Steering-based randomness certification with squeezed states and homodyne measurements

Marie Ioannou,[1,*] Bradley Longstaff,[2,*] Mikkel V. Larsen,[2] Jonas S. Neergaard-Nielsen,[2] Ulrik L. Andersen,[2] Daniel Cavalcanti,[3,4] Nicolas Brunner,[1] and Jonatan Bohr Brask[2]

[1]*Department of Applied Physics, University of Geneva, 1211 Geneva, Switzerland*

[2]*Center for Macroscopic Quantum States (bigQ), Department of Physics, Technical University of Denmark, Fysikvej, 2800 Kongens Lyngby, Denmark*

[3]*Bitflow, Carrer de Piquer 23, 08004 Barcelona, Spain*

[4]*Algorithmiq Ltd, Kanavakatu 3 C, FI-00160 Helsinki, Finland*

(Received 7 February 2022; accepted 22 September 2022; published 13 October 2022)

High-quality randomness, certified to be unpredictable by eavesdroppers, is key to secure information processing. Quantum mechanics enables randomness certification with minimal trust in the devices used, by exploiting quantum nonlocality. However, such full device independence is challenging to implement. We present a scheme for quantum randomness certification based on quantum steering. The protocol is one-sided device independent, providing high security, but requires only states and measurements that are simple to realize on quantum optics platforms—squeezed vacuum states and homodyne detection. This ease of implementation is demonstrated experimentally and implies that gigahertz random bit rates should be attainable with current technology. Furthermore, our scheme is immune to the detection loophole and represents the closest to full device independence that can be achieved using purely Gaussian states and measurements.

DOI: 10.1103/PhysRevA.106.042414

I. INTRODUCTION

Randomness is an important resource in science and technology for simulations and information processing. In particular, random numbers that are unpredictable by any adversary are key to cryptographic security [1]. Random numbers can be generated from hard-to-predict physical processes, and pseudorandom-number generators, implemented in software, can expand short random seeds into longer sequences that appear random. However, classical physics is fundamentally deterministic, as are software algorithms. Therefore guaranteeing security based on classical random-number generation requires assumptions about the knowledge and computational resources available to potential eavesdroppers. Such assumptions may be difficult to justify as the adversaries might not be known.

Randomness generation based on quantum physics provides an alternative free of this limitation [2–4]. For quantum systems, there exist measurements whose outcomes cannot be predicted even given a complete quantum-mechanical description of the system and measurement device. This implies that security can be guaranteed based only on the user's own knowledge, as long as the adversary is bound by quantum mechanics. That is, the user need only trust their own characterization of the randomness-generation device. For example, randomness can be generated by detecting the output path of a single photon impinging on a beam splitter [5]. When the beam splitting ratio and other characteristics of the setup are known, the unpredictability of the outcome can be certified relative to any quantum adversary, regardless of their computational power or available resources.

Remarkably, exploiting the nonlocality [6,7] of quantum mechanics allows randomness certification even with almost uncharacterized devices. In setups violating a Bell inequality, randomness can be certified device independently, i.e., without making any assumptions about the inner workings of the devices used [8,9]. This represents a very strong form of security, as the devices can be largely untrusted, and it has been demonstrated in several experiments [9–14]. However, it is also more challenging to implement than the device-dependent approach because loophole-free Bell violation requires low noise and high detection efficiencies. This motivates the search for trade-offs, where full device independence is relaxed in order to gain ease of implementation, while still maintaining high security. Many works have explored this semi-device-independent setting in prepare-and-measure setups without nonlocality, by allowing source or measurement devices to be partially characterized; see, e.g., Refs. [15–29]. An alternative approach is to exploit Einstein-Podolsky-Rosen steering [30–32], which is a form of nonlocality intermediate between full Bell nonlocality and quantum entanglement. In a bipartite steering scenario, the device of one party is untrusted while that of the other party is characterized. This setting is thus one-sided device independent and has been considered for applications in quantum cryptography [33,34] and randomness generation [35–37]. While experiments on quantum key distribution have been demonstrated [38,39], the practical implementation of these ideas for quantum random-number generation (QRNG) is mostly unexplored [40,41].

Here, we develop a steering-based quantum randomness-certification protocol that can be implemented with simple light sources and measurements. The setup requires only squeezed light and homodyne detection and can tolerate realistic levels of loss and noise. It is thus readily implementable

*These authors contributed equally to this work.

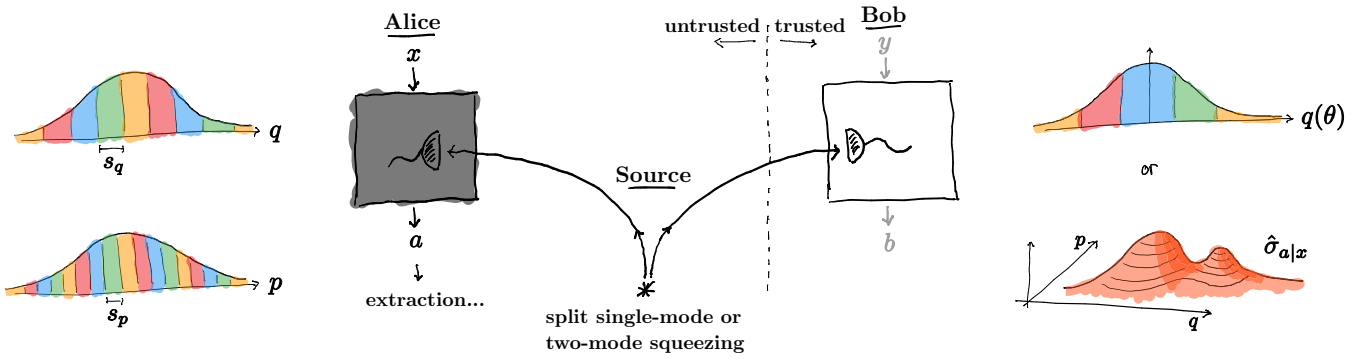

FIG. 1. Setup for steering test and randomness certification using Gaussian states and measurements, consisting of a source of squeezed, entangled states and two parties, Alice and Bob, who perform homodyne measurements. The source emits either a two-mode squeezed vacuum or a single-mode squeezed vacuum split on a balanced beam splitter. Alice measures one of two conjugate quadratures, according to a binary input x, and applies periodic binnings into o_A outcomes a. Bob either performs full state tomography or measures m_B different quadratures, according to input y, and applies a nonperiodic binning into o_B outcomes b. For certifying steering and randomness, Alice's device and the source state are untrusted, while Bob's device is assumed to be well characterized. Randomness is extracted from Alice's measurement outcome, for one of her inputs.

with existing technology, which we demonstrate by applying our protocol to data from the experiment of Ref. [42]. Randomness is certified, and we estimate that a rate of 70 kbits/s could be extracted. In a dedicated setup, significantly higher rates are expected. Fast squeezing sources, operating in the terahertz range, and homodyne detection in the gigahertz range have been realized [43]. Combined with a higher entropy per round, this should enable secret bit rates in the gigahertz range. We note that the scheme is free of any detection loophole, because (unlike single-photon detection) homodyne detection always provides an output and no data are discarded. Furthermore, the setup uses only Gaussian states and measurements. Bell nonlocality, and hence full device independence, is impossible with only Gaussian resources (this follows from the positivity of the Gaussian Wigner functions and Fine's theorem [44]). Thus our protocol in this sense provides the closest to device independence one may hope for in this setting.

Our work exploits entangled squeezed states, which are infinite dimensional, and homodyne measurements, which have continuous outcomes. Steering has been demonstrated with such resources [45–50]. However, for quantifying randomness it is convenient to work with measurements with a finite number of outcomes, where powerful methods based on semidefinite programming can be applied [51]. This can be achieved by coarse-graining the homodyne outcomes into a finite number of bins. To guide the choice of binning, we note that, as the dimension grows, a bipartite maximally entangled state in finite dimensions approaches a two-mode infinitely squeezed vacuum state. In finite dimensions, Skrzypczyk and Cavalcanti [37] found that optimal steering-based randomness generation is achieved by performing mutually unbiased measurements on maximally entangled states. The optimal measurements are conjugate, i.e., related by a Fourier transform. This suggests that randomness can be obtained by measurements of conjugate quadratures on two-mode squeezed states. In Ref. [52], Tasca *et al.* identified coarse grainings of homodyne measurements that preserve mutual unbiasedness. One may therefore expect that adopting this binning scheme will enable steering and randomness certification even at finite squeezing. Our results confirm this intuition.

II. CERTIFIED RANDOMNESS FROM STEERING

We consider a bipartite setup, as illustrated in Fig. 1. An entangled state $\hat{\rho}$ is distributed to two parties, Alice and Bob. For the purpose of certifying steering and randomness, Alice and the source are untrusted, while Bob's device is well characterized. In each round, Alice chooses one of m_A measurements each with a number o_A of outcomes. We denote her input (choice) x and output (outcome) a. Thus x and a can take m_A and o_A different values, respectively. Bob performs either full state tomography or some fixed set of measurements. In the former case, the information available after many repetitions consists of the conditional input-output probabilities of Alice $P(a|x)$ and the conditional states of Bob $\hat{\rho}_{a|x}$, or equivalently, in the assemblage of un-normalized states $\hat{\sigma}_{a|x} = P(a|x)\hat{\rho}_{a|x}$. A precise definition of steering was given in Ref. [32]. An assemblage is said to be steerable if it does not admit a local-hidden-state (LHS) model

$$\hat{\sigma}_{a|x} = \int_\Lambda \pi(\lambda) P(a|x,\lambda)\hat{\rho}_\lambda \, d\lambda, \tag{1}$$

where $\pi(\lambda)$ is a probability distribution over λ, which can be thought of as a classical common cause that determines both the output a and the quantum state $\hat{\rho}_\lambda$ of Bob. A steerable assemblage cannot be explained in terms of a classical common cause, and, in particular, $\hat{\rho}$ must then be entangled. Furthermore, a key observation from the point of view of randomness certification is that the lack of a LHS model implies that one cannot have $P(a|x) \in \{0, 1\}$ for all a, x, i.e., $P(a|x)$ cannot be completely deterministic [36]. In other words, if Bob's assemblage is steerable, then there must be some randomness in Alice's measurement outcomes. Note that randomness is extracted from the untrusted party and that only steering from Alice to Bob is required.

The amount of certifiable randomness can be quantified in terms of the maximal probability for an eavesdropper (Eve) to correctly predict the output given knowledge of the input and

other available side information (in particular, we allow Eve to be entangled with the source, but we do assume rounds to be independent and identically distributed with respect to Eve). We consider randomness to be generated for a particular input x^* and denote the corresponding guessing probability $p_g(x^*)$. By the leftover hash lemma [53], the asymptotic number of almost uniformly random bits extractable per round is given by the min-entropy $H_{\min}(x^*) = -\log_2 p_g(x^*)$. The guessing probability can be computed via the following optimization problem [36,51]:

$$\max_{\{\hat{\sigma}^e_{a|x}\}} \quad \mathrm{tr}\left[\sum_e \hat{\sigma}^e_{a=e|x^*}\right], \tag{2a}$$

$$\text{such that} \quad \sum_e \hat{\sigma}^e_{a|x} = \hat{\sigma}^{\mathrm{obs}}_{a|x} \quad \forall a, x, \tag{2b}$$

$$\sum_a \hat{\sigma}^e_{a|x} = \sum_a \hat{\sigma}^e_{a|x'} \quad \forall e, x \neq x', \tag{2c}$$

$$\hat{\sigma}^e_{a|x} \geqslant 0 \quad \forall a, x, e. \tag{2d}$$

This is equivalent to optimizing over all strategies of Eve that are compatible with the observed assemblage $\hat{\sigma}^{\mathrm{obs}}_{a|x}$ (2b) and with no-signaling from Alice to Bob and Eve (2c) [36]. Note that (2a)–(2d) constitute a semidefinite program (SDP) and can be solved efficiently numerically [54].

Performing full state tomography can be demanding experimentally, and it is then desirable to restrict Bob to some, ideally small, set of m_B measurements with o_B outcomes. In this case, the available observation from the experiment is not the assemblage, but the conditional probabilities $P(ab|xy)$, where y and b label Bob's input and output, respectively. Randomness can still be certified, and the guessing probability can again be computed via an SDP. Assuming that Bob performs positive-operator-valued measures (POVMs) with elements $\hat{M}_{b|y}$, the guessing probability is again given by the optimization (2a)–(2d), except that the condition (2b) is replaced by the requirement that Eve's strategy must reproduce the observed probabilities, $\sum_e \mathrm{tr}[\hat{M}_{b|y}\hat{\sigma}^e_{a|x}] = P(ab|xy) \quad \forall a, b, x, y$.

III. GAUSSIAN PROTOCOL

We now determine the amount of randomness certifiable in a setup using squeezed light and homodyne detection. The source distributes either a two-mode squeezed (TMS) vacuum state or a single-mode squeezed (SMS) vacuum state split on a balanced beam splitter (see Fig. 1). We let q_A, p_A and q_B, p_B denote conjugate quadratures for Alice and Bob, respectively. The initial states are chosen such that in the split single-mode case, $q_A + q_B$ is squeezed, and in the two-mode case, both $q_A + q_B$ and $p_A - p_B$ are squeezed. Alice makes $m_A = 2$ measurements of q_A and p_A (note that the local oscillator required for homodyne detection does not open up any loophole as it is untrusted). Following Ref. [52], her results are binned into o_A outcomes, resulting in POVMs

$$\hat{M}_{a|x} = \int_{\mathbb{R}} f_a(z, T_x)\, |z\rangle_x\langle z|\, dz, \tag{3}$$

where $x = q, p$ is the input, $|z\rangle_x$ are x-quadrature eigenstates, and $f_a(z, T_x)$ is a periodic mask function

$$f_a(z, T_x) = \begin{cases} 1 & \text{for } as_x \leqslant z \bmod T_x < (a+1)s_x \\ 0 & \text{otherwise.} \end{cases} \tag{4}$$

Here, T_x is the period, $s_x = T_x/o_A$ is the width of the bins (see Fig. 1), and $T_p = 2\pi/s_q$ to ensure mutual unbiasedness. We take $a \in \{0, \ldots, o_A - 1\}$.

Bob either performs tomography or performs a fixed set of measurements. In principle, optimal measurements could be determined (at least numerically) from the dual of the SDP (2a)–(2d) for tomography, which provides an optimal steering inequality. However, it is not clear that these measurements can be realized in practice, or how they might be approximated. Instead, we let Bob perform binned homodyne measurements as well: specifically, m_B quadrature measurements along directions in phase space equally spaced between q_B and p_B. He applies a binning consisting of $o_B - 1$ intervals dividing the range $[-r, r]$ evenly, and the last bin constitutes everything outside this range. We found that setting $r = 5\sigma$, where σ^2 is the largest variance in the (Gaussian) entangled initial state (i.e., the largest diagonal entry of the covariance matrix), works well for our parameter values. The central binned region is then sufficiently wide to capture the variation induced by Alice's measurements while also admitting sufficiently narrow bins for Bob's outcomes to reveal this variation without o_B being intractably large.

We model detector inefficiencies and other losses by fictitious beam splitters with transmittivity η between the source and each party. We take the losses to be symmetric for Alice and Bob, and we consider both pure loss, with vacuum entering the other port of the beam splitters, and noise, modeled by replacing the vacuum with thermal states. We compute the observed data [$\hat{\sigma}_{a|x}$ or $P(ab|xy)$] starting from the covariance matrix of the joint Gaussian state, including loss and noise. A derivation of the covariance matrix is provided in Appendix A. In order to implement the SDPs for the guessing probability, we need to work in finite dimensions. We therefore calculate the Fock-space representation of the state and measurement operators, applying a cutoff in photon number, and compute the data from there. The cutoff is chosen so as to be sufficiently large to not affect the final results; see Appendix B. We then run the SDPs given above to determine the guessing probability and min-entropy in each case. Finally, we optimize over Alice's binning period T_q.

The results are summarized in Fig. 2. We observe several interesting features. First, randomness can be generated at moderate levels of squeezing, with results shown for -4 dB for the TMS source and -6 dB for split SMS. Second, a significant amount of randomness can be certified even for sizable loss and the entropy is nonzero above $\eta \gtrsim 0.55$ for the TMS source and $\eta \gtrsim 0.75$ for split SMS. Third, allowing for added noise corresponding to 1% of the vacuum variance (0.01 shot-noise units; see Appendix A) does not dramatically decrease the performance. These numbers indicate that implementation of our protocol is well within reach of contemporary experimental techniques. Finally, performing just a few binned homodyne measurements for Bob is almost as good as tomography. For $m_B = 6$ measurements, $H_{\min}$ is within a few percent of the full-tomography result, and with

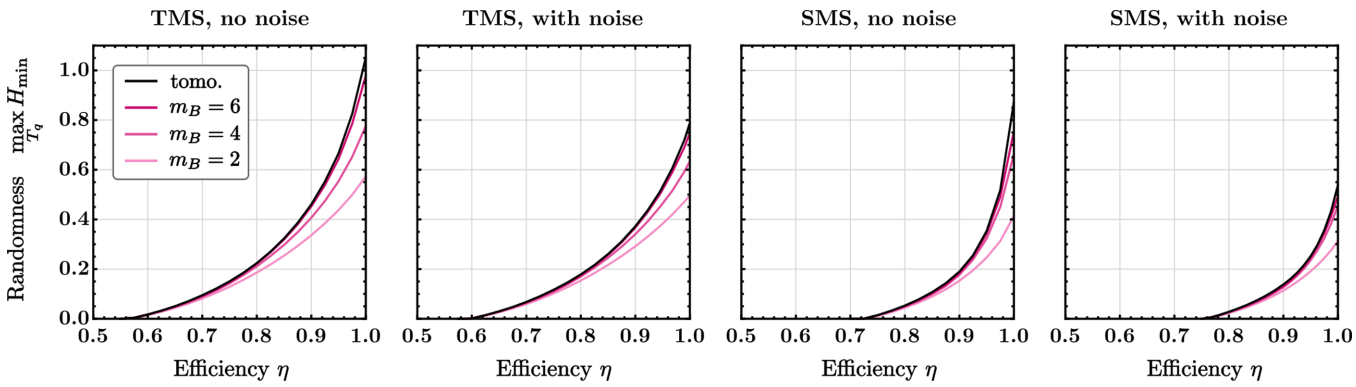

FIG. 2. Optimal min-entropy vs transmission efficiency, for the two-mode squeezed (TMS) and the split single-mode squeezed (SMS) vacuum source with and without noise (0.01 shot-noise units). $H_{\min}$ is maximized over Alice's binning period in the range $T_q \in [2, 10]$. In all cases, Alice has a choice of $m_A = 2$ observables, q and p, binned to $o_A = 8$ outcomes. Bob performs tomography (tomo.; black curve) or measures in $m_B = 2, 4, 6$ different directions equally spaced between q and p, binned to $o_B = 16$ outcomes. For TMS the squeezing is -4 dB, and for SMS it is -6 dB.

just $m_B = 2$ one obtains about half of the optimal entropy. This shows that the protocol already performs well in the simplest setting of just two measurements per party.

IV. EXPERIMENTAL RESULTS

Indeed, we can provide a proof-of-principle demonstration of the practicality of the protocol by applying it to existing experimental data, showing that randomness can in fact be certified in a setup that has already been realized. In Ref. [42], Larsen *et al.*, implemented a two-mode squeezed vacuum source by temporal multiplexing in fiber and characterized it via homodyne measurements of the two output modes. Assigning the two modes to Alice and Bob, respectively, an appropriate subset of the characterization measurements corresponds to q, p quadrature for each party, i.e., to the case of two settings per party, $m_A = m_B = 2$. Postprocessing the data, we can then apply binnings according to the strategies outlined above and estimate the joint probabilities $P(ab|xy)$. For Bob's binning, we use $r = 5$. Each data set (for a given combination of quadratures) contains 16 000 measurements, and we calculate $P_{\text{expt}}(ab|xy)$ from the frequencies of the outcomes.

Owing to finite statistics, the distribution $P_{\text{expt}}(ab|xy)$ is signaling and hence cannot be used directly as a constraint in the SDP for computing $H_{\min}$ (because the SDP is then always infeasible as the distribution cannot be obtained from any quantum strategy for Eve). Instead, we construct an idealized theoretical model of the experiment and obtain an approximation of the initial Gaussian state $\hat{\rho}_G$. We then compute the probability distributions $P_{\text{theory}}(ab|xy) = \text{tr}[\hat{M}_{a|x} \otimes \hat{M}_{b|y} \hat{\rho}_G]$, which are guaranteed to be no-signaling, and use these in the SDP. Finally, we extract the corresponding dual variables and use them together with the experimental distributions $P_{\text{expt}}(ab|xy)$ to obtain a lower bound on the min-entropy of the experimental data (see Appendix C for details).

The resulting optimal min-entropy is shown in Fig. 3 as a function of the number of outputs for Alice. We see that the experimentally certified lower bound on the min-entropy is in good agreement with the idealized theoretical model. The model predicts that about 0.17 bits of randomness per round can be certified with $o_A = 12$ and $o_B = 16$, with a lower bound of about 0.14 bits of randomness per round. While $H_{\min}$ might increase further, for computational reasons we cannot employ larger numbers of outputs. The observed squeezing (in the relevant temporal mode) is -3.88 dB in $q_A + q_B$ and -3.76 dB in $p_A - p_B$, and the overall efficiency is 68%. Furthermore, the repetition rate of the experiment was 500 kHz, from which we get an approximate extracted random bit rate of $\sim$70 kbits/s. These results clearly show that our scheme is feasible in practice. We expect that significantly higher $H_{\min}$ could be attained in a dedicated experiment. In particular, it should be possible to significantly improve the overall efficiency to around 90% and to lower phase noise,

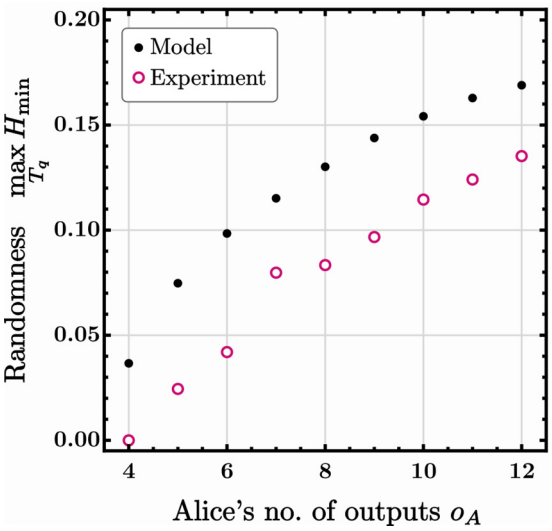

FIG. 3. Results obtained from experimental data of Ref. [42]. Min-entropy vs Alice's number of outputs. The optimal values of $H_{\min}$ from the idealized theoretical model (black dots) and the lower bounds on $H_{\min}$ from the experimental data (pink circles) are pictured. Alice and Bob both measure q and p, and randomness is extracted from Alice's q measurement. $H_{\min}$ is maximized over Alice's binning period in the range $T_q \in [2, 10]$. Bob has $o_B = 16$ outcomes.

thus improving the squeezing level, by avoiding the use of optical switching and fiber delays. Also, fast sources and detectors should enable gigahertz repetition rates [43], leading to gigahertz-range secret bit rates.

V. CONCLUSION AND OUTLOOK

In conclusion, we presented a scheme for quantum random-number certification at the one-sided device-independent security level which can be realized using purely Gaussian resources, namely, squeezed states and homodyne detection. The scheme is robust to realistic levels of loss and noise and can certify a significant amount of randomness (min-entropy approaching 1) for moderate squeezing levels well below 10 dB. It is hence feasible to implement with standard technology, as we also have shown by applying the protocol to existing experimental data from Ref. [42], providing a proof of principle.

One interesting future direction would be an experiment designed specifically for this protocol, which would likely perform significantly better. Spatial separation of the parties could also be implemented. A more thorough analysis accounting for finite-size effects would be required for an accurate calculation of the entropy. In particular, to certify more randomness than consumed (i.e., to achieve randomness expansion), the inputs should be biased, with x^* occurring more often while allowing $P(ab|xy)$ to be estimated sufficiently well. This trade-off can be made rigorous in a finite-size analysis. Ideally, real-time randomness extraction should also be applie.

Note added. We note that a complementary work demonstrating steering-based randomness certification with discrete variables appeared recently [55].

ACKNOWLEDGMENTS

J.B.B. and B.L. acknowledge support from the Carlsberg Foundation and the Independent Research Fund Denmark 7027-00044B. M.I. and N.B. acknowledge funding from the EU Q Flagship project QRANGE and the Swiss National Science Foundation (Project No. 2000021_192244/1 and NCCR QSIT). M.V.L., J.S.N.-N., and U.L.A. acknowledge the Danish National Research Foundation through the Center for Macroscopic Quantum States (bigQ, DNRF0142) and the EU's Horizon 2020 research and innovation program under Grant Agreement No. 820466 (CiViQ).

APPENDIX A: GAUSSIAN STATES WITH NOISE AND LOSS

Consider a continuous-variable system of d bosonic modes. Associated with each mode is a pair of creation and annihilation operators that satisfy the canonical commutation relations $[\hat{a}_j, \hat{a}_k^\dagger] = \delta_{jk}$, $[\hat{a}_j, \hat{a}_k] = 0$ and $[\hat{a}_j^\dagger, \hat{a}_k^\dagger] = 0$. The corresponding quadrature operators for each mode are defined as

$$\hat{q}_j = \frac{1}{\sqrt{2}}(\hat{a}_j^\dagger + \hat{a}_j), \quad \hat{p}_j = \frac{i}{\sqrt{2}}(\hat{a}_j^\dagger - \hat{a}_j) \tag{A1}$$

and fulfill the commutation relations $[\hat{q}_j, \hat{p}_k] = i\delta_{jk}$. By definition, a Gaussian state has a Wigner function of the form

$$W(z) = \frac{\sqrt{\det G}}{\pi^d} e^{-(z-Z)\cdot G(z-Z)}, \tag{A2}$$

where $z = (q, p) \in \mathbb{R}^d \times \mathbb{R}^d$ are canonical phase-space coordinates, Z is a vector of expectation values $Z_k = \langle \hat{z}_k \rangle$ with $\hat{z} = (\hat{q}_1, \ldots, \hat{q}_d, \hat{p}_1, \ldots, \hat{p}_d)$, and G is a real, symmetric, and positive definite matrix. A Gaussian state is therefore completely characterized by the first moments Z and the covariances of the quadrature operators

$$(G^{-1})_{jk} = \langle \hat{z}_j \hat{z}_k + \hat{z}_k \hat{z}_j \rangle - 2\langle \hat{z}_j \rangle \langle \hat{z}_k \rangle. \tag{A3}$$

The matrix elements of a Gaussian state in the Fock basis can be expressed in terms of Z, G, and multidimensional Hermite polynomials [56], where the latter can be generated recursively [57]. The Gaussian states $\hat{\rho}$ in this paper have first moments Z equal to zero. In the following, we assume $Z = 0$.

We model noise and loss by fictitious beam splitters with transmittivity η between the source and each party. Thermal states of mean photon number $\bar{n}$ enter the other port of the beam splitters. The noise and losses are thus assumed to be symmetric for Alice and Bob. The case of pure loss is obtained by setting $\bar{n} = 0$.

Before the beam splitters the total state is $\hat{\rho} \otimes \hat{\rho}_{th} \otimes \hat{\rho}_{th}$, where $\hat{\rho}$ is a two-mode Gaussian state produced by the source and each $\hat{\rho}_{th}$ is a thermal state with mean photon number $\bar{n}$. The corresponding Wigner function is $W_\rho(z) W_{th}(z_{t_1}) W_{th}(z_{t_2})$, where $W_\rho(z)$ is a Gaussian with G_ρ and $W_{th}(z_t)$ is a Gaussian with $G_{th} = (1 + 2\bar{n})^{-1} I$. By combining the phase-space coordinates of the thermal states into $z_t = (q_t, p_t) \in \mathbb{R}^2 \times \mathbb{R}^2$, it can be shown that the beam splitters perform the transformations

$$z \to \sqrt{\eta} z + \sqrt{1-\eta} z_t, \tag{A4}$$

$$z_t \to \sqrt{\eta} z_t - \sqrt{1-\eta} z. \tag{A5}$$

Integrating out the z_t coordinates of the transformed state yields a Gaussian Wigner function with first moments equal to zero and

$$G = \eta G_\rho + (1-\eta) G_t - \eta(1-\eta)(G_t - G_\rho)[\eta G_t + (1-\eta) G_\rho]^{-1} (G_t - G_\rho), \tag{A6}$$

where $G_t = G_{th} \oplus G_{th}$. This is the initial state with noise and loss applied.

The mean photon number is chosen such that the added noise corresponds to 1% of the vacuum variance (i.e., 0.01 shot-noise units), which is the case when $\bar{n} = [200(1-\eta)]^{-1}$.

APPENDIX B: FINITE DIMENSIONS

In order to numerically solve the SDPs we need to work in finite dimensions. We use the Fock-space representation and truncate both the two-mode squeezed (TMS) and the single-mode squeezed (SMS) vacuum states at a given photon number. In the following, we show that if this cutoff is taken to be sufficiently large, then the min-entropy is unaffected.

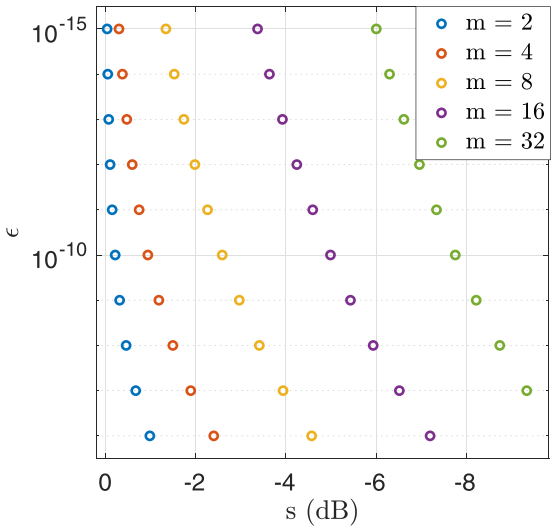

FIG. 4. Orthogonality parameter ϵ as a function of the squeezing parameter s and the cutoff in photon number m.

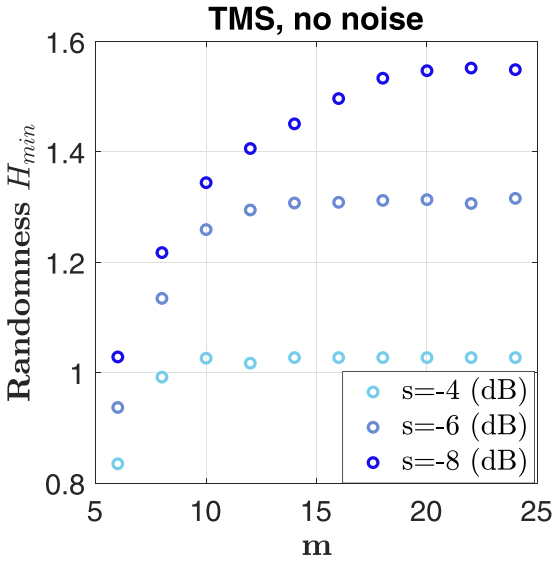

FIG. 5. Bound on the min-entropy $H_{\min}$ as a function of the cutoff m in the Fock basis for different squeezing parameters. Alice's measurement parameters are $o_A = 8$ and $T_q = 3$.

The TMS state in the Fock basis is given by

$$|\text{TMS}\rangle = \frac{1}{\cosh(\tilde{s})} \sum_{n=0}^{\infty} \tanh^n(\tilde{s})\,|nn\rangle\,, \tag{B1}$$

where $\tilde{s}$ is the squeezing parameter and s, expressed in decibels, is defined as $s = 10\log_{10}(e^{-2\tilde{s}})$. The normalized state after a cutoff at m photons has the form

$$|\text{TMS}, m\rangle = \sqrt{\frac{1-\tanh^2(\tilde{s})}{1-\tanh^{2(m+1)}(\tilde{s})}} \sum_{n=0}^{m} \tanh^n(\tilde{s})\,|nn\rangle\,. \tag{B2}$$

The deviation of the truncated state from the true state can be quantified in terms of the overlap $\langle \text{TMS}|\text{TMS}, m\rangle = 1-\epsilon$. Figure 4 illustrates the relation between the deviation ϵ, the squeezing s (decibels), and the cutoff m.

It is computationally expensive to apply a large cutoff. Indeed, in the SDP (2a)–(2d) of the main text, the dimension of the optimization variables $\hat{\sigma}^e_{a|x} \in \mathbb{C}^{(m+1)\times(m+1)}$ and the positivity constraints (2d) are bottlenecks of the optimization. Hence it is desirable to keep m as small as possible, while also minimizing the error in computing $H_{\min}$. In Fig. 5 we observe that the numerical calculations of $H_{\min}$ stabilize at sufficiently high cutoff numbers. Note that while we considered the TMS state in these plots, the same behavior holds for the SMS state.

APPENDIX C: A LOWER BOUND ON THE MIN-ENTROPY

Here, we provide details on how to lower-bound the min-entropy of the experimental data.

First we obtain an approximation of the initial Gaussian state using an idealized theoretical model of the experiment. To this end, we adapt the derivations in the supplementary information of Refs. [42,58] to find the quadrature squeezings

$$\text{Var}[\hat{z}] = \int_{\mathbb{R}}\int_{\mathbb{R}} f(t)f(t')\langle \hat{z}(t)\hat{z}(t')\rangle dt\,dt', \quad \hat{z} = \hat{q}, \hat{p}. \tag{C1}$$

Here,

$$f(t) = \frac{1}{\sqrt{N}} \sin(\omega t) e^{-t^2/2\sigma^2} \tag{C2}$$

is the temporal mode function, chosen to optimize the measured squeezing, with $\sigma = 270$ ns and $\omega = 2\pi \times 2.72$ MHz, and N is a normalization factor defined by $\int_{\mathbb{R}} f^2(t)dt = 1$. The quadrature autocovariance functions $\langle \hat{z}(t)\hat{z}(t')\rangle$ are given by

$$\langle \hat{q}(t)\hat{q}(t')\rangle = \frac{1}{2}\delta(t-t') + \frac{\eta\gamma\nu}{\gamma-\nu} e^{-(\gamma-\nu)|t-t'|}, \tag{C3}$$

$$\langle \hat{p}(t)\hat{p}(t')\rangle = \frac{1}{2}\delta(t-t') - \frac{\eta\gamma\nu}{\gamma+\nu} e^{-(\gamma+\nu)|t-t'|}, \tag{C4}$$

where $\eta = 0.68$, $\gamma = 2\pi \times 8.1$ MHz, and $\nu = 2\pi \times 5.2$ MHz are the overall efficiency, the OPO decay rate, and the pump rate, respectively.

From this we are able to calculate the matrix

$$G = \begin{pmatrix} g_1 & g_2 & 0 & 0 \\ g_2 & g_1 & 0 & 0 \\ 0 & 0 & g_1 & -g_2 \\ 0 & 0 & -g_2 & g_1 \end{pmatrix}, \tag{C5}$$

with $g_1 = 1.38$ and $g_2 = 1.2597$, which completely characterizes the Gaussian state (the first moments are zero). Using this state, together with the POVMs for Alice's and Bob's measurements, the probability distributions $P_{\text{theory}}(ab|xy) = \text{tr}[\hat{M}_{a|x} \otimes \hat{M}_{b|y}\hat{\rho}_G]$ can be computed.

Next we derive the dual of the SDP (2a)–(2d) in the main text. Recall that the condition (2d) must be replaced when Bob performs POVMs with the elements $\hat{M}_{b|y}$. We shall simply quote the result. However, a similar calculation can be found in Appendix C of Ref. [36]. In the dual formulation, given the data $P(ab|xy)$, the guessing probability can be computed via

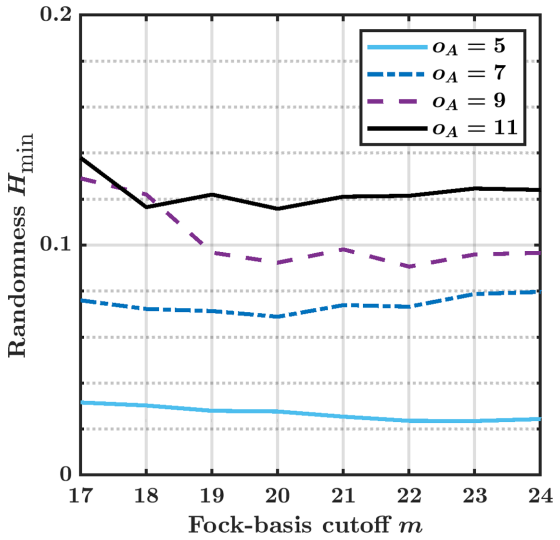

FIG. 6. Lower bound on the min-entropy vs Fock-basis cutoff, for several values of Alice's outputs o_A. The measurement settings at each value of o_A correspond to the maximum values of $H_{\min}$ in Fig. 3 of the main text.

the following optimization:

$$\min_{\{\xi_{abxy}\},\{G_x^e\}} \sum_{a,b,x,y} \xi_{abxy} P(ab|xy), \tag{C6}$$

$$\text{such that} \sum_{b,y} \xi_{abxy} \hat{M}_{b|y} - \delta_{ae}\delta_{xx^*}\hat{I} + \delta_{xx^*} \sum_{x'} G_{x'}^e - G_x^e \geqslant 0 \quad \forall a, e, x, \tag{C7}$$

where $\xi_{abxy} \in \mathbb{R}$ and the G_x^e are Hermitian matrices. Note that strong duality holds, and the optimal value of the dual is equal to the optimal value of the primal. After inserting the theoretical distributions $P_{\text{theory}}(ab|xy)$ into the dual SDP, the resulting optimal dual variables ξ_{abxy} can be used to obtain an upper bound on the guessing probability of the experimental data $u = \sum_{a,b,x,y} \xi_{abxy} P_{\text{expt}}(ab|xy)$. This then yields a lower bound on the min-entropy of the experimental data $h_l = -\log_2(u)$.

The Gaussian state (C5) is quite spread out in phase space; therefore we take the Fock-basis cutoff to be $m = 24$. In Fig. 6 we illustrate that the lower bound on the min-entropy of the experimental data is fairly well converged with this choice. While there are some small fluctuations, there is very little change between the cutoff numbers $m = 19$ and $m = 24$. We are unable to go higher due to numerical limitations.

[1] B. Hayes, Randomness as a resource, Am. Sci. **89**, 300 (2001).

[2] A. Acín and L. Masanes, Certified randomness in quantum physics, Nature (London) **540**, 213 (2016).

[3] M. Herrero-Collantes and J. C. Garcia-Escartin, Quantum random number generators, Rev. Mod. Phys. **89**, 015004 (2017).

[4] M. N. Bera, A. Acin, M. Kus, M. Mitchell, and M. Lewenstein, Randomness in quantum mechanics: Philosophy, physics and technology, Rep. Prog. Phys. **80**, 124001 (2017).

[5] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, Optical quantum random number generator, J. Mod. Opt. **47**, 595 (2000).

[6] J. Bell, On the Einstein Podolsky Rosen paradox, Phys. Phys. Fiz. **1**, 195 (1964).

[7] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Rev. Mod. Phys. **86**, 419 (2014).

[8] R. Colbeck, Quantum and relativistic protocols for secure multi-party computation, Ph.D. thesis, University of Cambridge, 2009, arXiv:0911.3814 [quant-ph].

[9] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Random numbers certified by Bell's theorem, Nature (London) **464**, 1021 (2010).

[10] B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat, Detection-Loophole-Free Test of Quantum Nonlocality, and Applications, Phys. Rev. Lett. **111**, 130406 (2013).

[11] P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W. Nam, M. J. Stevens, and L. K. Shalm, Experimentally generated randomness certified by the impossibility of superluminal signals, Nature (London) **556**, 223 (2018).

[12] Y. Liu, Q. Zhao, M.-H. Li, J.-Y. Guan, Y. Zhang, B. Bai, W. Zhang, W.-Z. Liu, C. Wu, X. Yuan, H. Li, W. J. Munro, Z. Wang, L. You, J. Zhang, X. Ma, J. Fan, Q. Zhang, and J.-W. Pan, Device-independent quantum random-number generation, Nature (London) **562**, 548 (2018).

[13] L. K. Shalm, Y. Zhang, J. C. Bienfang, C. Schlager, M. J. Stevens, M. D. Mazurek, C. Abellán, W. Amaya, M. W. Mitchell, M. A. Alhejji, H. Fu, J. Ornstein, R. P. Mirin, S. W. Nam, and E. Knill, Device-independent randomness expansion with entangled photons, Nat. Phys. **17**, 452 (2021).

[14] W.-Z. Liu, M.-H. Li, S. Ragy, S.-R. Zhao, B. Bai, Y. Liu, P. J. Brown, J. Zhang, R. Colbeck, J. Fan, Q. Zhang, and J.-W. Pan, Device-independent randomness expansion against quantum side information, Nat. Phys. **17**, 448 (2021).

[15] H.-W. Li, Z.-Q. Yin, Y.-C. Wu, X.-B. Zou, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Semi-device-independent random-number expansion without entanglement, Phys. Rev. A **84**, 034301 (2011).

[16] G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi, Quantum randomness certified by the uncertainty principle, Phys. Rev. A **90**, 052327 (2014).

[17] T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, Self-Testing Quantum Random Number Generator, Phys. Rev. Lett. **114**, 150501 (2015).

[18] P. Mironowicz, G. Cañas, J. Cariñe, E. S. Gómez, J. F. Barra, A. Cabello, G. B. Xavier, G. Lima, and M. Pawłowski, Quantum randomness protected against detection loophole attacks, Quantum Inf. Process. **20**, 39 (2021).

[19] Z. Cao, H. Zhou, and X. Ma, Loss-tolerant measurement-device-independent quantum random number generation, New J. Phys. **17**, 125011 (2015).

[20] D. G. Marangon, G. Vallone, and P. Villoresi, Source-Device-Independent Ultrafast Quantum Random Number Generation, Phys. Rev. Lett. **118**, 060503 (2017).

[21] Z. Cao, H. Zhou, X. Yuan, and X. Ma, Source-Independent Quantum Random Number Generation, Phys. Rev. X **6**, 011020 (2016).

[22] F Xu, J. H. Shapiro, and F. N. C. Wong, Experimental fast quantum random number generation using high-dimensional entanglement with entropy monitoring, Optica **3**, 1266 (2016).

[23] J. B. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, H. Zbinden, and N. Brunner, Megahertz-Rate Semi-Device-Independent Quantum Random Number Generators Based on Unambiguous State Discrimination, Phys. Rev. Appl. **7**, 054018 (2017).

[24] T. Gehring, C. Lupo, A. Kordts, D. Solar Nikolic, N. Jain, T. Rydberg, T. B. Pedersen, S. Pirandola, and U. L. Andersen, Homodyne-based quantum random number generator at 2.9 Gbps secure against quantum side-information, Nat. Commun. **12**, 605 (2021).

[25] T. Michel, J. Y. Haw, D. G. Marangon, O. Thearle, G. Vallone, P. Villoresi, P. K. Lam, and S. M. Assad, Real-Time Source-Independent Quantum Random-Number Generator with Squeezed States, Phys. Rev. Appl. **12**, 034017 (2019).

[26] D. Rusca, T. van Himbeeck, A. Martin, J. B. Brask, W. Shi, S. Pironio, N. Brunner, and H. Zbinden, Self-testing quantum random-number generator based on an energy bound, Phys. Rev. A **100**, 062338 (2019).

[27] D. Drahi, N. Walk, M. J. Hoban, A. K. Fedorov, R. Shakhovoy, A. Feimov, Y. Kurochkin, W. S. Kolthammer, J. Nunn, J. Barrett, and I. A. Walmsley, Certified Quantum Random Numbers from Untrusted Light, Phys. Rev. X **10**, 041048 (2020).

[28] D. Rusca, H. Tebyanian, A. Martin, and H. Zbinden, Fast self-testing quantum random number generator based on homodyne detection, Appl. Phys. Lett. **116**, 264004 (2020).

[29] M. Avesani, H. Tebyanian, P. Villoresi, and G. Vallone, Semi-Device-Independent Heterodyne-Based Quantum Random-Number Generator, Phys. Rev. Appl. **15**, 034034 (2021).

[30] A. Einstein, B. Podolsky, and N. Rosen, Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?, Phys. Rev. **47**, 777 (1935).

[31] M. D. Reid, Demonstration of the Einstein-Podolsky-Rosen paradox using nondegenerate parametric amplification, Phys. Rev. A **40**, 913 (1989).

[32] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Steering, Entanglement, Nonlocality, and the Einstein-Podolsky-Rosen Paradox, Phys. Rev. Lett. **98**, 140402 (2007).

[33] M. D. Reid, Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations, Phys. Rev. A **62**, 062308 (2000).

[34] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering, Phys. Rev. A **85**, 010301(R) (2012).

[35] Y. Z. Law, L. P. Thinh, J.-D. Bancal, and V. Scarani, Quantum randomness extraction for various levels of characterization of the devices, J. Phys. A: Math. Theor. **47**, 424028 (2014).

[36] E. Passaro, D. Cavalcanti, P. Skrzypczyk, and A. Acín, Optimal randomness certification in the quantum steering and prepare-and-measure scenarios, New J. Phys. **17**, 113010 (2015).

[37] P. Skrzypczyk and D. Cavalcanti, Maximal Randomness Generation from Steering Inequality Violations Using Qudits, Phys. Rev. Lett. **120**, 260401 (2018).

[38] T. Gehring, V. Händchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R. F. Werner, and R. Schnabel, Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks, Nat. Commun. **6**, 8795 (2015).

[39] N. Walk, S. Hosseini, J. Geng, O. Thearle, J. Y. Haw, S. Armstrong, S. M. Assad, J. Janousek, T. C. Ralph, T. Symul, H. M. Wiseman, and P. K. Lam, Experimental demonstration of gaussian protocols for one-sided device-independent quantum key distribution, Optica **3**, 634 (2016).

[40] A. Máttar, P. Skrzypczyk, G. H. Aguilar, R. V. Nery, P. H. S. Ribeiro, S. P. Walborn, and D. Cavalcanti, Experimental multipartite entanglement and randomness certification of the W state in the quantum steering scenario, Quantum Sci. Technol. **2**, 015011 (2017).

[41] J. Wang, S. Paesani, Y. Ding, R. Santagati, P. Skrzypczyk, A. Salavrakos, J. Tura, R. Augusiak, L. Mančinska, D. Bacco, D. Bonneau, J. W. Silverstone, Q. Gong, A. Acín, K. Rottwitt, L. K. Oxenløwe, J. L. O'Brien, A. Laing, and M. G. Thompson, Multidimensional quantum entanglement with large-scale integrated optics, Science **360**, 285 (2018).

[42] M. V. Larsen, X. Guo, C. R. Breum, J. S. Neergaard-Nielsen, and U. L. Andersen, Fiber-coupled EPR-state generation using a single temporally multiplexed squeezed light source, npj Quantum Inf. **5**, 46 (2019).

[43] T. Kashiwazaki, N. Takanashi, T. Yamashima, T. Kazama, K. Enbutsu, R. Kasahara, T. Umeki, and A. Furusawa, Continuous-wave 6-dB-squeezed light with 2.5-THz-bandwidth from single-mode PPLN waveguide, APL Photonics **5**, 036104 (2020).

[44] A. Fine, Hidden Variables, Joint Probability, and the Bell Inequalities, Phys. Rev. Lett. **48**, 291 (1982).

[45] Z. Y. Ou, S. F. Pereira, and H. J. Kimble, Realization of the Einstein-Podolsky-Rosen paradox for continuous variables in nondegenerate parametric amplification, Appl. Phys. B **55**, 265 (1992).

[46] V. Händchen, T. Eberle, S. Steinlechner, A. Samblowski, T. Franz, R. F. Werner, and R. Schnabel, Observation of one-way Einstein-Podolsky-Rosen steering, Nat. Photonics **6**, 596 (2012).

[47] S. Armstrong, M. Wang, R. Y. Teh, Q. Gong, Q. He, J. Janousek, H.-A. Bachor, M. D. Reid, and P. K. Lam, Multipartite Einstein-Podolsky-Rosen steering and genuine tripartite entanglement with optical networks, Nat. Phys. **11**, 167 (2015).

[48] X. Deng, Y. Xiang, C. Tian, G. Adesso, Q. He, Q. Gong, X. Su, C. Xie, and K. Peng, Demonstration of Monogamy Relations for Einstein-Podolsky-Rosen Steering in Gaussian Cluster States, Phys. Rev. Lett. **118**, 230501 (2017).

[49] Z. Qin, X. Deng, C. Tian, M. Wang, X. Su, C. Xie, and K. Peng, Manipulating the direction of Einstein-Podolsky-Rosen steering, Phys. Rev. A **95**, 052114 (2017).

[50] M. Wang, Y. Xiang, H. Kang, D. Han, Y. Liu, Q. He, Q. Gong, X. Su, and K. Peng, Deterministic Distribution of Multipartite Entanglement and Steering in a Quantum Network by Separable States, Phys. Rev. Lett. **125**, 260506 (2020).

[51] D Cavalcanti and P Skrzypczyk, Quantum steering: A review with focus on semidefinite programming, Rep. Prog. Phys. **80**, 024001 (2017).

[52] D. S. Tasca, P. Sánchez, S. P. Walborn, and Ł. Rudnicki, Mutual Unbiasedness in Coarse-Grained Continuous Variables, Phys. Rev. Lett. **120**, 040403 (2018).

[53] R. Impagliazzo, L. A. Levin, and M. Luby, Pseudo-random generation from one-way functions, in *STOC '89: Proceedings of the Twenty-first Annual ACM Symposium on Theory of Computing* (Association for Computing Machinery, New York, 1989), pp. 12–24.

[54] S. Boyd and L. Vandenberghe, *Convex Optimization* (Cambridge University Press, New York, 2004).

[55] D. J. Joch, S. Slussarenko, Y. Wang, A. Pepper, S. Xie, B.-B. Xu, I. R. Berkman, S. Rogge, and G. J. Pryde, Certified random number generation from quantum steering, arXiv:2111.09506 [quant-ph].

[56] V. V. Dodonov, O. V. Man'ko, and V. I. Man'ko, Multidimensional Hermite polynomials and photon distribution for polymode mixed light, Phys. Rev. A **50**, 813 (1994).

[57] P. Kok and S. L. Braunstein, Multi-dimensional Hermite polynomials in quantum optics, J. Phys. A: Math. Gen. **34**, 6185 (2001).

[58] M. V. Larsen, X. Guo, C. R. Breum, J. S. Neergaard-Nielsen, and U. L. Andersen, Deterministic multi-mode gates on a scalable photonic quantum computing platform, Nat. Phys. **17**, 1018 (2021).