Towards experimental demonstration of quantum position verification using true single photons

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

[1]*Leiden Institute of Physics, Leiden, The Netherlands*
[2]*Department of Physics, University of California, Santa Barbara, California, USA*
[3]*QuSoft, Amsterdam, The Netherlands*
[4]*CWI, Amsterdam, The Netherlands*
[5]*Sorbonne Université, CNRS, LIP6, France*
[6]*University of Amsterdam, The Netherlands*
[7]*Quantinuum, London, United Kingdom*

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. However, 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. 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 4 detectors is rendering the protocol resilient to loss. With this we are able to show first results towards an experimental demonstration of quantum position verification.

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 if a shared private key is established which requires physical contact of the parties [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 Fig. 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 quantum position verification 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].
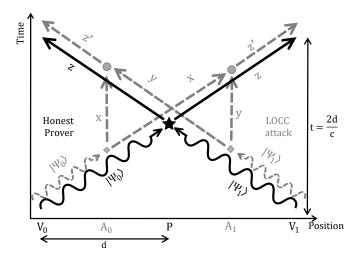
* kanneworff@physics.leidenuniv.nl
† loeffler@physics.leidenuniv.nl

Figure 1. Space-time diagram of a one-dimensional QPV protocol showing the prover (P) centered between two verifiers (V_0 and V_1, solid black) where curly (straight) lines indicate quantum (classical) information exchange. Dashed grey 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.

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 Refs. [11, 25]. We will in-

vestigate 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 recognizable. The second major loophole appears if we transport the photons through fiber networks, where the speed of light is reduced compared to free space, giving attackers using free-space communications an advantage. This 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 – 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 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 that can be avoided in principle as we show. We conclude with an outlook for future experiments.

I. PROTOCOL

Photon loss is one of the most important limiting factors for any experimental realization of quantum position verification. 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 full loss-tolerant QPV protocol was proposed by Qi and Siopsis [11] and a first experimental proposal for such a protocol was developed by Lim et al. [25]. We use here an adaptation of the latter by Allerstorfer et al. [24], the SWAP protocol, where instead of polarizing beamsplitters non-polarizing 50:50 beamsplitters are used and potentially all 3 mutually unbiased polarization bases (we show here one basis only).

The SWAP protocol entails, see Fig. 1:

1. **Preparation:** Verifiers V_0 and V_1 share via their private channel a uniformly drawn random sequence of basis choices and randomly parallel or orthogonal states in the basis, e.g. $|\Psi_0\rangle$ and $|\Psi_1\rangle$. Encoded in single photons, these qubits are sent to the prover such that they arrive simultaneously.

2. **Measurement ⋆:** The prover performs the quantum measurement based on two-photon Hong-Ou-Mandel (HOM) quantum interference [31] but with two additional beamsplitters and 4 detectors, which allows to discriminate HOM photon bunching from

loss as explained below. The prover returns a classical response $z = 0$ if $|\Psi_0\rangle \parallel |\Psi_1\rangle$, $z = 1$ if $|\Psi_0\rangle \perp |\Psi_1\rangle$, 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 $1 \dots 3$ the verifiers check if the distributions of answers returned by the prover $z = \{0, 1, \varnothing\}$ follows the expected distribution within a certain error margin.

II. EXPERIMENT

A. The single-photon source

Essential for our experiment shown in Fig. 2 is the source of single photons. We use a single negatively charged self-assembled InGaAs/GaAs quantum dot (QD) embedded in an optical microcavity [32–35]. 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 Refs. [33, 36, 37]. 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 [38]. This enables production of laser pulses with tunable pulse width (of around 100 ps) and pulse period (9 ns) at a well-defined center wavelength. These parameters provide a good trade-off between single-photon brightness and quality of the single photons [38]. The single photons are separated from the laser light using a cross-polarization technique enabling laser extinction on the order of 10^{-6} [39] and collected in a polarization-maintaining (PM) single-mode fiber.

B. QPV setup

The overall scheme of the QPV experiment is shown in Fig. 2. For the present implementation of the SWAP protocol, we demultiplex and distribute consecutive single photons from the quantum dot source to both verifiers. For this, we first temporally demultiplex photons using a fiber switch (Agiltron NPNS, 1 μs switching time). The time delay of the demultiplexer setup is adjusted to the switching frequency, 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. To simulate the distance between the verifiers and the prover, 200 m of single-mode optical fiber cable (780HP) is used. The overall
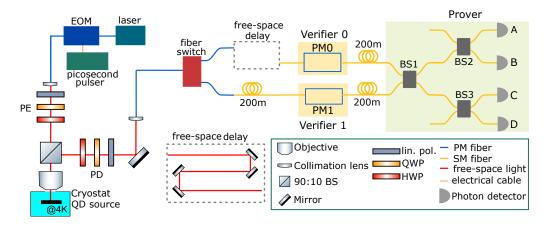
Figure 2. Schematic of the experimental setup. The electro-optic modulator (EOM) is used to generate the picosecond pulses, PE and PD are the polarization control elements of the excitation and detection paths, PM0 and 1 are the polarization modulators of the verifiers, and BS1..3 are 50:50 fiber-based beamsplitters.

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 non-polarization preserving 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.

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 (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. From these coincidence events, the prover determines their answer, and reports either an inconclusive result ($z = \oslash$, if zero, one, or more than two photons are detected) or a conclusive result if two

photons are detected. If conclusive, the prover returns $z = 0$ for AB and CD events, i.e., if both photons are detected in the same arm after the first beamsplitter BS1 (and HOM photon bunching probably did happen). If HOM bunching did not happen, that is for AC, AD, BC and BD events, the prover returns $z = 1$. As mentioned above, adding BS2 and BS3 makes the protocol resilient against loss since also bunched photons sometimes are detected as AB or CD coincidence events.
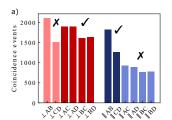
III. RESULTS

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-minute intervals. Steps (ii) and (iii) are repeated for the measurement time. Fig. 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 Fig. 3, red bars. If the qubits from the verifiers are equal ($\parallel$), we would expect perfect HOM photon bunching and that only AB and CD events appear. In Fig. 3(a), we indeed observe an enhancement of these events, but also a rather large amount of unexpected coincidences, which we will discuss below. In Fig. 3(b) we show the normalized coincidences

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

where CC_{ij} are the 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
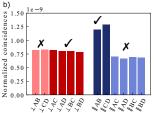
Figure 3. Photon correlations at the prover, raw coincidences CC_{ij} (a) and normalized coincidences CC_{ij}^{norm} (b) for a 5 hour long measurement. For orthogonal verifier qubits ($\perp$, red), theory predicts equal rates which is well reproduced in the experiment. For parallel qubits ($\parallel$, blue), only $\parallel$AB and $\parallel$CD events are expected - the unwanted events are due to imperfections of our single-photon source as explained in the text.

$CC_{AB}^{\parallel}$ and $CC_{CD}^{\parallel}$ in Fig. 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 I and Fig. 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 $\mathbb{P}(\oslash|\perp)=1/4$. In the case of parallel qubits ($\parallel$), HOM photon bunching happens at BS1 with certainty, and therefore the chance of an inconclusive result is twice as high: $\mathbb{P}(\oslash|\parallel) = 1/2$.

Now, we discuss the different probabilities conditioned on a conclusive answer, i.e., that two photons were detected. For the case of orthogonal qubits ($\perp$) arriving from the verifiers, since no HOM photon bunching happens, all 6 coincidence events are equally probable. We obtain $\mathbb{P}(0|\perp, \text{concl.}) = 2/6 = 1/3$ and $\mathbb{P}(1|\perp, \text{concl.}) = 4/6 = 2/3$. 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 $\parallel$ 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 $\mathbb{P}(0|\parallel, \text{concl.}) = 1$.

These expectations and the experimental results calculated from the data in Fig. 3 are shown in Table I and Fig. 4.

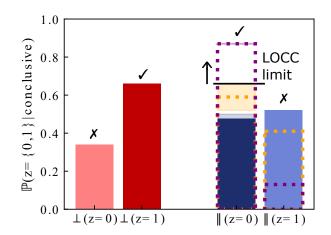|	Theory	Experiment
$\mathbb{P}(\oslash\|\perp)$	1/4	NA
$\mathbb{P}(\oslash\|\parallel)$	1/2	NA
$\mathbb{P}(0\|\perp, \text{concl.})$	1/3	0.34
$\mathbb{P}(1\|\perp, \text{concl.})$	2/3	0.66
$\mathbb{P}(0\|\parallel, \text{concl.})$	1	0.48
$\mathbb{P}(1\|\parallel, \text{concl.})$	0	0.52

Table I. Expected and measured probabilities.

Figure 4. Conditional probabilities of prover response for both orthogonal ($\perp$) and parallel ($\parallel$) qubits sent from the verifiers, conditioned on the response being conclusive. The dark colored bars indicate a 'correct' ($\checkmark$) response from the prover while the light color indicates an 'incorrect' answer ($\times$). 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 here by the total amount of 2-fold coincidences. The 'LOCC limit' of $2/3$ is the maximum probability of attackers responding correctly under the LOCC assumption. Dotted bars show the modeled conditional probabilities for a better quantum dot single-photon sources as explained in the text.

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 Fig. 1) the qubit sent by the verifier closest to them and measures it in a certain basis (diamonds in Fig. 1). Then, they share their results with the other adversary and formulate a response that is sent to the verifiers (circles in Fig. 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

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

A proper proof for this bound is given in Ref. [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.

IV. 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 Fig. 4, and we conclude that differences in efficiencies in the setup they are not significant for the prover responses in this case. For parallel ($\parallel$) 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 the single-photon purity P and the photon indistinguishability or wave-function overlap M [32, 34, 35, 40] - 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 type experiment. To obtain the wavefunction overlap M, we first measure in a Hong-Ou-Mandel type experiment the zero-time second-order correlation functions for orthogonal ($g^{(2)}_{\perp,HOM}$) and parallel and ($g^{(2)}_{\parallel,HOM}$) polarized photons. From this, the interferometric Hong-Ou-Mandel visibility $\mathcal{V}_{HOM}$ can be obtained from [41]

$$\mathcal{V}_{HOM} = \frac{g^{(2)}_{\perp} - g^{(2)}_{\parallel}}{g^{(2)}_{\perp}}. \quad (3)$$

Now we can calculate the bare photon indistinguishability or wave-function overlap from [34]

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

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

For our source, we measure $g^{(2)}_{\parallel,HOM} = (36.8 \pm 3.0)\%$ and $g^{(2)}_{\perp,HOM} = (58.8 \pm 3.6)\%$, resulting in a interferometric visibility of $\mathcal{V}_{HOM} = (37.4 \pm 6.4)\%$ and an indistinguishability of $M = (54.2 \pm 10.1)\%$. To figure out

	Here (A)	Tomm et al. (B)	Mix (C)
Purity P	0.776 ± 0.017	0.979 ± 0.001	0.979 ± 0.001
$g^{(2)}_{\parallel}(0)$	0.368 ± 0.030		
$g^{(2)}_{\perp}(0)$	0.588 ± 0.036		
$\mathcal{V}_{HOM}$	0.374 ± 0.064	0.916 ± 0.001	0.520 ± 0.100
M	0.542 ± 0.101	0.960 ± 0.005	0.542 ± 0.101
$\mathbb{P}(0|\parallel,\text{concl.})$	0.47 ± 0.03	0.870 ± 0.003	0.59 ± 0.07

Table II. Overview of the parameters and resulting conditional probability $\mathbb{P}(0|\parallel,\text{concl.})$ for our single-photon source (A), the source presented in Tomm et. al. (B, [34]) and for a source similar to our (A) but with improved single-photon purity (C).

the origin of our non-ideal result above, and to identify where our experiment can most easily be improved, we use our model to predict the most critical QPV probability $\mathbb{P}(0|\parallel,\text{concl.})$, i.e. that the prover answers $z = 0$ on parallel inputs $|\Psi_0\rangle \parallel |\Psi_1\rangle$. 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. [34]. 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 II. We see that a near-ideal single-photon source (case B, also indicated by the purple bar in Fig. 4) is sufficient to clearly exceed the threshold of $\mathbb{P}(0|\parallel,\text{concl.}) = 2/3$, but also just an improved purity would bring our experiment closer to this threshold (case C, orange bar in Fig. 4). In our case, this is caused by non-resonant background emission, finite cross-polarizastion laser extinction, and by re-excitation of the quantum dot since the length of the excitation pulse was similar to the QD lifetime.

Finally, we show in Fig. 5 how the probability $\mathbb{P}(0|\parallel,\text{concl.})$ 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.

V. 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 Hong-Ou-Mandel visibility of our single-photon source is the limiting factor to reach the threshold for quantum secure discrimination between a honest prover and adver-
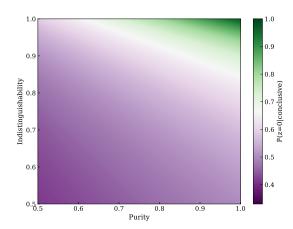
Figure 5. Probability of a correct $z = 0$ response $\mathbb{P}(0| \; \|$, concl.) depending on single-photon purity and indistinguishability using otherwise our experimental parameters. The white line marks the threshold of 2/3 above which (green) a LOCC attack is not successful.

saries that are restricted to local operations and classical communication (LOCC), i.e., not having shared entanglement. We also found that with an improved single photon source, this threshold can easily be reached. 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].

ACKNOWLEDGEMENTS

[1] Chandran, N., Goyal, V., Moriarty, R. & Ostrovsky, R. Position Based Cryptography. In Halevi, S. (ed.) *Advances in Cryptology - CRYPTO 2009*, 391–407 (Springer, Berlin, Heidelberg, 2009).

[2] Kent, A., Munro, W., Spiller, T. & Beausoleil, R. Tagging systems, 2006. *US patent* (2006).

[3] Kent, A., Munro, W. J. & Spiller, T. P. Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. *Physical Review A* **84**, 012326 (2011).

[4] Kent, A. Quantum tagging for tags containing secret classical data. *Physical Review A* **84**, 022335 (2011).

[5] Brassard, G. The conundrum of secure positioning. *Nature* **479**, 307 (2011).

[6] Unruh, D. Quantum position verification in the random oracle model (2014). Cryptoeprint:2014/118.

[7] Kent, A., Munro, W., Spiller, T. & Beausoleil, R. Tagging Systems (2006).

[8] Malaney, R. A. Location-Dependent Communications Using Quantum Entanglement. *Phys. Rev. A* **81**, 042319 (2010).

[9] Malaney, R. A. Quantum Location Verification in Noisy Channels. In *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, 1–6 (2010). 1004.4689.

[10] Buhrman, H., Chandran, N., Fehr, S., Gelles, R., Goyal, V., Ostrovsky, R. & Schaffner, C. Position-Based Quantum Cryptography: Impossibility and Constructions. *SIAM J. Comput.* **43**, 150 (2014).

[11] Qi, B. & Siopsis, G. Loss-Tolerant Position-Based Quantum Cryptography. *Phys. Rev. A* **91**, 042337 (2015). 1502.02020.

[12] Miller, C. A. & Alnawakhtha, Y. Perfect cheating is impossible for single-qubit position verification (2024). ArXiv:2406.20022 [quant-ph].

[13] Amer, O., Chakraborty, K., Cui, D., Kaleoglu, F., Lim, C., Liu, M. & Pistoia, M. Certified Randomness implies Secure Classical Position-Verification (2024). ArXiv:2410.03982 [quant-ph].

[14] Escolà-Farràs, L., Palais, L. C. & Speelman, F. A quantum cloning game with applications to quantum position verification (2024). ArXiv:2410.22157 [quant-ph].

[15] George, I., Allerstorfer, R., Lunel, P. V. & Chitambar, E. Orthogonality Broadcasting and Quantum Position Verification (2024). ArXiv:2311.00677 [quant-ph].

[16] May, A. Quantum tasks in holography. *Journal of High Energy Physics* **2019**, 233 (2019).

[17] Olivo, A., Chabaud, U., Chailloux, A. & Grosshans, F. Breaking simple quantum position verification protocols with little entanglement (2020). ArXiv:2007.15808 [quant-ph].

[18] Das, S. & Siopsis, G. Practically secure quantum position verification. *New Journal of Physics* **23**, 063069 (2021).

[19] Liu, J., Liu, Q. & Qian, L. Beating Classical Impossibility of Position Verification (2022). ArXiv:2109.07517 [quant-ph].

[20] Junge, M., Kubicki, A. M., Palazuelos, C. & Pérez-García, D. Geometry of Banach Spaces: A New Route Towards Position Based Cryptography. *Communications in Mathematical Physics* **394**, 625 (2022).

[21] Cree, J. & May, A. Code-routing: a new attack on position verification. *Quantum* **7**, 1079 (2023).

[22] Allerstorfer, R., Buhrman, H., May, A., Speelman, F. & Verduyn Lunel, P. Relating non-local quantum computation to information theoretic cryptography. *Quantum* **8**, 1387 (2024).

[23] Allerstorfer, R., Buhrman, H., Speelman, F. & Lunel, P. V. On the Role of Quantum Communication and Loss in Attacks on Quantum Position Verification (2022). 2208.04341.

[24] Allerstorfer, R., Buhrman, H., Speelman, F. & Lunel, P. V. Towards Practical and Error-Robust Quantum Position Verification (2022). 2106.12911.

[25] Lim, C. C. W., Xu, F., Siopsis, G., Chitambar, E., Evans, P. G. & Qi, B. Loss-Tolerant Quantum Secure Positioning with Weak Laser Sources. *Phys. Rev. A* **94**, 032315 (2016).

[26] Bluhm, A., Christandl, M. & Speelman, F. A Single-Qubit Position Verification Protocol That Is Secure

against Multi-Qubit Attacks. *Nat. Phys.* **18**, 623 (2022).

[27] Asadi, V., Cleve, R., Culf, E. & May, A. Linear gate bounds against natural functions for position-verification (2024). ArXiv:2402.18648 [quant-ph].

[28] Escolà-Farràs, L. & Speelman, F. Single-Qubit Loss-Tolerant Quantum Position Verification Protocol Secure against Entangled Attackers. *Physical Review Letters* **131**, 140802 (2023).

[29] Escolà-Farràs, L. & Speelman, F. Lossy-and-Constrained Extended Non-Local Games with Applications to Cryptography: BC, QKD and QPV (2024). ArXiv:2405.13717 [quant-ph].

[30] Allerstorfer, R., Bluhm, A., Buhrman, H., Christandl, M., Escolà-Farràs, L., Speelman, F. & Lunel, P. V. Making Existing Quantum Position Verification Protocols Secure Against Arbitrary Transmission Loss (2023). 2312.12614.

[31] Hong, C. K., Ou, Z. Y. & Mandel, L. Measurement of Subpicosecond Time Intervals between Two Photons by Interference. *Phys. Rev. Lett.* **59**, 2044 (1987).

[32] Somaschi, N., Giesz, V., De Santis, L., Loredo, J. C., Almeida, M. P., Hornecker, G., Portalupi, S. L., Grange, T., Antón, C., Demory, J., Gómez, C., Sagnes, I., Lanzillotti-Kimura, N. D., Lemaître, A., Auffeves, A., White, A. G., Lanco, L. & Senellart, P. Near-Optimal Single-Photon Sources in the Solid State. *Nature Photon* **10**, 340 (2016).

[33] Snijders, H. J., Frey, J. A., Norman, J., Flayac, H., Savona, V., Gossard, A. C., Bowers, J. E., van Exter, M. P., Bouwmeester, D. & Löffler, W. Observation of the Unconventional Photon Blockade. *Phys. Rev. Lett.* **121**, 043601 (2018).

[34] Tomm, N., Javadi, A., Antoniadis, N. O., Najer, D., Löbl, M. C., Korsch, A. R., Schott, R., Valentin, S. R., Wieck, A. D., Ludwig, A. & Warburton, R. J. A Bright and Fast Source of Coherent Single Photons. *Nat. Nanotechnol.* **16**, 399 (2021).

[35] Thomas, F. S., Nilsson, M., Ciaccia, C., Jünger, C., Rossi, F., Zannier, V., Sorba, L., Baumgartner, A. & Schönenberger, C. Spectroscopy of the Local Density of States in Nanowires Using Integrated Quantum Dots. *Phys. Rev. B* **104**, 115415 (2021).

[36] Steindl, P., Snijders, H., Westra, G., Hissink, E., Iakovlev, K., Polla, S., Frey, J. A., Norman, J., Gossard, A. C., Bowers, J. E., Bouwmeester, D. & Löffler, W. Artificial Coherent States of Light by Multiphoton Interference in a Single-Photon Stream. *Phys. Rev. Lett.* **126**, 143601 (2021).

[37] Steindl, P., Van Der Ent, T., Van Der Meer, H., Frey, J., Norman, J., Bowers, J., Bouwmeester, D. & Löffler, W. Resonant Two-Laser Spin-State Spectroscopy of a Negatively Charged Quantum-Dot–Microcavity System with a Cold Permanent Magnet. *Phys. Rev. Applied* **20**, 014026 (2023).

[38] Poortvliet, M., Steindl, P., Kuijf, I., Visser, H., van Amersfoort, A. & Löffler, W. Picosecond Laser Pulses for Quantum Dot-Microcavity Based Single Photon Generation by Cascaded Electro-Optic Modulation of a Narrow-Linewidth Laser (2024). 2408.08213.

[39] Steindl, P., Frey, J., Norman, J., Bowers, J., Bouwmeester, D. & Löffler, W. Cross-Polarization-Extinction Enhancement and Spin-Orbit Coupling of Light for Quantum-Dot Cavity Quantum Electrodynamics Spectroscopy. *Phys. Rev. Applied* **19**, 064082 (2023).

[40] Ding, X., Guo, Y.-P., Xu, M.-C., Liu, R.-Z., Zou, G.-Y., Zhao, J.-Y., Ge, Z.-X., Zhang, Q.-H., Liu, H.-L., Wang, L.-J., Chen, M.-C., Wang, H., He, Y.-M., Huo, Y.-H., Lu, C.-Y. & Pan, J.-W. High-efficiency single-photon source above the loss-tolerant threshold for efficient linear optical quantum computing (2023). ArXiv:2311.08347 [quant-ph].

[41] Patel, R. B., Bennett, A. J., Cooper, K., Atkinson, P., Nicoll, C. A., Ritchie, D. A. & Shields, A. J. Postselective Two-Photon Interference from a Continuous Nonclassical Stream of Photons Emitted by a Quantum Dot. *Phys. Rev. Lett.* **100**, 207405 (2008).

SUPPLEMENTAL INFORMATION

A. Experimental setup characterization

Here we present a precise characterization of the experimental setup, which is crucial for the model used in the main text. For this, we directly connected a continuous-wave (CW) laser to the input of the fiber switch using the wavelength of the single photons (around 935 nm) and measure the intensity of the laser light at every fiber connection with a power meter (Thorlabs PM100D). The position of every fiber connection is depicted in Fig. S1 and the measured transmission ratios are shown in Table S1. For intensity measurements behind BS1, we blocked the beam in the free-space delay stage to avoid interference effects. The transmission ratios given for the beamsplitters (BS1, BS2 and BS3) are the ratios between the input intensity and the sum of the intensities at the two outputs of the beamsplitter. The splitting ratios are presented in Table S2. The overall efficiency of the system is between 7.2% and 12.4% and depends on the path taken and detection efficiency of the detectors.
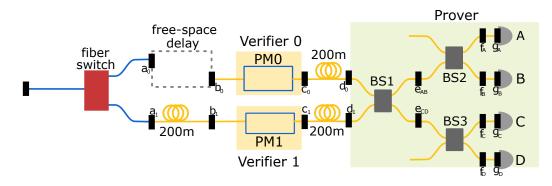

Figure S1. Sketch of a part of the experimental setup with labels indicating the measurement points for the characterization.

	Transmission (%)	Transmission (%)
	Verifier 0	Verifier 1
after switch (a)	71.2	60.3
delay stage (b)	95.4	91.5
polarization modulator (PM) (c)	81.4	89.4
200m fiber transmission (d)	86.2	85.2
total (a-d)	47.7	42.0
BS1* (e)	94.9	
BS2* ($f_{A/B}$)	99.7	
BS3* ($f_{C/D}$)	86.8	
detector A fiber (g_A)	90.6	
detector A efficiency**	100	
detector B fiber (g_B)	90.3	
detector B efficiency**	61.9	
detector C fiber (g_C)	90.7	
detector C efficiency**	68.9	
detector D fiber (g_D)	97.9	
detector D efficiency**	15.9	

Table S1. Overview of relative transmissions for each component in the experimental setup as shown in Fig. S1. The loss of the fiber-based beamsplitters (*) is measured as the ratio between the input of the beamsplitter and the sum of the two outputs. The splitting ratios themselves are described in Table S2. All detector efficiencies (**) are normalized to that of detector A.

Beamsplitter	Ratio upper output (%)	Ratio lower output (%)
BS1 (d_1)	54.5 (e_{AB})	45.5 (e_{CD})
BS2 (e_{AB})	44.1 (f_A)	55.9 (f_B)
BS3 (e_{CD})	53.0 (f_C)	47.0 (f_D)

Table S2. Overview of the splitting ratios of the fiber-based beamsplitters (Thorlabs TW930R5A2), not accounting for the total loss in transmission described in Table S1. The labels in brackets denotes between which points in the setup the ratios were measured.

B. Measured coincidence events and normalized coincidences

	Coincidence events		Normalized coincidences	
	$\perp$	$\parallel$	$\perp$ /10^{-9}	$\parallel$ /10^{-9}
AB	2115	1833	0.82	1.19
CD	1512	1261	0.83	1.29
AC	1906	934	0.82	0.70
AD	1897	893	0.81	0.67
BC	1610	770	0.81	0.69
BD	1640	784	0.79	0.68

Table S3. Overview of values reported in Fig. 3.