of a private key. Recently it has been shown that by combining quantum mechanics with the speed-of-light limit of special relativity, this might be possible: quantum position verification (QPV). Here we demonstrate experimentally a protocol that uses two-photon Hong–Ou–Mandel interference at a beamsplitter, which, in combination with two additional beam splitters and four detectors is rendering the protocol resilient to loss. With this, we are able to show first results towards an experimental demonstration of QPV.

Since the geographical location is often a good credential of a party in communications, verification thereof could add a useful layer to communication security—this is the case, for instance, with data centers, banks, government buildings, a lab in a quantum network, or even a satellite. Classically, position verification is only possible securely by prior physical exchange of keys [1]. In quantum mechanics, mainly thanks to the no-cloning theorem, this can be avoided [2–5]. The general scheme of quantum position verification (QPV) is shown in figure 1: two verifiers V_0 and V_1 share a private communication channel and aim to confirm the location of a third party, the prover P. The verifiers send classical and quantum information, the prover performs a task and returns classical (and possibly quantum) information. The verifiers use this information and the timing and conclude if the prover was at the claimed position or not. This scheme is one-dimensional but can be extended to higher dimensions [6].

However, it quickly was found that attackers with shared entanglement and exploiting quantum teleportation can break QPV protocols, after first attempts [7–9] a general attack was found [10]. This finding has stimulated broad research into the topic [11–25], and it was found that by including classical-information cryptographic tasks, QPV protocols can be made secure for all practical purposes such that attackers require a very large amount of shared entanglement that does only depend on the amount of classical information used in the QPV protocol [26, 27].

In real-world QPV, the quantum information is sent by photons, and two major loopholes emerge from this: First, photons are susceptible to loss during transmission, which opens up a generic attack strategy since the adversaries can claim loss if their measurements have been performed in the wrong basis, for instance. Therefore, fully loss-tolerant protocols are required [23, 28, 29], the first having been developed in [11, 25]. We will investigate here a variation of those protocols, the SWAP protocol developed and analyzed by some of us [24] where two-photon interference makes loss-based attacks detectable. The second major loophole appears if we transport the photons through fiber networks, where the speed of light c is reduced compared to free space, giving attackers using free-space communications an advantage. This slow quantum information loophole we do not address here, but we mention that recently, advanced protocols including a commitment step have been developed [30] that could mitigate this issue in future.

In this paper, we report our progress towards an experimental demonstration of QPV. We use single photons from a demultiplexed quantum dot (QD)—microcavity single-photon source, send them to the two verifiers, encode suitable qubits in the photons and send them to the prover. The prover performs the SWAP test using Hong–Ou–Mandel (HOM) two-photon interference and measures the result in a loss-tolerant way with 4 single-photon detectors. We analyze the results critically by comparing photon correlations to protocol simulations. Those results show that we currently cannot claim fully secure QPV, and we find that imperfections in our single-photon source are responsible. Finally, we compare our results to a simulated outcome based on our experimental conditions but using the properties of a higher-quality state-of-the-art single-photon source, this suggests that secure QPV with a quantum-dot single photon source is within reach.

1. Protocol

Photon loss is one of the most important limiting factors for any experimental realization of QPV. Most of the proposed QPV protocols are partially loss tolerant meaning that they can only tolerate loss up to a certain fraction such as 50%. However, any loss limit renders a real-world implementation very challenging due to the exponential loss with distance given by the Lambert-Beer law, and limited photon production and detection probability. The first ideas about a fully loss-tolerant QPV protocol were proposed by Qi and Siopsis [11] and a first experimental proposal for such a protocol was developed by Lim *et al* [25]. In this protocol, in each round, the verifiers send to the prover either parallel (equal) or orthogonal photonic qubits in a randomly chosen basis. At the prover, the photons interfere at a beamsplitter where the HOM effect [31] leads to a different output statistics depending on whether the photons were parallel or orthogonal. This allows the prover to test for qubit equality in a basis-independent way and avoids public communication of the basis which would open a loss-based attack [25]: adversaries can measure the qubit(s) in a particular basis, if this basis choice turns out to be wrong, they can claim loss. We use here an adaptation of the Lim protocol by Allerstorfer *et al* [24], the SWAP protocol. This allows use of all 3 mutually unbiased qubit bases (we, however, show here one basis only), which improves the resilience against noise.

The SWAP protocol entails, see figure 1:

1. **Preparation:** Verifiers V_0 and V_1 share via their private channel a uniformly drawn random sequence of basis choices and qubit states (parallel or orthogonal), e.g. $|\Psi_0\rangle$ and $|\Psi_1\rangle$. Encoded in the polarization of single photons, these qubits are sent to the prover such that they arrive simultaneously.
2. **Measurement $\star$:** The prover performs the quantum measurement based on two-photon HOM quantum interference, we use two additional beamsplitters (BSs) and 4 detectors that allows to discriminate HOM photon bunching from loss as explained below. The prover returns a classical response $z = 0$ if they suspect that $|\Psi_0\rangle \parallel |\Psi_1\rangle$, $z = 1$ for $|\Psi_0\rangle \perp |\Psi_1\rangle$, and $z = \varnothing$ if the measurement is not conclusive.
3. **Round check:** After each response of the prover, the verifiers review if the received response z is the same for both verifiers and if the response arrived within the set time constraint. If either check fails, the verifiers abort the protocol.
4. **Verification:** After n rounds of steps $1\ldots3$, the verifiers check if the distributions of answers returned by the prover $z = \{0, 1, \varnothing\}$ follow the expected distribution within a certain error margin.

2. Experiment

2.1. The single-photon source

Essential for our experiment shown in figure 2 is the source of single photons. Although single photons can be produced relatively easily using spontaneous parametric downconversion (see e.g. [32] for a comparison), we choose here to use a source based on QDs. We use a single negatively charged self-assembled InGaAs/GaAs QD embedded in an optical microcavity [33–36]. The QD is embedded in a p–i–n junction separated by a 31.8 nm thick tunnel barrier from the electron reservoir to enable tuning of the QD resonance wavelength at around 935 nm by the quantum-confined Stark effect, for details see [34, 37, 38]. We drive the QD resonantly with short optical pulses carved out of narrow-linewidth frequency-tunable continuous-wave laser light by using an electro-optic modulator (EOM) controlled by custom made electronics [39]. This enables production of laser pulses with tunable pulse width of around 100 ps and pulse period (9 ns) at a

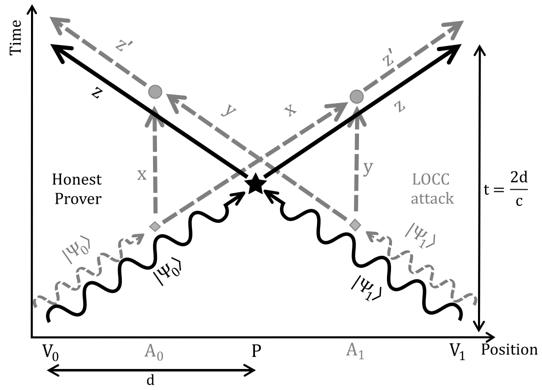


Figure 1. Space-time diagram of a one-dimensional QPV protocol showing the prover (P) centered at distance d between two verifiers (V_0 and V_1, solid black) where curly (straight) lines indicate quantum (classical) information exchange. Dashed gray lines show a potential form of attack by two adversaries (A_0 and A_1) positioned around the supposed location of the prover that try to mimic the honest prover responses and are restricted to local operations and classical communication (LOCC). Symbols are explained in the text.

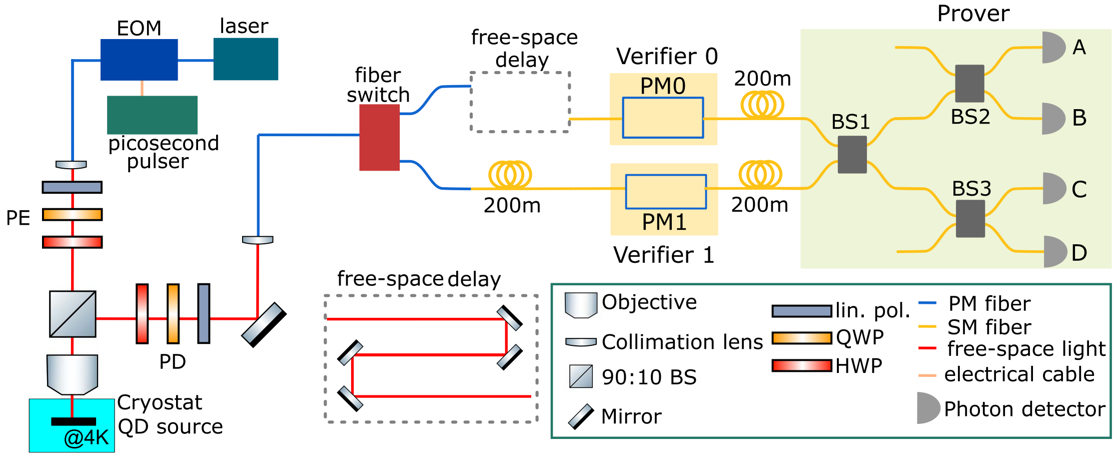


Figure 2. Schematic of the experimental setup. The electro-optic modulator (EOM) is used to generate the picosecond pulses, PE and PD are the polarization control elements of the excitation and detection paths, PM0 and PM1 are the polarization modulators of the verifiers, and BS1..3 are 50:50 fiber-based beamsplitters, where HOM interference for the SWAP test happens at BS1, and BS2 and BS3 split the outputs of BS1 to two detectors each, while the unused input ports of BS2 (top) and BS3 (bottom) are closed.

well-defined center wavelength. These parameters provide a good trade-off between single-photon brightness and quality of the single photons [39]. The single photons are separated from the laser light using a cross-polarization technique enabling laser extinction on the order of 10^{-6} [40] and collected in a polarization-maintaining (PM) single-mode (SM) fiber, resulting in an in-fiber single photon brightness or generation rate of around 3% [41].

2.2. QPV setup

The overall scheme of the QPV experiment is shown in figure 2. For the present implementation of the SWAP protocol, we demultiplex and distribute consecutive single photons from the QD source to both verifiers. For this, we first temporally demultiplex photons using a fiber switch (Agiltron NPNS, 500 kHz switching frequency). The time delay of the demultiplexer setup is adjusted to the switching frequency to around 1 μs to synchronize the photons, and an additional free-space delay is used to fine-tune the temporal profile of the single photons to maximally overlap at the first beamsplitter BS1 of the prover part of the setup. In a real-world application, one would of course use faster switches based on EOMs and synchronize them to the single photons, but those were not available to us for our operating wavelength. To simulate the distance between the verifiers and the prover, 200 m of SM optical fiber cable (780HP) is used. The overall transmission of the setup is between 7.2% and 12.4%, details are given in the supplementary material. We do not implement the classical channel for returning the prover answers to the verifiers, this can be done by standard radio-frequency techniques.

Verifiers. Both verifiers encode their qubits into the polarization state of the photons using piezo-electric fiber-based polarization modulators (PM0 and PM1, Polarite III PCD-M02), with which arbitrary polarization states can be prepared.

Calibration. All fibers behind the fiber switch are nonpolarization-maintaining SM fibers, and all induce polarization rotations. We use a fiber coupled polarimeter (Thorlabs PAX1000IR1/M) to calibrate the necessary polarization rotations such that polarization qubits from both verifiers experience during transmission to the beamsplitter BS1 the same unitary polarization transformation. To achieve this, we first replace one detector by the polarimeter, set the switch to send light through the path of verifier 0, and record the polarization state. Then we set the switch to direct light through the verifier 1 path, and adjust the polarization modulator PM1 such that the same polarization state is obtained. In this way we calibrate the transmission through the full setup and we do not have to change any fiber connections after this calibration, which avoids unavoidable drifts after reconnecting or moving a fiber. The fidelity of the produced polarization states is around 99.9%, it degrades by a few percent during the measurements, most likely due to temperature fluctuations.

Prover. To realize the SWAP protocol, the prover uses a system of 3 fiber-based beamsplitters (Thorlabs TW930R5A2) in combination with four avalanched single-photon detectors labeled A–D in figure 2(Excelitas SPCM-AQRH-14-FC-ND). We use a time-tagging card (Cronologic HPTDC, 100 ps resolution) and custom software to record all single counts and all combinations of 2, 3, and 4-fold coincidence detection events within a 1 ns time window (see supplemental section C for details). From these coincidence events, the prover determines their answer, and reports a conclusive result if exactly two photons are detected—otherwise, if less or more than 2 photons are detected, which can happen due to loss or dark counts, an inclusive result is reported: $z = \varnothing$. If conclusive, the prover wants to determine if the polarization of both photons is equal or not, for which the HOM effect is used—equal photons 'bunch' and exit beamsplitter BS1 through the same output port. In this case detectors AB or CD click and the prover returns $z = 0$. Otherwise, if detectors AC, AD, BC or BD click, HOM photon bunching did not happen and the prover returns $z = 1$.

3. Results

The experimental procedure is as follows: (i) we calibrate the polarization of the setup as described above, and record the settings. (ii) The single-photon source is optimized (laser power, polarization, quantum dot bias voltage). (iii) Data is recorded for 5 min intervals. Steps (ii) and (iii) are repeated for the measurement time. Figure 3 shows the raw and normalized coincidence events. We focus here on only one polarization basis, the HV basis. We note that we observe no 3 and 4-fold events in our one-hour long measurements.

If our experiment would be perfect, all coincidence events are equally probable for orthogonal qubits ($\perp$) from the verifiers. This is well recognizable in figure 3, red bars. If the qubits from the verifiers are equal ($\|$), we would expect perfect HOM photon bunching and that only AB and CD events appear. In figure 3(a), we indeed observe an enhancement of these events, but also a rather large amount of unexpected coincidences (AC, AD, BC, BD), which we will discuss below. In figure 3(b) we show the normalized coincidences

$$CC_{ij}^{\text{norm}} = \frac{CC_{ij}}{SC_i\, SC_j} \tag{1}$$

where CC_{ij} are the two-photon coincidence events of detectors i and j, and SC_i are the single-photon detection events of detector i. This shows that the large difference between $CC_{\text{AB}}^{\|}$ and $CC_{\text{CD}}^{\|}$ in figure 3(a) originates from unbalanced beam splitters and different transmissions of the respective paths, which is removed by this normalization.

Prover answers. The prover determines the answer from the photon detection events as explained above and in the final step in the verification process the verifiers check if the conclusive responses from the prover follow the expected distribution. This is done by calculating the ratio of correct and incorrect answers received from the prover. We now discuss the expected results, and compare to the experimental data. The results are shown in table 1 and figure 4.

First, what is the probability to obtain an inconclusive result, where the two photons are absorbed by the same detector—for the case of an ideal experiment without loss? In the case of orthogonal qubits ($\perp$) where no HOM photon bunching is happening, the chance that both photons leave the beamsplitter through the same port is 1/2, and this must happen twice, at BS1 and then at BS2 or BS3 - therefore $\mathbb{P}(\varnothing|\perp) = 1/4$. In the case of parallel qubits ($\|$), HOM photon bunching happens at BS1 with certainty, and therefore the chance of an inconclusive result is twice as high: $\mathbb{P}(\varnothing|\,\|) = 1/2$.

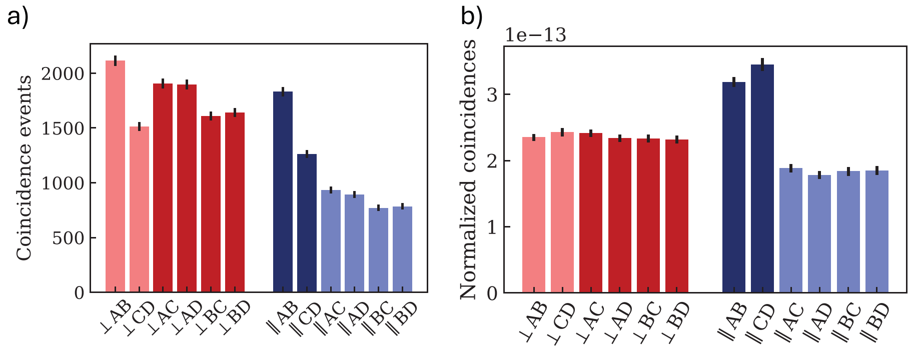


Figure 3. Photon correlations at the prover, raw coincidences CC_{ij} (a) and normalized coincidences CC_{ij}^{norm} (b) for a 5 h long measurement. For orthogonal verifier qubits (⊥, red), theory predicts equal rates which is well reproduced in the experiment. For parallel qubits (‖, blue), only ‖AB and ‖CD events are expected—the unwanted events are due to imperfections of our single-photon source as explained in the text. The error bars indicate the statistical uncertainties assuming uncorrelated errors (shot noise).

Table 1. Expected and measured probabilities, and their statistical errors (shot noise).

	Theory	Experiment
$\mathbb{P}(\oslash\mid\perp)$	$1/4$	NA
$\mathbb{P}(\oslash\mid\parallel)$	$1/2$	NA
$\mathbb{P}(0\mid\perp,\text{concl.})$	$1/3$	0.34 ± 0.01
$\mathbb{P}(1\mid\perp,\text{concl.})$	$2/3$	0.66 ± 0.01
$\mathbb{P}(0\mid\parallel,\text{concl.})$	1	0.48 ± 0.01
$\mathbb{P}(1\mid\parallel,\text{concl.})$	0	0.52 ± 0.01

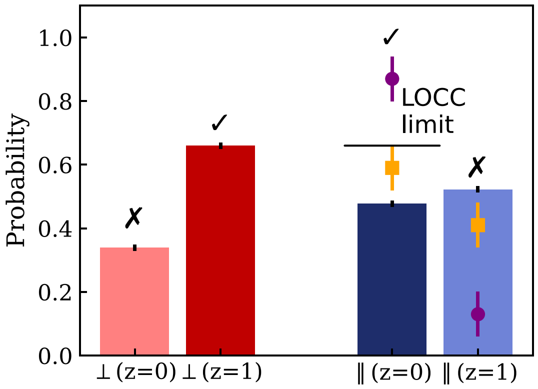


Figure 4. Conditional probabilities of prover response for both orthogonal (⊥) and parallel (‖) qubits sent from the verifiers, conditioned on the response being conclusive. The dark colored bars indicate a 'correct' (✓) response from the prover while the light color indicates an 'incorrect' answer (✗). The probability of $z=0$ is obtained from the sum of AB and CD coincidences and the probability for $z=1$ is determined from the sum of the other four 2-fold coincidences. To obtain probabilities, both are divided by the total amount of 2-fold coincidences. The 'LOCC limit' of $2/3$ is the maximal achievable probability for attackers under the LOCC assumption. Symbols show predictions for our setup but using an improved single photon source (orange squares for only an improved purity, purple circles for improved purity and indistinguishability).

Now, we discuss the different probabilities conditioned on a conclusive answer, i.e. that two photons were detected. For the case of orthogonal qubits (⊥) arriving from the verifiers, since no HOM photon bunching happens, all 6 coincidence events are equally probable. We obtain $\mathbb{P}(0\mid\perp,\text{concl.})=2/6=1/3$ and $\mathbb{P}(1\mid\perp,\text{concl.})=4/6=2/3$. This is important, also in the ideal case, the prover will return the 'wrong' answer $z=0$ that should indicate parallel qubits. Finally, for parallel ‖ qubits, the photons exit BS1 through the same port as a consequence of HOM photon bunching, only AB and CD coincidences can occur which results in $z=0$ and consequently $\mathbb{P}(0\mid\parallel,\text{concl.})=1$.

These expectations and the experimental results calculated from the data in figure 3 are shown in table 1 and figure 4. We see that the mentioned unexpected coincidences (AC, AD, BC, BD for ‖ qubits) results in a non-zero $\mathbb{P}(1\mid\parallel,\text{concl.})$, which by normalization ($\mathbb{P}(0\mid\parallel,\text{concl.})+\mathbb{P}(1\mid\parallel,\text{concl.})=1$) results in a reduced

$\mathbb{P}(0|\,\|,\text{concl.})$. Before discussing the origin of this deviation from expectation, we now discuss the theoretical bound for secure QPV.

Local operations and classical communication (LOCC) attack. We now sketch which best-case probabilities two adversaries can obtain, if they are restricted to LOCC. Every round, each adversary intercepts (see figure 1) the qubit sent by the verifier closest to them and measures it in a certain basis (diamonds in figure 1). Then, they share their results with the other adversary and formulate a response that is sent to the verifiers (circles in figure 1). Assuming that the verifiers use all three mutually unbiased bases, there is a $1/3$ probability that the adversaries have measured in the correct basis which enables them to return the correct expected result with certainty. For the other two basis choices (each also occurring with a $1/3$ probability), there is still a chance of $1/2$ to guess correctly the answer, therefore we obtain as the correct-guessing probability of the LOCC adversaries

$$\mathbb{P}^{\text{LOCC}}_{\text{succes}} = \frac{1}{3}\left(1+\frac{1}{2}+\frac{1}{2}\right) = \frac{2}{3}. \tag{2}$$

A proper proof for this bound is given in [24]. As mentioned before, even in an ideal experiment and without adversaries, for orthogonal qubits, the result is correct with only a chance of $2/3$. Since, however, ideally, equal amounts of rounds are played with orthogonal and parallel qubits, where the latter results always in the correct answer, the correct answer is sent with probability $5/6$.

4. Discussion

For orthogonal qubits ($\perp$) the measurement data follows the expected distribution where $2/3$ of the time the honest prover responds correctly as seen in figure 4, and we conclude that differences in efficiencies in the setup are not significant for the prover responses in this case. For parallel ($\|$) qubits, as we have mentioned, our data deviates from the expectations, the origin of this we explore now.

We have made a simple model of our experiment including photon source parameters, and all characteristics of the optical setup including loss, unbalanced fiber beam splitters, and detection efficiencies, a detailed characterization is given in the supplemental information. The single-photon source is characterized by the single-photon purity P and the photon indistinguishability or wave-function overlap M [33, 35, 36, 42]—because our protocol is loss-resilient, we ignore the single-photon brightness here. The single-photon purity P is given by $P = 1 - g^{(2)}$ where the zero-time second-order correlation function $g^{(2)}$ is measured in a Hanbury Brown and Twiss experiment. To obtain the wavefunction overlap M, we first measure in a HOM experiment the zero-time second-order HOM correlation functions for orthogonal ($g^{(2)}_{\perp}$) and parallel ($g^{(2)}_{\|}$) polarized photons. From this, the interferometric HOM visibility $\mathcal{V}_{\text{HOM}}$ can be calculated from [43, 44]

$$\mathcal{V}_{\text{HOM}} = \frac{g^{(2)}_{\perp} - g^{(2)}_{\|}}{g^{(2)}_{\perp}}. \tag{3}$$

Now we can calculate the bare photon indistinguishability or wave-function overlap from [43]

$$M = \mathcal{V}_{\text{HOM}}\left(1 + g^{(2)}\right), \tag{4}$$

which shows that the interferometric visibility $\mathcal{V}_{\text{HOM}}$ is reduced by a non-ideal single-photon purity.

For our source, we measure $g^{(2)}_{\|} = (36.8 \pm 3.0)\%$ and $g^{(2)}_{\perp} = (58.8 \pm 3.6)\%$, resulting in a interferometric visibility of $\mathcal{V}_{\text{HOM}} = (37.4 \pm 6.4)\%$ and an indistinguishability of $M = (45.8 \pm 10.1)\%$. To figure out the origin of these non-ideal results, and to identify where our experiment can most easily be improved, we use our model to predict the most critical QPV probability $\mathbb{P}(0|\,\|,\text{concl.})$, i.e. that the prover answers $z = 0$ on parallel inputs $|\Psi_0\rangle \,\|\, |\Psi_1\rangle$. We use all our experimental details but alter the single photon performance metrics—using experimental data from an excellent single photon source by Tomm *et al* [35]. We consider two cases in addition to ours (A), first using all metrics from Tomm *et al* (B), and then only their single photon purity but our indistinguishability (C). In each case, indistinguishability data of photons produced 1 μs apart are used. All results are shown in table 2. We see that a near-ideal single-photon source (case B, also indicated by the purple symbol in figure 4) is sufficient to clearly exceed the threshold of $\mathbb{P}(0|\,\|,\text{concl.}) = 2/3$, but also just an improved purity would bring our experiment closer to this threshold (case C, orange symbol in figure 4). In our case, this is caused by non-resonant background emission, finite cross-polarization laser extinction [45], and by re-excitation of the QD since the length of the excitation pulse was similar to the QD lifetime of around 100 ps [39].

Table 2. Overview of the parameters and resulting conditional probability $\mathbb{P}(0|\,\|, \text{concl.})$ for our single-photon source (A), the source presented in Tomm *et al* (B, [35]) and for a source similar to our (A) but with improved single-photon purity (C). The derivation of the correlation values and uncertainties is explained in supplemental section C.

	Our work (A)	Tomm *et al* (B)	Mix (C)
Purity P	0.776 ± 0.017	0.979 ± 0.001	0.979 ± 0.001
$g_{\|}^{(2)}$	0.368 ± 0.030		
$g_{\perp}^{(2)}$	0.588 ± 0.036		
$\mathcal{V}_{\text{HOM}}$	0.374 ± 0.064	0.940 ± 0.001	0.448 ± 0.100
M	0.458 ± 0.101	0.960 ± 0.005	0.458 ± 0.101
$\mathbb{P}(0|\,\|, \text{concl.})$	0.47 ± 0.03	0.890 ± 0.003	0.55 ± 0.06

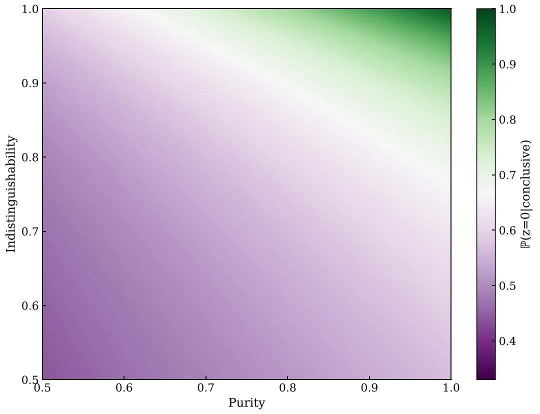


Figure 5. Probability of a correct $z = 0$ response $\mathbb{P}(0|\,\|, \text{concl.})$ depending on single-photon purity and indistinguishability using otherwise our experimental parameters. The white line marks the threshold of $2/3$ above which (green) a LOCC attack is not successful.

We show in figure 5 how the probability $\mathbb{P}(0|\,\|, \text{concl.})$ depends on the single-photon purity and indistinguishability, where otherwise our experimental parameters and inaccuracies given in the supplemental material section A are used. We see that both purity and indistinguishability need to be high to exceed the threshold of $2/3$.

Finally, although the initial polarization state fidelity at the prover is very high, this fidelity can decrease by around a few percent during the measurements, most likely by temperature fluctuations of the 200 m long fiber. This decreases the wave-function overlap by a similar amount and with this the HOM visibility.

5. Conclusions and outlook

We have shown first experimental results for a loss-tolerant quantum position verification protocol, using a temporally demultiplexed quantum dot—microcavity based single-photon source. We found that the HOM visibility of our single-photon source is the limiting factor to reach the threshold for quantum secure discrimination between a honest prover and adversaries that are restricted to LOCC, i.e. not having shared entanglement. We also found that with an improved single-photon source, this threshold is within reach—the single-photon purity and indistinguishability can be improved by using shorter excitation pulses to avoid re-excitation and improve the wave-function overlap, and improved cross-polarization to avoid contamination of the single-photon pulses by the excitation laser.

For future research, next to improvements of the single-photon source, we stress that, addressing the slow quantum information loophole is most urgent as it would allow using existing fiber networks, and a promising candidate is a functional single-photon QPV protocol [26] in combination with a commitment step [30].

Data availability statement

The data that support the findings of this study are openly available at the following URL/DOI: https://doi.org/10.5281/zenodo.15851088.

Acknowledgments

We acknowledge funding from NWO/OCW (Quantum Software Consortium, Nos. 024.003.037, 024.003.037/3368), from the Dutch Ministry of Economic Affairs (Quantum Delta NL, No. NGF.1582.22.025), and from the European Union's Horizon 2020 research and innovation program under Grant Agreement No. 862035 (QLUSTER).

ORCID iDs

Kirsten Kanneworff 0000-0002-4777-8966
Mio Poortvliet 0000-0003-3999-3962
Petr Steindl 0000-0001-9059-9202
Wolfgang Löffler 0000-0001-6587-8947

References

[1] Chandran N, Goyal V, Moriarty R and Ostrovsky R 2009 Position based cryptography *Advances in Cryptology - Crypto 2009* ed S Halevi (Springer) pp 391–407
[2] Kent A, Munro W, Spiller T and Beausoleil R 2006 Tagging systems *US Patent* (Patent number: US 7,075,438 B2)
[3] Kent A, Munro W J and Spiller T P 2011 Quantum tagging: authenticating location via quantum information and relativistic signaling constraints *Phys. Rev. A* **84** 012326
[4] Kent A 2011 Quantum tagging for tags containing secret classical data *Phys. Rev. A* **84** 022335
[5] Brassard G 2011 The conundrum of secure positioning *Nature* **479** 307
[6] Unruh D 2014 Quantum position verification in the random oracle model *Advances in Cryptology - CRYPTO 2014* (*Berlin, Heidelberg*) vol 8617, J A Garay and R Gennaro (*Lecture Notes in Computer Science*) (Springer)
[7] Lau H-K and Lo H-K 2011 Insecurity of position-based quantum-cryptography protocols against entanglement attacks *Phys. Rev. A* **83** 012322
[8] Malaney R A 2010 Location-dependent communications using quantum entanglement *Phys. Rev. A* **81** 042319
[9] Malaney R A 2010 Quantum location verification in noisy channels *2010 IEEE Global Telecommunications Conf. GLOBECOM 2010* pp 1–6 (arXiv:1004.4689)
[10] Buhrman H, Chandran N, Fehr S, Gelles R, Goyal V, Ostrovsky R and Schaffner C 2014 Position-based quantum cryptography: impossibility and constructions *SIAM J. Comput.* **43** 150
[11] Qi B and Siopsis G 2015 Loss-tolerant position-based quantum cryptography *Phys. Rev. A* **91** 042337
[12] Miller C A and Alnawakhtha Y 2024 Perfect cheating is impossible for single-qubit position verification (arXiv:2406.20022 [quant-ph])
[13] Amer O, Chakraborty K, Cui D, Kaleoglu F, Lim C, Liu M and Pistoia M 2024 Certified randomness implies secure classical position-verification (arXiv:2410.03982 [quant-ph])
[14] Escolà-Farràs L, Palais L C and Speelman F 2024 A quantum cloning game with applications to quantum position verification (arXiv:2410.22157 [quant-ph])
[15] George I, Allerstorfer R, Lunel P V and Chitambar E 2024 Orthogonality broadcasting and quantum position verification (arXiv:2311.00677 [quant-ph])
[16] May A 2019 Quantum tasks in holography *J. High Energy Phys.* JHEP10(2019)233
[17] Olivo A, Chabaud U, Chailloux A and Grosshans F 2020 Breaking simple quantum position verification protocols with little entanglement (arXiv:2007.15808 [quant-ph])
[18] Das S and Siopsis G 2021 Practically secure quantum position verification *New J. Phys.* **23** 063069
[19] Liu J, Liu Q and Qian L 2022 Beating classical impossibility of position verification (arXiv:2109.07517 [quant-ph])
[20] Junge M, Kubicki A M, Palazuelos C and Pérez-García D 2022 Geometry of banach spaces: a new route towards position based cryptography *Commun. Math. Phys.* **394** 625
[21] Cree J and May A 2023 Code-routing: a new attack on position verification *Quantum* **7** 1079
[22] Allerstorfer R, Buhrman H, May A, Speelman F and Verduyn Lunel P 2024 Relating non-local quantum computation to information theoretic cryptography *Quantum* **8** 1387
[23] Allerstorfer R, Buhrman H, Speelman F and Lunel P V 2022 On the role of quantum communication and loss in attacks on quantum position verification (arXiv:2208.04341)
[24] Allerstorfer R, Buhrman H, Speelman F and Lunel P V 2022 Towards practical and error-robust quantum position verification (arXiv:2106.12911)
[25] Lim C C W, Xu F, Siopsis G, Chitambar E, Evans P G and Qi B 2016 Loss-tolerant quantum secure positioning with weak laser sources *Phys. Rev. A* **94** 032315
[26] Bluhm A, Christandl M and Speelman F 2022 A single-qubit position verification protocol that is secure against multi-qubit attacks *Nat. Phys.* **18** 623
[27] Asadi V, Cleve R, Culf E and May A 2024 Linear gate bounds against natural functions for position-verification (arXiv:2402.18648 [quant-ph])
[28] Escolà-Farràs L and Speelman F 2023 Single-qubit loss-tolerant quantum position verification protocol secure against entangled attackers *Phys. Rev. Lett.* **131** 140802
[29] Escolà-Farràs L and Speelman F 2024 Lossy-and-constrained extended non-local games with applications to cryptography: BC, QKD and QPV (arXiv:2405.13717 [quant-ph])
[30] Allerstorfer R, Bluhm A, Buhrman H, Christandl M, Escolà-Farràs L, Speelman F and Lunel P V 2023 Making existing quantum position verification protocols secure against arbitrary transmission loss (arXiv:2312.12614)
[31] Hong C K, Ou Z Y and Mandel L 1987 Measurement of subpicosecond time intervals between two photons by interference *Phys. Rev. Lett.* **59** 2044

[32] Meyer-Scott E, Silberhorn C and Migdall A 2020 Single-photon sources: approaching the ideal through multiplexing *Rev. Sci. Instrum.* **91** 041101

[33] Somaschi N *et al* 2016 Near-optimal single-photon sources in the solid state *Nat. Photon* **10** 340

[34] Snijders H J, Frey J A, Norman J, Flayac H, Savona V, Gossard A C, Bowers J E, van Exter M P, Bouwmeester D and Löffler W 2018 Observation of the unconventional photon blockade *Phys. Rev. Lett.* **121** 043601

[35] Tomm N *et al* 2021 A bright and fast source of coherent single photons *Nat. Nanotechnol.* **16** 399

[36] Thomas F S, Nilsson M, Ciaccia C, Jünger C, Rossi F, Zannier V, Sorba L, Baumgartner A and Schönenberger C 2021 Spectroscopy of the local density of states in nanowires using integrated quantum dots *Phys. Rev. B* **104** 115415

[37] Steindl P *et al* 2021 Artificial coherent states of light by multiphoton interference in a single-photon stream *Phys. Rev. Lett.* **126** 143601

[38] Steindl P, Van Der Ent T, Van Der Meer H, Frey J, Norman J, Bowers J, Bouwmeester D and Löffler W 2023 Resonant two-laser spin-state spectroscopy of a negatively charged quantum-dot–microcavity system with a cold permanent magnet *Phys. Rev. Appl.* **20** 014026

[39] Poortvliet M, Steindl P, Kuijf I, Visser H, van Amersfoort A and Löffler W 2025 Picosecond laser pulses for quantum dot–microcavity-based single-photon generation by cascaded electro-optic modulation of a narrow-linewidth laser *Phys. Rev. Appl.* **23** 014017

[40] Steindl P, Frey J, Norman J, Bowers J, Bouwmeester D and Löffler W 2023 Cross-polarization-extinction enhancement and spin-orbit coupling of light for quantum-dot cavity quantum electrodynamics spectroscopy *Phys. Rev. Appl.* **19** 064082

[41] Bienfang J, Gerrits T, Kuo P, Migdall A, Polyakov S and Slattery O T 2023 Single-photon sources and detectors dictionary *Technical Report* NIST IR 8486 (National Institute of Standards and Technology (U.S.))

[42] Ding X *et al* 2023 High-efficiency single-photon source above the loss-tolerant threshold for efficient linear optical quantum computing (arXiv:2311.08347)

[43] Patel R B, Bennett A J, Cooper K, Atkinson P, Nicoll C A, Ritchie D A and Shields A J 2008 Postselective two-photon interference from a continuous nonclassical stream of photons emitted by a quantum dot *Phys. Rev. Lett.* **100** 207405

[44] Ollivier H *et al* 2021 Hong-Ou-Mandel interference with imperfect single photon sources *Phys. Rev. Lett.* **126** 063602

[45] González-Ruiz E M, Bjerlin J, Sandberg O A D and Sørensen A S 2025 Two-photon correlations and Hong-Ou-Mandel visibility from an imperfect single-photon source *Phys. Rev. Appl.* **23** 054063