
Article:
Lupo, Cosmo orcid.org/0000-0002-5227-4009, Ottaviani, Carlo orcid.org/0000-0002-0032-3999, Papanastasiou, Panagiotis et al. (1 more author) (2018) Parameter estimation with almost no public communication for continuous-variable quantum key distribution. Physical Review Letters. 220505. ISSN 1079-7114

https://doi.org/10.1103/PhysRevLett.120.220505

Parameter estimation with almost no public communication for continuous-variable quantum key distribution

Cosmo Lupo, Carlo Ottaviani, Panagiotis Papanastasiou, Stefano Pirandola
Department of Computer Science, University of York, York YO10 5GH, UK

One crucial step in any quantum key distribution (QKD) scheme is parameter estimation. In all known QKD protocols, if prior information is not available, the users have to sacrifice part of their raw data to estimate the parameters of the communication channel as, for example, the error rate. This introduces a tradeoff between the secret key rate and the accuracy or parameter estimation in the finite-size regime. Here we show that continuous-variable (CV) QKD is not subject to this constraint and the whole raw keys can be used for both parameter estimation and secret key generation, without compromising the security. First we show that this property holds for measurement-device independent (MDI) protocols, as a consequence of the fact that in an MDI protocol the correlations between Alice and Bob are post-selected by the measurement performed by an untrusted relay. This result is then extended beyond the MDI framework by exploiting the fact that MDI protocols can simulate device-dependent one-way QKD with arbitrarily high precision.

Introduction:– Quantum key distribution (QKD) exploits quantum physics to distribute secret keys between distant users that have access to an insecure quantum communication channel [1–4]. These secret keys can then be used as one-time pads to achieve information-theoretically secure communication [5]. A QKD protocol is an explicit recipe to achieve this goal and typically comprises two parts: a quantum part where quantum signals are transmitted through a quantum channel connecting two authenticated users (typically named Alice and Bob) and then measured at the output of the channel; a classical part where local classical information about the state preparation and measurement outputs are processed to extract a common, secret key.

One crucial part of classical post-processing is parameter estimation, a routine aiming at obtaining information about the quantum channel connecting Alice to Bob. The task of parameter estimation is similar to quantum channel (or state) tomography (see e.g. Ref. [6] and references therein), though in this case one is not interested in obtaining a full description of the quantum channel, but only in those features that are relevant for the security of the QKD protocol. Once the quantum channel is estimated, the principles of quantum mechanics impose an upper bound on the amount of information that has possibly leaked to a potential eavesdropper. In general, local information without classical communication is not sufficient to perform neither parameter estimation nor quantum state tomography [7–9]. For this reason, it is required that Alice and Bob exchange part of their local data in order to perform parameter estimation. Obviously, all the classical data that are communicated through an insecure channel must be considered compromised. It follows that the more data are used for parameter estimation, the lower is the final secret key rate. Viceversa, if less data are used for parameter estimation, then statistical errors will make the estimation less accurate. This tradeoff between secret key rate and parameter estimation accuracy is a common feature of all QKD protocols. The only exception known up to now was when Alice and Bob have prior information about the communication channel [10, 11].

In this Letter we show that for one-way continuous-variable (CV) QKD protocols (as for example those in Refs. [11–21]) one can use, without loss of security, the whole local data for both parameter estimation and secret key extraction, even if no prior information is available. This result is a consequence of two characteristic features of CV QKD: the first is the optimality of Gaussian attacks [13, 20, 22]; the second is that the knowledge of the covariance matrix (CM) is sufficient to fully characterize a quantum Gaussian state [23]. To prove this result we consider the framework of measurement-device independent (MDI) QKD, first introduced to achieve security against side-channel attacks on the measurement devices [24, 25]. Then, the result is extended to one-way CV QKD protocols by exploiting the fact that the latter can be simulated by an MDI protocol up to an arbitrarily small error [26].

The structure of a QKD protocol:– Up to a few conceptually significant advancements, the structure of QKD protocols has remained mostly constant since the first QKD protocol was proposed by Bennett and Brassard in 1984 (BB84) [27]. A typical QKD protocol consists of seven basic operations: (1) State preparation: Alice generates a sequence of n symbols, for each symbol she prepares a suitable quantum codeword. For example, in the original BB84 protocol Alice encodes a bit value $X \in \{0, 1\}$ in one qubit either using the computational basis $\{|0\rangle, |1\rangle\}$ or the diagonal basis $\{|+\rangle, |-\rangle\}$. (2) Communication: The quantum states are transmitted through an insecure quantum communication channel. (3) Measurement: Bob measures the quantum states coming out of the communication channel. For example, in the BB84 protocol Bob obtains a bit value $Y \in \{0, 1\}$ by either measuring in the computational or diagonal basis. (4) Sifting: For each signal transmitted, Alice and Bob publicly announce whether they have employed the computational or diagonal basis. Then they only retain the data corresponding to matching choices for preparation and measurement. The sifted data represent the local raw keys of Alice and Bob. (5) Parameter estimation: Alice and Bob publicly agree on a subset of their local data to estimate the parameters of the channel. For example, Bob sends to Alice a fraction f of his data, so that she can estimate the probability of error. Obviously, all the data sent through the public channel for parameter estimation are compromised and cannot be used for secret key extraction: the final rate will thus be reduced by a factor $1 - f$. (6) Error

correction: Alice sends to Bob error-correcting information. Bob can combine this information with his local data to reconstruct Alice's raw keys up to a small error (direct reconciliation). (7) Privacy amplification: Alice and Bob apply a random universal hash function to obtain a shorter key which a potential eavesdropper has virtually zero information about.

During the three decades that separate us from BB84, several main conceptual development of QKD has been introduced. One of the main advancements in QKD has been the introduction of CV protocols [28, 29], in which information is encoded in continuous degrees of freedom of the electromagnetic field, e.g., quadrature and phase [3, 23]. In Ref. [30] it was shown that even semi-classical states as coherent states can be employed for QKD. Up to 2002, it was believed that QKD could not possibly work for channel loss above 3 dB. This beliefs was proven wrong in Ref. [31]. Indeed, if it is Bob to send error correcting information to Alice (reverse reconciliation [32]) then one can in principle obtain secrecy in the presence of arbitrary high loss [14, 33–35]. In 2006 it was shown that switching between two different bases for state preparation and measurement is not necessary for CV QKD protocols based on coherent state preparation and heterodyne detection [12]. Thus with no-switching protocols one can avoid to sacrifice part of the data (roughly 50%) during the sifting phase.

Only very recently, MDI QKD has been introduced as a framework to prevent side-channel attacks on the measurement devices [36, 37]. In fact, in MDI QKD the honest users are only required to prepare quantum states, but not to measure them, as the measurement is delegated to an untrusted relay [24, 25]. In this way one does not need to make any assumption on the measurement device: a way to guarantee security against side-channel attacks.

Description of the CV MDI QKD protocol:– CV MDI QKD plays a central role to show that in CV QKD all the raw data can be used for both parameter estimation and secret key generation. Therefore, before proceedings, we need to recall the details of the CV MDI QKD protocol put forward in Ref. [26]. The security of this protocol was proven in Ref. [26] in the asymptotic limit, and in Ref. [38] in a finite-size, composable setting. The protocol, schematically summarized in Fig. 1, develops in five steps:

1. *Coherent states preparation.* Alice and Bob locally prepare $2n$ coherent states, with complex amplitudes denoted as $\alpha' = (q'_A + ip'_A)/2$ and $\beta' = (q'_B + ip'_B)/2$ [39]. The local variables $X' \equiv (q'_A, p'_A)$ and $Y' \equiv (q'_B, p'_B)$ are drawn i.i.d. from zero-mean, circular symmetric, Gaussian distributions with variances V_A and V_B, respectively.

2. *Operations of the relay.* The $2n$ coherent states are sent to a central relay. For each pair of coherent states received the relay operates a (lossy and noisy) CV Bell detection [40–42] and publicly announces a variable Z with complex value $\gamma = (q_Z + ip_Z)/2$.

3. *Parameter estimation.* Alice and Bob estimate the covariance matrix (CM) of the variables $(q'_A, p'_A, q'_B, p'_B, q_Z, p_Z)$. We remark that the property of extremality of Gaussian states implies that the knowledge of the CM is sufficient to assess the security of the protocol [13, 22].

4. *Conditional displacements.* Alice and Bob define the displaced variables $X = (q_A, p_A)$ and $Y = (q_B, p_B)$ as follows:

$$q_A = q'_A - g_{q'_A}(\gamma)\,,\ p_A = p'_A - g_{p'_A}(\gamma)\,, \tag{1}$$
$$q_B = q'_B - g_{q'_B}(\gamma)\,,\ p_B = p'_B - g_{p'_B}(\gamma)\,, \tag{2}$$

   where $g_\star$, for $\star = q'_A, p'_A, q'_B, p'_B$, is an affine function of γ. The variables X, Y represent the local raw keys of Alice and Bob, respectively.

5. *Classical post-processing.* To conclude the protocol, the raw keys are post-processed for error correction and privacy amplification.

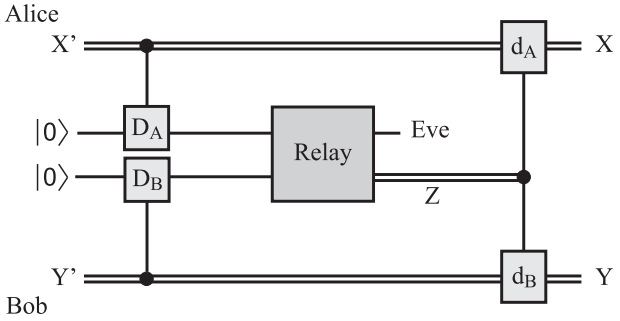

FIG. 1: The figure shows the scheme of the CV MDI QKD protocol of Ref. [26]. Single lines represent bosonic modes, double lines classical variables. Time flows from left to right. Alice and Bob initially prepare coherent states by applying displacement operators D_A, D_B to the vacuum state $|0\rangle$, according to the value of their local classical variables. The coherent states are collected by the relay that, through some (in principle unknown) physical transformation, outputs a classical variable Z and gives to Eve quantum side information. Finally, Alice and Bob apply *classical* displacement d_A, d_B, conditioned on the value of Z, to their local classical variables.

As a matter of fact, we have defined not just one protocol, but a whole family of CV MDI QKD protocol: one for each choice of the affine functions $g_\star$'s. In particular, the CV MDI protocol of Ref. [26] is defined for an optimal choice of the functions $g_\star$ (which is derived below).

Parameter estimation with almost no public communication:– The CV MDI QKD protocol described above has two main characteristic features. The first is that Alice and Bob do not apply any measurement: the only measurement is performed by the relay, which is assumed to be untrusted. This property defines the protocol as MDI, as we are not making any assumption on the measurement actually performed by the relay. The second feature represents the main contribution of this Letter: the estimation of the CM of $(q'_A, p'_A, q'_B, p'_B, q_Z, p_Z)$ can be done locally by either Alice and Bob. Obviously, Alice and Bob know, by definition of the protocol, the variances of q'_A, p'_A, q'_B, p'_B. Also, Alice can

locally compute the empirical correlations $\langle q'_A q_Z\rangle$, $\langle q'_A p_Z\rangle$, $\langle p'_A q_Z\rangle$, $\langle p'_A p_Z\rangle$, from her local data and from the amplitude $\gamma = (q_Z + ip_Z)/2$ that have been publicly announced by the relay. Similarly, Bob can locally compute the empirical correlations $\langle q'_B q_Z\rangle$, $\langle q'_B p_Z\rangle$, $\langle p'_B q_Z\rangle$, $\langle p'_B p_Z\rangle$. This implies that all the entries of the CM of $(q'_A, p'_A, q'_B, p'_B, q_Z, p_Z)$ can be locally computed by either Alice and Bob, without the need of public communication. Finally, the CM of (q_A, p_A, q_B, p_B) can be computed directly from the CM of $(q'_A, p'_A, q'_B, p'_B, q_Z, p_Z)$ by exploiting the relations (1)-(2). In conclusion, the CM of (q_A, p_A, q_B, p_B) can be determined only exploiting locally available information since, as we show in the following section, the functions $g_\star$ can be also computed from local data only.

In summary, Alice and Bob can locally estimate all the entries of the CM without having to communicate part of their local raw keys through a public channel. (They only need to share the entries of the estimated CM, which contain a negligible amount of information about the key). This is possible because in an MDI QKD the correlations between Alice's and Bob's raw keys are post-selected by the relay. Therefore, the public variable Z contains all the information about the correlations between Alice and Bob and is thus sufficient, together with the local data, to estimate the CM.

Having established that locally available information are sufficient to estimate the CM, then the calculation of the corresponding confidence intervals (error bars) can be performed in many different ways, for example as described in Refs. [38, 43, 44] under the assumption of Gaussian attacks, or along the lines of Ref. [11] for the case of general collective attacks. Notice that considering Gaussian attacks represents no loss of generality as recently proven in Ref. [20].

Optimal conditional displacements:– For completeness we now derive the optimal choice for the displacement functions $g_\star$ [45]. At the parameter estimation stage, Alice and Bob locally estimate the CM of $(q'_A, p'_A, q'_B, p'_B, q_Z, p_Z)$:

$$V_{A'B'Z} = \begin{pmatrix} V_A\mathbf{I} & 0 & \mathbf{c}_{AZ} \\ 0 & V_B\mathbf{I} & \mathbf{c}_{BZ} \\ \mathbf{c}_{AZ}^{\mathsf{T}} & \mathbf{c}_{BZ}^{\mathsf{T}} & \boldsymbol{v}_Z \end{pmatrix}, \tag{3}$$

where $\mathbf{I}$ denotes the two-dimensional identity matrix,

$$\boldsymbol{v}_Z = \begin{pmatrix} \langle q_Z^2\rangle & \langle q_Z p_Z\rangle \\ \langle q_Z p_Z\rangle & \langle p_Z^2\rangle \end{pmatrix} \tag{4}$$

is the empirical CM of (q_Z, p_Z), and

$$\mathbf{c}_{AZ} = \begin{pmatrix} \langle q'_A q_Z\rangle & \langle q'_A p_Z\rangle \\ \langle p'_A q_Z\rangle & \langle p'_A p_Z\rangle \end{pmatrix}, \mathbf{c}_{BZ} = \begin{pmatrix} \langle q'_B q_Z\rangle & \langle q'_B p_Z\rangle \\ \langle p'_B q_Z\rangle & \langle p'_B p_Z\rangle \end{pmatrix} \tag{5}$$

are the correlation terms.

We remark that the variables (q'_A, p'_A, q'_B, p'_B) are uncorrelated with known variances V_A, V_B by definition of the protocol, while all the entries involving the publicly known variables (q_Z, p_Z) must be estimated from the data.

The optimal choice for the displacements in Eqs. (1)-(2) is the one that minimizes the correlations between Alice's and Bob's variables and $\gamma = (q_Z + ip_Z)/2$. Therefore we put, for $\star = q'_A, p'_A, q'_B, p'_B$,

$$g_\star(\gamma) = u_\star\, q_Z + v_\star\, p_Z\,, \tag{6}$$

and require that $u_\star$ and $v_\star$ are chosen in such a way that

$$\langle q_Z q_A\rangle = \langle p_Z q_A\rangle = \langle q_Z p_A\rangle = \langle p_Z p_A\rangle = 0\,, \tag{7}$$
$$\langle q_Z q_B\rangle = \langle p_Z q_B\rangle = \langle q_Z p_B\rangle = \langle p_Z p_B\rangle = 0\,, \tag{8}$$

which implies

$$\langle \star\, q_Z\rangle = u_\star\,\langle q_Z^2\rangle + v_\star\langle q_Z p_Z\rangle\,, \tag{9}$$
$$\langle \star\, p_Z\rangle = u_\star\,\langle q_Z p_Z\rangle + v_\star\langle p_Z^2\rangle\,. \tag{10}$$

Solving for $u_\star$ and $v_\star$ we obtain

$$u_\star = \frac{\langle \star\, q_Z\rangle\langle p_Z^2\rangle - \langle \star\, p_Z\rangle\langle q_Z p_Z\rangle}{\langle p_Z^2\rangle\langle q_Z^2\rangle - \langle q_Z p_Z\rangle^2}\,, \tag{11}$$
$$v_\star = \frac{\langle \star\, p_Z\rangle\langle q_Z^2\rangle - \langle \star\, q_Z\rangle\langle q_Z p_Z\rangle}{\langle q_Z^2\rangle\langle p_Z^2\rangle - \langle q_Z p_Z\rangle^2}\,. \tag{12}$$

With this choice of the parameters $u_\star$, $v_\star$ the displaced variables (q_A, p_A, q_B, p_B) are independent of (q_Z, p_Z). We remark that in this way the CM V_{AB} of (q_A, p_A, q_B, p_B) equals the conditional CM of (q'_A, p'_A, q'_B, p'_B) conditioned on (q_Z, p_Z) (see Ref. [26]).

We remark that the parameters $u_\star$ and $v_\star$ can be computed locally by Alice and Bob exploiting the fact that the variable (q_Z, p_Z) is public. The communication through a public channel of the values of $u_\star$ and $v_\star$ implies no loss of security since they only contains a negligible amount of information about the raw keys.

As an example, put $V_A = V_B = 2N$ and suppose that the relay applies a Gaussian transformation that consists of (see Ref. [26]): first attenuating the signals from Alice and Bob by an attenuation factor η; and then perform an ideal, noiseless, CV Bell detection. In this case one obtains:

$$-u_{q'_A} = v_{p'_A} = u_{q'_B} = v_{p'_B} = \frac{N}{\eta N + 1/2}\sqrt{\frac{\eta}{2}}\,. \tag{13}$$

Other numerical examples are discussed in Ref. [38].

From MDI to general no-switching CV QKD:– In the MDI framework, Alice and Bob send quantum states to a central relay, which is untrusted and possibly operated by an eavesdropper. On the other hand, in a one-way DI QKD protocol, Alice sends a quantum state ρ to the receiver Bob, who measures it, typically by homodyne or heterodyne detection, as shown in Fig. 2(1).

First of all, an MDI protocol can simulate with arbitrary high precision any one-way protocol. In fact, if the relay is given to Bob, he can use it to teleport the signals from Alice into his lab, as shown in Fig. 2(2). Clearly, ideal CV teleportation requires Bob to employ as teleportation resource a two-mode squeezed vacuum (TMSV) state $\psi_{\rm TMSV}$ with infinite squeezing [40–42] . Otherwise, for any finitely squeezed TMSV state, the scheme in Fig. 2(2) simulates that in Fig. 2(1) with up to additive Gaussian noise [46–49]. Since the

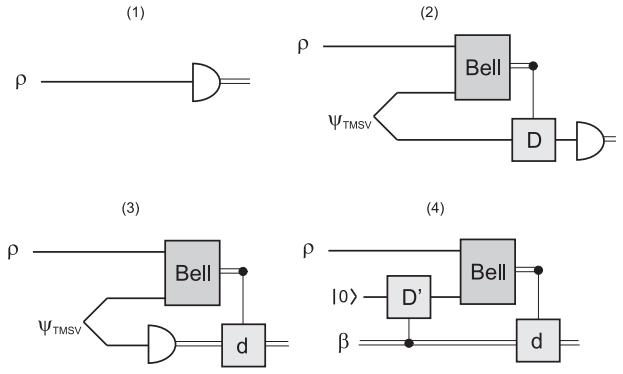

FIG. 2: The figures show: (1) direct heterodyne detection; and (4) MDI-inspired detection, obtained when the relay is given to the receiver Bob. Single lines indicate bosonic modes, double line classical variables. (2) and (3) show intermediate configurations that we exploit to prove the equivalence, up to an arbitrarily small error, between (1) and (4). Notice that in (4) we have described the preparation of a coherent state $|\beta\rangle$ of amplitude β as the application of a displacement D' on the vacuum, where the amplitude of the displacement is determined by a classical variable β.

displacement operation commutes with heterodyne detection, to apply a displacement D and then measure by heterodyne detection [as in Fig. 2(2)] is equivalent to first measure and then displace the (classical) outcome of the measurement [as in Fig. 2(3)]. Finally, it is well known that measuring by heterodyne detection one mode of an entangled pair in a TMSV state, conditionally prepares the other mode in a coherent state [35], this implies the equivalence between the schemes in Fig. 2(3) and Fig. 2(4). In conclusion, the MDI protocol in Fig. 2(4) can simulate the one-way CV QKD. If the complex amplitude β is sampled from a Gaussian distribution with finite variance V_B, then one simulates a noisy version of the QKD protocol, whereas the noiseless case is obtained in the limit that $V_B \to \infty$.

Discussion:– As discussed above, parameter estimation in CV MDI QKD can be performed with almost no public communication because correlations are post-selected by the central relay. This condition is necessary but would not be sufficient without the additional property that X, Y, Z are Gaussian variables. This implies that all their statistical features are determined by their first moments and CM. In particular, the conditional probability distribution $P(XY|Z)$, which is the relevant quantity for assessing the security of the protocol [24], can be estimated from the elements of the CM alone. In other words, the knowledge of the marginal probability distributions $P(XZ), P(YZ)$ is sufficient to know $P(XYZ)$. This is the property that we have exploited above.

It is meaningful to ask whether one can perform parameter estimation without public communication also in the case of discrete variable MDI QKD. The answer to this question is negative because, although correlations are still post-processed by the relay, the relevant random variables are no more Gaussian, and therefore they are not uniquely characterized by their second moments. Consider for example the qubit MDI protocol of Ref. [25], which can be viewed as an MDI version of BB84, where the variables X and Y assume values in $\{0, 1\}$, and $Z \in \{0, 1, 2, 3\}$ is the output of qubit Bell detection. One can easily check that in this setting the marginal probability distributions $P(XZ), P(YZ)$ do not uniquely determine $P(XYZ)$.

Conclusions:– The list of conceptual breakthroughs in the history of QKD includes the discoveries that reverse reconciliation allowed to beat the 3dB barrier, that coherent states were suitable for QKD despite being semiclassical, and that CV QKD did not require switching between different bases for encoding and measurement, thus allowing us to skip the sifting phase.

This Letter presents one new conceptual development of CV QKD, namely that the whole raw keys can be used for both parameter estimation and secret key extraction. This finding removes the tradeoff between secret key rate and accuracy of the parameter estimation in the finite-size regime of QKD. Unlike other works [10, 11], here it is not required to have prior knowledge on the communication channel.

Such a property is first obtained for CV MDI QKD protocols as a consequence of the fact that correlations between Alice and Bob are encoded in the variable that is publicly announced by the relay — even though such a variable does not contain information about the secret key. Since CV MDI QKD can simulate one-way CV DI QKD protocols with arbitrary precision, it then follows that the whole raw key can be used for both parameter estimation and secret key generation for this class of CV protocols as well.

Acknowledgments

This work was supported by the Innovation Fund Denmark (Qubiz project) and the UK Quantum Communications hub (EP/M013472/1). C.L. acknowledges the scientific support received from the Quantum Physics and Information Technology Group (QPIT).

[1] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[3] C. Weedbrook, S.Pirandola, R. García-Patrón, N. J. Cerf, T.C. Ralph, J. H. Shapiro, S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
[4] E. Diamanti, A. Leverrier, Entropy **17**, 6072 (2015).
[5] C. E. Shannon, Bell System Technical Journal **28**, 656 (1949).
[6] A. Bisio, G. Chiribella, G. M. D'Ariano, S. Facchini, P. Perinotti, IEEE Journal of Selected Topics in Quantum Electronics **15**, 1646 (2009).
[7] T. Xin, D. Lu, J. Klassen, N. Yu, Z. Ji, J. Chen, X. Ma, G. Long, B. Zeng, R. Laflamme, Phys. Rev. Lett. **118**, 020401 (2017).
[8] J. Chen, H. Dawkins, Z. Ji, N. Johnston, D. Kribs, F. Shultz, B.

Zeng, Phys. Rev. A **88**, 012109 (2013).
[9] N. Linden, S. Popescu, W. K. Wootters, Phys. Rev. Lett. **89**, 207901 (2002).
[10] N. Walenta, A. Burg, D. Caselunghe, J. Constantin, N. Gisin, O. Guinnard, R. Houlmann, P. Junod, B. Korzh, N. Kulesza, New J. Phys. **16**, 013047 (2014).
[11] A. Leverrier, Phys. Rev. Lett. **114**, 070501 (2015).
[12] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam. Phys. Rev. Lett. **93**, 170504 (2004).
[13] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).
[14] S. Pirandola, R. García-Patrón, S. L. Braunstein, S. Lloyd, Phys. Rev. Lett. **102**, 050503 (2009).
[15] C. Weedbrook, S. Pirandola, T. C. Ralph, Phys. Rev. A **86**, 022318 (2012).
[16] J. Fiurasek, N. J. Cerf, Phys. Rev. A **86**, 060302(R) (2012).
[17] A. Leverrier, Phys. Rev. A **85**, 022339 (2012).
[18] A. Leverrier, R. García-Patrón, R. Renner, N. J. Cerf, Phys. Rev. Lett. **110**, 030502 (2013).
[19] F. Furrer, Phys. Rev. A **90**, 042325 (2014).
[20] A. Leverrier, Phys. Rev. Lett. **118**, 200501 (2017).
[21] C. Ottaviani, S. Mancini, S. Pirandola, Phys. Rev. A **95**, 052310 (2017).
[22] M. M. Wolf, G. Giedke, and J. I. Cirac, Phys. Rev. Lett. **96**, 080502 (2006).
[23] A. Ferraro, S. Olivares, and M. G. A. Paris, *Gaussian States in Quantum Information* (Bibliopolis, Napoli, 2005).
[24] S. L. Braunstein, S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).
[25] H.-K. Lo, M. Curty, B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[26] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, U. L. Andersen, Nature Photon. **9**, 397 (2015).
[27] C. H. Bennett, G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1012 December 1984; Volume 175, p. 8.
[28] M. Hillery, Phys. Rev. A **61**, 022309 (2000)
[29] N. J. Cerf, M. Lévy, and G. Van Assche, Phys. Rev. A **63**, 052311 (2001)
[30] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[31] Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).
[32] U. Maurer, IEEE Trans. Inf. Theory **39**, 733 (1993).
[33] F. Grosshans and P. Grangier, Proceedings of the 6th International Conference on Quantum Communication, Measurement, and Computing; arXiv: 0204127 (2002).
[34] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, P. Grangier, Nature **421**, 238 (2003).
[35] F. Grosshans, N. J. Cerf, J. Wenger, R. Taulle-Brouri, P. Grangier, Quantum Inf. Comput. **3**, 535 (2003).
[36] V. Scarani, C. Kurtsiefer, Theoretical Computer Science **550**, 27 (2014); arXiv: 0906.4547 (2009).
[37] L. Lydersen, C, Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nature Photonics **4**, 686 (2010).
[38] C. Lupo, C. Ottaviani, P. Papanastasiou, S. Pirandola, arXiv: 1704.07924 (2017).
[39] We put $\hbar = 1$ and assume the commutation relations of the form $[q, p] = 2i$ [23]. In this way the output of homodyne detection over the vacuum state is a Gaussian variable with variance 1.
[40] L. Vaidman, Phys. Rev. A **49**, 1473 (1994).
[41] S. L. Braunstein, H. J. Kimble, Phys. Rev. Lett. **80**, 869 (1998).
[42] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, S. L. Braunstein, Nat. Photon. **9**, 641 (2015).
[43] P. Papanastasiou, C. Ottaviani, S. Pirandola, Phys. Rev. A **96**, 042332 (2017).
[44] L. Ruppert, V. C. Usenko, R. Filip, Phys. Rev. A **90**, 062310 (2014).
[45] To simplify the notation, we assume that $\langle q_Z \rangle = \langle p_Z \rangle = 0$ (one can always redefine the variables q_Z, p_Z to ensure this property is verified).
[46] M. Ban, M. Sasaki, M. Takeoka, J. Phys. A **35**, L401 (2002).
[47] A. Christ, C. Lupo, C. Silberhorn, New J. Phys. **14**, 083007 (2012).
[48] P. Liuzzo-Scorpo, A. Mari, V. Giovannetti, G. Adesso, Phys. Rev. Lett. **119**, 120503 (2017).
[49] R. Laurenza, S. L. Braunstein, S. Pirandola, arXiv:1706.06065 (2017).