Device-independent quantum cryptography for continuous variables

Kevin Marshall[1,*] and Christian Weedbrook[2,†]
[1]*Department of Physics, University of Toronto, Toronto, M5S 1A7, Canada*
[2]*QKD Corp., 60 St. George St., Toronto, M5S 1A7, Canada*
(Received 27 May 2014; published 9 October 2014)

We present a device-independent quantum cryptography protocol for continuous variables. Our scheme is based on the Gottesman-Kitaev-Preskill encoding scheme whereby a qubit is embedded in the infinite-dimensional space of a quantum harmonic oscillator. The application of discrete-variable device-independent quantum key distribution to this encoding enables a continuous-variable analog. Since the security of this protocol is based on discrete variables we inherit by default security against collective attacks and, under certain memoryless assumptions, coherent attacks. We find that our protocol is valid over the same distances as its discrete-variable counterpart, except that we are able to take advantage of high efficiency commercially available detectors where, for the most part, only homodyne detection is required. This offers the prospect of closing the loopholes associated with Bell inequalities.

DOI: 10.1103/PhysRevA.90.042311 PACS number(s): 03.67.Dd, 03.67.Hk, 42.50.−p, 89.70.Cf

I. INTRODUCTION

Quantum key distribution (QKD) [1,2] is a method by which two parties, Alice and Bob, may generate a shared secret key over an insecure quantum channel monitored by an eavesdropper, Eve. Any QKD protocol relies on several assumptions, namely, any eavesdropper must obey the laws of quantum mechanics; Alice and Bob have the freedom to choose at least one of two measurement settings; and there is no classical information leaking from Alice or Bob's laboratories. Most conventional QKD protocols further assume that Alice and Bob have near perfect control of their measurement devices as well as their state preparation. Device-independant QKD [3–5] is a protocol that, remarkably, is free from making these additional assumptions; Alice and Bob need no knowledge of the inner workings of their devices nor even the dimension of the space their quantum states reside in.

In this paper, we use the approach of combining the encoding scheme of [6] with the results of [3,4] to create a device-independent quantum cryptography protocol for continuous variables (CVs). CV quantum information offers higher efficiency detectors, cheap off-the-shelf components and the experimentally accessible Gaussian resources. Furthermore, by encoding the CV space of a harmonic oscillator into a finite-dimensional code space we are able to take advantage of results which have previously only been applied to discrete-variable (DV) QKD.

The first proposals for continuous-variable QKD [7] relied on "nonclassical" states of light such as squeezed states [8,9]. In fact, one of these protocols was proven unconditionally secure [9]. As the field matured it was recognized that such nonclassical states were not required and that the more experimentally available class of coherent states were sufficient [7,10].

Device-independent QKD provides a way by which two parties may share a private key despite having no knowledge of the inner workings of their respective devices. Conversely, in conventional QKD protocols it is regularly assumed that both parties have a high degree of control over both state preparation as well as measurement. Although, recently relaxing the condition of trusting the measurement device was achieved [11,12]. The security in this device-independent approach comes instead from the fact that the two parties are able to violate a Bell inequality [13], which can remarkably be used to put a bound on the amount of information that a potential eavesdropper could, in principle, obtain.

Here we introduce a CV version of device-independent QKD. Our protocol goes as follows. Alice first generates a Bell state which has been created using an encoding based on the Gottesman-Kitaev-Preskill scheme where a qubit is encoded into an infinite dimensional space of a harmonic oscillator. After this the protocol continues in a similar fashion where she keeps one encoded qubit and sends the other qubit to Bob over an insecure quantum channel. Hence, the results of DV device-independent QKD can then be applied to the system yielding the first implementation of device-independent QKD for CVs.

It is known in the field of CV quantum information that all Gaussian resources are insufficient for violating a Bell inequality [14,15]. This means that one should already expect non-Gaussian states or measurements as being a requirement [16–20], despite the fact that they are typically more difficult to produce in a laboratory. This highlights the challenges faced when attempting to create a CV version of device-independent QKD because most current CV-QKD protocols use Gaussian states. Fortunately, if we use, for example, a single mode of the electromagnetic field as our harmonic oscillator, we are able to use CV resources, including high efficiency detectors and off-the-shelf components. The major drawback of DV device-independent QKD is that in order to close the detector loophole one needs high efficiency detectors [21] which are possible but not yet standard tools. The detector loophole issue is often overcome by CV quantum information where we can take advantage of such high detection efficiencies [16–20,22].

This paper is structured as follows. In Sec. II we discuss separately the necessary encoding scheme as well as the results of DV device-independent QKD. In Sec. III we relate these concepts to CV quantum information and discuss formally

*marshall@physics.utoronto.ca
†christian.weedbrook@gmail.com

the kind of measurements that are necessary. Following this we investigate the resources required in order to implement the protocol in Sec. IV. Since we are only capable of making approximations of the desired encoding in the real world, we consider the effects of such approximations on the encoding and resulting key rate in Sec. V. Finally, Sec. VI presents some discussions and concluding comments as well as some interesting open questions.

II. BACKGROUND

The premise of this paper is to propose a method of implementing device-independent QKD with CV states. This is accomplished by embedding a two-level Hilbert space into the full infinite-dimensional space and then using results from DV-QKD. Here we discuss the encoding scheme proposed by Gottesman, Kitaev, and Preskill (GKP) in [6] as well as the DV version of device-independent QKD.

A. GKP encoding

The GKP encoding [6] provides a method to encode a qubit in the infinite-dimensional space of an oscillator in such a way that one can protect against arbitrary, but small, shifts in the canonical variables q and p as well as carrying out fault-tolerant universal quantum computation on the encoded space [6,23]. The stabilizer generators of a two-dimensional Hilbert space in an infinite-dimensional Hilbert space with canonical variables q,p are given by [9]

$$S_q = \exp(2iq\sqrt{\pi}), \quad S_p = \exp(-2ip\sqrt{\pi}). \tag{1}$$

The stabilizers are simply shift operators for q,p, and if the eigenvalues are $S_q = S_p = 1$ then the allowed values of q and p are integer multiples of $\sqrt{\pi}$. Since the code words are invariant under shifts by integer multiples of $2\sqrt{\pi}$ we can define a basis for the encoded qubit as

$$|\bar{j}_L\rangle \propto \sum_{s\in\mathbb{Z}} |(2s+j)\sqrt{\pi}\rangle_q, \tag{2}$$

for $j = 0,1$, and where the subscript q indicates the q ("position") basis. These states can be approximated optically using Schrödinger cat states [24], or by a variety of other methods [25–28]. Encoded Pauli gates are defined as $\bar{Z} \equiv \exp(iq\sqrt{\pi})$ and $\bar{X} \equiv \exp(-ip\sqrt{\pi})$; since these operators commute with the stabilizers they also preserve the code subspace.

The set of Clifford operations on the encoded subspace correspond to symplectic (or Gaussian) transformations on the CV space of the oscillator; these operations can be implemented in a fault-tolerant way [6]. To achieve universal quantum computation we must be able to implement a non-Clifford gate on the encoded subspace [29], for example, the addition of a $\pi/8$ gate (T gate) to the Clifford group will make for a universal set of gates. The T gate can be implemented with a nonsymplectic transformation on the oscillator; this is more experimentally difficult than symplectic transformations and requires a non-Gaussian resource such as photon counting. The physical resources required to implement these gates are discussed in more detail in Sec. IV.

B. Device-independent quantum key distribution

The DV-QKD protocol [3,4] begins with Alice and Bob sharing a quantum channel that emits pairs of entangled particles. To consider the worse case scenario, we allow Eve full control over the source [30] which, if she is honest, emits the state $|\psi_{AB}\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$. But in general she is free to create any arbitrary state ρ_{ABE} which may be entangled between not only Alice and Bob but herself as well. To generate a secret key, Alice chooses a basis to measure in from $\{A_0, A_1, A_2\}$ while Bob chooses a basis from $\{B_1, B_2\}$ and they get outcomes of $a_i, b_j \in \{+1,-1\}$, respectively [31]. After all measurements are performed, if Alice had chosen measurement A_0 and Bob chosen measurement B_1 they extract a single bit of raw key corresponding to their measurement outcome. Instead, if they had measurement settings corresponding to $\{A_0, B_2\}$, their outcomes are completely uncorrelated and so this case is discarded. For all other measurement settings Alice and Bob use their results to violate the CHSH inequality [13]:

$$\mathcal{S} = \langle a_1 b_1\rangle + \langle a_1 b_2\rangle + \langle a_2 b_1\rangle - \langle a_2 b_2\rangle \leqslant 2. \tag{3}$$

The CHSH inequality puts a bound on the values of $\mathcal{S}$ consistent with local hidden-variable theories in accordance with Bell's theorem [32,33]. Violation of this inequality by quantum mechanics arises due to the fact that entanglement can provide nonlocal correlations that cannot be produced by shared randomness. If Alice and Bob share a nonlocal correlation then, regardless of how this correlation came to exist, Eve cannot have full knowledge of the correlation or else she would be in possession of a local variable capable of reproducing the correlations [4].

A set of measurements which give the desired behavior in the above protocol and which maximize the violation of the CHSH inequality are given by [31]

$$\begin{aligned} A_0 = B_1 = Z, \quad A_1 = 1/\sqrt{2}(Z+X), \\ B_2 = X, \quad A_2 = 1/\sqrt{2}(Z-X). \end{aligned} \tag{4}$$

For the moment, Z and X in the above expression (4) have no relation to the encoded Pauli gates $\bar{Z}$ and $\bar{X}$; although we will make this connection in Sec. III. The main result shown by Acín *et al.* [4] is that the Holevo quantity between Eve and Bob, after Alice and Bob have symmetrized their marginals, is bounded as

$$\chi(B_1{:}E) \leqslant h\left(\frac{1+\sqrt{(\mathcal{S}/2)^2-1}}{2}\right), \tag{5}$$

where $\chi(B_1{:}E) = S(\rho_E) - \frac{1}{2}\sum_{b_1=\pm1} S(\rho_{E|b1})$ is the Holevo quantity and $h = -p\log_2 p - (1-p)\log_2(1-p)$ is the binary entropy. This provides a method which Alice and Bob can use to keep Eve honest and bound her knowledge using only their violation of the CHSH inequality.

III. CONTINUOUS-VARIABLE DEVICE INDEPENDENCE PROTOCOL

The CV version of device-independent QKD begins with Alice creating an encoded Bell state (see Fig. 1). This encoding is based on the GKP encoding as given in Sec. II A. Once this Bell state is created she keeps one qubit for herself and sends the other entangled qubit to Bob over an insecure and lossy

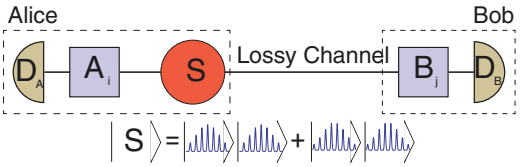

FIG. 1. (Color online) The layout of the proposed CV device-independent QKD protocol. Alice makes use of an entangled source S which emits an encoded Bell state $|S\rangle = |\bar{0}\bar{0}\rangle + |\bar{1}\bar{1}\rangle$, shown in the figure as the wave function in the position representation, to keep half of the pair for herself while sending the other half to Bob over a lossy channel. Both parties randomly choose a change of basis gate, A_i and B_j, before each making a homodyne measurement of the $\hat{q}$ quadrature with detectors D_A and D_B. There are many proposals on how to create the initial encoded GKP states (see Sec. II A), and the operations required to create the encoded Bell state as well as implement the desired measurement are discussed in Sec. IV.

quantum channel. Apart form this initial encoding, the protocol follows the same steps as in typical DV-QKD protocols [3,4].

A set of measurements which maximize the violation of the CHSH inequality, for the encoded state,

$$|\Phi^+\rangle = 1/\sqrt{2}(|\bar{0}\bar{0}\rangle + |\bar{1}\bar{1}\rangle), \tag{6}$$

consist of measurements A_1, A_2, B_1, B_2, as defined in Sec. II B, which act on the encoded subspace. We can destructively measure the observables $\bar{Z}$ and $\bar{X}$ by performing a suitable homodyne measurement of the $\hat{q}$ or $\hat{p}$ quadrature, respectively. By measuring the $\hat{q}$ quadrature we expect that the only outcomes possible will be integer multiples of $\sqrt{\pi}$; even multiples corresponding to a $|\bar{0}\rangle$ state and odd multiples corresponding to $|\bar{1}\rangle$. Imperfections in the measurement and the encoded state will result in other measured values, but we can apply classical error correction and adjust the value to the nearest $k\sqrt{\pi}$ for an integer k. The outcome of the measurement $\bar{Z}$ is then given by $(-1)^k$. We can measure the other three observables by first applying a change of basis gate which takes us to the $\bar{Z}$ basis, and in this way we need only consider homodyne measurements of the $\hat{q}$ quadrature.

We assume in this section that we are able to implement Clifford gates as well as $\pi/8$ gates on our encoded space and also that we can carry out homodyne measurements on the CV space; the resources required to do this are discussed in Sec. IV. From here onwards we drop the over-bar notation to denote encoded operations; all gates are to be understood as acting on the encoded space while symplectic transformations are understood to be in relation to the oscillator.

It is readily seen that we can measure in the X basis by using the change of basis gate H, and one can easily verify that $H^\dagger X H = Z$. Since the Hadamard gate H is in the Clifford group we can implement an encoded H by carrying out symplectic transformations on the full CV space. Unfortunately, it is not possible to change from the A_1 or A_2 basis to the Z basis by using only Clifford gates, which means that we will need to go beyond symplectic transformations in the CV space. This can be readily seen by recognizing that $A_1 = H$; suppose there existed a Clifford gate C such that $C^\dagger H C = Z$. This would imply that $CZC^\dagger = H$ and so C is not a Clifford gate by definition.

The required change of basis gates can be calculated as

$$\begin{aligned} \mathcal{I}B_1\mathcal{I} = Z, \quad H^\dagger B_2 H = Z, \\ \alpha^\dagger A_1 \alpha = Z, \quad \beta^\dagger A_2 \beta = Z, \end{aligned} \tag{7}$$

where $\alpha = PHTHP$, $\beta = ZPHTHP$, and T is an encoded $\pi/8$ gate. It is important to note that while the latter two gates are not Clifford gates, they can be decomposed exactly as a composition of Clifford gates with only one non-Clifford T gate. Furthermore, it is possible to shift the problem of implementing a T gate to a state preparation problem, and since preparation can be done "offline" we require only Gaussian operations and one auxiliary state to carry out our CV device-independent QKD.

IV. REQUIRED RESOURCES

In order for Alice and Bob to implement the necessary measurements they must be able to perform gates on the encoded states as well as homodyne detection on one quadrature. The necessary set of gates include H, P, T (no need for Z, since $Z = P^2$). The first two gates correspond to Clifford operations while the last one is a non-Clifford gate. The set of Clifford gates on the encoded states correspond to symplectic transformations on the CV space, given as [6] $H : (q,p) \to (p,-q)$, $P : (q,p) \to (q,p-q)$, and $C_{\mathrm{NOT}} : (q_1,p_1,q_2,p_2) \to (q_1,p_1-p_2,q_1+q_2,p_2)$. To create the Bell state one requires only the symplectic transformations associated with H and C_{NOT}, as well as encoded $|0\rangle$ states, thus this is not an experimentally demanding operation.

In order to implement an encoded $\pi/8$ gate we need a non-symplectic transformation which requires a non-Gaussian resource. The addition of photon counting to Gaussian resources is sufficient to carry out nonsymplectic transformations. In particular, one is able to create either a $\pi/8$ state or a cubic phase state which can then be used to implement a T gate on the encoded space [6,34]. Fortunately, one can generate these states offline and use them as required throughout the protocol, effectively shifting the issues of non-Gaussian operations to state preparation. In this way, one needs only to have a supply of non-Gaussian states and be capable of performing symplectic transformations (including homodyne detection) in order to implement the QKD protocol. In the case of an optical mode, the set of symplectic transformations can be achieved with linear optics (phase shifters and beam splitters) and squeezing operations (nonlinear crystals).

Fortunately, Alice and Bob do not need to choose a measurement basis, which is used to check for a CHSH violation, very often; the probability of choosing between the possible options need not be uniform, although this would work as well. If we suppose that Alice and Bob share N quantum states, it is enough to use $\sim\sqrt{N}$ pairs to check for a CHSH violation, so long as the measurements are causally independent [35]. This condition would be satisfied for memoryless devices, or devices which could have internal memory reliably cleared after every run. One protocol [35] also provides security against coherent attacks, which is the most general form attack. Since we have chosen the measurement basis corresponding to generating a key as Z, this means that in the limit of large N almost all of the time we need only perform Gaussian operations. Hence, we

need only perform non-Clifford operations a small fraction of the time, in order to estimate the CHSH violation and thus keep the eavesdropper honest. Many other such DV device-independent QKD protocols exist and offer different key rates with different underlying assumptions [36–38], but typically one still requires the ability to make measurements in a set of four bases which violates the CHSH inequality.

V. GAUSSIAN FINITE-SQUEEZING EFFECTS

In practice, the encoded GKP states will not consist of delta peaks at $\sqrt{\pi}$ intervals, but instead the peaks will have some finite width and they will be modulated by a larger envelope to ensure the state is of finite energy. One way to produce an ideal GKP state is to prepare a momentum eigenstate $|p = 0\rangle$, and then measure the value of $q(\mathrm{mod}\, 2\sqrt{\pi})$; although in practice one would probably create this state through other means [24–28]. Since the position is completely undetermined for a momentum eigenstate all values of q are equally likely, and this measurement will project out a state that differs from a Z eigenstate by a shift of q which can then be corrected.

If instead of an unphysical momentum eigenstate, which corresponds to infinite squeezing, we can consider a finitely squeezed state given by $\psi_{sq}(p) = \pi^{-1/4}\kappa^{-1/2}\exp(-\frac{1}{2}p^2/\kappa^2)$ [39], where $\kappa = e^{-r}$ for squeezing parameter $r \in [0,\infty)$. In the position representation this state is given by $\psi_{sq}(q) = \pi^{-1/4}\kappa^{1/2}\exp(-\frac{1}{2}q^2\kappa^2)$. An ideal homodyne measurement of q is a projection-valued measure (PVM) with projectors corresponding to position eigenstates $P_x = |x\rangle\langle x|$, or infinitely squeezed states in position. If we allow the homodyne measurement to have a Gaussian acceptance of width Δ, we replace the PVM with a positive-operator valued measure (POVM) which consists of an ideal homodyne measurement convolved with a Gaussian window. This leads to POVM elements given by

$$\Pi_x = (2\pi\Delta^2)^{-1/2}\int_{-\infty}^{\infty} dy e^{-\frac{1}{2}(x-y)^2/\Delta^2}|y\rangle\langle y|. \tag{8}$$

An ideal measurement of $q(\mathrm{mod}\, 2\sqrt{\pi})$ is described by the PVM with elements $P'_x = \sum_{s=-\infty}^{\infty} P_{x-2s\sqrt{\pi}}$ for $x \in [0,2\sqrt{\pi})$, and if we let $P_x \to \Pi_x$ we obtain the result for a homodyne detector with a Gaussian acceptance. Without loss of generality suppose we obtain a result corresponding to Π_0, then the state will be transformed to

$$\psi_{\bar{0}}(q) \propto \sum_{s=\mathbb{Z}} e^{-\frac{1}{2}q^2\kappa^2}\psi'_{sq}(q + 2s\sqrt{\pi}), \tag{9}$$

where ψ'_{sq} is a squeezed vacuum state in position with width Δ. If we obtain a result other than Π_0 we can simply apply a shift to correct the state. This is of the same type of approximate code word proposed in the GKP paper [6]. Notice that our initial squeezing determines the size of the overall envelope, width κ^{-1}, while the precision of our homodyne measurement determines the width of the individual peaks.

If we further approximate by replacing $\exp(-\frac{1}{2}q^2\kappa^2) \to \exp(-\frac{1}{2}(2s\sqrt{\pi})^2\kappa^2)$ in the summation above, which corresponds to scaling each peak by a constant factor, we find

$$|\psi_{\bar{0}}(q)|^2 = \frac{2\kappa}{\Delta\sqrt{\pi}}\sum_{s=-\infty}^{\infty} e^{-4\pi\kappa^2 s^2}e^{-(q-2s\sqrt{\pi})^2/\Delta^2}. \tag{10}$$

We can correct for shifts in the position which are less than $\sqrt{\pi}/2$, and thus bound the error by adding up the contribution from all of the tails further than $\sqrt{\pi}/2$ from their respective peak. Assuming that $\kappa\sqrt{\pi} \ll 1$ the probability of error is bounded as $P_e < 2\Delta^2/(\kappa\pi)\exp(-\frac{1}{4}\pi/\Delta^2)$ [9].

The errors from incorrectly identifying an encoded state will determine the amount by which one is able to violate the CHSH inequality. Consider one term in the CHSH quantity $\mathcal{S}$. The correlator is defined as $\langle a_i b_j\rangle = P(a = b|ij) - P(a \neq b|ij)$ for outcomes a,b and measurement choices i,j. If we assume that our gates are perfect then all errors will come from incorrectly identifying an encoded state. We can calculate the value of $\mathcal{S}$ after error correction by computing the expectation values of the various measurements. This value is plotted in Fig. 2, and it can be seen that we start to violate the CHSH inequality for parameters $\Delta = \kappa$ corresponding to squeezing greater than 5 dB. This shows that the value of the CHSH quantity is scaled according to the error rate, assuming perfect gates.

The quantum bit error rate (QBER) [2] is defined as $Q = P(a \neq b|01) = 2P_e(1 - P_e)$ since we are only extracting a key for the cases where Alice does measurement A_0 and Bob does measurement B_1. This corresponds to either Alice or Bob incorrectly identifying the state while the other party does not make an error. The secret-key rate r, under collective attacks, with one-way classical postprocessing from Bob to Alice, is lower bounded by the Devetak-Winter rate [4,40],

$$r \geqslant r_{\mathrm{DW}} = I(A_0{:}B_1) - \chi(B_1{:}E), \tag{11}$$

where $I(A_0{:}B_1) = 1 - h(Q)$ is the mutual information between Alice and Bob (h being the binary entropy), and $\chi(B_1{:}E)$ is the Holevo quantity.

In Fig. 2, we plot both the QBER and the key rate r. Notice that the extractable key rate remains zero even for values of $\mathcal{S}$ slightly larger than two. The key rate grows rapidly for squeezing beyond 6 dB, for example, a squeezing of 10 dB yields a key rate of ≈98%. Note that the well-known critical

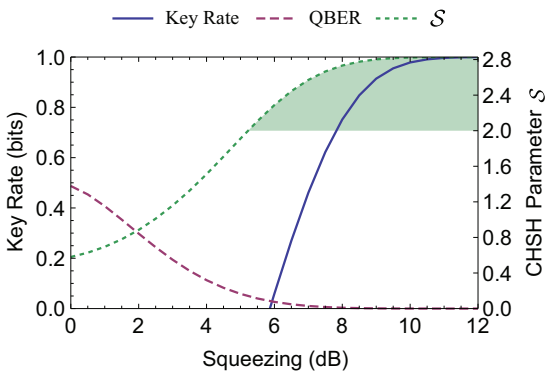

FIG. 2. (Color online) The extractable secret-key rate is plotted as a function of the squeezing for the symmetric case $\Delta = \kappa$, where Δ is the width of the individual peaks and κ^{-1} is the width of the Gaussian envelope in the GKP encoding. Note that currently the maximal amount of single-mode squeezing achieved is 12.7 dB [41,42]. The shaded region indicates a violation of the CHSH inequality. The QBER is plotted in units where 0 corresponds to no error and 0.5 corresponds to Alice and Bob guessing randomly.

QBER of 11% for BB84 [43] as well as 7.1% for DV device-independent QKD [4] are higher than the ≈3.5% critical QBER for this proposal. This is due to the fact that one requires a suitable enough approximation to a GKP encoded state in order to have a high enough violation of the CHSH inequality, and by doing so one immediately achieves a corresponding low probability of error P_e. Typically one desires a high critical QBER as it generally tolerates more imperfections in the protocol. However, in this case the difficulty arises from the need to violate the CHSH inequality and if one is able to do so then one already obtains a small QBER. Intuitively, as the width of the individual peaks Δ in the encoded state become larger, and equivalently the QBER, the overall state resembles a Gaussian state and thus cannot violate the CHSH inequality.

VI. DISCUSSION OF LOSS, COMPARISON TO DISCRETE VARIABLES AND CONCLUSION

By harnessing the results of discrete-variable QKD, with a qubit encoding in a harmonic oscillator, we provided the first device-independent QKD protocol for continuous variables. This protocol derived its security from the ability to violate a Bell inequality and, remarkably, does not require Alice or Bob to know the inner workings of their devices. We showed how both the CHSH violation and the resulting extractable key rate depended on the quality of the approximate code words. We also showed that, in terms non-Gaussian resources, we required a modest one T gate for each of $\sim\sqrt{N}$ of N total Bell pairs. Thankfully, from an experimental point of view, what this means is that only Gaussian operations (e.g., homodyne detection) are needed most of the time.

It should be noted that our encoding scheme is experimentally challenging. However, it is still practical, with many proposals already existing [24–28]. It is hoped that our paper will further motivate experimental advances using such encodings. Given the technological challenges, distances in our scheme will be limited (although not fundamentally). However, it should be noted that such limitations are also faced by the discrete-variable version of device-independent QKD, which is currently limited to a few kilometers. This is because it requires a detection efficiency of approximately 95% to achieve a key rate on the order of 10^{-10} per pulse [44].

Interestingly, one can also consider the distances over which our continuous-variable protocol will perform well. We do this by calculating the Wigner function of an approximate encoded state and then send it through an amplitude damping channel. We numerically find that, for example, at 2.3 km, with 0.2 dB/km loss, we get a key rate of 0.35 bits/state. This is comparable to discrete-variable device-independent QKD where such schemes are limited to only a few kilometers [44]. Furthermore, we note that the distance of our protocol can also be improved by using distillers as was shown for discrete-variable states [45] or by the application of heralded amplifiers [46].

The encoding itself is fault tolerant in the sense that a small shift in q or p will not significantly impact measurement results. As such, the protocol will generally perform well when noise in the channel is weak, i.e., results in only small shifts in q or p [9]. In the case of loss this condition corresponds to transmission distances small compared to a characteristic damping constant [6].

It is an interesting open question whether one can devise a device-independent continuous-variable QKD protocol with more readily accessible states. One possible avenue to explore is lifting the requirement of a CHSH inequality violation by considering a protocol where only one party trusts their device. This one-sided device-independent QKD requires one to violate only an EPR-steering inequality [22,47], which amounts to Alice and Bob checking that they have entanglement and ruling out local hidden state models [48]. This notion has recently been explored for both coherent and squeezed states for a variety of different setups [49].

ACKNOWLEDGMENTS

C. W. acknowledges support from NSERC. We are grateful to Hoi-Kwong Lo and Norbert Lütkenhaus for fruitful discussions.

APPENDIX

Here we justify the use of several results in the paper. In Sec. V we identified the approximate encoded state $\psi_{\bar{0}}(q)$ that would result when a finitely squeezed state $\psi_{sq}(p) = \pi^{-1/4}\kappa^{-1/2}\exp(-\frac{1}{2}p^2/\kappa^2)$ was measured with a POVM [Eq. (8)] subject to $q \bmod 2\sqrt{\pi}$. Supposing that we find an outcome corresponding to Π_0, we have

$$\begin{aligned}|\psi_{\bar{0}}\rangle &\propto \sum_{s=-\infty}^{\infty}(2\pi\Delta^2)^{-1/2}\int_{-\infty}^{\infty}dy e^{-\frac{1}{2}(2s\sqrt{\pi}+q)^2/\Delta^2}\\ &\quad\times\pi^{-1/4}\kappa^{1/2}e^{-\frac{1}{2}q^2\kappa^2}\delta(q-y),\\ &\propto \sum_{s=-\infty}^{\infty}e^{-\frac{1}{2}q^2\kappa^2}e^{-\frac{1}{2}(2s\sqrt{\pi}+q)^2/\Delta^2},\\ &\propto \sum_{s=-\infty}^{\infty}e^{-\frac{1}{2}q^2\kappa^2}\psi'_{sq}(q+2s\sqrt{\pi}).\end{aligned} \tag{A1}$$

Thus we recover the fact that this measurement projects the state onto a superposition of squeezed states in $\hat{q}$ with a spacing of $2\sqrt{\pi}$ and width of Δ weighted by an overall Gaussian envelope of width κ^{-1}.

In Sec. V we stated that the value of $\mathcal{S}$, with error correction, can be calculated by finding the appropriate expectation values. Consider the box function,

$$\Pi(x) = \begin{cases}1 & \text{if} \quad |x| \leqslant 1/2\\ 0 & \text{if} \quad |x| > 1/2\end{cases}. \tag{A2}$$

To calculate the value of $\mathrm{Tr}(|m\rangle\langle n|Z)$, with $m,n \in \{0,1\}$, for an element of the density matrix, we simply perform the integral,

$$\int_{-\infty}^{\infty}\psi_m(q)Z(q)\psi_n(q)dq, \tag{A3}$$

where $Z(q) = 2\{\sum_{s\in Z}\Pi[(q-2s\sqrt{\pi})/\sqrt{\pi}] - 1/2\}$ is $+1$ (-1) for q closer to an even (odd) multiple of $\sqrt{\pi}$ (see Fig. 3). Calculating a trace involving X is similar to q being replaced by p and using the corresponding Fourier transforms of the wave functions, while the other two necessary measurements,

$$\alpha = \begin{pmatrix}-i\cos\frac{\pi}{8} & -i\sin\frac{\pi}{8}\\ -i\sin\frac{\pi}{8} & i\cos\frac{\pi}{8}\end{pmatrix}, \tag{A4}$$

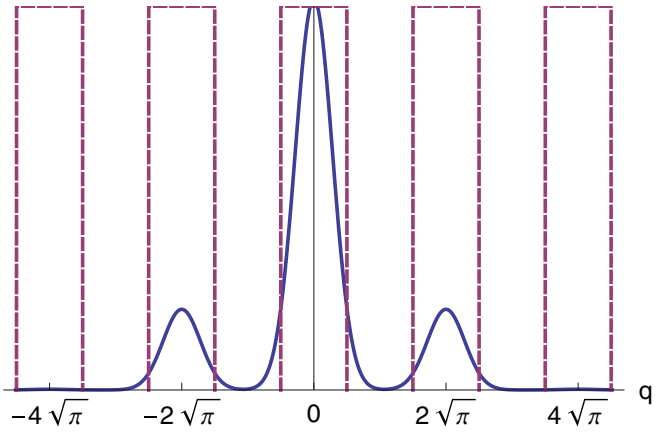

FIG. 3. (Color online) The wave function for an encoded $|\bar{0}\rangle$ state (solid) with Δ,κ corresponding to 6 dB squeezing. The regions where $Z(q)$ is positive is enclosed by the dashed plot.

$$\beta = \begin{pmatrix} -i\cos\frac{\pi}{8} & -i\sin\frac{\pi}{8} \\ i\sin\frac{\pi}{8} & -i\cos\frac{\pi}{8} \end{pmatrix}, \tag{A5}$$

can be decomposed into a sum of Z,X and calculated using the linearity of the trace function.

To study the effect of transmission on our protocol one can work within the Wigner function formalism. In this framework the amplitude damping channel can be expressed as an integral transform where

$$W(\alpha,z) = \frac{2}{T\pi}\int\left[-\frac{2}{T}|\alpha-\beta e^{-\kappa z}|^2\right]W(\beta,0), \tag{A6}$$

where $T = 1-e^{-2\kappa z}$, z is the transmission distance and κ is the corresponding decay constant. Fortunately, we are working with all Gaussian functions, or the sum of Gaussian functions as each peak in the encoded state is a Gaussian, where we can invoke the linearity of the Wigner function. Since the product and convolution of Gaussian functions are simple and remain a Gaussian it is easy to see what happens to each part in the sum of the encoded state when applying an amplitude damping channel. One can then construct suitable approximations of the damped encoded state numerically by choosing an appropriate cutoff in the infinite summation.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[3] D. Mayers and A. Yao, Quant. Inf. Comp. **4**, 273 (2004).
[4] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[5] A. Ekert and R. Renner, Nature (London) **507**, 443 (2014).
[6] D. Gottesman, A. Kitaev, and J. Preskill, Phys. Rev. A **64**, 012310 (2001).
[7] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
[8] M. Hillery, Phys. Rev. A **61**, 022309 (2000).
[9] D. Gottesman and J. Preskill, Phys. Rev. A **63**, 022309 (2001).
[10] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[11] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[12] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).
[13] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).
[14] J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics* (Cambridge University Press, Cambridge, 1987).
[15] M. Paternostro, H. Jeong, and T. C. Ralph, Phys. Rev. A **79**, 012101 (2009).
[16] J. Wenger, M. Hafezi, F. Grosshans, R. Tualle-Brouri, and P. Grangier, Phys. Rev. A **67**, 012105 (2003).
[17] R. García-Patrón, J. Fiurášek, and N. J. Cerf, Phys. Rev. A **71**, 022105 (2005).
[18] E. G. Cavalcanti, C. J. Foster, M. D. Reid, and P. D. Drummond, Phys. Rev. Lett. **99**, 210405 (2007).
[19] J. B. Brask, N. Brunner, D. Cavalcanti, and A. Leverrier, Phys. Rev. A **85**, 042116 (2012).
[20] X.-F. Qian, C. J. Broadbent, and J. H. Eberly, New J. Phys. **16**, 013033 (2014).
[21] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland, Nature (London) **409**, 791 (2001).
[22] B. Opanchuk, L. Arnaud, and M. D. Reid, Phys. Rev. A **89**, 062101 (2014).
[23] N. C. Menicucci, Phys. Rev. Lett. **112**, 120504 (2014).
[24] H. M. Vasconcelos, L. Sanz, and S. Glancy, Opt. Lett. **35**, 3261 (2010).
[25] B. C. Travaglione and G. J. Milburn, Phys. Rev. A **66**, 052322 (2002).
[26] S. Pirandola, S. Mancini, D. Vitali, and P. Tombesi, Europhys. Lett. **68**, 323 (2004).
[27] S. Pirandola, S. Mancini, D. Vitali, and P. Tombesi, Eur. Phys. J. D **37**, 283 (2006).
[28] S. Pirandola, S. Mancini, D. Vitali, and P. Tombesi, J. Phys. B **39**, 997 (2006).
[29] S. Lloyd and S. L. Braunstein, Phys. Rev. Lett. **82**, 1784 (1999).
[30] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[31] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New J. Phys. **11**, 045021 (2009).
[32] J. S. Bell, Physics **1**, 195 (1964).
[33] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[34] M. Gu, C. Weedbrook, N. C. Menicucci, T. C. Ralph, and P. van Loock, Phys. Rev. A **79**, 062318 (2009).
[35] L. Masanes, S. Pironio, and A. Acín, Nature Communications **2**, 238 (2011).
[36] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).

[37] Charles Ci Wen Lim, C. Portmann, M. Tomamichel, R. Renner, and N. Gisin, Phys. Rev. X **3**, 031006 (2013).
[38] U. Vazirani and T. Vidick, arXiv:1210.1810.
[39] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).
[40] I. Devetak and A. Winter, Proc. Ro. Soc. A **461**, 207 (2005).
[41] T. Eberle, S. Steinlechner, J. Bauchrowitz, V. Händchen, H. Vahlbruch, M. Mehmet, H. Müller-Ebhardt, and R. Schnabel, Phys. Rev. Lett. **104**, 251102 (2010).
[42] M. Mehmet, S. Ast, T. Eberle, S. Steinlechner, H. Vahlbruch, and R. Schnabel, Opt. Express **19**, 25763 (2011).
[43] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[44] M. Curty and T. Moroder, Phys. Rev. A **84**, 010304 (2011).
[45] N. Gisin, S. Pironio, and N. Sangouard, Phys. Rev. Lett. **105**, 070501 (2010).
[46] D. Pitkanen, X. Ma, R. Wickert, P. van Loock, and N. Lütkenhaus, Phys. Rev. A **84**, 022325 (2011).
[47] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Phys. Rev. Lett. **109**, 100502 (2012).
[48] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, Phys. Rev. A **85**, 010301 (2012).
[49] N. Walk, H. M. Wiseman, and T. C. Ralph, arXiv:1405.6593.