nature photonics

Article

https://doi.org/10.1038/s41566-023-01190-4

Exact solution for the quantum and private capacities of bosonic dephasing channels

Received: 31 May 2022

Accepted: 1 March 2023

Published online: 6 April 2023

Check for updates

Ludovico Lami [1,2,3,4] & Mark M. Wilde [5,6]

The capacities of noisy quantum channels capture the ultimate rates of information transmission across quantum communication lines, and the quantum capacity plays a key role in determining the overhead of fault-tolerant quantum computation platforms. Closed formulae for these capacities in bosonic systems were lacking for a key class of non-Gaussian channels, bosonic dephasing channels, which are used to model noise affecting superconducting circuits and fibre-optic communication channels. Here we provide an exact calculation of the quantum, private, two-way assisted quantum and secret-key-agreement capacities of all bosonic dephasing channels. We prove that they are equal to the relative entropy of the distribution underlying the channel with respect to the uniform distribution, solving a problem that was originally posed over a decade ago.

One of the great promises of quantum information science is that remarkable tasks can be achieved by encoding information into quantum systems[1]. In principle, algorithms executed on quantum computers can factor large integers[2], simulate complex physical dynamics[3], solve unstructured search problems with proven speedups[4] and perform linear-algebraic manipulations on large matrices encoded into quantum systems[5,6]. In addition, ordinary ('classical') information can be transmitted securely over quantum channels via quantum key distribution[7].

However, all of these possibilities are hindered in practice because all quantum systems are subject to decoherence[8]. A very simple decoherence process takes a density operator $\rho = \sum_{n,m} \rho_{nm} |n\rangle\langle m|$ to $\rho' = \sum_{n,m} \rho_{nm} \mathrm{e}^{-\frac{\gamma}{2}(n-m)^2} |n\rangle\langle m|$, where $\gamma \geq 0$ measures the extent to which the off-diagonal elements are reduced in magnitude. This process is also called dephasing, because it reduces or eliminates relative phases. Decoherence is a ubiquitous phenomenon that affects all quantum physical systems. In fact, in various platforms for quantum computation, experimentalists employ the T2 time as a phenomenological quantity that roughly measures the time that it takes for a coherent superposition to decohere to a probabilistic mixture. Dephasing noise in some cases is considered to be the dominant source of errors affecting quantum information encoded into superconducting systems[9], as well as other platforms[10,11]. If those systems are employed to carry out quantum computation, then the errors must be amended using error-correcting codes, which typically cause expensive overheads in the amount of physical qubits needed. Not only does dephasing affect quantum computers but it also affects quantum communication systems. Indeed, temperature fluctuations[12] or Kerr nonlinearities[13] in a fibre, imprecision in the path length of a fibre[14] or the lack of a common phase reference between the sender and receiver[15] lead to decoherence as well, and this can affect quantum communication and key distribution schemes adversely.

Many of the aforementioned forms of decoherence can be unified under a single model, known as the bosonic dephasing channel (BDC)[16,17]. The action of such a channel on the density operator ρ of a single-mode bosonic system is given by

$$\mathcal{N}_p(\rho) := \int_{-\pi}^{\pi} \mathrm{d}\phi\, p(\phi)\, \mathrm{e}^{-ia^\dagger a\phi} \rho\, \mathrm{e}^{ia^\dagger a\phi}, \tag{1}$$

where p is a probability density function on the interval $[-\pi,\pi]$ and $a^\dagger a$ is the photon number operator. Since each unitary operator $\mathrm{e}^{-ia^\dagger a\phi}$ realizes a phase shift of the state ρ, the action of the channel $\mathcal{N}_p$ is to

[1]Institut für Theoretische Physik und IQST, Universität Ulm, Ulm, Germany. [2]QuSoft, Amsterdam, The Netherlands. [3]Korteweg–de Vries Institute for Mathematics, University of Amsterdam, Amsterdam, The Netherlands. [4]Institute for Theoretical Physics, University of Amsterdam, Amsterdam, The Netherlands. [5]Hearne Institute for Theoretical Physics, Department of Physics and Astronomy, and Center for Computation and Technology, Louisiana State University, Baton Rouge, LA, USA. [6]School of Electrical and Computer Engineering, Cornell University, Ithaca, NY, USA.
e-mail: ludovico.lami@gmail.com; wilde@cornell.edu

randomize the phase of this state according to the probability density p. Representing $\rho = \sum_{n,m} \rho_{nm} |n\rangle\langle m|$ in the photon number basis, it is a straightforward calculation to show that

$$\mathcal{N}_p(\rho) = \sum_{n,m} \rho_{nm} (T_p)_{nm} |n\rangle\langle m|, \tag{2}$$

where T_p is the infinite matrix with entries

$$(T_p)_{nm} := \int_{-\pi}^{\pi} \mathrm{d}\phi\, p(\phi)\, \mathrm{e}^{-i\phi(n-m)}. \tag{3}$$

This channel thus generalizes the simple dephasing channel considered above. Its action preserves diagonal elements of ρ but reduces the magnitude of the off-diagonal elements, a key signature of decoherence. As the name suggests, the BDC can be seen as a generalization to bosonic systems of the qudit dephasing channel[18].

Of primary interest is understanding the information-processing capabilities of the BDC in equation (1). We can do so using the formalism of quantum Shannon theory[19,20], in which we assume that the channel acts many times to affect multiple quantum systems. Not only does this formalism model the dephasing that acts on quantum information encoded in a memory, as in superconducting systems, but also the dephasing that affects communication systems. Here, a key quantity of interest is the quantum capacity $Q(\mathcal{N}_p)$ of the BDC $\mathcal{N}_p$, which is equal to the largest rate at which quantum information can be faithfully sustained in the presence of dephasing[20]. The quantum capacity has been traditionally studied with applications to quantum communication in mind; however, recent evidence[21] indicates that it is also relevant for understanding the overhead of fault-tolerant quantum computation, that is, the fundamental ratio of physical to logical qubits to perform quantum computation indefinitely with little chance of error. The private capacity $P(\mathcal{N}_p)$ is another operational quantity of interest[20], being defined as the largest rate at which private classical information can be faithfully transmitted over many independent uses of the channel $\mathcal{N}_p$ (Fig. 1). One can also consider both of these capacities in the scenario in which classical processing or classical communication is allowed for free between every channel use[22,23], and here we denote the respective quantities by $Q_{\leftrightarrow}(\mathcal{N}_p)$ and $P_{\leftrightarrow}(\mathcal{N}_p)$ (Fig. 2). The secret-key-agreement capacity $P_{\leftrightarrow}(\mathcal{N}_p)$ is directly related to the rate at which quantum key distribution is possible over the channel[23], and as such it is a fundamental limit of experimental interest. One can also study strong converse capacities (see, for example, Equation (9.122) in ref. 19, Definition 9.15 in ref. 24 and ref. 25), which sharpen the above operational interpretations by considering decoding error probabilities between zero and one. If the usual capacity is equal to the strong converse capacity, then we say that the strong converse property holds for the channel under consideration, and the implication is that the capacity demarcates a very sharp dividing line between achievable and unachievable rates for communication. We let $Q^{\dagger}(\mathcal{N}_p)$, $P^{\dagger}(\mathcal{N}_p)$, $Q^{\dagger}_{\leftrightarrow}(\mathcal{N}_p)$ and $P^{\dagger}_{\leftrightarrow}(\mathcal{N}_p)$ denote the various strong converse capacities for the communication scenarios mentioned above. Understanding all of the aforementioned capacities is essential for the forthcoming quantum internet[26], which will consist of various nodes in a network exchanging quantum and private information using the principles of quantum information science.

We note here that, although the quantum capacity[16,17] and the assisted quantum capacity[27] of the BDC $\mathcal{N}_p$ in equation (1) have been investigated, neither of them has been calculated so far. The determination of the quantum capacity of this channel in particular has been an open problem since the publication of ref. 16 in 2010. The main difficulty is that $\mathcal{N}_p$ is in general a non-Gaussian channel, which makes the techniques in refs. 28,29 inapplicable.

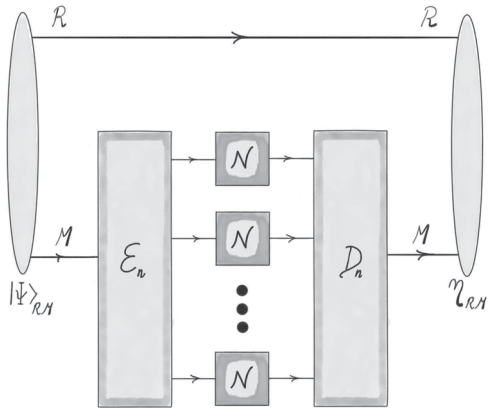

Fig. 1 | A depiction of a quantum communication protocol that uses the channel $\mathcal{N}$ a total of n times to send a quantum system M reliably. The initial state of the protocol is Ψ_{RM} and the final state is $\eta_{RM} := \left(\mathrm{id}_R \otimes \left(\mathcal{D}_n \circ \mathcal{N}^{\otimes n} \circ \mathcal{E}_n\right)_M\right)(\Psi_{RM})$, where id_R denotes the identity channel acting on R. The encoding and decoding channels $\mathcal{E}_n$ and $\mathcal{D}_n$ are operated by the sender Alice and the receiver Bob, respectively. The system M, initially entangled with a reference system R, is encoded via a suitable encoding map $\mathcal{E}_n$, transmitted via n parallel uses of the channel $\mathcal{N}$, and decoded at the receiving end by a decoding map $\mathcal{D}_n$. The error associated with the transmission is $\varepsilon := \sup_{|\psi\rangle}(1 - \langle\Psi_{RM}|\eta_{RM}|\Psi_{RM}\rangle)$ and the number of transmitted qubits is $\log_2|M|$, where $|M|$ is the dimension of M. Thus, the rate of transmitted qubits with n uses of $\mathcal{N}$ and error ε is given by $\sup_{\mathcal{E}_n,\mathcal{D}_n}(\log_2|M|)/n =: \frac{1}{n}Q_\varepsilon(\mathcal{N}^{\otimes n})$, with the maximization being over all encoding and decoding operations achieving error at most ε. The quantum capacity is then obtained by taking the limit $n \to \infty$ and requiring that ε vanishes in this limit, that is, $Q(\mathcal{N}) := \inf_{\varepsilon\in(0,1)} \liminf_n \frac{1}{n}Q_\varepsilon(\mathcal{N}^{\otimes n})$. The strong converse quantum capacity, instead, is constructed by allowing a non-zero error ε also asymptotically, with the only requirement that it stays bounded away from its maximum value of 1: in formula the $Q^{\dagger}(\mathcal{N}) := \sup_{\varepsilon\in(0,1)} \limsup_n \frac{1}{n}Q_\varepsilon(\mathcal{N}^{\otimes n})$. The private capacity $P(\mathcal{N})$ and the associated strong converse capacity $P^{\dagger}(\mathcal{N})$ are defined analogously, with the main differences being that (1) the transmitted message M is classical, (2) an eavesdropper Eve is granted access to all environment systems interacting with the input signals of $\mathcal{N}$ and (3) the main goal of the protocol is to transmit the message reliably in such a way that Eve does not learn about it. See ref. 24 for further expositions.

Results

In this paper, we completely solve all of the aforementioned eight capacities of the BDCs, finding that they all coincide and are given by the following simple expression:

$$\begin{aligned} \mathcal{C}(\mathcal{N}_p) &:= \log_2(2\pi) - h(p) \\ &= Q(\mathcal{N}_p) = P(\mathcal{N}_p) = Q_{\leftrightarrow}(\mathcal{N}_p) = P_{\leftrightarrow}(\mathcal{N}_p) \\ &= Q^{\dagger}(\mathcal{N}_p) = P^{\dagger}(\mathcal{N}_p) = Q^{\dagger}_{\leftrightarrow}(\mathcal{N}_p) = P^{\dagger}_{\leftrightarrow}(\mathcal{N}_p), \end{aligned} \tag{4}$$

where

$$h(p) := -\int \mathrm{d}\phi\, p(\phi) \log_2(p(\phi)) \tag{5}$$

is the differential entropy of the probability density p. Supplementary Section 3B contains a detailed derivation of the above result. We note here that the first expression in equation (4) can be written in terms of the relative entropy as

$$\log_2(2\pi) - h(p) = D(p\|u), \tag{6}$$

where u is the uniform probability density on the interval $[-\pi,\pi]$, and the relative entropy is defined as

$$D(r\|s) := \int \mathrm{d}\phi\, r(\phi) \log_2\left(\frac{r(\phi)}{s(\phi)}\right) \tag{7}$$

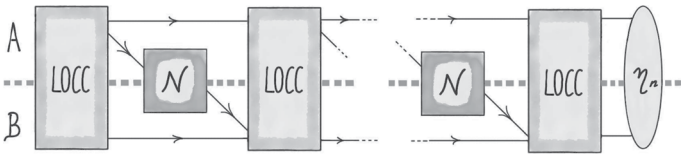

Fig. 2 | An LOCC-assisted protocol that involves n uses of the quantum channel $\mathcal{N}$, assumed to connect two spatially separated laboratories belonging to Alice and Bob. The upper arrows correspond to quantum registers of Alice and the lower arrows to quantum registers of Bob. Between each channel use and the next, Alice and Bob can implement an arbitrary protocol composed of local operations assisted by classical communication (LOCC). The final output of the protocol is a state η_n that should resemble a maximally entangled state Φ_K of local dimension K. The associated error is $\varepsilon := 1 - \langle \Phi_K | \eta_n | \Phi_K \rangle$ and the rate of entanglement generation with n uses is given by $\sup(\log_2 K)/n =: Q_{\leftrightarrow,n,\varepsilon}(\mathcal{N})$, with the maximization being over all sequences of LOCC protocols. The assisted quantum capacity of $\mathcal{N}$ is then defined by taking the limit $n \to \infty$ as $Q_{\leftrightarrow}(\mathcal{N}) := \inf_{\varepsilon\in(0,1)} \liminf_n Q_{\leftrightarrow,n,\varepsilon}(\mathcal{N})$, with the associated strong converse capacity being $Q^{\dagger}_{\leftrightarrow}(\mathcal{N}) := \sup_{\varepsilon\in(0,1)} \limsup_n Q_{\leftrightarrow,n,\varepsilon}(\mathcal{N})$. The assisted private capacity $P_{\leftrightarrow}(\mathcal{N})$ and its strong converse capacity $P^{\dagger}_{\leftrightarrow}(\mathcal{N})$ are constructed similarly, with the difference that the target state is a private state instead of a maximally entangled state.

for general probability densities r and s. By invoking basic properties of the relative entropy[30], this rewriting indicates that all of the capacities are strictly positive unless the density p is uniform, which represents a complete dephasing of the channel input state.

As indicated in equation (4), there is a remarkable simplification of the capacities for BDCs. The ultimate rate of private communication over these channels is no larger than the ultimate rate for quantum communication. Furthermore, unlimited classical communication between the sender and receiver does not enhance the capacities. Finally, the strong converse property holds, meaning that the rate $D(p\|u)$ represents a very sharp dividing line between possible and impossible communication rates. As mentioned in the introduction, since dephasing is a prominent source of noise in both quantum communication and computation, we expect our finding to have practical relevance in both scenarios. Based on the recent findings of ref. 21, we expect that $[D(p\|u)]^{-1}$ can be related to the ultimate overhead (the ratio of physical systems to logical qubits) of fault-tolerant quantum computation with superconducting systems, although further work is needed to demonstrate this definitively.

Our results can be extended to all multimode BDCs that act simultaneously on a collection of m bosonic modes with photon number operators $a_j^{\dagger} a_j$ as

$$\mathcal{N}_p^{(m)}(\rho) := \int_{[-\pi,\pi]^m} \mathrm{d}^m \boldsymbol{\phi}\, p(\boldsymbol{\phi})\, \mathrm{e}^{-i\sum_j a_j^{\dagger} a_j \phi_j} \rho\, \mathrm{e}^{i\sum_j a_j^{\dagger} a_j \phi_j}, \tag{8}$$

where $\boldsymbol{\phi} := (\phi_1, \ldots, \phi_m)$ and p is a probability density function on the hypercube $[-\pi,\pi]^m$. The eight capacities listed in equation (4) are all equal also for the channel $\mathcal{N}_p^{(m)}$, and we denote them using $\mathcal{C}\left(\mathcal{N}_p^{(m)}\right)$. They are given by the formula

$$\mathcal{C}\left(\mathcal{N}_p^{(m)}\right) = m \log_2(2\pi) - h(p), \tag{9}$$

where

$$h(p) = -\int_{[-\pi,\pi]^m} \mathrm{d}^m \boldsymbol{\phi}\, p(\boldsymbol{\phi}) \log_2(p(\boldsymbol{\phi})), \tag{10}$$

constituting a straightforward generalization of equation (4). As a special case of equation (8), when p is concentrated on the line $\boldsymbol{\phi} = (\phi, \ldots, \phi)$ and $\phi \in [-\pi,\pi]$ is uniformly distributed, one obtains the completely dephasing channel considered in refs. 31,32.

The most paradigmatic example of a BDC is that corresponding to a normal distribution $\widetilde{p}_\gamma(\phi) := (2\pi\gamma)^{-1/2} \mathrm{e}^{-\phi^2/(2\gamma)}$ of ϕ over the whole real line. This is the main example studied in refs. 16,17 and it is based on a physical model discussed in those works. Here, $\gamma > 0$ parametrizes the uncertainty of the rotation angle in equation (1): the larger γ, the stronger the dephasing. Since values of ϕ that differ modulo 2π can be identified, we obtain as an effective distribution p on $[-\pi,\pi]$ the wrapped normal distribution (p_γ):

$$p_\gamma(\phi) := \frac{1}{\sqrt{2\pi\gamma}} \sum_{k=-\infty}^{+\infty} \mathrm{e}^{-\frac{1}{2\gamma}(\phi+2\pi k)^2}. \tag{11}$$

The matrix T_{p_γ} obtained by plugging this distribution into equation (3) has entries $(T_{p_\gamma})_{nm} = \mathrm{e}^{-\frac{\gamma}{2}(n-m)^2}$, and therefore the corresponding BDC is the one discussed in the introduction. We find that

$$\mathcal{C}(\mathcal{N}_{p_\gamma}) = \log_2 \varphi(\mathrm{e}^{-\gamma}) + \frac{2}{\ln 2} \sum_{k=1}^{\infty} \frac{(-1)^{k-1} \mathrm{e}^{-\frac{\gamma}{2}(k^2+k)}}{k\left(1-\mathrm{e}^{-k\gamma}\right)}, \tag{12}$$

where $\varphi(q) := \prod_{k=1}^{\infty}(1-q^k)$ is the Euler function. See Supplementary Section 4A for details. In the physically relevant limit $\gamma \lesssim 1$, p_γ and $\widetilde{p}_\gamma$ are both concentrated around 0, and their entropies are nearly identical. In this regime

$$\begin{aligned} \mathcal{C}(\mathcal{N}_{p_\gamma}) &\approx \tfrac{1}{2}\log_2 \tfrac{2\pi}{\mathrm{e}\gamma} \\ &\approx \left(0.604 + \tfrac{1}{2}\log_2 \tfrac{1}{\gamma}\right) \text{ bits/channel use}, \end{aligned} \tag{13}$$

which demarcates the ultimate limitations on quantum and private communication in the presence of small dephasing noise. In the opposite case $\gamma \gg 1$ we obtain that

$$\mathcal{C}(\mathcal{N}_{p_\gamma}) \approx \frac{\mathrm{e}^{-\gamma}}{\ln 2}. \tag{14}$$

The above formula generalizes and makes quantitative the claim found in Section VI of ref. 17, that the quantum capacity of $\mathcal{N}_{p_\gamma}$ vanishes exponentially for large γ. In Fig. 3, we plot the capacity formula (equation (12)) as a function of γ, comparing it with the capacities $\mathcal{C}(\mathcal{N}_p)$ obtained for other important probability distributions p on the circle.

Discussion

Our main result represents important progress for quantum information theory, solving the capacities of a physically relevant class of non-Gaussian bosonic channels. Although many capacities of bosonic Gaussian channels have been solved in earlier work[25,28,29,33–36], we are not aware of any other class of non-Gaussian channels that represent relevant models of noise in bosonic systems and whose capacity can be computed to yield a non-trivial value (neither zero nor infinite).

Our findings have non-trivial implications for the design of quantum error-correcting codes[37,38] that encode and protect quantum information against the deleterious effects of BDCs. In particular, there is no superadditivity effect that occurs, as is the case with other quantum channels such as the depolarizing and dephrasure channels[39–41]. Thus, we now know that the random selection schemes of ref. 42,43 are optimal designs for BDCs. It would be interesting to design quantum polar codes tailored to BDCs, as these codes are known to be capacity-achieving for certain kinds of finite-dimensional channels[44,45]. As stated previously, another implication of our findings is that classical communication between the sender and receiver does not increase the quantum and private capacities of BDCs.

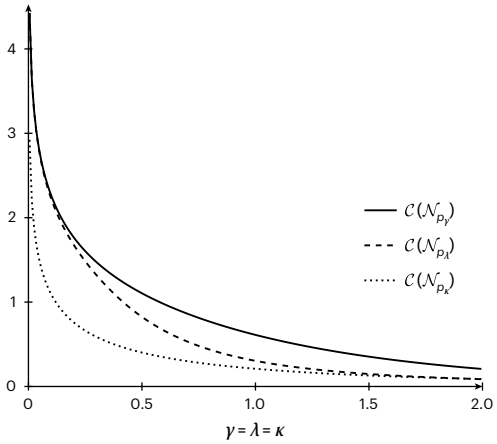

Fig. 3 | The capacities of the BDCs associated with the wrapped normal distribution (p_γ), the von Mises distribution (p_λ) and the wrapped Cauchy distribution (p_κ). The units of the vertical axis are qubits or private bits per channel use, and the horizontal axis features the main parameter governing the various distributions. The wrapped normal distribution is given by equation (11), which gives a Gaussian-modulated dephasing $(T_{p_\gamma})_{nm} = \mathrm{e}^{-\gamma(n-m)^2/2}$, and the capacity of the associated BDC $\mathcal{N}_{p_\gamma}$ is given by equation (12). The von Mises distribution p_λ is a better analogue of the normal distribution in the case of a circle. It is given by $p_\lambda(\phi) := \frac{\mathrm{e}^{\cos(\phi)/\lambda}}{2\pi I_0(1/\lambda)}$, where $\lambda > 0$ is a scale parameter analogous to γ above and I_k is a modified Bessel function of the first kind. The obtained dephasing matrix has entries $(T_{p_\lambda})_{nm} = \frac{I_{|n-m|}(1/\lambda)}{I_0(1/\lambda)}$, and the capacities of the BDC $\mathcal{N}_{p_\lambda}$ can be expressed as $\mathcal{C}(\mathcal{N}_{p_\lambda}) = \frac{1}{\ln 2}\frac{I_1(1/\lambda)}{\lambda I_0(1/\lambda)} - \log_2 I_0(1/\lambda)$. Finally, the wrapped Cauchy distribution defined by $p_\kappa(\phi) := \frac{1}{2\pi}\frac{\sinh\sqrt{\kappa}}{\cosh\sqrt{\kappa}-\cos\phi}$ corresponds to a dephasing matrix $(T_{p_\kappa})_{nm} = \mathrm{e}^{-\sqrt{\kappa}|n-m|}$, yielding a capacity equal to $\mathcal{C}(\mathcal{N}_{p_\kappa}) = -\log_2\left(1-\mathrm{e}^{-2\sqrt{\kappa}}\right)$.

Our formula can be seen as a natural generalization to bosonic systems of that given in refs. 18,36,46 for the quantum and private capacities of the qudit dephasing channel. However, the similarity of the final formula should not obscure the fact that the techniques used for its derivation are quite different. In particular, a key technical tool employed here is the Szegő theorem from asymptotic linear algebra[47,48], in addition to a teleportation[49] simulation argument that is rather different from those presented previously[22,25,29,36,50,51].

The collapse that occurs in equation (4), where eight different capacities are shown to coincide, also occurs for the quantum-limited bosonic amplifier channel, as a consequence of the findings of refs. 25,29,36,52. It would be interesting to determine other channels of physical interest for which this collapse occurs. It is known that this kind of collapse does not occur for the quantum erasure and pure-loss bosonic channels, because classical feedback from receiver to sender can increase the quantum and private capacities of these channels[36,53,54]. Such an increase has long been known to have practical implications for the design of quantum key distribution protocols, as discussed in refs. 36,54.

Going forward from here, it is of interest to address the capacities of bosonic lossy dephasing channels in which both loss and dephasing act at the same time. Such channels are modelled as the serial concatenation $\mathcal{L}_\eta \circ \mathcal{N}_p$, where $\mathcal{L}_\eta$ is a pure-loss channel of transmissivity $\eta \in [0,1]$; they provide realistic noise models for communication and computation, given that both kinds of noise are relevant in these systems[55]. Our result here, combined with the main result of ref. 29 and a data-processing bottlenecking argument, leads to the following upper bound on the quantum and private capacities of the bosonic lossy dephasing channel:

$$\begin{aligned} Q(\mathcal{L}_\eta \circ \mathcal{N}_p) &\leq P(\mathcal{L}_\eta \circ \mathcal{N}_p) \\ &\leq \min\{P(\mathcal{L}_\eta), P(\mathcal{N}_p)\} \\ &= \min\left\{\left(\log_2(\eta/(1-\eta))\right)_+, D(p\|u)\right\}, \end{aligned} \tag{15}$$

where $x_+ := \max\{x,0\}$. By the same argument, but invoking the results of refs. 25,36, the following upper bounds hold for the quantum and private capacities assisted by classical communication:

$$\begin{aligned} Q_{\leftrightarrow}(\mathcal{L}_\eta \circ \mathcal{N}_p) &\leq Q^{\dagger}_{\leftrightarrow}(\mathcal{L}_\eta \circ \mathcal{N}_p), P_{\leftrightarrow}(\mathcal{L}_\eta \circ \mathcal{N}_p) \\ &\leq P^{\dagger}_{\leftrightarrow}(\mathcal{L}_\eta \circ \mathcal{N}_p) \\ &\leq \min\{\log_2(1/(1-\eta)), D(p\|u)\}. \end{aligned} \tag{16}$$

The same data-processing argument can be employed for BDCs composed with other common bosonic Gaussian channels to obtain upper bounds on the composed channels' capacities, while using known upper bounds from earlier work[25,36,56–59].

It also remains open to determine the energy-constrained quantum and private capacities of BDCs, as well as their classical-communication-assisted counterparts[17,27]. Note that the lower bound in equation (23) is a legitimate lower bound on the energy-constrained quantum capacity of $\mathcal{N}_p$ when the mean photon number of the channel input cannot exceed $(d-1)/2$. In addition, it is clear that the energy-constrained classical capacity of $\mathcal{N}_p$ is equal to $g(E) := (E+1)\log_2(E+1) - E\log_2 E$, where E is the energy constraint. This identity depends essentially on the fact that Fock states can be perfectly transmitted through any BDC (see Section 3.1 of ref. 31). Finally, it is an open question to determine the energy-constrained entanglement-assisted classical capacity of BDCs[60].

In conclusion, in this work we have found an analytic expression for the quantum and private, assisted and unassisted, weak and strong converse capacities of all multimode bosonic dephasing channels, solving a problem that has been open for over a decade. BDCs are among the first non-Gaussian channels for which these capacities are calculated.

Online content

Any methods, additional references, Nature Portfolio reporting summaries, source data, extended data, supplementary information, acknowledgements, peer review information; details of author contributions and competing interests; and statements of data and code availability are available at https://doi.org/10.1038/s41566-023-01190-4.

References

1. Nielsen, M. A. & Chuang, I. L., *Quantum Computation and Quantum Information* (Cambridge Univ. Press, 2000).
2. Shor, P. W., Algorithms for quantum computation: discrete logarithms and factoring. In *Proc. 35th Annual Symposium on Foundations of Computer Science* 124–134 (IEEE, 1994)
3. Childs, A. M., Maslov, D., Nam, Y., Ross, N. J. & Su, Y. Toward the first quantum simulation with quantum speedup. *Proc. Natl Acad. Sci. USA* **115**, 9456–9461 (2018).
4. Grover, L. K. A fast quantum mechanical algorithm for database search. In *Proc. 28th ACM Symposium on Theory of Computing (STOC)* 212–219 (Association for Computing Machinery, 1996).
5. Harrow, A. W., Hassidim, A. & Lloyd, S. Quantum algorithm for linear systems of equations. *Phys. Rev. Lett.* **103**, 150502 (2009).
6. Gilyén, A., Su, Y., Low, G. H. & Wiebe, N. Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics. In *Proc. 51st Annual ACM SIGACT Symposium on Theory of Computing* 193–204 (Association for Computing Machinery, 2019).

7. Xu, F., Ma, X., Zhang, Q., Lo, H.-K. & Pan, J.-W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **92**, 025002 (2020).
8. Schlosshauer, M. Decoherence, the measurement problem, and interpretations of quantum mechanics. *Rev. Mod. Phys.* **76**, 1267–1305 (2005).
9. Brito, F., DiVincenzo, D. P., Koch, R. H. & Steffen, M. Efficient one- and two-qubit pulsed gates for an oscillator-stabilized Josephson qubit. *New J. Phys.* **10**, 033027 (2008).
10. Taylor, J. M. et al. Fault-tolerant architecture for quantum computation using electrically controlled semiconductor spins. *Nat. Phys.* **1**, 177–183 (2005).
11. Ospelkaus, C. et al. Trapped-ion quantum logic gates based on oscillating magnetic fields. *Phys. Rev. Lett.* **101**, 090502 (2008).
12. Wanser, K. H. Fundamental phase noise limit in optical fibres due to temperature fluctuations. *Electron. Lett.* **28**, 53–54(1) (1992).
13. Gordon, J. P. & Mollenauer, L. F. Phase noise in photonic communications systems using linear amplifiers. *Opt. Lett.* **15**, 1351–1353 (1990).
14. Derickson, D. *Fiber Optic Test and Measurement* (Prentice Hall, 1998).
15. Bartlett, S. D., Rudolph, T. & Spekkens, R. W. Reference frames, superselection rules, and quantum information. *Rev. Mod. Phys.* **79**, 555–609 (2007).
16. Jiang, L.-Z. & Chen, X.-Y. Evaluating the quantum capacity of bosonic dephasing channel. *Proc. SPIE* **7846**, 784613 (2010).
17. Arqand, A., Memarzadeh, L. & Mancini, S. Quantum capacity of a bosonic dephasing channel. *Phys. Rev. A* **102**, 042413 (2020).
18. Devetak, I. & Shor, P. W. The capacity of a quantum channel for simultaneous transmission of classical and quantum information. *Commun. Math. Phys.* **256**, 287–303 (2005).
19. Hayashi, M. *Quantum Information Theory: Mathematical Foundation* 2nd edn (Springer, 2017).
20. Wilde, M. M. *Quantum Information Theory* 2nd edn (Cambridge Univ. Press, 2017).
21. Fawzi, O., Müller-Hermes, A. & Shayeghi, A. A lower bound on the space overhead of fault-tolerant quantum computation. In *Proc. 13th Innovations in Theoretical Computer Science Conference (ITCS 2022)* Vol. 215 (ed. Braverman, M.) 68:1–68:20 (Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2022).
22. Bennett, C. H., DiVincenzo, D. P., Smolin, J. A. & Wootters, W. K. Mixed-state entanglement and quantum error correction. *Phys. Rev. A* **54**, 3824–3851 (1996).
23. Takeoka, M., Guha, S. & Wilde, M. M. The squashed entanglement of a quantum channel. *IEEE Trans. Inf. Theory* **60**, 4987–4998 (2014).
24. Khatri, S. & Wilde, M. M. Principles of quantum communication theory: a modern approach. Preprint at https://arxiv.org/abs/2011.04672v1 (2020).
25. Wilde, M. M., Tomamichel, M. & Berta, M. Converse bounds for private communication over quantum channels. *IEEE Trans. Inf. Theory* **63**, 1792–1817 (2017).
26. Wehner, S., Elkouss, D. & Hanson, R. Quantum internet: A vision for the road ahead. *Science* **362**, eaam9288 (2018).
27. Arqand, A., Memarzadeh, L. & Mancini, S. Energy-constrained LOCC-assisted quantum capacity of bosonic dephasing channel. Preprint at https://arxiv.org/abs/2111.04173 (2021).
28. Holevo, A. S. & Werner, R. F. Evaluating capacities of bosonic Gaussian channels. *Phys. Rev. A* **63**, 032312 (2001).
29. Wolf, M. M., Pérez-García, D. & Giedke, G. Quantum capacities of bosonic channels. *Phys. Rev. Lett.* **98**, 130501 (2007).
30. van Erven, T. & Harremos, P. Rényi divergence and Kullback–Leibler divergence. *IEEE Trans. Inf. Theory* **60**, 3797–3820 (2014).
31. Fanizza, M., Rosati, M., Skotiniotis, M., Calsamiglia, J. & Giovannetti, V. Squeezing-enhanced communication without a phase reference. *Quantum* **5**, 608 (2021).
32. Zhuang, Q. Quantum-enabled communication without a phase reference. *Phys. Rev. Lett.* **126**, 060502 (2021).
33. Giovannetti, V. et al. Classical capacity of the lossy bosonic channel: the exact solution. *Phys. Rev. Lett.* **92**, 027902 (2004).
34. Giovannetti, V., García-Patrón, R., J. Cerf, N. & Holevo, A. S. Ultimate classical communication rates of quantum optical channels. *Nat. Photonics* **8**, 796–800 (2014).
35. Giovannetti, V., Lloyd, S., Maccone, L. & Shor, P. W. Entanglement assisted capacity of the broadband lossy channel. *Phys. Rev. Lett.* **91**, 047901 (2003).
36. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043 (2017).
37. Shor, P. W. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A* **52**, R2493–R2496 (1995).
38. Lidar, D. A. & Brun, T. A. (eds) *Quantum Error Correction* (Cambridge Univ. Press, 2013).
39. DiVincenzo, D. P., Shor, P. W. & Smolin, J. A. Quantum-channel capacity of very noisy channels. *Phys. Rev. A* **57**, 830–839 (1998).
40. Smith, G. & Smolin, J. A. Degenerate quantum codes for Pauli channels. *Phys. Rev. Lett.* **98**, 030501 (2007).
41. Leditzky, F., Leung, D. & Smith, G. Dephrasure channel and superadditivity of coherent information. *Phys. Rev. Lett.* **121**, 160501 (2018).
42. Devetak, I. & Winter, A. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. A* **461**, 207–235 (2005).
43. Devetak, I. The private classical capacity and quantum capacity of a quantum channel. *IEEE Trans. Inf. Theory*, **51**, 44–55 (2005).
44. Renes, J. M., Dupuis, F. & Renner, R. Efficient polar coding of quantum information. *Phys. Rev. Lett.* **109**, 050504 (2012).
45. Renes, J. M. & Wilde, M. M. Polar codes for private and quantum communication over arbitrary channels. *IEEE Trans. Inf. Theory* **60**, 3090–3103 (2014).
46. Tomamichel, M., Wilde, M. M. & Winter, A. Strong converse rates for quantum communication. *IEEE Trans. Inf. Theory* **63**, 715–727 (2017).
47. Szegő, G. Beiträge zur Theorie der Toeplitzschen Formen. *Math. Z.* **6**, 167–202 (1920).
48. Serra-Capizzano, S. Test functions, growth conditions and Toeplitz matrices. *Rend. Circ. Mat. Palermo Ser. II* **68**(Suppl.), 791–795 (2002).
49. Bennett, C. H. et al. Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. *Phys. Rev. Lett.* **70**, 1895–1899 (1993).
50. Niset, J., Fiurasek, J. & Cerf, N. J. No-go theorem for Gaussian quantum error correction. *Phys. Rev. Lett.* **102**, 120501 (2009).
51. Müller-Hermes, A. Transposition in Quantum Information Theory. MSc thesis, Technische Universität München (2012).
52. Wilde, M. M. & Qi, H. Energy-constrained private and quantum capacities of quantum channels. *IEEE Trans. Inf. Theory* **64**, 7802–7827 (2018).
53. Bennett, C. H., DiVincenzo, D. P. & Smolin, J. A. Capacities of quantum erasure channels. *Phys. Rev. Lett.* **78**, 3217–3220 (1997).
54. Pirandola, S., García-Patrón, R., Braunstein, S. L. & Lloyd, S. Direct and reverse secret-key capacities of a quantum channel. *Phys. Rev. Lett.* **102**, 050503 (2009).
55. Leviant, P., Xu, Q., Jiang, L. & Rosenblum, S. Quantum capacity and codes for the bosonic loss-dephasing channel. *Quantum* **6**, 821 (2022).
56. Sharma, K., Wilde, M. M., Adhikari, S. & Takeoka, M. Bounding the energy-constrained quantum and private capacities of phase-insensitive bosonic Gaussian channels. *New J. Phys.* **20**, 063025 (2018).

57. Rosati, M., Mari, A. & Giovannetti, V. Narrow bounds for the quantum capacity of thermal attenuators. *Nat. Commun.* **9**, 4339 (2018).
58. Noh, K., Albert, V. V. & Jiang, L. Quantum capacity bounds of Gaussian thermal loss channels and achievable rates with Gottesman–Kitaev–Preskill codes. *IEEE Trans. Inf. Theory* **65**, 2563–2582 (2019).
59. Fanizza, M., Kianvash, F. & Giovannetti, V. Estimating quantum and private capacities of Gaussian channels via degradable extensions. *Phys. Rev. Lett.* **127**, 210501 (2021).
60. Holevo, A. S. Entanglement-assisted capacities of constrained quantum channels. *Theory Probab. Appl.* **48**, 243–255 (2004).

Methods

In this section, we provide a short overview of the techniques used to prove our main result (equation (4)). We establish the following two inequalities:

$$Q(\mathcal{N}_p) \geq D(p\|u), \tag{17}$$

$$P^{\dagger}_{\leftrightarrow}(\mathcal{N}_p) \leq D(p\|u). \tag{18}$$

Note that equations (17) and (18) together imply the main result, because $Q(\mathcal{N}_p)$ is the smallest among all of the capacities listed and $P^{\dagger}_{\leftrightarrow}(\mathcal{N}_p)$ is the largest. For a precise ordering of the various capacities, see Equations (5.6)–(5.13) of ref. 25.

To prove equation (17), let us recall that the coherent information of a quantum channel is a lower bound on its quantum capacity[20]. Specifically, the following inequality holds for a general channel $\mathcal{N}$:

$$Q(\mathcal{N}) \geq \sup_{\rho} \left\{ H(\mathcal{N}(\rho)) - H((\mathrm{id} \otimes \mathcal{N})(\psi^{\rho})) \right\}, \tag{19}$$

where the von Neumann entropy of a state σ is defined as $H(\sigma) := -\mathrm{Tr}[\sigma \log_2 \sigma]$, the optimization is over every state ρ that can be transmitted into the channel $\mathcal{N}$, and ψ^{ρ} is a purification of ρ (such that one recovers ρ after a partial trace). We can apply this lower bound to the BDC $\mathcal{N}_p$. For a fixed photon number $d-1$, let us choose ρ to be the maximally mixed state of dimension d, that is, $\rho = \tau_d := \frac{1}{d}\sum_{n=0}^{d-1} |n\rangle\langle n|$. This state is purified by the maximally entangled state $\Phi_d := \frac{1}{d}\sum_{n,m=0}^{d-1} |n\rangle\langle m| \otimes |n\rangle\langle m|$

To evaluate the first term in equation (19), consider from equations (2) and (3) that the output state is maximally mixed, that is, $\mathcal{N}_p(\tau_d) = \tau_d$, because the input state τ_d has no off-diagonal elements and the diagonal elements of the matrix T_p in equation (3) are all equal to one. Thus, we find that $H(\mathcal{N}_p(\tau_d)) = \log_2 d$. For the second term in equation (19), we again apply equations (2) and (3) to determine that

$$\begin{aligned} \omega_{p,d} &:= (\mathrm{id} \otimes \mathcal{N}_p)(\Phi_d) \\ &= \frac{1}{d} \sum_{n,m=0}^{d-1} (T_p)_{nm} |n\rangle\langle m| \otimes |n\rangle\langle m|. \end{aligned} \tag{20}$$

As the entropy is invariant under the action of an isometry, and the isometry $|n\rangle \to |n\rangle|n\rangle$ takes the state

$$\frac{T_p^{(d)}}{d} := \frac{1}{d} \sum_{n,m=0}^{d-1} (T_p)_{nm} |n\rangle\langle m| \tag{21}$$

to $\omega_{p,d}$, we find that the entropy $H(\omega_{p,d})$ reduces to

$$H(\omega_{p,d}) = H\left(T_p^{(d)}/d\right). \tag{22}$$

By a straightforward calculation, we then find that

$$\begin{aligned} H(\mathcal{N}_p(\tau_d)) - H(\omega_{p,d}) &= \log_2 d - H\left(T_p^{(d)}/d\right) \\ &= \frac{1}{d}\mathrm{Tr}\left[T_p^{(d)} \log_2 T_p^{(d)}\right]. \end{aligned} \tag{23}$$

This establishes the value in equation (23) to be an achievable rate for quantum communication over $\mathcal{N}_p$. Since this lower bound holds for every photon number $d-1 \in \mathbb{N}$, we can then take the limit $d \to \infty$ and apply the Szegő theorem[47,48] to conclude that the following value is also an achievable rate:

$$\begin{aligned} &\lim_{d\to\infty} \frac{1}{d}\mathrm{Tr}\left[T_p^{(d)} \log_2 T_p^{(d)}\right] \\ &\quad = \frac{1}{2\pi} \int_{-\pi}^{\pi} \mathrm{d}\phi\, 2\pi p(\phi) \log_2(2\pi p(\phi)) \\ &\quad = D(p\|u). \end{aligned} \tag{24}$$

Thus, this establishes the lower bound in equation (17).

To prove the upper bound in equation (18), we apply a modified teleportation simulation argument. This kind of argument was introduced in Section 5 of ref. 22 for the specific purpose of finding upper bounds on the quantum capacity assisted by classical communication, and it has been employed in a number of studies since then[25,29,36,50,51]. Since we are interested in bounding the strong converse secret-key-agreement capacity $P^{\dagger}_{\leftrightarrow}(\mathcal{N}_p)$, we apply reasoning similar to that given in ref. 25 (here see also refs. 61,62). However, there are some critical differences in our approach here.

To begin, let us again consider the state in equation (20). As we show in Supplementary Section 3B, by performing the standard teleportation protocol[49] with the state in equation (20) as the entangled resource state, rather than the maximally entangled state, we can simulate the action of the channel $\mathcal{N}_p$ on a fixed input state, up to an error that vanishes in the limit as $d \to \infty$. This key insight demonstrates that the state in equation (20) is approximately equivalent in a resource-theoretic sense to the channel $\mathcal{N}_p$. In more detail, we can express this observation in terms of the following equality: for every state ρ, it holds that

$$\lim_{d\to\infty} \left\| (\mathrm{id} \otimes \mathcal{N}_p)(\rho) - (\mathrm{id} \otimes \mathcal{N}_{p,d})(\rho) \right\|_1 = 0, \tag{25}$$

where $\mathcal{N}_{p,d}(\sigma) := \mathcal{T}(\sigma \otimes \omega_{p,d})$ is the channel resulting from the teleportation simulation. That is, the simulating channel $\mathcal{N}_{p,d}$ is realized by sending one subsystem of the maximally entangled state Φ_d through $\mathcal{N}_p$, which generates $\omega_{p,d}$, and then acting on the input state σ and the resource state $\omega_{p,d}$ with the standard teleportation protocol $\mathcal{T}$. By invoking the main insight from refs. 61,62 (as used later in ref. 23), we next note that a protocol for secret-key agreement over the channel is equivalent to one for which the goal is to distill a bipartite private state. Such a protocol involves only two parties, and thus the tools of entanglement theory come into play[61,62].

Now let $\mathcal{P}_{n,\varepsilon}$ denote a general, fixed protocol for secret-key agreement, involving n uses of the channel $\mathcal{N}_p$ and achieving an error ε for generating a bipartite private state of rate $R_{n,\varepsilon}$ (where the units of $R_{n,\varepsilon}$ are secret-key bits per channel use). Using the two aforementioned tools, teleportation simulation and the reduction from secret-key agreement to bipartite private distillation, the protocol $\mathcal{P}_{n,\varepsilon}$ can be approximately simulated by the action of a single LOCC channel on n copies of the resource state $\omega_{p,d}$. Associated with this simulation are two trace norm errors ε and δ_d, the first of which is the error of the original protocol $\mathcal{P}_{n,\varepsilon}$ in producing the desired bipartite private state and the second of which is the error of the simulation. We then invoke Equation (5.37) of ref. 25 to establish the following inequality, which, for the fixed protocol $\mathcal{P}_{n,\varepsilon}$, relates the rate $R_{n,\varepsilon}$ at which the secret key can be distilled to the aforementioned errors and an entanglement measure called the sandwiched Rényi relative entropy of entanglement:

$$R_{n,\varepsilon} \leq \tilde{E}_{R,\alpha}(\omega_{p,d}) + \frac{2\alpha}{n(\alpha-1)} \log_2\left(\frac{1}{1-\delta_d-\varepsilon}\right), \tag{26}$$

where $\alpha > 1$ and the sandwiched Rényi relative entropy of entanglement of a general bipartite state ρ is defined as[25]

$$\tilde{E}_{R,\alpha}(\rho) := \inf_{\sigma\in\mathrm{SEP}} \frac{2\alpha}{\alpha-1} \log_2 \left\| \rho^{1/2} \sigma^{(1-\alpha)/2\alpha} \right\|_{2\alpha}, \tag{27}$$

with SEP denoting the set of separable (unentangled) states. By choosing the separable state to be $(\mathrm{id} \otimes \mathcal{N}_p)\left(\overline{\Phi}_d\right)$, where $\overline{\Phi}_d := \frac{1}{d}\sum_{n=0}^{d-1} |n\rangle\langle n| \otimes |n\rangle\langle n|$, we find that

$$\tilde{E}_{R,\alpha}(\omega_{p,d}) \leq \frac{1}{\alpha-1} \log_2 \frac{1}{d} \mathrm{Tr}\left[\left(T_p^{(d)}\right)^{\alpha}\right]. \tag{28}$$

We refer the reader to Supplementary Section 3B for a detailed derivation. Thus, we find that the following rate upper bound holds for the secret-key-agreement protocol $\mathcal{P}_{n,\varepsilon}$ for all $d \in \mathbb{N}$:

$$R_{n,\varepsilon} \leq \frac{1}{\alpha-1}\log_2 \frac{1}{d}\mathrm{Tr}\left[\left(T_p^{(d)}\right)^{\alpha}\right] + \frac{2\alpha}{n(\alpha-1)}\log_2\left(\frac{1}{1-\delta_d-\varepsilon}\right). \tag{29}$$

Since this bound holds for all $d \in \mathbb{N}$, we can take the limit $d \to \infty$ and then arrive at the following upper bound:

$$\begin{aligned} R_{n,\varepsilon} &\leq \liminf_{d\to\infty}\left(\frac{1}{\alpha-1}\log_2 \frac{1}{d}\mathrm{Tr}\left[\left(T_p^{(d)}\right)^{\alpha}\right] + \frac{2\alpha}{n(\alpha-1)}\log_2\left(\frac{1}{1-\delta_d-\varepsilon}\right)\right) \\ &= D_\alpha(p\|u) + \frac{2\alpha}{n(\alpha-1)}\log_2\left(\frac{1}{1-\varepsilon}\right). \end{aligned} \tag{30}$$

In the above, we again applied the Szegő theorem[47,48] to conclude that

$$\lim_{d\to\infty}\frac{1}{\alpha-1}\log_2 \frac{1}{d}\mathrm{Tr}\left[\left(T_p^{(d)}\right)^{\alpha}\right] = D_\alpha(p\|u). \tag{31}$$

We also used the fact that $\lim_{d\to\infty}\delta_d = 0$, which is a consequence of equation (25). The bound in the last line only depends on the error ε of the original protocol $\mathcal{P}_{n,\varepsilon}$ and the Rényi relative entropy

$$D_\alpha(p\|u) := \frac{1}{\alpha-1}\log_2 \int_{-\pi}^{\pi} \mathrm{d}\phi\, p(\phi)^{\alpha} u(\phi)^{1-\alpha}. \tag{32}$$

As such, it is a uniform upper bound, applying to all n-round secret-key-agreement protocols that generate a private state of rate $R_{n,\varepsilon}$ and with error ε. Now noting that the n-shot secret-key-agreement capacity $P_{\leftrightarrow}(\mathcal{N}_p, n, \varepsilon)$ is defined as the largest rate $R_{n,\varepsilon}$ that can be achieved using the channel $\mathcal{N}_p$ a total of n times along with classical communication for free, while allowing for ε error, it follows from the uniform bound in equation (30) that

$$P_{\leftrightarrow}(\mathcal{N}_p, n, \varepsilon) \leq D_\alpha(p\|u) + \frac{2\alpha}{n(\alpha-1)}\log_2\left(\frac{1}{1-\varepsilon}\right), \tag{33}$$

holding for all $\alpha > 1$. Remembering that the strong converse secret-key-agreement capacity is defined as

$$P^{\dagger}_{\leftrightarrow}(\mathcal{N}_p) := \sup_{\varepsilon\in(0,1)} \limsup_{n\to\infty} P_{\leftrightarrow}(\mathcal{N}_p, n, \varepsilon) \tag{34}$$

we take the limit $n \to \infty$ to find that

$$\begin{aligned} P^{\dagger}_{\leftrightarrow}(\mathcal{N}_p) &\leq \sup_{\varepsilon\in(0,1)} \limsup_{n\to\infty}\left\{D_\alpha(p\|u) + \frac{2\alpha}{n(\alpha-1)}\log_2\left(\frac{1}{1-\varepsilon}\right)\right\} \\ &= D_\alpha(p\|u). \end{aligned} \tag{35}$$

This upper bound holds for all $\alpha > 1$. Thus, we can finally take the $\alpha \to 1$ limit and use a basic property of the Rényi relative entropy[30] to conclude the desired upper bound:

$$P^{\dagger}_{\leftrightarrow}(\mathcal{N}_p) \leq \lim_{\alpha\to 1} D_\alpha(p\|u) = D(p\|u). \tag{36}$$

This concludes the proof of the capacity formula (equation (4)) for the BDC. The argument required to establish its multimode generalization (equation (9)) is very similar, with the only substantial technical difference being the application of the multi-index Szegő theorem[48] (see Supplementary Section 3C for details).

Data availability

No data sets were generated during this study.

References

61. Horodecki, K., Horodecki, M., Horodecki, P. & Oppenheim, J. Secure key from bound entanglement. *Phys. Rev. Lett.* **94**, 160502 (2005).
62. Horodecki, K., Horodecki, M., Horodecki, P. & Oppenheim, J. General paradigm for distilling classical key from quantum states. *IEEE Trans. Inf. Theory* **55**, 1898–1929 (2009).

Acknowledgements

We thank S. Mancini for discussions. L.L. was partially supported by the Alexander von Humboldt Foundation. M.M.W. acknowledges support from the National Science Foundation under grant no. 2014010.

Author contributions

Both authors contributed to all aspects of this manuscript and to the writing of the paper.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41566-023-01190-4.

Correspondence and requests for materials should be addressed to Ludovico Lami or Mark M. Wilde.

Peer review information *Nature Photonics* thanks Javier Fonollosa and the other, anonymous, reviewer(s) for their contribution to the peer review of this work.