Quantum bit commitment under Gaussian constraints

Aikaterini Mandilara

Quantum Information and Communication, École Polytechnique de Bruxelles, CP 165/59, Université Libre de Bruxelles,
1050 Brussels, Belgium

Nicolas J. Cerf

Quantum Information and Communication, École Polytechnique de Bruxelles, CP 165/59, Université Libre de Bruxelles,
1050 Brussels, Belgium, and W. M. Keck Center for Extreme Quantum Information Theory, Massachusetts Institute of Technology,
77 Massachusetts Avenue, Cambridge, Massachusetts 02139, USA

Quantum bit commitment has long been known to be impossible. Nevertheless, just as in the classical case, imposing certain constraints on the power of the parties may enable the construction of asymptotically secure protocols. Here, we introduce a quantum bit commitment protocol and prove that it is asymptotically secure if cheating is restricted to Gaussian operations. This protocol exploits continuous-variable quantum optical carriers, for which such a Gaussian constraint is experimentally relevant as the high optical nonlinearity needed to effect deterministic non-Gaussian cheating is inaccessible.

I. INTRODUCTION

Quantum bit commitment (QBC) is probably one of most studied quantum cryptographic primitives, just after quantum key distribution (see, e.g., [1]). It belongs to the class of mistrustful cryptography problems, which involve two parties (Alice and Bob) who do not trust each other. More specifically, bit commitment is a primitive in which Alice commits to a certain bit while this bit should remain hidden to Bob until Alice later reveals its value. In the first stage, called "commit phase," Alice locks her bit in such a way that it is hidden and sends it to Bob. The protocol is said to be "concealing" if Bob cannot cheat by learning information about this bit before the second stage. In this second stage, called "unveil phase," Alice sends information to Bob so that he can unlock the bit and find its value. The protocol is said to be "binding" if Alice cannot cheat by changing the value of the bit once she has committed to it. A bit commitment protocol is secure if it prevents Alice and Bob from cheating, that is, if it is both binding and concealing.

The original proof of the impossibility of QBC due to Mayers consists of two steps [2]. The first, which is the most subtle one and is not discussed here, is to show that the security of any QBC reduces to the security of a generic QBC scenario as described hereunder. The second step is then to show that this generic QBC scenario, also known as a "purification" QBC protocol [3], is insecure [4]. In this scenario, Alice uses a bipartite Hilbert space $H_p \otimes H_t$, which is the tensor product of the so-called "proof" and "token" spaces. Alice chooses to commit the bit b (0 or 1) and prepares one of the two orthogonal states $|\chi_b\rangle$ in the total Hilbert space by applying a unitary transformation U_b on a state $|\psi\rangle$, that is, $|\chi_b\rangle = U_b|\psi\rangle$. In the Schmidt representation, these states may be written as

$$|\chi_0\rangle = \sum_i a_i |p_i\rangle |t_i\rangle, \quad |\chi_1\rangle = \sum_i a_i' |p_i'\rangle |t_i'\rangle. \qquad (1)$$

In the commit phase, Alice transmits to Bob the token system lying in H_t, which is in state $\rho_b = \text{tr}_p |\chi_b\rangle\langle\chi_b|$. In the unveil phase, Alice transmits to Bob the proof system lying in

H_p, so Bob can determine the value of the committed bit b by projectively measuring the state $|\chi_b\rangle$ using orthogonal projectors. Now, the insecurity of this generic QBC protocol against cheating can easily be proven. The requirement that Bob gains no information before the unveil phase simply translates into $\rho_1 = \rho_0$, or equivalently $|t_i'\rangle = |t_i\rangle$ (up to a phase) and $a_i' = a_i$, $\forall\, i$. Remarkably, if this condition is fulfilled, Alice can perfectly cheat after the commit phase by changing $\{|p_i\rangle\} \to \{|p_i'\rangle\}$ with some appropriate unitary transformations $U_p \otimes \mathbb{1}$ on her proof system. This implies that QBC cannot be both perfectly concealing and binding [2,4].

This proof leaves open the possibility that if certain restrictions are imposed on the operations available to the parties, a QBC may be constructed that is secure or at least partially secure. There is some literature on this topic for both classical and quantum bit commitment (see, for instance, [5] and references therein, or [6–8]), with positive and negative results. What we examine here is a simpler and less-studied scenario, where restrictions are imposed on Alice's cheating operations only. One can easily construct a secure QBC that falls into this category: Simply encode the committed bit into a subspace of the total Hilbert space that remains invariant under Alice's permitted local transformations on the proof system. To illustrate this idea, let us give a trivial example using a system consisting of two spin-$\frac{1}{2}$ particles. Let us encode 0 and 1 into the eigenvalue of the total spin $\mathbf{S}^2 = (\mathbf{S}_1 + \mathbf{S}_2)^2$ by choosing

$$\begin{aligned}
|\chi_0\rangle &= |s=0, m=0\rangle = (|\uparrow\rangle|\downarrow\rangle - |\downarrow\rangle|\uparrow\rangle)/\sqrt{2}, \\
|\chi_1\rangle &= |s=1, m=0\rangle = (|\uparrow\rangle|\downarrow\rangle + |\downarrow\rangle|\uparrow\rangle)/\sqrt{2},
\end{aligned} \qquad (2)$$

where s stands for the total spin quantum number and m for the quantum number associated with its projection onto the z axis. It is obvious that the condition $\rho_1 = \rho_0$ is satisfied and that the protocol is not secure if Alice has all local operations [i.e., the algebra $SU(2) \otimes 1$] at her disposal. However, let us suppose that her local operations are restricted to a subgroup of $SU(2) \otimes 1$ that commutes with $\mathbf{S}^2$. For the case of spins there

is no such subgroup, but one can still restrict Alice to use the trivial operation generated by $\mathbf{S}_1$, that is, a rotation around the $(1,1,1)$ vector in the Bloch sphere representation. Under this restriction, the protocol becomes secure since cheating would require a rotation around the z axis or $(0,0,1)$ vector, that is, an operation known as a "phase gate" in which $|\uparrow\rangle$ remains unchanged while $|\downarrow\rangle$ gets a minus sign.

This example is rather unrealistic since there is no objective reason for justifying this restriction on Alice's local operations while, in the total Hilbert space $H_p \otimes H_t$, she can apply the global operations that generate $|\chi_b\rangle$ as defined in Eq. (2). On the contrary, in the QBC scheme that we introduce in this paper, it will appear that a specific constraint on Alice's cheating operations can be experimentally well motivated, giving rise to an asymptotically secure protocol. We devise a "continuous-variable" QBC protocol based on quantum states lying in an infinite-dimensional Hilbert space, which can be realized as states of the electromagnetic field (see, e.g., [9,10]). In this quantum optical QBC protocol, we assume that Alice is restricted to carry out Gaussian operations only, which is consistent with the current experimental ability to engineer quantum states of light in a deterministic way. Only a few very challenging experiments have been successful to prepare and manipulate non-Gaussian states of traveling light (see, e.g., [11–16]), and all of these schemes are based on heralded photon subtraction [17] or addition [18], hence are probabilistic in nature. A deterministic non-Gaussian operation would require high optical nonlinearities that are not accessible in the laboratory today. Since probabilistic cheating does not endeavor the security of QBC if the success probability is low (this even holds true otherwise, though in the asymptotic protocol only), such a restriction to Gaussian cheating operations is justified in the context of QBC.

Thus, although it is not impossible, in principle, to realize deterministic non-Gaussian optical operations based on giant nonlinearities, there is a natural boundary separating the Gaussian from non-Gaussian deterministic operations, and it is relevant to investigate a QBC scenario where Alice is not allowed to carry out non-Gaussian cheating operations. This scenario has been introduced in [8], where a strong "no-go theorem" was derived: Secure QBC is forbidden in continuous-variable protocols where both players are restricted to use Gaussian states and operations. In other words, if the protocol is built on Gaussian states $|\chi_b\rangle$, it is sufficient for the players to carry out Gaussian operations in order to cheat perfectly. Therefore, it was concluded in [8] that a secure QBC protocol with Gaussian constrained cheating, if it exists, should necessarily be built on non-Gaussian states $|\chi_b\rangle$. In the present paper, we prove that this holds by exhibiting an explicit secure non-Gaussian QBC protocol. It should not be viewed as a directly usable QBC protocol since, as we will see, it still requires the use of either a quantum memory or a very long time delay in an optical interferometer. Instead, our goal is to point toward a conceptual method to reach asymptotic security in continuous-variable QBC under Gaussian constraints. A restricted proof-of-principle demonstration of this protocol seems nevertheless feasible within the currently available technologies.

In Sec. II, we define our QBC protocol and analyze first how it works when the two parties are honest. In Sec. III, we go beyond the honest scheme and investigate Alice's best possible

cheating if restricted to Gaussian operations. In Sec. IV, we consider Bob's cheating, which allows us to probe the trade-off between Alice and Bob's cheating. In Sec. V, we suggest an improvement to the scheme in order to make it asymptotically secure, while we conclude in Sec. VI.

II. THE HONEST SCHEME

Let us consider the following purification protocol [3] in an infinite-dimensional Hilbert space, which is in direct analogy with the above-mentioned spin-$\frac{1}{2}$ example. The 0 and 1 values of the committed bit b are encoded into the orthogonal two-mode non-Gaussian states,

$$|\chi_0\rangle = (|\alpha\rangle|-\alpha\rangle - |-\alpha\rangle|\alpha\rangle)/\sqrt{2(1 - e^{-4|\alpha|^2})},$$
$$|\chi_1\rangle = (|\alpha\rangle|-\alpha\rangle + |-\alpha\rangle|\alpha\rangle)/\sqrt{2(1 + e^{-4|\alpha|^2})}, \quad (3)$$

where $|\alpha\rangle = D(\alpha)|0\rangle = \exp(\alpha a^\dagger - \alpha^* a)|0\rangle$ is a coherent state of complex amplitude α. Moving from orthogonal qubit states $|0\rangle$ and $|1\rangle$ in a two-dimensional Hilbert space to near-orthogonal coherent states $|\alpha\rangle$ and $|-\alpha\rangle$ ($\alpha \gg 1$) in an infinite-dimensional Hilbert space has already been put forward in the context of quantum computation [19,20], and our treatment of QBC follows on this. Note that the states of Eq. (3) correspond to entangled "Schrödinger cat" states, whose experimental generation has recently been demonstrated in [21].

Let us suppose that $\alpha \gtrsim 2$ (in practice, this is sufficient to be very close to the asymptotic situation where $|\alpha\rangle$ and $|-\alpha\rangle$ are orthogonal). One of the two modes (token system) of state $|\chi_b\rangle$ is sent to Bob in the commit phase, while the second mode (proof system) is kept by Alice. At this stage, Bob can almost not distinguish between $|\chi_0\rangle$ and $|\chi_1\rangle$ whatever measurement he uses since $\rho_1 \simeq \rho_0$. On the other hand, it is immediate to see how Bob can distinguish between these mutually orthogonal states $|\chi_b\rangle$ in the total Hilbert space during the unveil phase. Consider the two modes of $|\chi_b\rangle$ as incident beams on the two ports of a balanced beam splitter, effecting the unitary operation B. By adjusting the phases, the outgoing state $|\chi'_b\rangle = B|\chi_b\rangle$ can be written as

$$|\chi'_0\rangle = (|\alpha'\rangle - |-\alpha'\rangle)|0\rangle/\sqrt{2(1 - e^{-2|\alpha'|^2})},$$
$$|\chi'_1\rangle = (|\alpha'\rangle + |-\alpha'\rangle)|0\rangle/\sqrt{2(1 + e^{-2|\alpha'|^2})}, \quad (4)$$

which is the tensor product of a Schrödinger cat state of amplitude $\alpha' = \sqrt{2}\alpha$ and the vacuum state. Note that the cat state is odd (even) for $b = 0$ ($b = 1$). The states $|\chi'_b\rangle$ are perfectly distinguishable by applying a photon number parity measurement on the first mode, corresponding to the observable $P = (-1)^{a^\dagger a}$; that is,

$$\langle \chi'_0 | P \otimes 1 | \chi'_0 \rangle = -1, \quad \langle \chi'_1 | P \otimes 1 | \chi'_1 \rangle = 1. \quad (5)$$

Note that this measurement may be realized by photon counting using a number-resolving photodetector as has very recently become available (see, e.g., [22,23]).

Now, we are ready to describe the honest QBC protocol as illustrated in Fig. 1. In the commit phase, Alice prepares one of the states $|\chi'_b\rangle$ as defined in Eq. (4) according to the value of the bit b she wants to commit. Using a balanced beam splitter, she converts $|\chi'_b\rangle$ into $|\chi_b\rangle$ as defined in Eq. (3), and then sends the token mode (in state ρ_b) to Bob. In the unveil
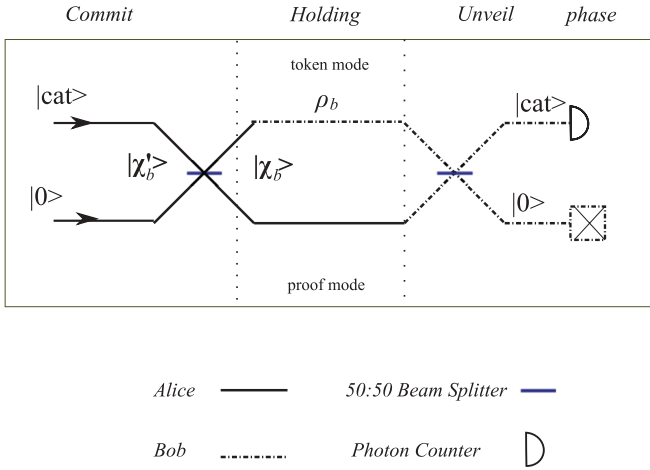
FIG. 1. (Color online) Honest protocol. The state $|cat\rangle$ can either be an even or an odd Schrödinger's cat state of amplitude α' depending on the bit b to be committed [see the first mode in Eq. (4)]. The token mode is transmitted in the commit phase, while the proof mode is transmitted in the unveil phase. Bob combines the two modes at a balanced beam splitter and measures the photon number parity in the first mode.

phase, she sends the proof mode to Bob, which he combines with his token mode in a balanced beam splitter to obtain the unentangled state $|\chi_b'\rangle$ as originally held by Alice. Finally, Bob discards the mode corresponding to the vacuum state and performs a parity measurement on the cat state in order to unveil the value of bit b. We assume that the interferometric scheme is perfectly balanced and that the holding phase (the period after the commit phase but before the unveil phase) can be achieved by inserting equal time delays in the two branches of the interferometer. Ideally, a quantum memory should of course be available to Bob in order to achieve a longer-time holding phase.

III. ALICE'S BEST CHEATING STRATEGY

Let us first assume that the QBC protocol is concealing, that is, secure against any measurement by Bob trying to cheat during the holding phase. In other words, we assume that the coherent state amplitude $\alpha \gtrsim 2$, so that $\rho_1 \simeq \rho_0$. Under this assumption, which we make rigorous in Sec. IV, we can investigate the security of the protocol against Alice's cheating strategies.

A. Non-Gaussian cheating

Obviously, if all local operations on the proof mode were available to Alice, then she could convert the value of her committed bit at will during the holding phase. However, this would require her ability to perform a notably non-Gaussian local operation, where $|\alpha\rangle$ remains unchanged while $|-\alpha\rangle$ gets a minus sign. Such an operation, which can be viewed as the continuous-variable analog to the phase gate that we referred to in the case of spin-$\frac{1}{2}$ particles, corresponds in the limit $\alpha \gg 1$ to the non-Gaussian unitary

$$U_{NG} = D(-\alpha)\exp[i\pi|0\rangle\langle 0|]D(\alpha). \quad (6)$$

It cannot be implemented deterministically with accessible optical nonlinearities, so for cheating one would have to turn to probabilistic schemes based on heralded photon subtraction, whose probability of success is very low [24,25]. Therefore, we may fairly impose such a Gaussian restriction on Alice's cheating operation in the holding phase (or assume that the probability of success of such a non-Gaussian local operation is negligible).

One may rightly argue, of course, that within the current experimental settings, the generation of Schrödinger cat states as needed in Alice's preparation of $|\chi_b'\rangle$ cannot be deterministic either. However, during the commit phase, Alice can determine whether $|\chi_b'\rangle$ has been successfully prepared or not, and, if not, she can repeat the operation again until it is successful (or send the state to Bob but later notify him of the failed trial). Thus, the probabilistic occurrence of a failure is not detrimental to the commit phase, while it prevents an efficient non-Gaussian cheating. In other words, the Gaussian restriction we impose on Alice's cheating operations is justified within the present experimental limitations, while, at the same time, Alice's preparation of the non-Gaussian state $|\chi_b'\rangle$ needed to overcome the no-go theorem [8] can very well be done probabilistically.

B. Gaussian cheating

The essential task to be completed now is to find the best cheating strategy for Alice if only Gaussian operations are available to her. Here, "best" should be interpreted according to the unveil procedure that has been defined for the honest protocol, that is, when Bob uses a balanced beam splitter and performs a parity measurement on the first mode. If, when Alice cheats, Bob reconstructs the state $|\chi_\#'\rangle$ at the output of his beam splitter while Alice had initially committed $|\chi_b'\rangle$, the best cheating strategy is obviously the one where $\langle\chi_\#'|P \otimes 1|\chi_\#'\rangle$ reaches the closest value to $\langle\chi_{\neg b}'|P \otimes 1|\chi_{\neg b}'\rangle$, where $\neg b$ is the complement of the bit b. The probability of success of the best Gaussian cheating strategy can be measured with Alice's "maximum control" C_{max}, as defined in [3].

Let us review the operations available to Alice. The most general Gaussian unitary operation U_G on a single mode is an exponential of a linear combination of the elements of the two-photon algebra h_6, namely $\{1, a, a^2, a^\dagger, a^{\dagger 2}, 1/2 + a^\dagger a\}$, so it relies on six real parameters. This general Gaussian transformation can also be casted as a sequence of standard optical operations, for instance [26],

$$U_G = D(\beta)U(\varphi)S(r)U(\theta), \quad (7)$$

where $S(r) = \exp[\frac{r}{2}(a^2 - a^{\dagger 2})]$ is a squeezing of parameter r of the x quadrature, $U(\theta) = \exp(i\theta a^\dagger a)$ is a phase rotation of angle θ, and $D(\beta) = \exp(\beta a^\dagger - \beta^* a)$ is a displacement of complex coherent amplitude β. We ignore the global phase operation, which plays no role here.

The information about the committed bit b is encoded into the parity of the first mode of $|\chi_b'\rangle$, or, adopting a phase-space point of view, in the interference pattern of the Wigner function ($\hbar = 1$),

$$W(x,p) = \frac{1}{2\pi}\int_{-\infty}^{\infty} \exp(ipq)\left\langle x - \frac{q}{2}\left|\rho\right|x + \frac{q}{2}\right\rangle dq. \quad (8)$$

Note that the quadrature variables (x,p) in phase space are defined here using the convention $a = (x + ip)/\sqrt{2}$. This phase-space interpretation, which is very useful in the following, originates from the relation between the mean parity and the Wigner function at the origin in phase space, namely

$$W(0,0) = \frac{1}{\pi}\langle P\rangle. \qquad (9)$$

The interference pattern of the Wigner function of the Schrödinger cat state $|\chi'_b\rangle$—hence the parity information—is smoothed out during the commit phase since Alice looses a handle on the token system, and it is revived in the unveil phase once the token and proof systems can be measured jointly. One can visually understand this smoothing out procedure by comparing the Wigner function of the first mode in Eq. (4) during the commit phase (before the beam splitter) with the Wigner function of the traced out mode in Eq. (3) during the holding phase. What we need to analyze is the effect on the mean parity $\langle P\rangle$ of the first mode of $|\chi'_b\rangle$ when Alice applies any Gaussian unitary U_G on the proof mode of $|\chi_b\rangle$. The most general operation is actually a Gaussian CP map, but we argue later on that the best cheating is necessarily a Gaussian unitary.

In the simplest scenario, involving displacements only, Alice can, for example, displace the proof system by d along the positive p quadrature direction. In the unveiling phase, Bob will then get the initially committed cat state displaced by $-d/\sqrt{2}$ along the p quadrature, where the factor $\sqrt{2}$ is due to the second beam splitter. In other words, Alice can alter the parity of the unveiled state by freely displacing the origin of phase space to another point of the interference pattern where the Wigner function has another value, even possibly the opposite sign. We now prove that this simplest scenario actually provides the best Gaussian cheating strategy for Alice, so that no squeezing or phase-rotation is helpful.

The key observation is that the most general Gaussian unitary of Eq. (7) corresponds to a special case of an affine transformation in phase space [27], namely a linear symplectic transformation followed by a translation. Intuitively, this means that the Wigner function of the initial state may be displaced, squeezed, or rotated, but its maximum and minimum values $W_{\max,\min}$ remain invariant under these operations. Alternatively, using Eq. (9), this means that the maximum and minimum values of the mean parity $\langle\hat{P}\rangle_{\max,\min}$ that can be reached under Gaussian unitaries are invariant for a given input state. They can be reached simply by translating the Wigner function in such a way that the origin is moved toward the highest peak or the deepest dip in phase space, respectively, with no squeezing or rotation needed.

Remember that, when cheating, Alice can only apply her Gaussian operation on the proof mode, not on the token mode. However, since Bob only checks the first outgoing mode of his beam splitter (the one containing the cat state whose parity encodes b), an arbitrary displacement on this mode can be achieved via a displacement of the proof mode only, so Alice can indeed freely translate the Wigner function of the cat state. Now, leaving displacements aside, if Alice's cheating operation involves a rotation or squeezing operation, the outgoing modes of Bob's beam splitter become inevitably entangled, so the unveiled state becomes mixed. Since mixing can only wash out the interference pattern, the maximum parity

$\langle P\rangle_{\max}$ can only decrease while $\langle P\rangle_{\min}$ can only increase. Thus, rotation and squeezing can only make cheating worse, and are useless to Alice. The same reasoning also implies that a Gaussian CP map cannot do better than a Gaussian unitary since it eventually implies tracing over some ancillary system after applying a Gaussian unitary onto the joint system, hence smearing out the Wigner function.

This confirms that Alice's best Gaussian cheating strategy for reaching the target bit value $\neg b = 0$ (1) is by displacing her proof system so that Bob obtains the originally committed cat state $|\chi'_b\rangle$ displaced in such a way that the minimum (maximum) value of its Wigner function $W_{\min}$ ($W_{\max}$) is now located at the origin. Perfect cheating will be achieved if $W_{\min} = -1$ ($W_{\max} = 1$).

C. Alice's maximum control $C_{\max}$

To illustrate this optimal Gaussian cheating, suppose that Alice has initially committed the bit $b = 0$ (odd Schrödinger cat with $\langle\chi'_0|P\otimes 1|\chi'_0\rangle = -1$) and attempts to cheat during the holding phase so that Bob would measure a bit $\neg b = 1$ (even Schrödinger cat with $\langle\chi'_\#|P\otimes 1|\chi'_\#\rangle = 1$) in the unveil phase. The optimal cheating strategy is easy to understand in Fig. 2, where we have plotted the Wigner function of the initially committed cat state. Alice needs to displace her proof system by $\sqrt{2}\,d$ along the p quadrature, so that $|\chi'_\#\rangle$ becomes the original odd cat state displaced by $-d$ along the p quadrature
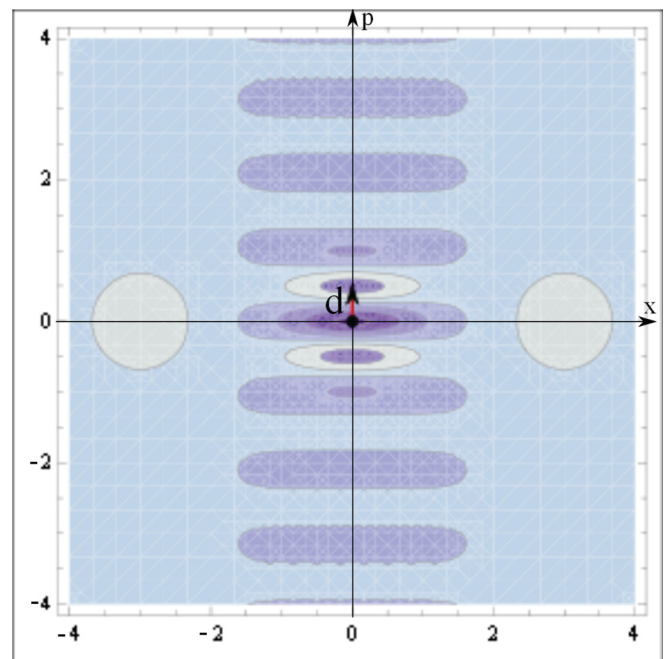

FIG. 2. (Color online) Contour plot of the Wigner function of an odd Schrödinger cat state of amplitude $\alpha' = 3/\sqrt{2}$. Bob obtains this state in the unveil phase if Alice has committed the bit 0 and has not cheated. The best cheating strategy for Alice during the holding phase is to displace her proof system by $\sqrt{2}d$ along the p quadrature, so that the unveiled state is displaced by $-d$ (or the origin in phase space is shifted upward by d, as illustrated by the arrow). Then, the origin of the unveiled state is located on the global maximum of the original Wigner function. For an even Schrödinger cat, the situation is exactly analogous.
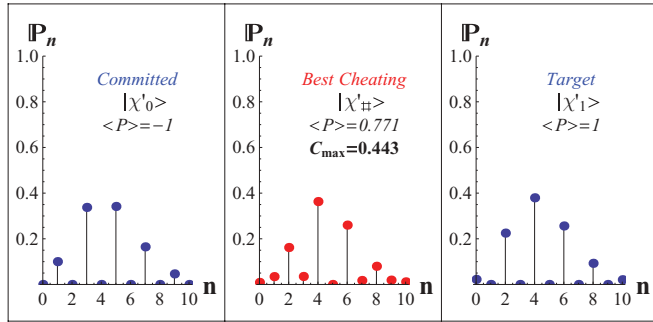
FIG. 3. (Color online) Photon number distribution for (a) the committed cat state ($\alpha' = 3/\sqrt{2}$) corresponding to bit 0; (b) the state achieved by Alice's best Gaussian cheating strategy; and (c) the target state corresponding to bit 1. The symbol $\langle P \rangle$ denotes the mean photon number parity, while C_{max} denotes Alice's maximum control.

(equivalently, the origin of phase space is shifted upward by d as illustrated by an arrow in Fig. 2). The parameter d is just the distance (along the p quadrature direction) from the origin to the first maximum of the interference pattern, which is also the global maximum of the Wigner function.

For a cat state of amplitude α' there is no analytical expression for d as a function of α', and one has to numerically solve the equation

$$p \cos(2\sqrt{2}p\alpha') + \sqrt{2}\alpha \sin(2\sqrt{2}p\alpha') = pe^{-2\alpha'^2} \qquad (10)$$

for p. The best cheating is then a displacement by d, which corresponds to the smallest positive and nonzero solution of Eq. (10). Let us analyze precisely the effect of such a cheating in the specific example of Fig. 2, that is, when Alice commits an odd cat state of amplitude $\alpha' = 3/\sqrt{2}$. By solving Eq. (10), we get that the best Gaussian cheating requires a displacement of $d = 0.496$. The corresponding photon number distributions with and without cheating are schematically presented in Fig. 3, where we observe that the distribution with cheating qualitatively resembles the target distribution.

The probability of success of this best Gaussian cheating strategy can be measured with Alice's "maximum control" C_{max} as defined in [3], that is, the largest difference between Alice's probability of unveiling whatever bit she wants when she is cheating and when she is honest. Assuming that the bit she wishes to unveil is equiprobable, this can be expressed as one half of her cheating probability. Using the relations $\langle P \rangle = \langle P_+ \rangle - \langle P_- \rangle$ and $\langle P_+ \rangle + \langle P_- \rangle = 1$, where $\langle P_{+(-)} \rangle$ stands for the probability to measure an even (odd) number of photons at the displaced origin, we can deduce $\langle P_{+(-)} \rangle$ from the mean parity at the displaced origin $\langle P \rangle = \pi W(0,d)$. Since Alice had committed a bit $b = 0$, here $\langle P_+ \rangle$ is the probability that she successfully cheats and unveils a bit $b = 1$. Thus, in the present case, we get

$$C_{max} \equiv \tfrac{1}{2}\langle P_+ \rangle = \tfrac{1}{4}(\langle P \rangle + 1) = 0.443. \qquad (11)$$

The success probability of Alice's optimal Gaussian cheating C_{max} increases with the amplitude α' since the contrast in the interference pattern of the Wigner function of the cat state becomes stronger. In Fig. 4, we illustrate this dependence as derived numerically. Note that for small values of α', there is a different behavior for odd and even cats related to the fact
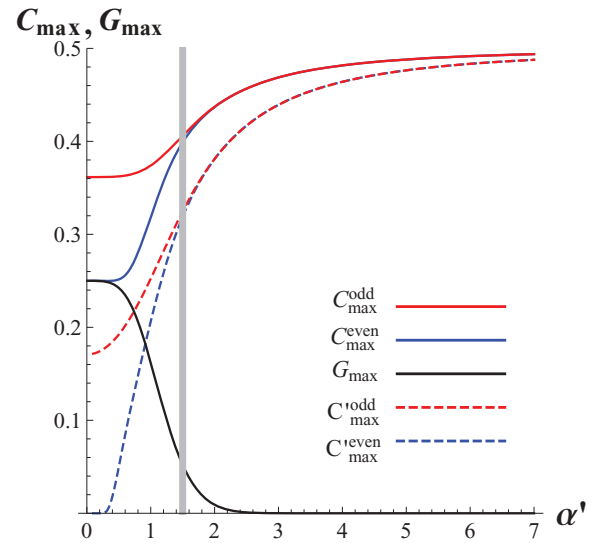

FIG. 4. (Color online) Alice's maximum control C_{max} (one half of the success probability of her optimal Gaussian cheating) as a function of the coherent amplitude α'. For small values of α' ($\alpha' \lesssim 3/2$), on the left of the vertical gray bar, the committed even and odd cat states behave differently; that is, $C_{max}^{odd} \neq C_{max}^{even}$. We also plot C'_{max}, Alice's maximum control when the vacuum mode is also monitored by Bob in the unveil phase, for both an initially committed even and odd cat state. Bob's maximum information gain G_{max} (one half of the probability of successfully determining the committed bit) is also plotted as a function of α'.

that their mean photon number significantly differs (the even cat tends to the vacuum state $|0\rangle$ as $\alpha' \to 0$, while the odd cat tends to the first number state $|1\rangle$). For large values of α' ($\gtrsim 3/2$), it can be analytically shown that the dependence simply scales as $C_{max} \simeq \exp(-\pi^2/8\alpha'^2)/2$; that is, C_{max} tends to $1/2$ with a difference following a polynomial dependence in $1/\alpha'$. This feature is crucial in Sec. V, where we consider the asymptotic security of the protocol. It is simply obtained by using the approximation $d \approx \pi/(2\sqrt{2}\alpha')$, resulting from the fact that in this limit the global maximum (minimum) approximately coincides with the maxima (minima) of the oscillating interference term $\cos(2\sqrt{2}p\alpha')$.

Interestingly, Alice's maximum control C_{max} can be further reduced if, during the unveil stage, Bob also verifies that the second outgoing mode of his beam splitter is in the vacuum state $|0\rangle$ as it should be in the absence of cheating. If Alice applies the above optimal Gaussian cheating during the holding phase, the second outgoing mode experiences the same displacement as the cat state, so that the probability that no photon is detected is $P_{NoP} = \exp(-d^2/2)$. This was irrelevant in the above calculation of C_{max} as Bob disregarded the second mode in the unveil phase. However, one can make use of this fact and measure the second mode with photon counting in order to further improve the security of the protocol since the probability of successful cheating is then reduced to $C'_{max} = C_{max} \times P_{NoP}$. We present the modified curve C'_{max} in Fig. 4 with dashed lines. It must be stressed, however, that the optimal cheating strategy we derived in the original protocol (without monitoring the second mode) does

not necessarily remain optimum for this modified protocol. Finding the optimal C'_{max} is an open problem.

It is important to mention here that throughout our analysis, we have only considered the case where Alice applies her cheating operations during the holding phase. Alice could as well cheat in the commit phase already by committing a state that is different from the state $|\chi'_b\rangle$ of Eq. (4) and try to change it during the hold phase. An example of such a successful cheating strategy would be to commit a state of amplitude α higher than the one agreed upon and displace her proof mode at will during the commit phase. In this way, and if $\alpha \gg 1$, she could obviously achieve C_{max} asymptotically close to 1/2. However, the detection of such a cheating during the commit phase could easily be detected in the asymptotic protocol that we suggest in Sec. V.

IV. BOB'S BEST CHEATING STRATEGY

In the previous section, we have assumed that the amplitude α was large enough to guarantee that the protocol was perfectly concealing. We will now make this statement more accurate, and determine the relation between α and Bob's maximum information gain G_{max} (as defined in [3]) during the holding phase while assuming that Alice is honest. The most appropriate measure to quantify G_{max} uses the trace distance [28]

$$D(\rho_0, \rho_1) = \tfrac{1}{2}\mathrm{Tr}|\rho_0 - \rho_1|, \qquad (12)$$

which corresponds to the probability of successfully distinguishing the two quantum states with the best POVM measurement, so-called Helstrom measurement [29]. If ρ_0 and ρ_1 correspond to the single-mode reduced states of $|\chi_0\rangle$ and $|\chi_1\rangle$ from Eq. (3), it is easy to show that

$$\rho_0 - \rho_1 = \frac{e^{4|\alpha|^2}}{(e^{8|\alpha|^2} - 1)}[(|\alpha\rangle\langle\alpha| + |-\alpha\rangle\langle-\alpha|).$$
$$- e^{2|\alpha|^2}(|\alpha\rangle\langle-\alpha| + |-\alpha\rangle\langle\alpha|)]. \qquad (13)$$

It remains to find the eigenvalues of the Hermitian matrix $H = \rho_0 - \rho_1$, which is not a difficult task once we observe that it can be rewritten in terms of cat states,

$$H = \lambda_+|+\rangle\langle+| + \lambda_-|-\rangle\langle-|, \qquad (14)$$

with $|\pm\rangle = (|\alpha\rangle \pm |-\alpha\rangle)/\sqrt{2(1 \pm e^{-2|\alpha|^2})}$ and $\lambda_\pm = \pm e^{2|\alpha|^2}/(1 + e^{4|\alpha|^2})$. It then follows that

$$\mathrm{Tr}|H| = 2e^{2|\alpha|^2}/(1 + e^{4|\alpha|^2}) \qquad (15)$$

and

$$G_{max} \equiv \frac{1}{2}D(\rho_0, \rho_1) = \frac{e^{-2|\alpha|^2}}{2(1 + e^{-4|\alpha|^2})}. \qquad (16)$$

This implies that Bob's capability to optimally distinguish between the two states decays exponentially with α, analogously to the behavior of the overlap $\langle\alpha|-\alpha\rangle$. In Fig. 4, we have also plotted G_{max} as a function of the amplitude of the committed cat state $\alpha' = \sqrt{2}\alpha$, which illustrates this exponential decay. We observe a trade-off between Alice's cheating and Bob's cheating: The more control Alice has on the committed state (large C_{max}), the less information Bob is able to gain (small G_{max}). This trade-off is exhibited in Fig. 5, where we plot C_{max} versus G_{max} for an initially committed odd
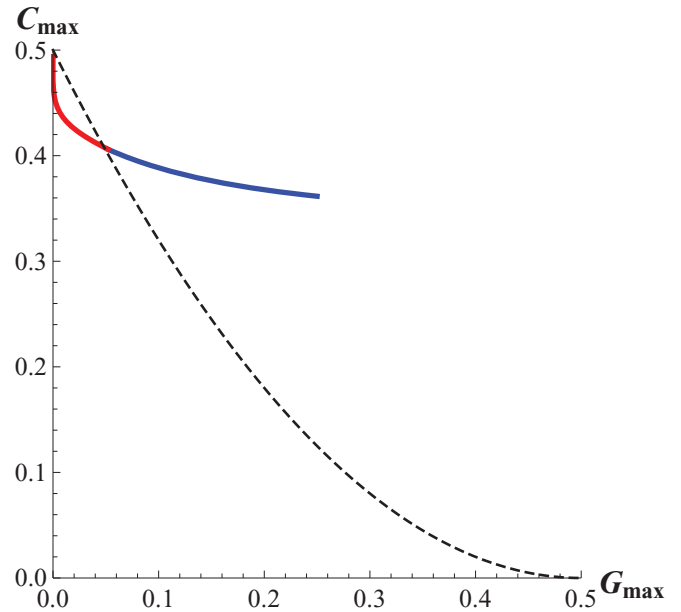

FIG. 5. (Color online) Solid red (blue) line, Alice's maximum control $C_{max\text{-}odd}$ versus Bob's maximum information gain G_{max} for $\alpha' \geqslant 3/2$ ($\alpha' < 3/2$); dotted black line, lower bound on the C_{max} versus G_{max} trade-off for QBC protocols as derived in [3].

cat state (bit 0). For comparison, we also plot the (not necessary reachable) lower bound on this trade-off for QBC protocols as derived in [3] (we refer the reader to Ref. [30] for some recently obtained results on the exact bounds). It appears that, while our protocol as such cannot be both perfectly concealing and binding (there is no value of α such that G_{max} and C_{max} tend to zero simultaneously), it enters (for $\alpha' \geqslant 3/2$) in the area that is not accessible to QBC protocols without restrictions.

V. ASYMPTOTICALLY SECURE PROTOCOL

The fact that Bob's maximum information gain G_{max} is *exponentially* decreasing with α' while the success probability of Alice's best Gaussian cheating C_{max} is only *polynomially* increasing with α' can be exploited to improve the security of our QBC protocol in a similar manner as in the original QBC protocol of Ref. [31].

This is achieved by modifying the setting of Fig. 1 and using a sequence (a tensor product) of N identical states $|\chi'_b\rangle$ instead of a single one for the encoding. In this modified scheme, we may assume that Alice's best Gaussian cheating strategy factorizes. A collective Gaussian attack on N states cannot increase the maximum value of the total Wigner function of the N states, and therefore it cannot give a better cheating on average. With this argument, we can estimate that her maximum success probability is simply $C_{max}^{(N)} = 2^{N-1}(C_{max})^N$ since the cheating remains undetected only if all N states are successfully controlled by Alice. Hence $C_{max}^{(N)}$ decreases *exponentially* with N. In contrast, assuming that entangled measurements are of no use, Bob's maximum information gain becomes $G_{max}^{(N)} = [1 - (1 - 2G_{max})^N]/2$ since $(1 - 2G_{max})$ is the probability of not distinguishing the states. Hence, $G_{max}^{(N)}$ increases linearly (at most polynomially [28]) with the number of states N provided that G_{max} is small (α' is large).
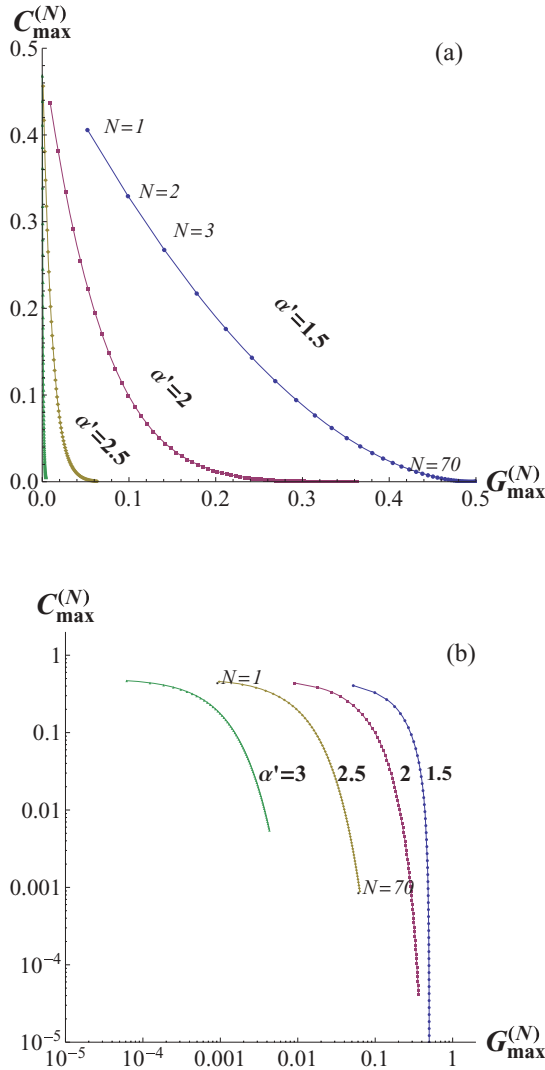
FIG. 6. (Color online) (a) Alice's maximum control $C_{max}^{(N)}$ versus Bob's maximum information gain $G_{max}^{(N)}$ for different amplitude α'. (b) The same plot in logarithmic axes.

Then, by choosing a large amplitude α' so that G_{max} is exponentially small, $C_{max}^{(N)}$ can be made exponentially small as well by choosing a large enough N (not too large to keep $G_{max}^{(N)}$ small, which is possible given the linear scaling). In this way, we can construct a QBC protocol that is *asymptotically secure* in the sense that $G_{max}^{(N)} \to 0$ and $C_{max}^{(N)} \to 0$.

As a matter of concreteness, we plot in Fig. 6 the value of $C_{max}^{(N)}$ versus $G_{max}^{(N)}$ for different values of the coherent amplitude α'. For a given α', the point moves to the right for increasing N, and we tend to a protocol where Alice cannot cheat anymore while Bob is able to cheat perfectly. If the value of α' is increased, the starting point for $N = 1$ corresponds to a better control for Alice and a lower information gain for Bob. Then, if α' is taken large enough, we can reach an interesting region where both $C_{max}^{(N)}$ and $G_{max}^{(N)}$ are small by choosing an appropriate large value of N.

In practice, achieving really small values of G_{max} and C_{max} is probably not possible within the current available technology. For instance, a security of the order of 10^{-5} would require $\alpha' \approx 4$ and $N \approx 300$. More realistically, a value of

G_{max} and C_{max} of the order of 10^{-1} would only require $\alpha' \approx 2$ and $N \approx 10$, which may be feasible if the N committed cat states are sent iteratively. For $N = 1$, as can be seen in Fig. 5, we are far from the secure region as C_{max} remains too large. It may be interesting, however, to demonstrate this protocol for $N = 1$ and $\alpha' \geqslant 3/2$ as it then beats any possible QBC protocol with no restriction [3], as already mentioned.

The asymptotic protocol can also efficiently protect against cheating strategies of Alice during the commit phase if the parity measurement at the unveil phase is replaced by photon-number counting. In this case, by measuring $N \gg 1$ states, Bob obtains the photon-number distribution of the committed state and thus may easily conclude if Alice has initially committed another state than than the states $|\chi_b'\rangle$ of Eq. (4). For instance, in the case where Alice decides to commit a state of amplitude α higher than the one agreed upon, the photon-number distribution obtained by Bob will have a mean that is higher than expected.

Note finally that if the vacuum mode is monitored in the unveil phase and if for this modified protocol the Gaussian cheating strategy we have examined is proven to be the optimum, then C_{max} may be further reduced by a significant factor. The maximum information gain G_{max} is also expected to be, in practice, less than the values we have calculated since Helstrom measurements for continuous variables require the use of non-Gaussian resources. Finding an operational measurement scheme realizing the POVM described in Sec. IV or finding a (more convenient) tomographic procedure for $N \gg 1$ that achieves the maximum information gain is another open question.

VI. CONCLUSIONS

We have investigated continuous-variable QBC protocols with Gaussian constraints. It had been proven in a recent work [8] that restricting both parties to Gaussian states and operations cannot lead to a secure QBC protocol. Here, we have gone one step further and have introduced a QBC protocol that is based on non-Gaussian (Schrödinger cat) states of light, thereby circumventing such a Gaussian no-go theorem, but that still imposes a Gaussian restriction on Alice's cheating operations. This continuous-variable QBC protocol is shown to be asymptotically secure in the sense that Alice's control and Bob's information gain can be both made arbitrarily small. Even though the Gaussian restriction we put on Alice is not of a fundamental nature, the non-Gaussian deterministic operations as needed by Alice in order to cheat would require high optical nonlinearities that are inaccessible today in the laboratory. In contrast, the probabilistic procedures that can effect non-Gaussian operations based on postselection, as already demonstrated in the laboratory, can be used by Alice in order to prepare the cat states that are necessary to initiate the protocol.

In conclusion, we envision that a restricted proof-of-principle demonstration of this continuous-variable QBC protocol may become realizable within the near-future state of technology given the recent experimental progress on non-Gaussian state of light generation [21–23]. An interesting extension of this work would be to devise more practical continuous-variable QBC protocols going beyond the purification protocol investigated here, but instead following the lines

of the original QBC protocol of Ref. [31] for discrete variables, for which no entanglement or quantum memory is required.

ACKNOWLEDGMENTS

[1] G. M. D'Ariano, D. Kretschmann, D. Schlingemann, and R. F. Werner, Phys. Rev. A **76**, 032328 (2007).

[2] The original proof can be found in the Appendix of G. Brassard, C. Crépeau, D. Mayers, and L. Salvail, arXiv:quant-ph/9712023.

[3] R. W. Spekkens and T. Rudolph, Phys. Rev. A **65**, 012310 (2001).

[4] H.-K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997); D. Mayers, *ibid.* **78**, 3414 (1997).

[5] D. P. DiVincenzo, J. A. Smolin, and B. M. Terhal, New J. Phys. **6**, 80 (2004).

[6] A. Kent, Phys. Rev. Lett. **83**, 1447 (1999).

[7] I. B. Damgard, S. Fehr, L. Salvail, and C. Schaffner, SIAM J. Comput. **37**, 1865 (2008).

[8] L. Magnin, F. Magniez, A. Leverrier, and N. J. Cerf, Phys. Rev. A **81**, 010302(R) (2010).

[9] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).

[10] N. J. Cerf, G. Leuchs, and E. S. Polzik (eds.), *Quantum Information with Continuous Variables of Atoms and Light* (Imperial College Press, London, 2007).

[11] J. S. Neergaard-Nielsen, B. M. Nielsen, C. Hettich, K. Molmer, and E. S. Polzik, Phys. Rev. Lett. **97**, 083604 (2006).

[12] A. Ourjoumtsev, R. Tualle-Brouri, J. Laurat, and P. Grangier, Science **312**, 83 (2006).

[13] A. Ourjoumtsev, H. Jeong, R. Tualle-Brouri, and P. Grangier, Nature (London) **448**, 784 (2007).

[14] V. Parigi, A. Zavatta, M. Kim, and M. Bellini, Science **317**, 1890 (2007).

[15] K. Wakui, H. Takahashi, A. Furusawa, and M. Sasaki, Opt. Express **15**, 3568 (2007).

[16] H. Takahashi, K. Wakui, S. Suzuki, M. Takeoka, K. Hayasaka, A. Furusawa, and M. Sasaki, Phys. Rev. Lett. **101**, 233605 (2008).

[17] J. Fiurasek, R. Garcia-Patron, and N. J. Cerf, Phys. Rev. A **72**, 033822 (2005).

[18] M. Dakna, J. Clausen, L. Knoll, and D.-G. Welsch, Phys. Rev. A **59**, 1658 (1999); **60**, 726 (1999).

[19] H. Jeong and M. S. Kim, Phys. Rev. A **65**, 042305 (2002).

[20] T. C. Ralph, A. Gilchrist, G. J. Milburn, W. J. Munro, and S. Glancy, Phys. Rev. A **68**, 042319 (2003).

[21] A. Ourjoumtsev, F. Ferreyrol, R. Tualle-Brouri, and P. Grangier, Nat. Phys. **5**, 189 (2009).

[22] T. Gerrits, S. Glancy, T. S. Clement, B. Calkins, A. E. Lita, A. J. Miller, A. L. Migdall, S. W. Nam, R. P. Mirin, and E. Knill, Phys. Rev. A **82**, 031802(R) (2010).

[23] N. Namekata, Y. Takahashi, G. Fujii, D. Fukuda, S. Kurimura, and S. Inoue, Nat. Photon. **4**, 655 (2010).

[24] J. S. Neergaard-Nielsen, M. Takeuchi, K. Wakui, H. Takahashi, K. Hayasaka, M. Takeoka, and M. Sasaki, Phys. Rev. Lett. **105**, 053602 (2010).

[25] P. Marek and J. Fiurasek, Phys. Rev. A **82**, 014304 (2010).

[26] W.-M. Zhang, D. H. Feng, and R. Gilmore, Rev. Mod. Phys. **62**, 867 (1990).

[27] W. P. Schleich, *Quantum Optics in Phase Space* (Wiley-VCH Verlag, Berlin, 2001).

[28] C. A. Fuchs and J. van de Graaf, IEEE Trans. Inf. Theory **45**, 1216 (1999).

[29] C. W. Helstrom, *Quantum Detection and Estimation Theory*, Mathematics in Science and Engineering Vol. 123 (Academic Press, New York, 1976).

[30] A. Chailloux and I. Kerenidis, in *Proceedings of 52nd IEEE Symposium on Foundations of Computer Science* (IEEE, Palm Springs, USA, 2011), pp. 354–362.

[31] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), p. 175.