


ARTICLE

DOI: 10.1038/s41467-017-00961-2

OPEN

Capacity estimation and verification of quantum channels with arbitrarily correlated errors

Corsin Pfister^{1,2}, M. Adriaan Rol^{1,3}, Atul Mantri⁴, Marco Tomamichel ⁵ & Stephanie Wehner¹

The central figure of merit for quantum memories and quantum communication devices is their capacity to store and transmit quantum information. Here, we present a protocol that estimates a lower bound on a channel's quantum capacity, even when there are arbitrarily correlated errors. One application of these protocols is to test the performance of quantum repeaters for transmitting quantum information. Our protocol is easy to implement and comes in two versions. The first estimates the one-shot quantum capacity by preparing and measuring in two different bases, where all involved qubits are used as test qubits. The second verifies on-the-fly that a channel's one-shot quantum capacity exceeds a minimal tolerated value while storing or communicating data. We discuss the performance using simple examples, such as the dephasing channel for which our method is asymptotically optimal. Finally, we apply our method to a superconducting qubit in experiment.

¹QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands. ²Centre for Quantum Technologies, 3 Science Drive 2, Singapore, 117543, Singapore. ³Kavli Institute of Nanoscience, Delft University of Technology, P.O. Box 50462600 GA Delft, The Netherlands. ⁴Singapore University of Technology and Design, 20 Dover Drive, Singapore, 138682, Singapore. ⁵Centre for Quantum Software and Information, University of Technology Sydney, Broadway, NSW 2007, Australia. Correspondence and requests for materials should be addressed to S.W. (email: s.d.c.wehner@tudelft.nl)

One of the main obstacles on the way to quantum computers and quantum communication networks is the problem of noise due to imperfections in the devices. Noise is caused by uncontrolled interactions of the quantum information carriers with their environment. These interactions take place at all stages: when the carriers are processed, when they are transmitted, and when they are stored. Physicists and engineers spend large efforts in developing noise protection measures, and assessing their performance is crucial for the development of quantum information processing devices. In this article, we focus on the estimation of noise in the storage and transmission of the quantum information carriers, that is, we describe methods to assess quantum memory and quantum communication devices.

In the language of quantum information theory, memory and communication devices are described by a quantum channel, which is a function Λ that maps an input state ρ_{in} of the device to its output state $\rho_{\text{out}} = \Lambda(\rho_{\text{in}})$. In this unified description, assessing the noise in a quantum device reduces to estimating the decoherence of a quantum channel. One way to achieve this is through quantum process tomography¹, which aims at completely determining the channel from measurement data (see e.g., refs. 2,3 for more recent works on tomography, and, e.g., refs. 4,5 for surveys on specific types of tomography). This comes with two major disadvantages. First, process tomography typically only works for channels that behave the same way in every run of the experiment (formalized by the i.i.d. assumption—for independent and identically distributed), or under some symmetry assumptions. This assumption is violated for many devices that are used in practice, which typically show correlated errors. Second, since process tomography aims at a complete characterization of the channel, it requires the collection of large amounts of data for many combinations of input states and measurement settings. A complete characterization of a channel is certainly useful (as all properties of the channel can be inferred from it), but it is very costly if the task at hand is to simply estimate a figure of merit of the channel. For quantum storage and quantum communication devices, a central figure of merit is the quantum capacity of the channel, which quantifies the amount of quantum information that can be stored or transmitted by the device⁶. While the deployment of a suitable error-correcting code requires knowledge of the specifics of the channel, an estimate of the quantum capacity is of great use when assessing the usefulness of the tested device.

In this work, we present a method to estimate the one-shot quantum capacity $Q^\varepsilon(\Lambda)$ of a quantum channel Λ . While the quantum capacity Q only makes statements for devices that behave identically under many repeated uses, the one-shot quantum capacity Q^ε applies to the more general case of devices with arbitrarily correlated errors. It quantifies the number of qubits that can be sent through the channel with a fidelity of at least $1 - \varepsilon$ in a single use of the device using the best possible error-correcting code (we will explain this in more detail in the next section). We present a protocol that allows to estimate $Q^\varepsilon(\Lambda)$ from data obtained from simple measurements. In addition to dealing with arbitrarily correlated errors, it has the advantage of requiring fewer measurement settings than quantum process tomography.

Our method can also be used to assess whether a possibly imperfect error-correction scheme forms an improvement. This is the case if the error-corrected channel has a higher capacity than what we would otherwise expect. Similarly, our protocols can be employed to test whether a quantum repeater actually forms an improvement for sending quantum information, that is, whether it yields a higher quantum capacity than a direct quantum communication link.

Results

The one-shot quantum capacity. Noise can be modeled as a channel Λ , which is given as a map

$$\Lambda : \mathcal{S}(\mathcal{H}) \rightarrow \mathcal{S}(\mathcal{H}), \quad (1)$$

where $\mathcal{S}(\mathcal{H})$ denotes the set of quantum states on the Hilbert space of the system that is being stored or transmitted. For reasons of illustration, we will discuss channels of storage devices here, but mathematically, nothing is different for communication devices. In the realm of communication, it is convenient to think of a sender (Alice) who wants to relay qubits to a receiver (Bob). For memory device, Alice and Bob simply label the input and output.

Consider a quantum memory device designed for storing a quantum system with Hilbert space \mathcal{H} for some time interval Δt . Ideally, it leaves the state of the system completely invariant over that time span, but real storage devices are always subject to noise. A measure for how well the channel Λ preserves the state of the system is obtained by minimizing the square of the fidelity between the input state $|\phi\rangle$ and the output state $\Lambda(\phi)$,

$$F(|\phi\rangle, \Lambda(\phi)) = \sqrt{\langle \phi | \Lambda(\phi) | \phi \rangle}, \quad (2)$$

over all possible input states $|\phi\rangle \in \mathcal{H}$,

$$\min_{|\phi\rangle \in \mathcal{H}} F^2(|\phi\rangle, \Lambda(\phi)) = \min_{|\phi\rangle \in \mathcal{H}} \langle \phi | \Lambda(\phi) | \phi \rangle. \quad (3)$$

Low values of the quantity Eq. (3) imply that if the device is used without modification, then at least some states of the system are strongly affected by the channel, therefore introducing errors. However, this does not necessarily mean that the device is useless as a storage device, as this quantity does not account for the possibility that such errors can be corrected using quantum error correction (QEC).

An error-correcting code for a channel Λ consists of an encoding \mathcal{E} , which is applied before the channel, and a decoding \mathcal{D} , which is applied after the channel (see the explanations in

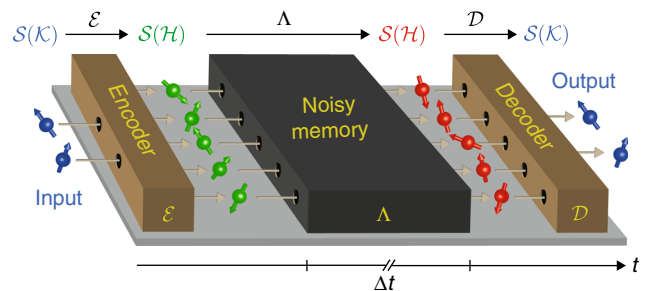


Fig. 1 Time diagram of an error-corrected quantum memory. An error-correcting code can turn a noisy quantum memory for some system with a Hilbert space \mathcal{H} into an approximately noise-free memory for some smaller system with a lower-dimensional Hilbert space \mathcal{K} . Such a code consists of an encoder \mathcal{E} , which is applied before the quantum memory, and a decoder \mathcal{D} , which is applied after the quantum memory. The encoder maps the state space \mathcal{K} of the smaller system into a subspace $\mathcal{H}' \subseteq \mathcal{H}$ of the larger system that is stored by the quantum memory, so it implements an encoding channel $\mathcal{E} : \mathcal{S}(\mathcal{K}) \rightarrow \mathcal{S}(\mathcal{H})$. The goal is to design the encoder such that the image $\mathcal{E}(\mathcal{S}(\mathcal{K})) = \mathcal{S}(\mathcal{H}') \subseteq \mathcal{S}(\mathcal{H})$ is a subspace that is left approximately intact by the quantum memory, up to an operation that may have mapped it elsewhere. Then, the decoder can be chosen such that it implements a channel $\mathcal{D} : \mathcal{S}(\mathcal{H}) \rightarrow \mathcal{S}(\mathcal{K})$ which maps that subspace back to the state space of the smaller system. This leads to an error-corrected memory for the smaller system which implements the channel $\mathcal{D} \circ \Lambda \circ \mathcal{E} : \mathcal{S}(\mathcal{K}) \rightarrow \mathcal{S}(\mathcal{K})$. Note that this figure shows a time diagram, so the three devices are not necessarily placed in the same spatial order as they appear in the figure

Fig. 1). Together, these devices form an error-corrected quantum memory for a smaller system, implementing a channel

$$\mathcal{D} \circ \Lambda \circ \mathcal{E} : \mathcal{S}(\mathcal{K}) \rightarrow \mathcal{S}(\mathcal{K}), \tag{4}$$

where \mathcal{K} is the Hilbert space of the smaller system and where \circ denotes the composition of maps. Instead of evaluating the quantity Eq. (3) for the channel Λ directly, it should be evaluated for such a corrected channel $\mathcal{D} \circ \Lambda \circ \mathcal{E}$. A figure of merit for the usefulness of the quantum memory is then given by the size of the largest system \mathcal{K} that can be stored in the memory using such an error-correcting code. This is identical to the largest subspace $\mathcal{H}' \subseteq \mathcal{H}$ that is left approximately invariant by the memory, where the choice of encoding corresponds to the choice of subspace. This is quantified by the one-shot quantum capacity $Q^\epsilon(\Lambda)$, defined by^{7,8}

$$Q^\epsilon(\Lambda) := \max\{\log_2 m \mid F_{\min}(\Lambda, m) \geq 1 - \epsilon\}, \tag{5}$$

where

$$F_{\min}(\Lambda, m) := \max_{\substack{\mathcal{H}' \subseteq \mathcal{H} \\ \dim(\mathcal{H}')=m}} \min_{|\phi\rangle \in \mathcal{H}'} \langle \phi | (\mathcal{D} \circ \Lambda)(\phi) | \phi \rangle \tag{6}$$

and where the inner maximum is taken over all possible decoders $\mathcal{D} : \mathcal{S}(\mathcal{H}) \rightarrow \mathcal{S}(\mathcal{H})$. This way, the one-shot quantum capacity corresponds to the maximal number of qubits that can be stored and retrieved with a fidelity of at least $1 - \epsilon$ using the best possible error-correcting code.

The one-shot quantum capacity tells us strictly more than the asymptotic quantum capacity, in the sense that the latter can be obtained from the former:

$$Q(\Lambda) = \lim_{\epsilon \rightarrow 0} \lim_{N \rightarrow \infty} \frac{1}{N} Q^\epsilon(\Lambda^{\otimes N}). \tag{7}$$

The asymptotic quantum capacity is the number of qubits that can be transmitted or stored per use of a device with asymptotically vanishing error, in the limit where it is used infinitely often under the i.i.d. assumption. Therefore, it is an asymptotic rate, while the one-shot quantum capacity is the total number of qubits that can be transmitted or stored in a single use of a (possibly non-tensor product) channel, allowing some error $\epsilon \geq 0$.

One-shot quantum capacity estimation. Now that the one-shot quantum capacity is identified as the relevant figure of merit for quantum memory and communication devices, the question is whether we can estimate this quantity for a given device. We answer this question in the affirmative for the case where Λ is a channel that stores or communicates (arbitrarily many) qubits.

We present a simple protocol (see Protocol 1 in Table 1) that estimates a lower bound on the one-shot quantum capacity $Q^\epsilon(\Lambda)$ for an N -to- N -qubit channel Λ . Our protocol only requires the preparation and measurement of single qubit states in two bases. Specifically, even though it is known that the optimal encoder for a given channel Λ may require the creation of a highly entangled state, no entanglement is required to execute our test. For simplicity, we assume here that N is an even number (for more general cases, see Supplementary Notes 4–6). The protocol does not make any assumption on whether the qubits are processed sequentially, as in communication devices, or in parallel, as in storage devices (potentially with correlated errors in both cases). The data collection of the protocol is very simple. Alice and Bob agree on two qubit bases X and Z . These two bases should be chosen to be “incompatible”, in the sense that the preparation quality q , which is defined as

$$q = -\log_2 \max_{i,j=0,1} |\langle i_X | j_Z \rangle|^2, \tag{8}$$

Table 1 Protocol 1: The estimation protocol

One-shot quantum capacity estimation

Protocol parameter

- $N \in \mathbb{N}$, even: total number of qubits

The protocol

- Alice chooses $s \in \{0, 1\}^N$ and $b \in \{X, Z\}^{N/2}$ fully at random and communicates them to Bob, where $\{X, Z\}^{N/2} = \{b \in \{X, Z\}^{N/2} \mid X, Z \text{ each occur } N/2 \text{ times in } b\}$.
- For each qubit slot $i = 1, \dots, N$ of the channel, Alice prepares a test qubit i in the state S_i with respect to basis $b_i \in \{X, Z\}$ and sends it through the channel to Bob.
- For each qubit $i = 1, \dots, N$ that Bob receives, he measures test qubit i in the basis b_i and records the outcome $s'_i \in \{0, 1\}$.
- Bob determine the error rates

$$e_x = \frac{2}{N} \sum_{i \in I_x} s_i \oplus s'_i, \quad e_z = \frac{2}{N} \sum_{i \in I_z} s_i \oplus s'_i,$$

where

$$I_x = \{i \in \{1, \dots, N\} \mid b_i = X\}, \\ I_z = \{i \in \{1, \dots, N\} \mid b_i = Z\}.$$

- Knowing the two error rates e_x and e_z , Bob determines a lower bound on the one-shot quantum capacity according to Theorem 1.

is as high as possible, where $|i_X\rangle$ and $|j_Z\rangle$ are eigenstates of X and Z , respectively. In the ideal case, where the two bases X and Z are mutually unbiased bases, such as the Pauli- X and Z basis, it holds that $q = 1$. Our protocol can be seen as exploiting the idea that the ability to transmit information in two complementary bases relates to a channel’s ability to convey (quantum) information^{9,10}, which we show holds even with correlated noise. We remark that Pauli- X and Z basis have also been used to estimate the process fidelity of a quantum operation^{11,12} in the i.i.d. case, which however we are precisely trying to avoid here.

The bound for the capacity estimate is a function of the number of qubits N , the preparation quality q , the maximally allowed decoding error probability ϵ of $Q^\epsilon(\Lambda)$, the two measured error rates e_x and e_z , and some probability p that quantifies the typicality of the protocol run (we will discuss this parameter in the Discussion section). More precisely, the bound is given as follows.

Theorem 1. Let $N \in \mathbb{N}_+$ be an even number, let e_x and e_z be error rates determined in a run of Protocol 1 where the used bases X and Z had a preparation quality of q (see Eq. (8) above). Then, for every $\epsilon > 0$ and for every $p \in [0, 1]$, it holds that

- either, the probability that at least one error rate exceeds e_x or e_z , respectively, was higher than p ,
- or the one-shot quantum capacity of the N -qubit channel Λ is bounded by

$$Q^\epsilon(\Lambda) \geq \sup_{\eta \in (0, \sqrt{\epsilon/2})} \left[N(q - h(e_x + \mu) - h(e_z + \mu)) - 2 \log_2(\kappa) - 4 \log_2\left(\frac{1}{\eta}\right) - 2 \right], \tag{9}$$

where h is the binary entropy function

$$h(x) := -x \log_2(x) - (1 - x) \log_2(1 - x) \tag{10}$$

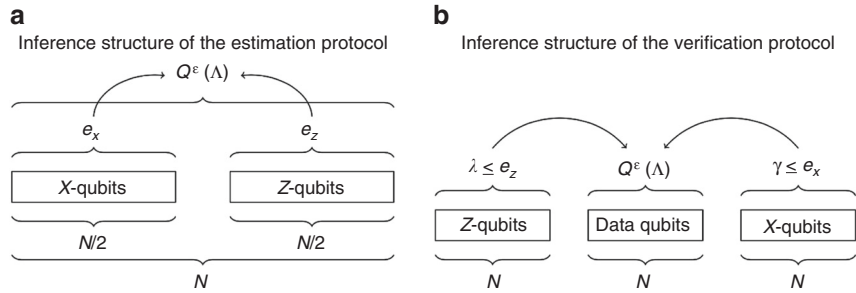


Fig. 2 Comparison of the inference structures of the two protocols. **a** In the estimation protocol, all qubits are test qubits, and the goal is to estimate the capacity for the channel on all qubits. **b** In the verification protocol, one third of the qubits are data qubits that are left untouched. The remaining $2N$ qubits are test qubits, whose error rates allow to bound the capacity of the channel on the N data qubits

and μ and κ are given by

$$\mu = \sqrt{\frac{N+2}{N^2} \ln\left(\frac{3 + \frac{5}{\sqrt{1-p}}}{\sqrt{\epsilon/2} - \eta}\right)}, \quad \kappa = 2 \left(\frac{3 + \frac{5}{\sqrt{1-p}}}{\sqrt{\epsilon/2} - \eta}\right)^2. \quad (11)$$

In the asymptotic limit where $N \rightarrow \infty$, the bound on the right hand side of inequality⁹ converges to $N(q - h(e_x) - h(e_z))$. All the other terms can be seen as correction terms that account for finite-size effects. We will discuss this in more detail in the Discussion section below. One may wonder, why we do not also obtain an upper bound. First of all, there exist no way to distinguish noise in the rest of the experimental apparatus from the noise on the channel. Second and more significantly, however, fixing any estimation procedure, arbitrarily correlated noise can always conspire to defeat the procedure tricking us into believing the capacity is low, while actually it is quite high. An upper bound could be obtained under the assumption that the noise is i.i.d., but this is precisely what we wish to avoid here.

One-shot capacity verification. Protocol 1 above estimates how much quantum information can be stored in a quantum memory device. This is of great use when the task is to figure out whether a device is potentially useful as a quantum memory device. When eventually, an error-correcting code is implemented, the corrected memory might be used without further testing.

In some cases, however, one wants to implement the memory with a means to verify its quality while using it. For example, one may suspect the quality of the memory to diminish (say, due to damage or overuse). In that case, the capacity estimation that was made before the implementation of the error-correcting code may no longer be valid. A method to verify that the quality of the memory is good enough for the implemented code may be required whenever it is used. Protocol 2, as given in Table 2, shows such a verification protocol.

The protocol assumes that Alice holds N data qubits that she wants to send to Bob in a way that allows her to verify the quality of the transmission. To this end, she uses a channel for $3N$ qubits and places her N data qubits in random slots of this channel. The other $2N$ slots are used for test qubits, half of which are prepared and measured in the X basis and half of which are prepared and measured in the Z basis (just as in the estimation protocol), while Alice and Bob leave the data qubits untouched. The error rates on the test bits allows to infer a bound on the capacity of the channel on the data qubits.

For this protocol, we denote the measured error rate in X by γ and the measured error rate in Z by λ . Bob checks whether these error rates exceed some tolerated values e_x and e_z , respectively, which has been specified before the protocol run. If one or both error rates exceed the tolerated value, the protocol aborts because the transmission quality is considered too low. If both error rates

Table 2 Protocol 2: The verification protocol

One-shot quantum capacity verification

Protocol parameters

- $N \in \mathbb{N}$: number of data qubits
- $e_x, e_z \in [0, 1]$: tolerated error rate in X, Z

The protocol

- Alice chooses $s \in \{0, 1\}^{3N}$ and $b \in \{X, Z, D\}_N^{3N}$ fully at random and communicates them to Bob, where $\{X, Z, D\}_N^{3N} = \{b \in \{X, Z, D\}^{3N} | X, Z, D \text{ occur } N \text{ times in } b\}$.
- For each qubit slot $i=1, \dots, 3N$ of the channel, if $b_i \in \{X, Z\}$, Alice prepares a test qubit l in the state s_i with respect to basis $b_i \in \{X, Z\}$ and sends it through the channel to Bob. If $b_i = D$, Alice uses the slot for a data qubit.
- For each qubit $i=1, \dots, 3N$ that Bob receives, if $b_i \in \{X, Z\}$, Bob measures test qubit l in the basis b_i and records the outcome $s'_i \in \{0, 1\}$. If $b_i = D$, Bob leaves the data qubit untouched.
- They determine the error rates

$$\gamma = \frac{1}{N} \sum_{i \in I_X} s_i \oplus s'_i, \quad \lambda = \frac{1}{N} \sum_{i \in I_Z} s_i \oplus s'_i,$$

where

$$I_X = \{i \in \{1, \dots, 3N\} | b_i = X\},$$

$$I_Z = \{i \in \{1, \dots, 3N\} | b_i = Z\}.$$

If $\gamma \leq e_x$ and $\lambda \leq e_z$, they continue with the conclusion below. Otherwise, they abort the protocol.

- They conclude that the one-shot quantum capacity of the channel Λ on the N data qubits is bounded as in Theorem 2.

are below their tolerated value, Bob concludes that the transmission was of high quality, in the sense that the channel on the data qubits had a high one-shot quantum capacity. This is stated more precisely in the following theorem.

Theorem 2. Let $N \in \mathbb{N}_+$, let $e_x, e_z \in [0, 1]$. Assume that Protocol 2 is run successfully without abortion, where the used bases X and Z had a preparation quality of q . Then, for every $\epsilon > 0$ and for every $p \in [0, 1)$, it holds that

- either, the probability that the protocol aborts was higher than p ,
- or the one-shot quantum capacity of the channel Λ on the N data qubits is bounded by inequality Eq. (9), where κ is as in Eq. (11) and where μ is given by

$$\mu = \sqrt{\frac{2(N+1)}{N^2} \ln\left(\frac{3 + \frac{5}{\sqrt{1-p}}}{\sqrt{\epsilon/2} - \eta}\right)}. \quad (12)$$

The bound for the verification protocol looks formally almost identical to the one for the estimation protocol, but there are

three differences. First, the function μ has a different dependence on N , which is a consequence of the different structure of the protocol as explained in Fig. 2. Second, the error rates e_x and e_z are preset accepted error rates instead of calculated error rates from data, and the bound holds when the measured rates are below those preset values. Third, the probability p in the bound is the abort probability of the protocol. Hence, another way to read the statement of the theorem is that either the protocol succeeds (does not abort) with a probability at most $1 - p$, or the capacity is indeed high. This again quantifies what we consider to be typical data: even if the channel is completely noisy and useless, there might be a tiny probability $1 - p$ that the observed error rates are nevertheless small. In this case, we saw highly atypical data. We will say more about this probability in the Discussion section. Recall, that in the verification protocol we use $3N$ rounds, hence there is no factor of $1/3$ on N (see also Fig. 2).

Experiment. We demonstrate the use of this protocol by implementing it on a Transmon qubit. The experiment is performed on qubit A_T previously reported in ref. 13. We measure a relaxation time of $T_1 = 18.5 \pm 0.6 \mu\text{s}$ and a Ramsey dephasing time of $T_2^* = 3.8 \pm 0.3 \mu\text{s}$ before performing the experiment. Readout of the qubit state is performed by probing the readout resonator with a microwave tone. The resulting transients are amplified using a traveling-wave parametric amplifier (TWPA)¹⁴ at the front end of the amplification chain. This results in a readout fidelity $F_{\text{RO}} = 11 - (p_{01} + p_{10})/2 = 98.0\%$, where p_{01} (p_{10}) is the probability of declaring state 1 (0) when the input state was $|0\rangle$ ($|1\rangle$) respectively. The qubit state is controlled using resonant microwave pulses.

The experiment implements Protocol 01 to estimate the capacity of the idling operation $I(\Delta t)$. We do this by generating 8000 pairs of random numbers corresponding to the bases $b \in \{X, Z\}$ and states $s \in \{0, 1\}$. These are then used to generate pulse sequences that rotate $|0\rangle$ to the required state, and wait for a time Δt before measuring the qubit in the Z basis and declaring a state. If the required state was in the X basis, a recovery pulse is applied that rotates the state to the Z basis before it is read out. This protocol is repeated 130 times, with a distinct randomization for each repetition, yielding a total of $N = 1.04 \times 10^6$ measurement outcomes in approximately one and a half hours. Results are reported in Fig. 3, which illustrates the estimate using the totality of the N outcomes for different values of ϵ . In Fig. 4 we furthermore plot variations in the error rate over time, as well as a bound for partial measurement sequences which highlight the (likely) non i.i.d. nature of the actual noise process affecting the qubits. We estimate $q = 0.985 \pm 0.047$ (see Supplementary Note 7) before taking the data, but use $q = 0.9$ as a conservative estimate to account for a potential drift during the experimental run.

Discussion

In this section, we shall discuss our bound as a bound on the rate $\frac{1}{N} Q^\epsilon(A)$, which quantifies the amount of quantum information that can be sent per qubit. This has the advantage that it makes comparisons easier. To discuss our bound on the capacity rate, we have plotted its value as a function of N in Fig. 5. We plotted the bound for the estimation protocol, but qualitatively, the bound for the verification protocol behaves identically, so our discussion applies to both protocols.

Example dephasing channel. In order to assess the strength of our bound, it is helpful to consider some example channels. A particularly insightful example is the case where the channel Λ is given by N independent copies of a dephasing channel of strength

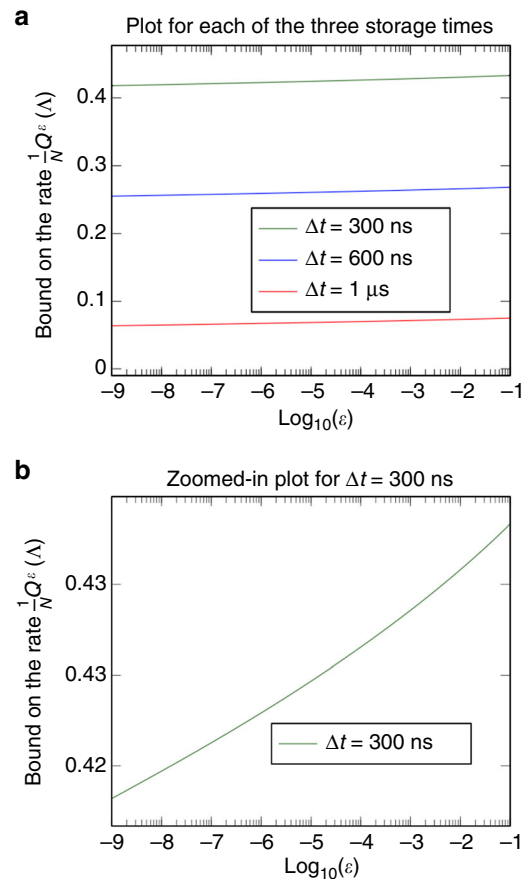


Fig. 3 Bound on the rate for the experimental data as a function of ϵ . This figure shows the bound on the one-shot quantum capacity rate for the data gained in the transmon qubit. We pick $p = 1/2$, and use $q = 0.9$ as preparation quality to account for the experimental imperfections (see Supplementary Note 7 for details). **a** The experiment was carried out three times with different storage times Δt , for each of which we plotted the bound resulting from the estimation protocol as a function of the decoding error probability ϵ . Since the number of qubit preparations and measurements was high ($N = 1.04 \times 10^6$), the dependence on ϵ is rather small. **b** For a better visibility of the ϵ -dependence, we show the plot for the shortest storage time separately and more zoomed-in in the direction of the bound

$\alpha \in [0, 1]$, that is,

$$\Lambda = \Lambda_D^{\otimes N}, \quad \Lambda_D(\rho) : \rho \mapsto \left(1 - \frac{\alpha}{2}\right)\rho + \frac{\alpha}{2}\sigma\rho\sigma, \quad (13)$$

where σ denotes one of the qubit Pauli operators with respect to some basis. Of particular interest is the case where the dephasing happens with respect to one of the two bases X or Z in which Alice and Bob prepare and measure the test qubits. Let us assume that $\sigma = \sigma_z$. In order to see what happens when our estimation protocol is used in this case, we could simulate a protocol run and see what bound on the one-shot quantum capacity would be obtained. However, the estimation protocol does essentially nothing but determine the two error rates e_x and e_z . The expected values of these rates can be readily obtained from Eq. (13). The error rate e_z vanishes, because dephasing in the Z basis leaves the Z -diagonal invariant. In the X basis the bits are left invariant with probability $1 - \alpha/2$, and flipped with probability $\alpha/2$, so asymptotically $e_x = \alpha/2$. Hence, for the dephasing channel, the

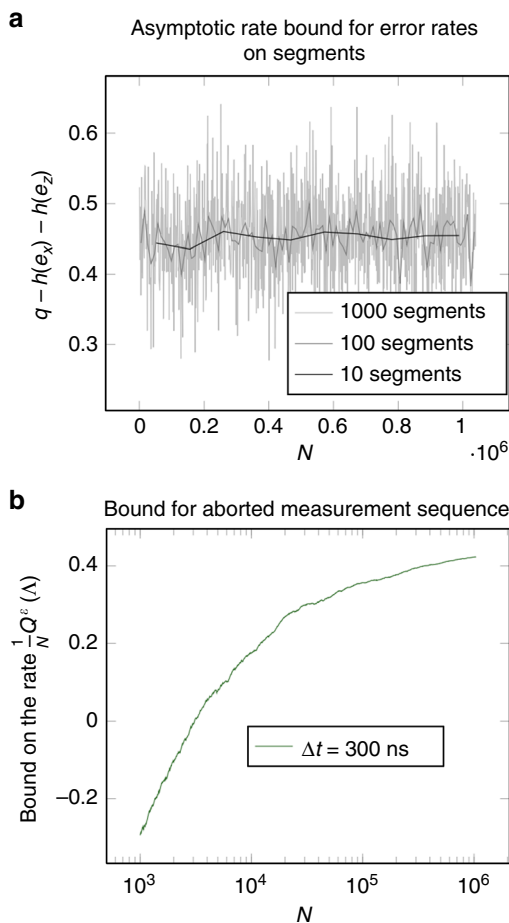


Fig. 4 Error fluctuations across the measurements. Here we visualize the statistical fluctuations in the measurement outcomes over the course of the transmon qubit experiment. **a** For the experiment with $\Delta t = 300$ ns, we split up the $N=1.04 \times 10^6$ sequential measurement outcomes into equally large and chronologically ordered segments and calculate the error rates e_x and e_z on each segment. For a meaningful and comparable quantity for comparison, we calculate the asymptotic bound $q - h(e_x) - h(e_z)$ for each of segment with $q = 0.9$, that is, the bound on the capacity rate that would be obtained if infinitely many measurements with the error rates as on the respective segments would be measured. As expected, the fluctuations decrease with the number of segments, or in other words, the larger the segments, the smaller the differences between them. Note that in contrast to all other plots, this is a linear plot. **b** For a glimpse on the cumulative effect of the fluctuations, we set 1000 logarithmically distributed “break points” and calculate the bound as if the experiment ended at each of those points where $q = 0.9$, $\epsilon = 10^{-6}$, and we pick $p = 1/2$. The resulting plot is to be compared with the plots in Fig. 5. The fluctuations that make the curve deviate from a smooth curve come from the fact that the measured error rates are not constant throughout the experiment, indicating that the noise affecting the transmon qubit is indeed unlikely to correspond to an i.i.d. process

estimation protocol is expected to yield the bound in inequality Eq. (9) with $e_z = 0$ and $e_x = \alpha/2$.

Asymptotic tightness of the bound. As one can see in Fig. 5, the bound on the one-shot quantum capacity, expressed as a rate, converges to $q - h(e_x) - h(e_z)$, which in the case of the dephasing channel is given by $q - h(\alpha/2)$. If we additionally assume that the bases X and Z are mutually unbiased (as are Pauli- X and Z), this is equal to $1 - h(\alpha/2)$. This is precisely the

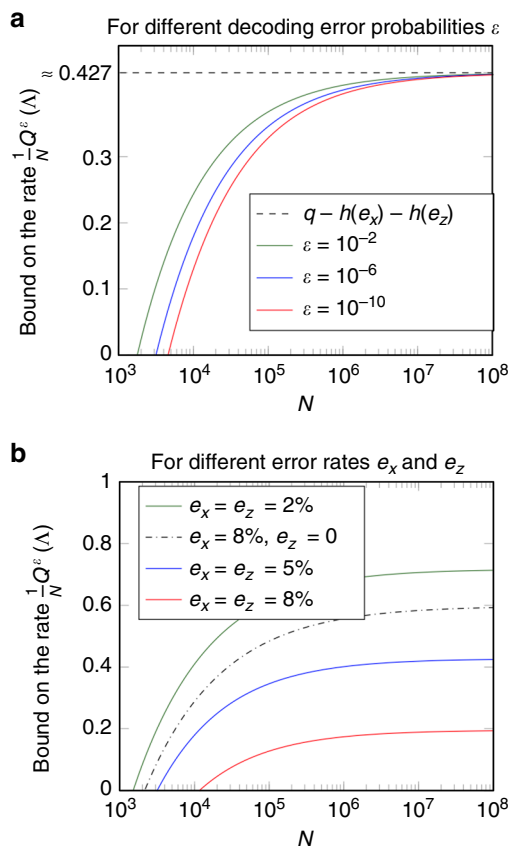


Fig. 5 Bound on the rate for the capacity estimation protocol as a function of the number of qubits. This figure shows the bound on the one-shot quantum capacity for the estimation protocol expressed as a rate, that is, the right hand side of inequality⁹ divided by the number of qubits N . The plots show the bound as a function of N with the parameters as $q = 1$, and $p = 1/2$. **a** We plotted the bound for fixed error rates $e_x = e_z = 5\%$ for a few different values of ϵ in order to visualize the dependence on the decoding error probability. The lower the allowed decoding error probability ϵ is set, the higher the number of qubits needs to be in order to get a positive bound on the rate (note that the N -axis is logarithmic). In the asymptotic limit $N \rightarrow \infty$, the bound converges to $q - h(e_x) - h(e_z)$. If $q = 1$, this coincides exactly with the (asymptotic) capacity for some important classes of channels, such as depolarizing channels. This shows that our bound is asymptotically optimal, and therefore, improvements are only possible in the finite-size correction terms. **b** To see the dependence on the error rates, we plotted our bound for a fixed value of $\epsilon = 10^{-6}$ for a few different values of e_x and e_z . The higher the error rate, the higher the number of qubits needs to be in order to achieve a positive rate. For every pair of error rates e_x and e_z , the bound is monotonically increasing in N and converges to $q - h(e_x) - h(e_z)$. Therefore, the bound can only be positive when $q - h(e_x) - h(e_z)$ is positive, which yields an easy criterion for the potential usefulness of a channel with known error rates (although the full version of the bound with the correction terms is not hard to evaluate either)

(asymptotic) quantum capacity of the dephasing channel. This means that our bound on the one-shot quantum capacity is asymptotically tight; if our bound can be improved, then only in the finite-size correction terms. In particular, our bound cannot be improved by a constant factor. Since most estimates that enter the derivation of the bound are of the same type as the estimates used in modern security proofs of quantum key distribution (QKD)¹⁵, any possible improvements of the QKD security bounds would also lead to an improvement of our bound on the one-shot quantum capacity (if there is any). In this sense, our

bound is essentially as tight as the corresponding security bounds for QKD in the finite regime.

Measurement calibration. Above, we have assumed that Alice and Bob were very lucky: they set up their bases X and Z such that one of them is exactly aligned with the dephasing basis, and therefore optimally exploited the asymmetry of the channel. In general, since they do not know the channel whose capacity they estimate, they do not know about the direction of the asymmetry. Instead, they have to calibrate their devices by trying out several pairs of bases until they find one with low error rates. Otherwise, the bound on the one-shot quantum capacity that they infer is suboptimal. It is an interesting open question how such a calibration can be optimized.

Example fully depolarizing channel. Another insightful example is the case where Λ is given by the channel which outputs the fully mixed state of N qubits, independently of the input state. The capacity of this channel is zero, yet with probability 2^{-N} , Alice and Bob measure error rates $e_x = e_z = 0$. One may think that these vanishing error rates lead to a highly positive bound on the capacity, but this is not the case. As one can read in Theorem 1 and Theorem 2, the bound depends on a probability p , and the term $1-p$ corresponds precisely to the probability of such an unlikely case. In fact, for $1-p = 2^{-N}$, the bound is never positive. This example shows that in the one-shot regime, a meaningful capacity estimation can only be made under the assumption that the observed data is not extremely atypical for the channel. However, this is only a problem for very low values of N : thanks to the natural logarithm in μ (see Eq. (11) above), the concern reduces to atypical events with an exponentially (in N) small probability. For reasonable numbers of N , the influence of p on the bound is negligible, except for extremely low values of $1-p$.

Quantifying typicality. We remark that p is a parameter to choose before executing the estimation protocol, which essentially just defines what we consider atypical. The statement of the estimation theorem can then be understood as simply stating that either the observed data is highly atypical (as defined by the choice of p), or the capacity is indeed high. From a practical point of view, note that for any constant p , the bound is essentially independent of p for even relatively small values of N and $\mu \rightarrow 0$ in (Eq. (11)) as $N \rightarrow \infty$. For this reason, we simply choose $p = 1/2$ in our plots as an illustration. Similarly, the maximally tolerated error rates e_x and e_z can be chosen freely when conducting the verification protocol. It is merely that the conclusions of the test depend on it, since we choose to abort—that is, draw no conclusion—if the observed error rates are higher than e_x and e_z . The probability p_{pass} that we do not abort then corresponds to $p_{\text{pass}} = 1-p$. So p also arises here, and corresponds to the probability of aborting, namely to the probability that data is produced which we do not regard as typical. Aborting may still seem like a different approach to the one taken during the verification protocol where we always draw a conclusion, but we can see that it is in fact exactly analogous: In the estimation protocol, Alice and Bob essentially decide to make a test in which e_x and e_z correspond exactly to the measured error rates instead of setting a maximum error rate ahead of time. Clearly, they will never abort in this case. Nevertheless, one can consider the probability that in any run, the measured error rates would stay below the rates that have been measured in this particular run of the test. This probability can be seen as a measure of typicality of the protocol, and corresponds precisely to p_{pass} if we were to execute the test again, but now fixing the error rates to what we observed. Hence,

again $p = 1 - p_{\text{pass}}$ which corresponds precisely to a quantification of such typicality.

For more information on the probability p and e_x and e_z , see Supplementary Notes 5 and 6. Note that the need to characterize typicality of the data observed is not only given in our context of capacity estimation, but arises in all statistical tests on a finite sample, including quantum key distribution where security statements are formulated in an analogous fashion.

Usage to assess quantum repeaters. An important challenge in the experimental realization of quantum repeaters is to demonstrate that they improve our ability to communicate compared to a direct fiber connection without a repeater. To demonstrate that they improve our ability to produce key, one proceeds by calculating the private capacity P of the direct communication channel without a repeater, followed by the implementation of a QKD protocol using the quantum repeater. If the rate R of generating key in the QKD protocol with the repeater satisfies $R > P$, then the quantum repeater improved our ability to produce encryption keys (see e.g., refs. 16–18). It turns out that it is in general harder to send qubits, then it is to produce key¹⁹. That is, the quantum capacity Q satisfies $Q \leq P$, where the inequality is in general strict. Demonstrating that a repeater improves our ability to produce key thus does not allow us to draw conclusions on whether the repeater improves our ability for sending qubits without further analysis.

Our result now precisely allows one to perform such a demonstration, even in the regime of arbitrarily correlated noise while in fact being no more difficult than performing BB84 QKD²⁰. Crucially, this means that in order to demonstrate a quantum repeaters ability to send qubits it is thus not necessary to perform quantum error correction (QEC) or entanglement distillation. First, one needs to calculate the quantum capacity $Q_{DF}^e(N)$ of the direct fiber (DF) connection, or a bound $Q_{DF}^e(N) \leq B_{DF}^e(N)$. We note that theoretical bounds $B_{DF}^e(N)$ on the one-shot capacity $Q_{DF}^e(N)$ are known for finite number of channel uses N and error ϵ , which are much tighter than employing the asymptotic capacity for $N \rightarrow \infty$ and $\epsilon \rightarrow 0$ ^{8,21}. We can now run our capacity estimation protocol over the quantum repeater link which yields a lower bound $L(N) \leq Q_{WR}^e(N)$ for the capacity with repeater (WR). If we find that $L(N) > B_{DF}^e(N)$, then we have successfully demonstrated that the quantum repeater improves our ability to transmit qubits over a direct transmission line.

Usage to assess quantum error-correcting schemes. We note that in a similar way we can make statements about the performance of a QEC scheme for storing qubits with arbitrarily correlated errors. Suppose that we wish to compare how well an error-correcting scheme encoding one logical qubit using multiple physical qubits compares to using just one of the physical qubits directly. We can again employ the result of⁸ to first derive (a bound on) the one-shot quantum capacity $B_p^e(N)$ if we used the physical qubit (P) N times with error ϵ . We then execute the capacity estimation protocol to estimate the capacity of the logical (LO) qubit channel $L(N) < Q_{LO}^e(N)$. If we find that $L(N) > B_p^e(N)$, then we can conclude that the logical qubit is an improvement for storing quantum information over one physical qubit.

Other open questions. Our result assumes that the system on which the channel acts is composed of qubits. An interesting open question is whether this restriction can be removed and an analogous bound can be derived for channels of arbitrary dimension and composition.

It would also be interesting to see our bound extended to continuous variable systems. There are many tools already available^{22–25} that may be useful to perform such an analysis, but it remains to be determined how exactly they can be applied to such systems.

Methods

To prove the bound on the one-shot quantum capacity, we combine several results. First, as we recapitulate in more detail in the Supplementary Note 1 through 4, it has been shown that the one-shot quantum capacity is bounded by the one-shot capacity of entanglement transmission $Q_{\text{ent}}^{\varepsilon}(A)$ ²⁶. More precisely, it holds that for every channel Λ and for every $\varepsilon > 0$,

$$Q^{\varepsilon}(A) \geq Q_{\text{ent}}^{\varepsilon/2}(A) - 1. \quad (14)$$

The one-shot capacity of entanglement transmission, in turn, has been proved to be bounded by the smooth min-entropy $H_{\text{min}}^{\varepsilon}(A|E)_{\rho}$, which is defined by

$$H_{\text{min}}^{\varepsilon}(A|B)_{\rho} := \max_{\rho' \in \mathcal{B}^{\varepsilon}(\rho)} H_{\text{min}}(A|B)_{\rho'}, \quad (15)$$

where

$$H_{\text{min}}(A|B)_{\rho} := \max_{\sigma_B} \sup \{ \lambda \in \mathbb{R} \mid \rho_{AB} \leq 2^{-\lambda} I_A \otimes \sigma_B \}. \quad (16)$$

It has been shown that^{7,8,27}

$$Q_{\text{ent}}^{\varepsilon}(A) \geq \sup_{\eta \in (0, \sqrt{\varepsilon})} \left(H_{\text{min}}^{\sqrt{\varepsilon} - \eta}(A|E)_{\rho} - 4 \log_2 \frac{1}{\eta} - 1 \right), \quad (17)$$

Here, the smooth min-entropy is evaluated for the state

$$\rho_{AE} = (I_A \otimes \Lambda_{A' \rightarrow E}^c)(\Phi_{AA'}), \quad (18)$$

where $\Phi_{AA'}$ is a maximally entangled state over the input system A' and a copy A of it, and where $\Lambda_{A' \rightarrow E}^c$ is the complementary channel of the channel $\Lambda_{A' \rightarrow B}$. The system E is the environment of the channel (see refs. 8,28 and Supplementary Note 2 for more details). Taking together the results Eqs. (14) and (17), we get that for all $\varepsilon > 0$,

$$Q^{\varepsilon}(A) \geq \sup_{\eta \in (0, \sqrt{\varepsilon/2})} \left(H_{\text{min}}^{\sqrt{\varepsilon/2} - \eta}(A|E)_{\rho} - 4 \log_2 \frac{1}{\eta} - 2 \right). \quad (19)$$

Therefore, the min-entropy bounds the one-shot quantum capacity.

Estimating the min-entropy has been a subject of intense research in quantum key distribution (QKD). However, min-entropy estimation protocols in QKD cannot be directly applied here, because they estimate the min-entropy $H_{\text{min}}^{\varepsilon}(X|E)$ for classical information X , while in the bound Eq. (17), the system A holds quantum information. We bridge this gap: as our main technical contribution, we show in the Supplementary Note 3 that for a system A that is composed of qubits, it holds that for every $\varepsilon > 0$ and every $\varepsilon', \varepsilon'' \geq 0$,

$$H_{\text{min}}^{3\varepsilon + \varepsilon' + 4\varepsilon''}(A|E)_{\rho} \geq Nq - \left(H_{\text{max}}^{\varepsilon''}(X|B)_{\rho} + H_{\text{max}}^{\varepsilon'}(Z|B)_{\rho} \right) - 2 \log_2 \frac{2}{\varepsilon^2}. \quad (20)$$

Inequality Eq. (20) reduces estimating the min-entropy of quantum information A to estimating the max-entropy of measurement outcomes X and Z on the system A .

We prove inequality Eq. (20) using three main ingredients. First, we use an uncertainty relation for the smooth min- and max-entropies²⁹. Second, we use a duality relation for the smooth min- and max-entropies^{30,31}. These two ingredients were also used in modern security proofs of quantum key distribution¹⁵. We combine these two tools with a third tool, namely a chain rule theorem for the smooth max-entropy³² to arrive at the bound in inequality Eq. (20).

Given inequalities Eqs. (17) and (20), all we are left to do is to devise a protocol that estimates the max-entropies of X and Z given Bob's quantum information B . Here we can make use of protocols in quantum key distribution that estimate exactly such a quantity. We show in the Supplementary Notes 4–6 how two such protocols (one for the max-entropy of X and one for the max-entropy of Z) can be combined into one protocol, which estimates both quantities simultaneously. The resulting protocol, which we presented in two versions, is given by Protocol 1 and Protocol 2 in the Results section. Our bound on the one-shot quantum capacity of the channel, inequality Eq. (9), is obtained by combining inequalities Eqs. (14) and (17) with these max-entropy estimation techniques.

Data availability. The authors declare that all data supporting this study are contained within the article and its supplementary files.

Received: 9 December 2016 Accepted: 8 August 2017

Published online: 02 January 2018

References

- Chuang, I. L. & Nielsen, M. A. Prescription for experimental determination of the dynamics of a quantum black box. *J. Mod. Opt.* **44**, 2455–2467 (1997).
- Faist, P. & Renner, R. Practical and reliable error bars in quantum tomography. *Phys. Rev. Lett.* **117**, 010404 (2016).
- Ferrie, C. & Blume-Kohout, R. Minimax quantum tomography: estimators and relative entropy bounds. *Phys. Rev. Lett.* **116**, 090407 (2016).
- Greenbaum, D. Introduction to quantum gate set tomography. *ArXiv* **1509**, 02921 (2015).
- D'Ariano, G. M. in *Quantum State Estimation* 1st edn, Vol. 649 (eds Paris, M. & Rehacek, J.) Ch. 8 (Springer-Verlag, Berlin, 2004).
- Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
- Buscemi, F. & Datta, N. The quantum capacity of channels with arbitrarily correlated noise. *IEEE Trans. Inf. Theory* **56**, 1447–1460 (2010).
- Tomamichel, M., Berta, M. & Renes, J. M. Quantum coding with finite resources. *Nat. Commun.* **7**, 11419 (2016).
- Renes, J. M. & Boileau, J.-C. Conjectured strong complementary information tradeoff. *Phys. Rev. Lett.* **103**, 020402 (2009).
- Christandl, M. & Winter, A. Uncertainty, monogamy, and locking of quantum correlations. *IEEE Trans. Inf. Theory* **51**, 3159–3165 (2005).
- Hofmann, H. F. Complementary classical fidelities as an efficient criterion for the evaluation of experimentally realized quantum operations. *Phys. Rev. Lett.* **94**, 160504 (2005).
- Sedláč, M. & Fiurášek, J. Generalized hofmann quantum process fidelity bounds for quantum filters. *Phys. Rev. A* **93**, 042316 (2016).
- Risté, D. et al. Detecting bit-flip errors in a logical qubit using stabilizer measurements. *Nat. Commun.* **6**, 6983 (2015).
- Macklin, C. et al. A near-quantum-limited Josephson traveling-wave parametric amplifier. *Science* **350**, 307–310 (2015).
- Tomamichel, M., Lim, C., Gisin, N. & Renner, R. Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **3**, 634 (2012).
- Takeoka, M., Guha, S. & Wilde, M. M. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nat. Commun.* **5**, 5235 (2014).
- Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043 (2017).
- Goodenough, K., Elkouss, D. & Wehner, S. Assessing the performance of quantum re-peaters for all phase-insensitive gaussian bosonic channels. *New J. Phys.* **18**, 063005 (2016).
- Horodecki, K., Horodecki, M., Horodecki, P., Leung, D. & Oppenheim, J. Unconditional privacy over channels which cannot convey quantum information. *Phys. Rev. Lett.* **100**, 110502 (2008).
- Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, vol. 175, 8 (1984).
- Kaur, E. & Wilde, M. M. Upper bounds on secret key agreement over lossy thermal bosonic channels. Preprint at <https://arxiv.org/abs/1706.04590> (2017).
- Furrer, F. et al. Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks. *Phys. Rev. Lett.* **109**, 100502 (2012).
- Furrer, F., Aberg, J. & Renner, R. Min- and max-entropy in infinite dimensions. *Commun. Math. Phys.* **306**, 165–186 (2011).
- Berta, M., Furrer, F. & Scholz, V. B. The smooth entropy formalism for von neumann algebras. *J. Math. Phys.* **57**, 015213 (2016).
- Furrer, F., Berta, M., Tomamichel, M., Scholz, V. B. & Christandl, M. Position-momentum uncertainty relations in the presence of quantum memory. Preprint at <https://arxiv.org/abs/1308.4527> (2014).
- Barnum, H., Knill, E. & Nielsen, M. A. On quantum fidelities and channel capacities. *IEEE Trans. Inf. Theory* **46**, 1317–1329 (2000).
- Morgan, C. & Winter, A. Pretty strong converse for the quantum capacity of degradable channels. *IEEE Trans. Inf. Theory* **60**, 317–333 (2014).
- Wilde, M. *Quantum Information Theory* (Cambridge University Press, Cambridge, 2013).
- Tomamichel, M. & Renner, R. Uncertainty relation for smooth entropies. *Phys. Rev. Lett.* **106**, 110506 (2011).
- König, R., Renner, R. & Schaffner, C. The operational meaning of min- and max-entropy. *IEEE Trans. Inf. Theory* **55**, 4337–4347 (2009).
- Tomamichel, M., Colbeck, R. & Renner, R. Duality between smooth min- and max-entropies. *IEEE Trans. Inf. Theory* **56**, 4674–4681 (2010).

32. Vitanov, A., Dupuis, F., Tomamichel, M. & Renner, R. Chain rules for smooth min- and max-entropies. *IEEE Trans. Inf. Theory* **59**, 2603–2612 (2013).

Acknowledgements

We thank the Leo DiCarlo group at QuTech for the experimental infrastructure necessary for MAR to conduct the experiment to collect the test data for a superconducting qubit. We also thank Mario Berta, Thanh Le Phuc, and Jeremy Ribeiro for insightful discussions, and Julia Cramer for helpful comments on an earlier version of this manuscript. C.P., A.M., and M.T. were supported by MOE Tier 3A grant “Randomness from quantum processes”, NRF CRP “Space-based QKD”. S.W. was supported by STW, Netherlands, an NWO VIDI Grant, and an ERC Starting Grant. M.A.R. was supported by an ERC Synergy grant.

Author contributions

S.W. devised the project, and the main conceptual and proof ideas. C.P. worked out the theoretical details with help from A.M. and M.T.; M.A.R. performed the experiment. C.P. and M.A.R. analyzed the data with help from S.W.; C.P., M.A.R. and S.W. wrote the manuscript.

Additional information

Supplementary Information accompanies this paper at <https://doi.org/10.1038/s41467-017-00961-2>.

Competing interests: The authors declare no competing financial interests.

Reprints and permission information is available online at <http://npg.nature.com/reprintsandpermissions/>

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/>.

© The Author(s) 2017