Continuous-Variable Protocols in the Noisy-Storage Model

Fabian Furrer,[1,2] Christian Schaffner,[3,4] and Stephanie Wehner[5]

[1]*NTT Basic Research Laboratories, NTT Corporation,*
3-1 Morinosato-Wakamiya, Atsugi, Kanagawa, 243-0198, Japan.
[2]*Department of Physics, Graduate School of Science, University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo, Japan, 113-0033.*
[3]*Institute for Logic, Language and Computation (ILLC) University of Amsterdam, The Netherlands*
[4]*Centrum Wiskunde & Informatica (CWI), Amsterdam, The Netherlands*
[5]*QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, Netherlands*

We present the first protocol for oblivious transfer that can be implemented with an optical continuous-variable system, and prove its security in the noisy-storage model. This model allows security to be achieved by sending more quantum signals than an attacker can reliably store at one specific point during the protocol. Concretely, we determine how many signals need to be sent in order to achieve security by establishing a trade-off between quantum uncertainty generated in the protocol and the classical capacity of the memory channel. As our main technical tool, we study and derive new uncertainty relations for continuous-variable systems. Finally, we provide explicit security parameters for realistic memory models.

I. INTRODUCTION

Quantum key distribution (QKD) offers security that rests only on the laws of quantum mechanics [1–3]. Yet, there are still important cryptographic protocols which cannot be realized without additional assumptions, even using quantum communication [4–10]. Examples of such protocols are oblivious-transfer (OT), bit commitment (BC), and secure password-based identification, where two distrustful parties (Alice and Bob) engage in a protocol and want to be ensured that the other party cannot cheat, or maliciously influence the outcome.

Due to the great practical importance of problems such as secure identification one is willing to rely on assumptions in order to achieve security. Classically, these are usually computational assumptions that are not fully future proof and can possibly be broken retroactively using a quantum computer. Another line of research pursues physical assumptions on the adversary, such as imposing limits on his abilities to store information [11, 12]. This assumption is especially appealing in quantum communication where advanced technologies such as long-lived quantum memories are very challenging and expensive. Moreover, as opposed to computational assumptions, it provides the benefit that they are indeed fully future proof: even if the adversary obtains a much larger quantum memory after the protocol, security cannot be broken retroactively.

Given any constraint on the adversary's storage device, security can always be obtained by sending sufficiently many signals during the course of the protocol. Generalizing the model of classical bounded storage [11], the so-called bounded-quantum-storage model assumes that the adversary can only store a certain number of qubits [13, 14]. More generally, the noisy-storage model [15] ensures security for arbitrary noisy memory devices. Specifically, a link has been made between security and the classical capacity [16], entanglement cost [17], and quantum capacity [18, 19] of the adversary's quantum storage device. An important feature of the corresponding protocols is that they do not require the honest protocol participants to have any quantum memory at all. In particular, they can be implemented using BB84 or six-state QKD protocols, which have been experimentally demonstrated [20, 21].

Yet, all protocols proposed so far [13, 15–17, 20, 22, 23] are based on discrete-variable systems requiring single-photon detectors that are, despite recent improvements, still challenging technologies [24]. Here, we propose the first protocols based on optical continuous-variable systems, where the information is encoded in the X and P quadrature of the electromagnetic field (see, e.g., [25]). Optical continuous variable implementations provide practical benefits since transmission, measurements (homodyne detection) and sometimes also preparations require only standard telecommunication technologies. These benefits allow easy integration of the protocols into current classical networks. Moreover, state preparation and homodyne detection are highly efficient and robust technologies permitting high clock rates, and they are available as on-chip components [26].

We present a protocol for OT as well as BC, and derive sufficient conditions for security in the noisy-storage model depending on the classical capacity of the malicious party's memory channel similar to [16]. For instance, we show that security can be obtained if twice the classical capacity is lower than the uncertainty that is generated by X and P measurements plus the error-correction (EC) amount that is required to overcome the information loss during transmission. The latter term is crucial for CV protocols since, compared to discrete variable protocols, CV protocols require the exchange of a significant amount of EC information.

The main technical ingredients in our security proof are novel entropic uncertainty relations. While we derive an uncertainty relation that holds without assumptions by using majorization techniques from [27], it turns out that even though security is in principle possible it is not sufficient to obtain a good trade-off in parameters. We overcome this technical problem by showing uncertainty relations under reasonable assumptions, namely, that the adversary's encoding is Gaussian or independent and identical over only a limited number of modes. The security trade-off is then analyzed in both cases for a memory channel modeled by a lossy and noisy bosonic Gaussian channel. Our work opens the door for the development of continuous-variable protocols in the noisy-storage

model.

II. OBLIVIOUS TRANSFER IN THE NOISY-STORAGE MODEL

We first focus on OT along which we discuss the essential ideas behind the security in the noisy-storage model. A protocol for OT is especially appealing since any two-party cryptographic problem in which Alice and Bob do not trust each other can in principle be solved using OT as a building block [28]. While the quantum part of the protocols for OT and BC protocol are similar, the classical post-processing is different. We consider a randomized version of OT, where Alice has no input and gets as output two bit strings s_0, s_1 and Bob has input t and obtains a bit string $\tilde{s}$. If both are honest, we require that $\tilde{s} = s_t$ (correctness). If Alice is honest, we require that Bob can only know one of the strings. If Bob is honest, we demand that Alice does not learn t. No requirements are made if both are dishonest. These security requirements are made precise in a composable fashion in B 1 by demanding that it is indistinguishable from a perfectly correct protocol with probability ϵ_C, and from a perfectly secure protocol for honest Alice and Bob with ϵ_A, ϵ_B.

The quantum part of the protocol for CV is based on a QKD protocol using Gaussian modulated squeezed states. As it is conceptually simpler, we consider an entanglement based version of the protocol, although its prepare and measure version is straightforward. The source is given by the CV equivalent of a maximally entangled state, namely, a two-mode squeezed state simply referred to as EPR (Einstein,Podolski,Rosen [29]) state in the following (see Appendix D). The measurements are homodyne detections with a discretized outcome range into binnings of length δ. Mathematically, they are modeled as coarse-grained X and P measurements and in the following denoted by X_δ and P_δ (see, e.g., [30]). The measurement choice of Alice (Bob) in round i are denoted by θ_A^i (θ_B^i), where $\theta_A^i = 0, 1$ stands for performing X_δ, P_δ. The quantum protocol is then simply:

(Q1) Alice creates n EPR pairs of which she sends each half to Bob.

(Q2) Alice and Bob measure independently X_δ ($\theta = 0$) or P_δ ($\theta = 1$) according to $\theta_A = \theta_A^1 \ldots \theta_A^n$ and $\theta_B = \theta_B^1 \ldots \theta_B^n$, where θ_A and θ_B are chosen uniformly random in $\{0, 1\}^n$ [31]. The strings of outcomes for Alice and Bob are denoted by Z and Y.

(Q3) They wait for a fixed time Δt.

The crucial property of this protocol is that approximately half of the strings Z and Y are strongly correlated. However, neither party knows which part. This concept has been formalized in [16] under the name of *weak string erasure*.

The classical part of the protocol proceeds as follows:

(OT1) Alice sends Bob her basis choice θ_A. Bob defines the set $I_t = \{i \mid \theta_A^i = \theta_B^i\}$ and its complement I_{1-t} according to his choice bit t. He sends I_0, I_1 to Alice.
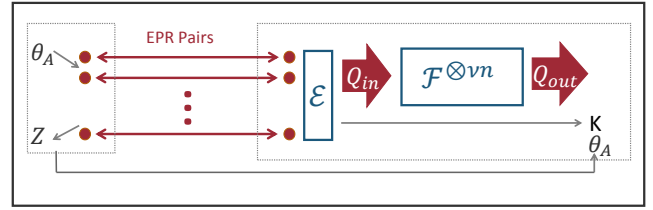

FIG. 1. The scenario of a dishonest Bob. The memory attack is modeled by an encoding $\mathcal{E}$ that maps (conditioned on some classical outcome K) the n modes to the memory input Q_{in}. The memory $\mathcal{M}$ is modeled by νn uses of the channel $\mathcal{F}$. We consider the situations where the encoding $\mathcal{E}$ is arbitrary, a mixture of Gaussian channels or independent and identical over a small numbers of signals m.

(OT2) Alice forms the strings $Z_k = (Z^i)_{i \in I_k}$ for $k = 0, 1$, and computes error-correction information W_0, W_1 individually for Z_0, Z_1 and sends it to Bob. Bob then corrects the string corresponding to his choice $Y_t = (Y^i)_{i \in I_t}$ using W_t to obtain Y_t'. [32]

(OT3) Alice selects random 2-universal hash functions f_0, f_1 from X_0 and X_1 to ℓ-bit strings and outputs $s_k = f_k(X_k)$, $k = 0, 1$. She then sends f_0, f_1 to Bob who outputs $\tilde{s} = f_t(Y_t')$.

We further assume that if a honest party obtains a value from the other party that is not conformal with the protocol, it generates a random output. This ensures that the protocol always terminates with an output.

It is easy to verify that executing the above classical protocol after (Q1)-(Q3) satisfies the correctness condition for OT with ϵ_C that depends on the error-correction protocol. Moreover, security for honest Bob simply follows since the only information leaving his lab are the sets I_0, I_1, which are uncorrelated with t. For a more rigorous proof of composable security, we refer to [14].

More interesting is the security for honest Alice. In fact, if Bob has a quantum memory that allows him to faithfully store all the modes sent by Alice over a time longer than Δt, he can cheat perfectly. He only has to wait to receive Alice's basis choice θ_A and measure all modes in the corresponding basis. But if Bob has only noisy quantum storage he might not have enough information to obtain both strings s_0 and s_1. As illustrated in Fig. 1, we model Bob's memory attack by an encoding operation $\mathcal{E}$ that maps the n modes to the input space Q_{in} of his quantum memory correlated to classical information K. After that Bob stores Q_{in} in his quantum memory for time Δt until he receives θ_A. We model the corresponding memory channel $\mathcal{M}$ of νn quantum channels $\mathcal{F}$, i.e., $\mathcal{M} = \mathcal{F}^{\otimes \nu n}$. Bob's information at the end of the protocol is denoted by B' and given by all the classical information obtained from Alice plus K and $\mathcal{M}(Q_{in})$.

Our goal is to quantify the relation between the capacity of Bob's quantum memory and the security for Alice. The latter is obtained if one of the strings, let's say s_0 for simplicity, is uniformly random and uncorrelated with B'. Fortunately, a standard method known in cryptography as privacy amplifi-

cation can be used to ensure the desired property even if the adversary still holds significant amount of information about Z_0: if the length ℓ of the hashed string s_0 is roughly equal to the conditional smooth min-entropy $H_{\min}^{\epsilon_1}(Z_0|B')$ of the input of the hash function Z_0 given Bob's information B', i.e., $\ell = H_{\min}^{\epsilon_1}(Z_0|B') - 2\log 1/(\epsilon_A - 4\epsilon_1)$ [33], then s_0 is ϵ_A-close in trace distance to uniform and uncorrelated from B'. For $\epsilon_1 = 0$, the smooth min-entropy is equal to the negative logarithm of the success probability that Bob can guess Z_0 by measuring B', and its generalization for $\epsilon \geq 0$ is obtained by maximizing it over all states that are ϵ-close [33, 34] (see Appendix A 1 for details).

We thus have to lower bound $H_{\min}^{\epsilon_1}(Z_0|B')$, for which we follow ideas developed for the discrete variable case [16, 23]. First we use an inequality from [16] to bound $H_{\min}^{\epsilon}(Z_0|B')$ by means of the classical capacity of Bob's memory channel. Note that Bob's information B' at the end of the protocol is given by $B' = \mathcal{M}(Q_{\text{in}})B_{\text{cl}}$ with classical information $B_{\text{cl}} = K\theta_A W_0 W_1$. Then, if we denote by $\mathcal{P}_{\text{succ}}^{\mathcal{M}}(k)$ the optimal success probability to reliably send k classical bits through $\mathcal{M}$, we have that [16]

$$2^{-H_{\min}^{\epsilon_1}(Z_0|B')} \leq \mathcal{P}_{\text{succ}}^{\mathcal{M}}(\lfloor H_{\min}^{\epsilon_2}(Z_0|B_{\text{cl}}) - \log 1/(\epsilon_1 - \epsilon_2)^2 \rfloor). \tag{1}$$

This inequality reduces the problem to bounding the smooth min-entropy conditioned on Bob's classical information only.

An additional problem arises because we do not know which of the two strings Z_0, Z_1 Bob does not learn. This problem can be solved by using the min-entropy splitting theorem [35], which says that if the uncertainty about the whole string is high, i.e. $H_{\min}^{\epsilon_2}(Z|B_{\text{cl}}) \geq \lambda$, then so it is in average for the sub-strings Z_0 and Z_1. More precisely, there exists a random variable D such that $H_{\min}^{\epsilon_2}(Z_D|B_{\text{cl}}D) \geq \lambda/2 - 1$. Note that this result relies crucially on the fact that the information upon which one conditions, i.e., $B_{\text{cl}}D$ is classical and not quantum [36]. Finally, we can remove the dependence on the error-correction information W_0, W_1 by simply subtracting the maximal information contained in W_0, W_1, i.e., the number of bits $\ell_{\text{EC}} = \log |W_0 W_1|$.

In conclusion, we obtain security for Alice if $\ell = -1/2\log \mathcal{P}_{\text{succ}}^{\mathcal{M}}(nr_{\text{OT}}) - \log 1/(\epsilon_A - 4\epsilon_1)$ where

$$r_{\text{OT}} = 1/2\left(\lambda^{\epsilon_2}(n) - \frac{\ell_{\text{EC}}}{n}\right) - \frac{1}{n}\left(2\log\frac{1}{(\epsilon_1 - \epsilon_2)} - 1\right), \tag{2}$$

and $\epsilon_A > 4\epsilon_1 > \epsilon_2 \geq 0$. Here, $\lambda^{\epsilon}(n)$ stands for a lower bound on the smooth min-entropy rate

$$\frac{1}{n}H_{\min}^{\epsilon}(Z|\theta_A K) \geq \lambda^{\epsilon}(n). \tag{3}$$

We can now relate Alice's security to the classical capacity $C_{\text{cl}}(\mathcal{F})$ of $\mathcal{F}$ whenever the success probability of reliably sending classical information through $\mathcal{F}$ at a rate R higher than $C_{\text{cl}}(\mathcal{F})$ decays exponentially $\mathcal{P}_{\text{succ}}^{\mathcal{F}^{\otimes n}}(nR) \leq 2^{-n\xi(R-C_{\text{cl}}(\mathcal{F}))}$ [37] (see Discussion for examples). Then, by a simple calculation we find that security for Bob can be obtained for large enough n if the condition

$$r_{\text{OT}}(n) - \nu C_{\text{cl}}(\mathcal{F}) > 0 \tag{4}$$

is satisfied. Moreover, the length of s_0, s_1 can be chosen as $\ell = n\xi(r_{\text{OT}}(n) - C_{\text{cl}}(\mathcal{F})) - \mathcal{O}(\log 1/\epsilon_A)$.

In order to analyse the security we have to find tight lower bounds $\lambda^{\epsilon}(n)$ for the inequality (3), which is a special kind of uncertainty relation. The other important quantity is the EC rate which in practice is directly determined by the protocol. For the following discussions we use the standard formula $\ell_{\text{EC}}/n = H(X_{\delta}^A) - \beta I(X_{\delta}^A : X_{\delta}^B)$, where X_{δ}^A and X_{δ}^B are the random variables induced if both players are measuring X_{δ}. The parameter $\beta \leq 1$ is called the efficiency of the EC protocol and values of about 0.96 are practical using currently available codes [38–40].

III. BIT COMMITMENT IN THE NOISY STORAGE MODEL

A bit commitment protocol consists of a commitment phase where Bob commits to a bit c, and an open phase where Alice learns c. Honest Alice wants to be ensured that Bob cannot change his commitment c after completion of the commitment phase (binding). And Bob wants that Alice cannot learn c before the open phase (hiding). Similarly to the OT protocol, we use composable security definitions (described in Appendix C 1) using security parameters $\epsilon_C, \epsilon_H, \epsilon_B$ for the correctness, hiding and binding conditions.

The protocol for commitment is similar to the quantum part of OT and consists of steps (Q1)-(Q3) except that in (Q2) Bob is measuring all his signals in the basis corresponding to the bit c he wants to commit to $\theta_B = c, \ldots, c$. The open phase is purely classical [13]:

(BC1) Bob sends c and Y to Alice who defines the substring Z_I, Y_I of Z, Y containing the elements $I = \{i|\theta_A^i = c\}$. She then accepts if $Y_I \in B_{\epsilon_C}(Z_I)$ and rejects otherwise.

Here, the set $B_{\epsilon}(Z_I)$ is the ϵ-typical set of outcomes for Bob if both measure in the same basis and Alice obtains outcome Z_I. If n is large enough, Alice will accept with probability ϵ_C due to the property of typical sequences. Moreover, the hiding condition is satisfied perfectly since Bob does not send any information in the commitment phase.

As in OT, it is evident that Bob can cheat perfectly if he has a perfect quantum memory. But under the same assumptions on Bob's memory as discussed for the OT protocol, we show in Appendix C 2 that the hiding condition is satisfied for sufficiently large n if

$$1/2(\xi\lambda^{\epsilon}(n) - \log V_{\epsilon_C}/n) - \nu C_{\text{cl}}(\mathcal{F}) > 0, \tag{5}$$

where $V_{\epsilon_C} = \max_Y |B_{\epsilon_C}^{-1}(Y)|$ with $B_{\varepsilon}^{-1}(Y) = \{Z | Y \in B_{\varepsilon}(Z)\}$ the set of Alice's outcomes Z for which Y would be accepted. Note that in our case, $|B_{\epsilon}^{-1}(Y)|$ is independent of Y and the maximization can be omitted. In particular, if the transmissivity of the channel between Alice and Bob is τ, one finds that $\log V_{\epsilon} = nH(X_{\sqrt{\tau}\delta}^B|X_{\delta}^A)$, which is approximately the reverse reconciliation rate $H(Y_{\delta}|Z_{\delta})$ increased by $\log 1/\sqrt{\tau}$ (see Appendix C 2 for details).
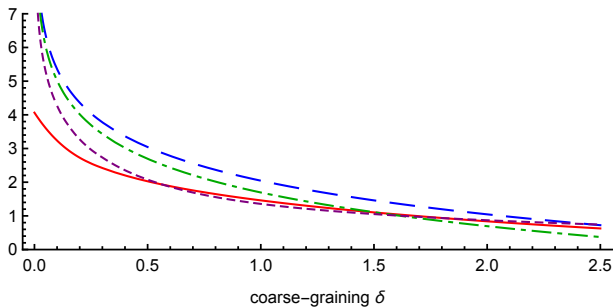
FIG. 2. One can achieve security in the noisy storage model without assumptions if the error-correction rate ℓ/n (short dashed) is below the entropy rate $\lambda_{\text{Maj}}^{\epsilon}$ (straight), under Gaussian encoding assumption if ℓ/n is below $\lambda_{\text{Gauss}}^{\epsilon}$ (long dashed), and under independent and identical encodings over $m = 25$ signals if ℓ/n is below $\lambda_{\text{IID}}^{\epsilon}$ (dashed-dotted). The horizontal axis describes the coarse graining δ of the homodyne detection of the X and P quadrature. We chose practical protocol parameters of $n = 10^8$ signals and security parameters $\epsilon_A = \epsilon_B = 10^{-9}$. The error-correction rate is plotted for an efficiency of $\beta = 0.96$ and correlations obtained by an EPR state with squeezing of 10.8dB and one-sided losses of 5%. We further emphasize that the situation looks similar for the BC protocol for the considered parameters.
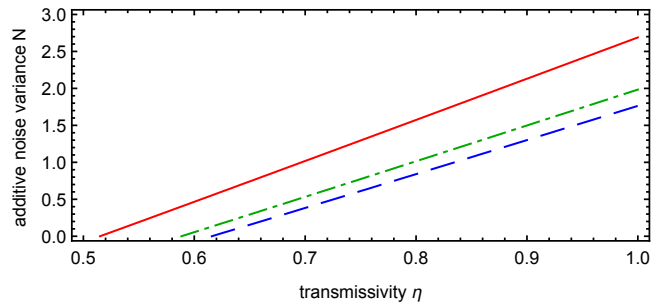
FIG. 3. The left side of the plots correspond to secure regions for the OT protocol under Gaussian encoding assumption ($\lambda_{\text{Gauss}}^{\epsilon}$), depending on the transmissivity η (horizontal axis) and the additive noise variance N (vertical axis) of malicious Bob's Gaussian memory channel. The thermal noise of the memory is set to $N_{\text{th}} = 0$ and the maximal photon constraint to $N_{\text{max}} = 30$. The different curves correspond to different numbers of quantum memories νn, squeezing strengths s and one-sided transmissivity τ of the EPR state for values $(\nu, s, \tau) = (1/8, 10.8, 0.95)$ (solid), $(1/10, 10.8, 0.90)$ (dashed) and $(1/12, 7.8, 0.9)$ (dashed-dotted). We further set the coarse graining to $\delta = 0.2$ (largest optimal value) and choose the other parameters as in Fig. 2.

IV. CV UNCERTAINTY RELATIONS FOR THE NOISY STORAGE MODEL

Both the security of OT and BC rely on tight bounds λ^{ϵ} in (3). To obtain such bounds using (1) we first need an uncertainty relation. In order to derive it, let us grant additional power to a dishonest Bob who can prepare an ensemble of states $\{\rho^k\}_k$ according to K himself and send it to Alice who performs on any mode randomly X_δ or P_δ. After completing all measurements, Alice sends her basis choice θ_A to Bob who has to guess the outcomes Z of the measurements. As Bob does not know the measurement choice prior to preparation, the uncertainty principle forbids Bob to know Z perfectly, i.e., there is no state for which the outcomes of both X and P are certain. As the uncertainty principle holds independently for any state of the ensemble, it is intuitively clear that K cannot bring any advantage, which is why we omit it in the following (see e.g. [41] for details).

Traditionally, the uncertainty principle for X and P is captured as a lower bound on the product of their standard deviations $\sigma_X \sigma_P \geq \hbar/2$ [42]. Here, we are interested in an entropic version for coarse grained measurements. For the sake of illustration, let us first consider the equivalent relation for the well-known Shannon entropy, i.e., $H(X) = -\sum_x p_x \log p_x$ if X is distributed according to $\{p_x\}$. For $n = 1$, the conditional Shannon entropy of interest is given by $H(Z|\theta_A) = 1/2(H(X_\delta) + H(P_\delta))$, where $H(X_\delta)$ denotes the Shannon entropy of the outcomes of the X_δ measurement and similar for P_δ. However, it is known that $H(X_\delta) + H(P_\delta) \geq -\log c(\delta)$ with $c(\delta) = \delta^2/(\pi e \hbar)$ [43], and thus, $H(Z|\theta_A) \geq -1/2 \log c(\delta)$. This inequality can straightforwardly be generalized to $n \geq 1$.

Let us now turn to the uncertainty relation of interest in (3) expressed by the smooth min-entropy instead of the von Neumann entropy. Such uncertainty relations have previously been analysed for maximally complementary qubit measurements [14, 41]. Here, we analyze this uncertainty relation for the first time for X and P measurements. In strong contrast to the situation of the Shannon entropy discussed before, a non-trivial relation is only possible for coarse-grained X and P measurement but not for continuous ones (see Appendix A 2 a). Hence, the lower bound has to be derived for X_δ and P_δ directly, which makes it very challenging.

We derive three different uncertainty bounds denoted by $\lambda_{\text{Maj}}^{\epsilon}$, $\lambda_{\text{Gauss}}^{\epsilon}$ and $\lambda_{\text{IID}}^{\epsilon}$. The first $\lambda_{\text{Maj}}^{\epsilon}$ is valid without restrictions on the states ρ^k. The derivation is based on a result by Landau and Pollak [44] that for any two fixed intervals $I, J \in \mathbb{R}$, the probability $q[I]$ to measure X in I, and $p[J]$ to measure P in J have to satisfy the constraint $\cos^{-1} \sqrt{q[I]} + \cos^{-1} \sqrt{p[J]} \geq \cos^{-1} \gamma$ where γ is a function of the length of the intervals of I and J. This relation yields an infinite number of constraints for the probability distributions for X_δ and P_δ. However, it is difficult to derive a lower bound by including all constraints. The bound $\lambda_{\text{Maj}}^{\epsilon}$ is obtained by a relaxation using the majorization technique from [27] and can be computed recursively (see Appendix A 2 b for details). The drawback is that the relaxation is not optimal leading to a lose bound leaving the problem open to find a tighter relaxation.

This problem is overcome in the other two bounds at the expense of additional assumptions. The bound $\lambda_{\text{Gauss}}^{\epsilon}$ holds under the assumption that the state is a mixture of Gaussian states. Applied to the noisy-storage model, this assumption requires that the encoding operation $\mathcal{E}$ (not the quantum memory $\mathcal{F}$) has to be a mixture of Gaussian operations, which can be justified since non-Gaussian operations are still very chal-

lenging in practice and more importantly, their implementations are generally not deterministic. The explicit form is $\lambda_{\text{Gauss}}^{\epsilon}(n) = \sup(B_{\text{Gauss}}^{\alpha}(\delta) - 1/(n(\alpha-1)) \log 2/\epsilon^2)$, where

$$B_{\text{Gauss}}^{\alpha}(\delta) = \frac{1}{1-\alpha} \log \frac{1}{2}(1 + (1/\alpha)(\delta^2/(\pi\hbar))^{(\alpha-1)}) \quad (6)$$

and the optimization is over all $\alpha > 1$. The bound is derived using continuous approximations and the details are in Appendix A 2 c.

The last bound $\lambda_{\text{IID}}^{\epsilon}$ applies under the assumption that the ensemble states are independent and identical over only m-mode states ($m \ll n$). This assumption requires that Bob's encoding operation $\mathcal{E}$ acts in an identical and independent way on only m modes, which in the language of QKD corresponds to collective attacks. It is a reasonable assumption since coherent operations of all the n modes may require a lot of resources. Moreover, if Bob wants to coherently act on all n modes he has to store all the incoming modes until all n modes arrived, which in principle already requires a short-time memory. It might also be possible for Alice to send the modes with delays in order to enhance her security. The bound is derived via a reduction of the smooth min-entropy for independent and identical distributions to the Shannon entropy [33, 45] and given by $\lambda_{\text{IID}}^{\epsilon} = -1/2 \log c(\delta) - \mathcal{O}(m^2\sqrt{m/n})$ (see Appendix A51).

The three bounds are shown in Fig. 2. We see that for large n, $\lambda_{\text{Gauss}}^{\epsilon}$ and $\lambda_{\text{IID}}^{\epsilon}$ are approximately equal. In fact, in the limit $n \to \infty$ we find that both converge to the optimal bound determined by the Shannon entropy $-1/2 \log c(\delta)$. We further plotted the EC rate for the OT protocol since a necessary condition for security is that $\lambda^{\epsilon}(n)$ has to be larger. We assume an EPR state with variance $V = 3\hbar$ (about 10.8dB) and transmission losses on Bob's mode of 0.05, an error-correction efficiency of 0.95 and excess noise $0.0005\hbar$. We see that $\lambda_{\text{Maj}}^{\epsilon}$ does not provide a very tight bound on the entropy rate such that security can only be achieved under very restrictive assumptions on the quantum memory of a malicious Bob.

V. SECURITY FOR REALISTIC MEMORY DEVICES

To obtain explicit parameters from (1), the second ingredient is a strong converse for the memory in question. Here, we consider the security conditions for OT (4) and BC (5) for a specific class of memory channels, namely, bosonic thermal-loss channels with additive Gaussian noise. The question of the classical capacity of such channels has only recently been completely solved after settling the minimal output entropy conjecture [46, 47]. Moreover, the exponential decay of successful transmittance above the classical capacity has been established for $\xi = 1$ under a maximal photon constraint $N_{\max}$ [48], i.e., every code word has (up to negligible probability) maximal $N_{\max}$ photons. In Fig. 3, we show when equality in the condition for OT (4) is attained under Gaussian restriction of a malicious Bob's encoding map $\mathcal{E}$ (i.e., $\lambda_{\text{Gauss}}^{\epsilon}$) depending on the transmissivity η and the additive noise variance N and different fractions of quantum memories ν. Since

there is only a week dependence for low thermal noise variance $V_{\text{th}} \leq 0.1$, we set it equal to 0. We see that for $\nu \leq 1/8$ security can already been obtained for memory channels with small losses and additive noise. Note that since $\xi = 1$ and that $\log V_{\epsilon_C}$ is approximately ℓ_{EC} (see Fig. 2), the same result holds for the BC protocol. The approximately same curves are obtained if one restricts the memory attacks to independent and identical encodings over $m \leq 10$ signals, i.e., exchanging $\lambda_{\text{Gauss}}^{\epsilon}$ by $\lambda_{\text{IID}}^{\epsilon}$ in (4). Moreover, security without any restriction on the encoding (i.e., $\lambda_{\text{Maj}}^{\epsilon}$) can be obtained if the fraction of the quantum memory is about $\nu \approx 5 \cdot 10^{-3}$. We finally note that independent of the memory model, security for OT and BC can only be obtained with squeezed states and if the transmissivity between Alice and Bob is larger than $1/2$.

VI. CONCLUSION

We have presented a protocol for OT and BC using optical CV systems that provide security in the noisy-storage model. The protocol is practical and uses similar resources as CV QKD. As a key ingredient, we analyze and derive uncertainty relations for CV systems, that can be used along similar lines to analyze the security in the noisy-storage model for other two-party protocols such as secure password-based identification [16, 22, 23]. We leave as open problem the task of finding optimal uncertainty relations without any further assumptions. It is possible that such relations can be obtained by linking security again to the quantum capacity of the storage device [17, 19], requiring however more sophisticated techniques. Such a result would also pose a challenge to find an explicit strong converse for the quantum capacity of bosonic channels.

Appendix A: CV uncertainty relations for the smooth min-entropy

1. Smooth min-entropy

Let us consider a classical random variable Z with values in a discrete but possibly infinite set $\mathcal{Z}$ that is correlated to a quantum system B modeled by a Hilbert space $\mathcal{H}_B$. If Z is distributed according to p_z, the situation can be conveniently be described by the state

$$\rho_{ZB} = \sum_z p_z |z\rangle\langle z| \otimes \rho_B^z, \quad (A1)$$

where ρ_B^z is the state of system B conditioned on $z \in \mathcal{Z}$ and $|z\rangle$ an orthonormal basis. The conditional min-entropy of Z

given B is then defined [34] as minus the logarithm of the maximal success probability to correctly infer Z given access to B, that is,

$$H_{\min}(Z|B)_\rho = -\log\left(\sup_{\{E_z\}}\sum_z p_z \operatorname{tr}(E_z\rho_B^z)\right), \quad \text{(A2)}$$

with the supremum taken over all positive operator valued measures (POVM) $\{E_z\}$, i.e., $E_z \geq 0$ and $\sum_z E_z = \mathbb{1}$. If system B is a classical random variable Y jointly distributed according to $p(z, y)$, the min-entropy is defined for the state $\rho_{ZY} = \sum_{z,y} p(z, y)|z\rangle\langle z| \otimes |y\rangle\langle y|$ with $|y\rangle$ an orthonormal basis.

The smooth min-entropy is then defined as the maximization of the min-entropy over states that are ϵ-close in the purified distance $\mathcal{P}(\rho, \sigma) = \sqrt{1 - F(\rho, \sigma)}$ [49]. Here $F(\rho, \sigma) = (\operatorname{tr}|\sqrt{\rho}\sqrt{\sigma}|)^2$ denotes the fidelity. In formulas, this means that

$$H_{\min}^\epsilon(Z|B)_\rho = \sup_{\tilde{\rho}_{ZB}} H_{\min}(Z|B)_{\tilde{\rho}}, \quad \text{(A3)}$$

where $\mathcal{P}(\rho_{ZB}, \tilde{\rho}_{ZB}) \leq \epsilon$.

The smooth min-entropy satisfies many entopy-like properties. For instance, we will frequently use the following chain rule

$$H_{\min}^\epsilon(A|BZ) \geq H_{\min}^\epsilon(A|B) - \log|Z|, \quad \text{(A4)}$$

where A, B are arbitrary systems (quantum or classical) and Z a classical system of dimension $|Z|$. For further properties of the smooth min-entropy, we refer the reader to [50] in the finite-dimensional and to [45, 51] in the infinite-dimensional case.

Reduction to R'enyi Entropy. We are interested in lower bounding the smooth min-entropy

$$\frac{1}{n}H_{\min}^\epsilon(Z|\theta K) \geq \lambda^\epsilon \quad \text{(A5)}$$

in which the side-information K is classical as well. Note that we omit the subscript A in Alice's measurement choice θ. Because of the maximization in the definition of the smooth min-entropy (A3), it is very difficult to bound the smooth min-entropy directly. Instead, it is easier to use that it can be related to the conditional α-Rényi entropies

$$H_\alpha(A|B)_\rho = \frac{1}{1-\alpha}\log \operatorname{tr}[\rho_{AB}^\alpha(\operatorname{id}_A \otimes \rho_B)^{1-\alpha}]. \quad \text{(A6)}$$

In particular, it holds for $\alpha \in (1, 2]$ and any two random variables X and Y that [52]

$$H_{\min}^\epsilon(X|Y) \geq H_\alpha(X|Y) - \frac{1}{\alpha-1}\log\frac{2}{\epsilon^2}, \quad \text{(A7)}$$

We present in Lemma F.1 a simple generalization of the result to unbounded classical variables X and Y. Hence, if we find a bound on the Rényi-entropies

$$\frac{1}{n}H_\alpha(Z|\theta K) \geq B^\alpha \quad \text{(A8)}$$

we obtain a lower bound on the smooth min-entropy with

$$\lambda^\epsilon = \sup_{1<\alpha\leq 2}\left(B^\alpha - \frac{1}{n(\alpha-1)}\log\frac{2}{\epsilon^2}\right). \quad \text{(A9)}$$

Moreover, as shown in [41], it suffices to find a bound $H_\alpha(Z|\theta) \geq B^\alpha$ for $n = 1$ and without K, as such a bound implies that $H_\alpha(X|\theta K) \geq n\lambda$ for strings X and Θ of any length n. This implication basically follows from the fact that the conditional Rényi entropies can be expanded as

$$2^{(1-\alpha)H_\alpha(Z|Y)} = \sum_y 2^{(1-\alpha)H_\alpha(X|Y=y)}, \quad \text{(A10)}$$

where $H_\alpha(X|Y = y)$ denotes the α-Rényi entropy of X given $Y = y$.

2. Uncertainty relation for Rényi entropy

a. Preliminaries

According to the discussion in the previous section it is sufficient to consider the case of $n = 1$ and trivial K. That is, the system A is a position-momentum system and $\theta \in \{0, 1\}$ is a uniformly distributed random variable indicating the measurement choice, i.e., $\theta = 0$ and $\theta = 1$ corresponding to X_{δ_x} and P_{δ_p}. For the sake of generality, we allow for different binning δ_x and δ_p for the coarse-grained X and P measurement.

In the following we assume that $\{I_k\}_{k\in\mathbb{N}}$ and $\{J_k\}_{k\in\mathbb{N}}$ are two partitions of $\mathbb{R}$ into intervals of constant length δx and δp, respectively. We denote the probability to measure X (P) in interval I_k (J_l) by q_k (p_l). Using the definition of the Rényi entropy together with the expansion in (A10), we find that

$$2^{(1-\alpha)H_\alpha(X|\theta)} = \frac{1}{2}\left(\sum_k q_k^\alpha + \sum_l p_l^\alpha\right). \quad \text{(A11)}$$

Given that $\alpha > 1$, an upper bound on the above sums results in a lower bound on $H_\alpha(X|\theta)$.

For simplicity, let us first consider the continuous case for $\delta_x, \delta_p \to 0$. In this case, the sums in (A11) become integrals and we obtain

$$2^{(1-\alpha)h_\alpha(X|\theta)} = \frac{1}{2}\left(\int q(x)^\alpha \mathrm{d}x + \int p(x)^\alpha \mathrm{d}x\right), \quad \text{(A12)}$$

where q and p are the probability distributions corresponding to X and P, and $h_\alpha(X|\theta)$ denotes the differential conditional Rényi entropy. While q, p are integrable functions, that is not necessarily true for q^α, p^α. Hence, it is possible that (A12) diverges when optimizing over all possible states. So, no uncertainty relation can be shown for continuous measurements.

The right hand side of (A12) can be made arbitrarily large even for Gaussian states. For a normal distribution with standard deviation σ, the differential α-Rényi entropy is

$$h_\alpha(X) = \log\left[\sqrt{2\pi}\sigma\alpha^{\frac{1}{2(\alpha-1)}}\right]. \quad \text{(A13)}$$

Hence, we obtain for a Gaussian state with standard deviation σ_X and σ_P in X and P that

$$2^{(1-\alpha)h_\alpha(X|\theta)_\rho} = (2\pi)^{(1-\alpha)/2}\alpha^{-1/2}\left(\frac{1}{\sigma_Q^{\alpha-1}} + \frac{1}{\sigma_P^{\alpha-1}}\right). \tag{A14}$$

This quantity can be made arbitrarily large by taking a sufficiently small standard deviation for either σ_Q or σ_P. However, the divergence is not a problem for coarse-grained outcomes as both of the sums in (A11) are upper bounded by 1.

In order to bound (A11), we have to use that not all possible distributions q_k and p_l are possible since they origin from measurements of the complementary observables X and P that are related via Fourier transform. This relation has been made rigorous by Landau and Pollak [44] (see also [53, Section 2.9]), who show that the probability $q[I]$ to measure X in an interval I ($a = |I|$) and the probability $p[J]$ to measure P in an interval J ($b = |J|$) have to satisfy the inequality

$$\cos^{-1}\sqrt{q[I]} + \cos^{-1}\sqrt{p[J]} \geq \cos^{-1}\sqrt{\gamma(a,b)} \tag{A15}$$

where

$$\gamma(a,b) := \frac{ab}{2\pi\hbar}S_0^{(1)}\left(1, \frac{ab}{4\hbar}\right)^2 \tag{A16}$$

with $S_0^{(1)}$ the 0th radial prolate spheroidal wave function of the first kind. For ab sufficiently small $\gamma(a,b) \approx ab/(2\pi\hbar)$.

The condition (A15) can be reformulated in the following way [53]:

i) If $0 \leq q[I] \leq \gamma(a,b)$, then all values for $p[J]$ are possible, and

ii) if $\gamma(a,b) \leq q[I]$, then $p[J] \leq g(q[I], a, b)$ for

$$g(q,a,b) := \left(\sqrt{q\gamma(a,b)} + \sqrt{(1-q)(1-\gamma(a,b))}\right)^2. \tag{A17}$$

This reformulation yields an infinite number of constraints for the probability distributions. Let us assume that $\{q_k\}_k$ and $\{p_l\}_l$ are decreasingly ordered. Then for all $M, N \in \mathbb{N}$, $\{q_k\}_k$ and $\{p_l\}_l$ have to satisfy the constraints

$$\sum_{j=1}^{N} p_{k_j} \leq g\left(\sum_{i=1}^{M} q_i, M\delta_x, N\delta_p\right). \tag{A18}$$

However, it is non-trivial to turn these constraints into an explicit and tight upper bound for (A11). In the following we discuss a particular way that connects the above constraints with a majorization approach, which leads to $\lambda_{\text{Maj}}^\epsilon$.

b. Majorization uncertainty relation

This bound follows from an idea in [27]. Let us denote by r the decreasingly ordered sequence of both probabilities $\{q_k\}$

and $\{p_l\}$. Then, the expression (A11) can be written as

$$2^{(1-\alpha)H_\alpha(X|\theta)} = \frac{1}{2}\sum_j r_j^\alpha. \tag{A19}$$

Since the function $r \mapsto \sum_j r_j^\alpha$ is Schur convex, we get an upper bound on (A11) if we find a sequence w which majorizes any physically possible sequence r. Such a w can be constructed in the following way [27].

First note that according to property ii), $q[I]+p[J] \leq q[I]+g(q[I],a,b)$, which optimized over all $0 \leq q[I] \leq 1$ is equal to $1 + \sqrt{\gamma(a,b)}$. Hence, we obtain the constraint

$$q[I] + p[J] \leq 1 + \sqrt{\gamma(a,b)}. \tag{A20}$$

This constraint implies further that

$$\sum_{j=1}^{n} r_j \leq 1 + F_n(\delta q, \delta p), \tag{A21}$$

where

$$F_n(\delta_x, \delta_p) = \max_{1 \leq k \leq n}\sqrt{c\left(k\delta_x, (n-k)\delta_p\right)}. \tag{A22}$$

Note that in the case $\delta_x = \delta_p$ the maximum is attained for $k = \lfloor \frac{n}{2} \rfloor$.

We can construct a majorizing sequence w by setting recursively

$$w_1 = 1, \text{ and } w_k = F_k - w_{k-1} \text{ for } k \geq 2. \tag{A23}$$

The obtained bound on the Rényi-entropy is

$$H_\alpha(X|\theta) \geq B_{\text{Maj}}^\alpha \tag{A24}$$

where

$$B_{\text{Maj}}^\alpha = \frac{1}{1-\alpha}\log\left(\frac{1}{2}\sum_k w_k^\alpha\right). \tag{A25}$$

By using (A9), we obtain the following bound on the smooth min-entropy

$$\lambda_{\text{Maj}}^\epsilon := \sup_{1 < \alpha \leq 2}\left(B_{\text{Maj}}^\alpha - \frac{1}{n(\alpha-1)}\log\frac{2}{\epsilon^2}\right). \tag{A26}$$

Since B_{Maj}^α depends on the recursively defined sequence w in (A23), there is no closed form and it can only be computed numerically. However, one can easily check that B^α is monotonically increasing in α, which simplifies the optimization over α required for the calculation of $\lambda_{\text{Maj}}^\epsilon$.

c. Uncertainty relation for Gaussian states

In order to obtain a tighter bound, we consider an uncertainty relation that holds for arbitrary Gaussian states or any mixture thereof. In fact, for our application it is important to allow arbitrary and even continuous mixtures of Gaussian

states. The reason is that a coarse-grained quadrature measurement with finite binning on one mode of a multi-mode Gaussian state results in a continuous mixture of Gaussian states in the remaining modes (and not in a Gaussian state itself). Since conditioning on part of the measurement outcomes on Alice's mode is needed to generalize the uncertainty relation from $n = 1$ to $n > 1$ [41], this level of generality is crucial.

Theorem A.1. *Let $\alpha \in (1, 2]$. For an arbitrary and possibly continuous convex combination of Gaussian states and coarse-grained measurements X_{δ_x} and P_{δ_p} holds that*

$$H_\alpha(Z|\theta) \geq B_{Gauss}^\alpha(\delta), \qquad (A27)$$

where

$$B_{Gauss}^\alpha(\delta_x, \delta_p) = \frac{1}{1-\alpha} \log \frac{1}{2} \left(1 + \frac{1}{\alpha} \left(\frac{\delta_x \delta_x}{\pi \hbar} \right)^{(\alpha-1)} \right) \qquad (A28)$$

Proof. We first assume that the state is a Gaussian state. Let us recall that we have to upper bound the sums in (A11). Denoting the probability density function of the continuous X measurement by $q(x)$, a simple application of Jensen's inequality results in

$$q_k^\alpha = \left(\int_{I_k} q(x) dx \right)^\alpha \leq \delta_x^{\alpha-1} \int_{I_k} q(x)^\alpha dx. \qquad (A29)$$

Hence, using the formula for the Rényi entropy of a Gaussian state (A13), we find for a state with standard deviation σ_X for the X measurement that

$$\sum_k q_k^\alpha \leq \delta^{\alpha-1} \int q(x)^\alpha dx = g(\tilde{\sigma}_X), \qquad (A30)$$

where $\tilde{\sigma}_X = \sigma_X/\delta_X$ is the relative standard deviation and

$$g(x) = \frac{1}{\sqrt{\alpha}(\sqrt{2\pi}x)^{\alpha-1}}. \qquad (A31)$$

Note that the bound $g(\tilde{\sigma}_X)$ becomes very bad if $\tilde{\sigma}_X$ is very small. In particular, it can exceed the trivial upper bound on $\sum_k q_k^\alpha$ given by 1. We avoid that problem by simply bounding

$$\sum_k q_k^\alpha \leq \min\{g(\tilde{\sigma}_X), 1\}. \qquad (A32)$$

Let us use that the standard deviations of the X and P distribution satisfy $\sigma_X \sigma_P \geq \hbar/2$, which translates into $\tilde{\sigma}_X \tilde{\sigma}_P \geq \hbar/(2\delta_x \delta_p)$ for the relative standard deviations. For the following it is convenient to define $\tilde{\hbar} := \hbar/(\delta_x \delta_p)$. Given that we want to maximize the quantity over all Gaussian states, we can without loss of generality assume that $\tilde{\sigma}_X \geq \tilde{\hbar}/\sqrt{2}$ and that $\tilde{\sigma}_P = \tilde{\hbar}/(2\tilde{\sigma}_X) \leq \tilde{\sigma}_X$. A straightforward calculation then results in

$$\sum_k q_k^\alpha + \sum_k p_k^\alpha \leq \min\{g(\tilde{\sigma}_X), 1\} + \min\{g(\tilde{\sigma}_P), 1\}$$

$$\leq \begin{cases} g(\tilde{\sigma}_X) + g(\tilde{\sigma}_P) & \text{if } \tilde{\sigma}_X \leq \tilde{\hbar}\sqrt{\frac{\pi}{2}}\alpha^{\frac{1}{2(\alpha-1)}}, \\ 1 + g(\tilde{\sigma}_X) & \text{otherwise.} \end{cases}$$

One can check easily that $g(\tilde{\sigma}_X) + g(\tilde{\hbar}/(2\tilde{\sigma}_X))$ is monotonically increasing in $\tilde{\sigma}_X$, and $1 + g(\tilde{\sigma}_X)$ is monotonically decreasing in $\tilde{\sigma}_X$. Hence, the maximum of the right hand side is attained exactly for $\tilde{\sigma}_X = \tilde{\hbar}\sqrt{\frac{\pi}{2}}\alpha^{\frac{1}{2(\alpha-1)}}$. Plugging this value in, we obtain that

$$\sum_k q_k^\alpha + \sum_k p_k^\alpha \leq 1 + \frac{1}{\alpha} \left(\frac{1}{\pi} \right)^{\alpha-1} \left(\frac{(\delta_x \delta_p)}{\hbar} \right)^{(\alpha-1)}, \qquad (A33)$$

which finishes the proof for Gaussian states.

Let us now assume that the state is given by $\rho = \int_Y d\mu(y)p(y)\rho^y$ with $(Y, d\mu)$ a sigma-finite measure space, p a probability distribution over Y and ρ^y a Gaussian state for any y. It then follows that the X measurement maps ρ to an element of $L^1(\mathbb{R})$ that can be written as $\rho_Q = \int_Y d\mu(y)p(y)\rho_Q^y$ with ρ_Q^y the Gaussian distribution of the position of ρ^y. The same holds for the P measurement. It thus follows that

$$\sum_k \left(\int_{I_k} dx \int_Y d\mu(y)p(y)\rho_Q^y(x) \right)^\alpha \qquad (A34)$$

$$= \sum_k \left(\int_Y d\mu(y)p(y) \int_{I_k} dx\rho_Q^y(x) \right)^\alpha \qquad (A35)$$

$$\leq \sum_k \int_Y d\mu(y)p(y) \left(\int_{I_k} dx\rho_Q^y(x) \right)^\alpha \qquad (A36)$$

$$= \int_Y d\mu(y)p(y) \sum_k \left(\int_{I_k} dx\rho_Q^y(x) \right)^\alpha, \qquad (A37)$$

where the two equalities follow from Fubini's theorem (since all integrals and sums are bounded) and the inequality from the convexity of the function $x \mapsto x^\alpha$ on the non-negative reals (for $\alpha \in (1, 2]$). Thus, by the linearity of the integral we obtain the desired result. $\square$

Similar to the majorization uncertainty relation, we get a bound on the smooth min-entropy via (A9)

$$\frac{1}{n}H_{\min}^\epsilon(Z|\theta K) \geq \lambda_{\text{Gauss}}^\epsilon(\delta_x, \delta_p, n), \qquad (A38)$$

with

$$\lambda_{\text{Gauss}}^\epsilon(\delta_x, \delta_p, n) := \sup_\alpha \left(B_{\text{Gauss}}^\alpha(\delta_x, \delta_p) - \frac{1}{n(\alpha - 1)} \log \frac{2}{\epsilon^2} \right). \qquad (A39)$$

Let us show that the performance of the inequality in the asymptotic limit is optimal in the sense that it converges to the bound obtained for the Shannon entropy. In order to do so, we consider the limit

$$\lim_{\epsilon \to 0} \lim_{n \to \infty} \lambda_{\text{Gauss}}^\epsilon(\delta_x, \delta_p, n) = \lim_{\alpha \to 1} B_{\text{Gauss}}^\alpha(\delta_x, \delta_p), \qquad (A40)$$

where we used that $B_{\text{Gauss}}^\alpha(\delta_x, \delta_p)$ is independent of n and monotonically decreasing in α. A straightforward calculation yields that

$$\lim_{\alpha \to 1} B_{\text{Gauss}}^\alpha(\delta_x, \delta_p) = -\frac{1}{2} \log c(\delta_x, \delta_p), \qquad (A41)$$

where $c(\delta_x, \delta_p) := \delta_x \delta_p/(\pi e \hbar)$ is the uncertainty bound for the Shannon entropy, i.e., $H(X|\theta) \geq -(1/2) \log c(\delta_x, \delta_p)$ [43].

Intuitively, the reason for this convergence is that we use Jensen inequality (A29) to bound the discrete entropy to the differential entropy, i.e., $H_\alpha(X_\delta) \geq h_\alpha(X) - \log \delta$, together with the fact that the uncertainty relation for differential Shannon entropies [54, 55] becomes an equality for any pure Gaussian state. Hence, for the limit case $\alpha \to 1$, we simply obtain

$$2H(X_\delta|\theta) = H(Q_\delta) + H(P_\delta) \qquad (A42)$$
$$\geq h(Q) + h(P) - \log \delta^2 \qquad (A43)$$
$$\geq -\log \pi e \hbar - \log \delta^2 \qquad (A44)$$
$$= -\log c(\delta), \qquad (A45)$$

where we used $\delta_Q = \delta_P = \delta$ for simplicity.

3. Uncertainty relation under iid assumption

The following bound is based on the property that the smooth min-entropy of n independent and identically distributed (iid) random variables converges to the Shannon entropy in the asymptotic limit [33]. We use a result derived in [52], which for iid random variables X^n and Y^n reads as

$$\frac{1}{n} H_{\min}^\epsilon(X^n|Y^n) \geq H(X|Y) - \frac{4}{\sqrt{n}} \log(\eta(X)_\rho)^2 \sqrt{\log \frac{2}{\epsilon^2}} \qquad (A46)$$

where $\eta(X) = 2 + 2^{H_{1/2}(X)_\rho/2}$. The above result holds also for random variables over infinite alphabets if $H(X) < \infty$ [45]. The crucial point for the application of the inequality in (A46) is that the correction term beside the Shannon entropy is independent of the conditioning variable Y.

Let us assume that Bob produces an ensemble of n-mode states according to an independent and identical distribution (iid) over only m modes such that the state on A and K has the form $\rho_{A^n K^n} = (\sigma_{A^m K^m})^{\otimes n/m}$, where we assume that $n/m \in \mathbb{N}$. Then, also the random variable Z^n obtained by measuring randomly either X_{δ_x} or P_{δ_p} has the same structure. Applying the inequality (A46), we obtain that

$$\frac{1}{n} H_{\min}^\epsilon(Z^n|\theta^n K^n) \geq \frac{1}{m} H(Z^m|\theta^m K^m) \qquad (A47)$$
$$- 4\sqrt{\frac{m}{n}} \log(\eta(Z^m))^2 \sqrt{\log \frac{2}{\epsilon^2}}. \qquad (A48)$$

At this point, we can simply use the uncertainty relation for the Shannon entropy [43]

$$H(Z^m|K^m\Theta = \theta) + H(Z^m|K\Theta = \bar{\theta}) \geq -m \log c(\delta_x, \delta_p), \qquad (A49)$$

where $\bar{\theta} = (1 - \theta_i)_{i=1}^m$ denotes the complementary basis

choice of $\theta = (\theta_i)_{i=1}^m$. This inequality implies that

$$H(Z^m|\Theta K)$$
$$= \frac{1}{2^m} \sum_\theta \frac{1}{2} \left(H(Z^m|K\Theta = \theta) + H(Z^m|K\Theta = \bar{\theta}) \right)$$
$$\geq -\frac{m}{2} \log c(\delta_x . \delta_p).$$

Hence, we obtain the uncertainty relation

$$\frac{1}{n} H_{\min}^\epsilon(Z^n|\theta^n K^n) \geq \lambda_{\text{IID}}^\epsilon(\delta, m, n), \qquad (A50)$$

where

$$\lambda_{\text{IID}}^\epsilon(\delta, m, n) = -\frac{1}{2} \log c(\delta_x, \delta_p) \qquad (A51)$$
$$- 4\sqrt{\frac{m}{n}} \log(\eta(Z^m))^2 \sqrt{\log \frac{2}{\epsilon^2}}. \qquad (A52)$$

Note that even though the right-hand side still depends on the distribution of Z^m, it is not conditioned on K and Alice can estimate it. Particularly, in the application to oblivious transfer or bit commitment, we can assume that Alice distributes the average ensemble state, and thus, knows the distribution over Z by herself. Note further that $\log(\eta(Z^m)) = \mathcal{O}(m)$ such that

$$\lambda_{\text{IID}}^\epsilon(\delta, m, n) = -\frac{1}{2} \log c(\delta_x, \delta_p) - \mathcal{O}(m^2\sqrt{\frac{m}{n}}). \qquad (A53)$$

Similarly to when we restricted to Gaussian states, we find that in the asymptotic limit, the bound converges to $-1/2 \log c(\delta_x, \delta_p)$.

Appendix B: Oblivious Transfer

1. Composable security definitions

In the following, we denote random variables by capital letters, e.g., S_0, S_1 for Alice's output. The uniform distribution of a random variable X is denoted by τ_X and the classically maximally correlated state of two random variables X and Y with same range by Ω_{XY}, i.e., $\Omega_X = \tau_X$, $\Omega_Y = \tau_Y$, and $\Omega_{X|Y=y} = \delta_{x,y}$. Moreover, we set $[n] = \{1, 2, ..., n\}$ and $\bar{x} = 1 - x$ for any binary variable x.

We use the composable security definitions from [16].

Definition B.1. *A protocol between two parties Alice and Bob that takes input T in $\{0, 1\}$ from Bob and outputs on Alice's side two bit strings S_0, S_1 in $\{0, 1\}^\ell$ and on Bob's side $\tilde{S}$ in $\{0, 1\}^\ell$ is called an $(\epsilon_C, \epsilon_A, \epsilon_B)$-secure (sender-randomized) OT^ℓ protocol if the following conditions hold:*

- *The protocol is ϵ_C-correct. That is, if both parties follow the protocol, then the output of the protocol $\rho_{S_0 S_1 \tilde{S} T}$ satisfies for $t \in \{0, 1\}$*

$$\|\rho_{S_0 S_1 \tilde{S}|T=t} - \tau_{S_{\bar{t}}} \otimes \Omega_{S_t \tilde{S}}\|_1 \leq \epsilon_C. \qquad (B1)$$

- *The protocol is ϵ_A-secure for Alice. That is, if Alice follows the protocol, then for any strategy of Bob with output $\rho_{S_0 S_1 B'}$, where B' denotes Bob's register at the end of the protocol, there exists a random variable D with range $\{0, 1\}$ such that*

$$\| \rho_{S_{\bar{D}} S_D D B'} - \tau_{S_{\bar{D}}} \otimes \rho_{S_D D B'} \|_1 \leq \epsilon_A. \qquad (B2)$$

- *The protocol is ϵ_B-secure for Bob. That is, if Bob follows the protocol, then for any strategy of Alice with output A', resulting in the joint output state $\rho_{A' \tilde{S} T}$, there exist random variables S_0', S_1' such that $\rho_{A' S_0' S_1' \tilde{S} T}$ satisfies $\Pr[\tilde{S} \neq S_T'] \leq \epsilon_B$ and*

$$\| \rho_{A' S_0' S_1' | T=0} - \rho_{A' S_0' S_1' | T=1} \|_1 \leq \epsilon_B. \qquad (B3)$$

2. Security analysis for oblivious transfer

The conditions for correctness are that $\tilde{S}$ is with high probability equal to S_t and that $S_0 S_1$ are uniformly distributed. The first condition relies on the error-correction protocol. We assume in the following that the procedure manages to correct the error with probability ϵ_{EC}. The second condition follows from the security definition for Alice (B2) by using the monotonicity of the trace norm. Hence, if security for Alice holds with ϵ_A, correctness holds with at least $\epsilon_C = \epsilon_{EC} + 2\epsilon_A$.

Security for Bob holds since he only sends the sets I_0, I_1 during the entire protocol, which due to the random choice of the measurement by Bob are independent of t. This has been made precise in [14].

Let us consider security for Alice. Recall that Bob's memory attack is given by an encoding $\mathcal{E}$ mapping the n modes to systems Q_{in} and K, where Q_{in} is the input of his memory channel $\mathcal{M} = \mathcal{F}^{\otimes \nu n}$ and K some additional classical information. Hence, after completing the entire protocol, Bob's system is given by $B' = Q_{out} B_{cl}$, where $Q_{out} = \mathcal{M}(Q_{in})$ and $B_{cl} = \theta_A K W H C$ all his classical information. Here, $W = (W_0, W_1)$ denotes the error-correction information, and $H = (F_0, F_1)$ the 2-universal hash functions used for privacy amplification.

According to (B2), we have to show that there exists a random variable D such that

$$\| \rho_{S_D S_{\bar{D}} D Q_{out} B_{cl}} - \tau_{S_D} \otimes \rho_{S_{\bar{D}} D Q_{out} B_{cl}} \|_1 \leq \epsilon_A. \qquad (B4)$$

The privacy amplification lemma [33, 56] against infinite-dimensional quantum adversaries [51] tells us that (B4) is satisfied for

$$\ell \geq H_{\min}^{\epsilon_1}(Z_D | S_{\bar{D}} D Q_{out} B_{cl}) - 2 \log \frac{1}{\epsilon_A - 4\epsilon_1}, \qquad (B5)$$

with $\epsilon_1 \geq 0$ arbitrary such that $\epsilon_A \geq 4\epsilon_1$.

Hence, it remains to find a tight lower bound on the smooth min-entropy $H_{\min}^{\epsilon_1}(Z_D | S_{\bar{D}} D Q_{out} B_{cl})$. For this purpose we follow similar arguments as in [16, 23]. Therein, a central ingredient is a bound of the smooth min-entropy $H_{\min}(U | \mathcal{M}(Q_{in})V)$ with U, V classical and $\mathcal{M}$ a quantum

channel by the success probability to send classical information at a rate R through $\mathcal{M}$

$$\mathcal{P}_{succ}^{\mathcal{M}}(nR) := \sup_{\rho_k, D_k} \frac{1}{2^{nR}} \sum_k \mathrm{tr}(D_k \mathcal{M}(\rho_k)), \qquad (B6)$$

where the supremum runs over ensembles of code states $(\rho_k)_{k=1}^{nR}$ and POVM's $(D_k)_{k=1}^{nR}$ acting as a decoder. It has been shown in [16] that (see also Lemma F.2)

$$H_{\min}^{\epsilon + \epsilon'}(U | \mathcal{M}(Q_{in})V) \geq -\log \mathcal{P}_{succ}^{\mathcal{M}}\left(\lfloor H_{\min}^{\epsilon}(U | V)_\rho - \log \frac{1}{\epsilon'^2} \rfloor \right). \qquad (B7)$$

Applying the chain rule (A4), we first bound

$$H_{\min}^{\epsilon_1}(Z_D | S_{\bar{D}} D Q_{out} B_{cl}) \geq H_{\min}^{\epsilon_1}(Z_D | D Q_{out} B_{cl}) - \ell,$$

where we used that $\log |S_{\bar{D}}| = \ell$. The smooth min-entropy $H_{\min}^{\epsilon_1}(Z_D | D Q_{out} B_{cl})$ on the right hand side can then be lower bounded by means of inequality (B5) by

$$-\log \left(\mathcal{P}_{succ}^{\mathcal{M}}\left(\lfloor H_{\min}^{\epsilon_2}(Z_D | D B_{cl}) - \log \frac{1}{(\epsilon_1 - \epsilon_2)^2} \rfloor \right) \right).$$

Plugging the bounds in (B5) and solving for ℓ, one easily finds that (B4) is satisfied if we choose ℓ smaller or equal to

$$-\frac{1}{2} \log \left(\mathcal{P}_{succ}^{\mathcal{M}}\left(\lfloor H_{\min}^{\epsilon_2}(Z_D | D B_{cl}) - \log \frac{1}{(\epsilon_1 - \epsilon_2)^2} \rfloor \right) \right) - \log \frac{1}{\epsilon_A - 4\epsilon_1}.$$

The goal of the next part is to lower bound the smooth min-entropy $H_{\min}^{\epsilon_2}(Z_D | D B_{cl})$. For that lower bound, we use the min-entropy splitting theorem [14], (see also Lemma F.3), which tells us that there exists a random variable D such that

$$H_{\min}^{\epsilon}(Z_D | D B_{cl}) \geq \frac{1}{2} H_{\min}^{\epsilon}(Z_0 Z_1 | B_{cl}) - 1. \qquad (B8)$$

Given that Bob's classical register B_{cl} is given by $\theta_A K W H C$, we finally get via (A4) that

$$H_{\min}^{\epsilon}(Z_0 Z_1 | B_{cl}) \geq H_{\min}^{\epsilon}(Z_0 Z_1 | \theta_A K) - \log |W| - \log |C|$$
$$\geq H_{\min}^{\epsilon}(Z_0 Z_1 | \theta_A K) - \ell_{EC} - 2 \log \frac{1}{\epsilon_C},$$

where $\ell_{EC} = \log |W|$, and we used that the hash functions are drawn independently at random.

Concluding the above discussion, we arrive at the following bound on the length of the string that enables security for Alice.

Theorem B.2. *Let us assume that $H_{\min}^{\epsilon}(Z | K\theta) \geq n\lambda_\epsilon(n)$ and Bob's memory channel is given by $\mathcal{M}$. Then the protocol for OT consisting of steps (Q1)-(Q3) followed by (OT1)-(OT3) is ϵ_A-secure for Alice if*

$$\ell = -\frac{1}{2} \log \mathcal{P}_{succ}^{\mathcal{M}}\left(\lfloor n r_{OT} \rfloor \right) - \log \frac{1}{\epsilon_A - 4\epsilon_1}, \qquad (B9)$$

where

$$r_{OT} := \lambda_{\epsilon_2}(n) - r_{EC} - \frac{1}{n}\left(2\log\frac{1}{\epsilon_C} - \log\frac{1}{(\epsilon_1 - \epsilon_2)^2} - 1\right)$$
(B10)

and $\epsilon_1, \epsilon_2 \geq 0$ arbitrary such that $\epsilon_A > 4\epsilon_1 > 4\epsilon_2$.

Note that when the right-hand side of (B9) is negative, a secure implementation of the OT protocol is not possible.

Let us consider the case where Bob's quantum channel $\mathcal{F}$ is such that the success probability to send classical bits above the classical capacity $\mathcal{C}_{cl}(\mathcal{F})$ decreases exponentially

$$\mathcal{P}_{succ}^{\mathcal{F}^{\otimes n}}(nR) \leq 2^{-n\xi(R - \mathcal{C}_{cl}(\mathcal{F}))}.$$
(B11)

This property is generally referred to as *strong converse* for the classical capacity. Note that for channels $\mathcal{F}$ for which it is only known that property (B11) is satisfied for a rate $C_{sc} > \mathcal{C}_{cl}(\mathcal{F})$ usually referred to as a strong converse capacity of $\mathcal{F}$, the following discussion holds similarly with $\mathcal{C}_{cl}(\mathcal{F})$ replaced by C_{sc}.

A simple calculation shows that if Bob's memory is of the form $\mathcal{M} = \mathcal{F}^{\otimes \nu n}$ and (B11) holds, then the condition

$$`r_{OT} > \nu\mathcal{C}_{cl}(\mathcal{F})$$
(B12)

is sufficient to obtain security for a large enough n. Moreover the length of the strings s_0, s_1 can be chosen as

$$\ell = n\xi(r_{OT} - \mathcal{C}_{cl}(\mathcal{F})).$$
(B13)

A necessary condition for security is thus

$$1/2(\lambda^\epsilon - r_{EC}) > 0.$$
(B14)

Let us analyse the above condition in the asymptotic limit. We know according to (A41) and (A53) that λ_{Gauss}^ϵ and λ_{IID}^ϵ converge to $-1/2\log c(\delta)$, where we assume in the following for simplicity that $\delta_x = \delta_p = \delta$. Using the exponential deFinetti theorem or the post-selection technique applied to CV protocols [57, 58], it is easy to convince oneself that this bound holds in the asymptotic limit without any assumptions (e.g., Gauss or iid). This insight yields the asymptotic formula $\lambda_{as}(\delta) := -1/2\log c(\delta)$.

The error-correction rate in the asymptotic scenario is given according to the Slepian-Wolf theorem [59] as the conditional Shannon entropy $H(X_\delta^A | X_\delta^B)$, where X_δ^A (X_δ^B) is the outcome of Alice's (Bob's) coarse-grained X measurement. We assume here that the state is symmetric with respect to X and P. This assumption is reasonable because if both parties are honest, the state is an EPR state with one-sided loss. Let us denote the conditional variance of X^A given X^B by $V_{A|B}$ [60]. Then, if $\delta \ll V_{A|B}$, we find with good approximation that $r_{EC} = H(X_\delta^A | X_\delta^B) \approx h(X^A | X^B) - \log\delta$, where $h(X^A | X^B)$ is the conditional differential Shannon entropy of X^A given X^B. Hence, we obtain

$$\lambda_{as} - r_{EC} \approx \log\sqrt{e\pi} - h(X^A | X^B)$$
$$= \log\sqrt{e\pi\hbar} - \log\left(\sqrt{2\pi e V_{A|B}}\right)$$
$$= \log\left(\sqrt{\frac{\hbar}{2V_{A|B}}}\right).$$

In order to satisfy (B14), we need that $V_{A|B} < \sqrt{\hbar/2}$. Given a Gaussian state with covariance matrix as in (D1) (that is, an EPR state with one-sided losses $1 - \tau$ and $\xi = 0$), the condition above reads as ($\hbar = 2$)

$$V_{A|B} = \frac{(1-\tau)V + \tau}{(1-\tau) + \tau V} < 1.$$
(B15)

Since $V \geq 1$, the condition can only be satisfied if the transmissivity $\tau > 1/2$ and for a non-trivial squeezing $V > 1$.

Appendix C: Bit commitment

1. Security definitions

Let us first introduce the notation. In the bit commitment phase, Bob inputs a bit C to which he commits. In the open phase Alice outputs a bit $\tilde{C}$ and a flag F, where $F \in \{accept, reject\}$ depending whether Alice accepts or rejects the commitment.

We use composable security definitions adapted from [16].

Definition C.1. *A protocol between two parties Alice and Bob that consists of a commitment phase where Bob commits to a bit C and an open phase in which Alice outputs $\tilde{C}$ and a flag $F \in \{accept, reject\}$ is called an $(\epsilon_C, \epsilon_H, \epsilon_B)$-secure bit commitment protocol if the following conditions hold:*

- *The protocol is ϵ_C-correct. That is, if both parties are honest, then it holds that $\Pr[\tilde{C} \neq C \mid F = accept] \leq \epsilon_C$ and $\Pr[F = reject] \leq \epsilon_C$.*

- *The protocol is ϵ_H-hiding. That is, if Bob is honest then for any strategy of Alice with joint output state $\rho_{A'C}$, it holds after the commitment phase that*

$$\|\rho_{A'|C=0} - \rho_{A'|C=1}\|_1 \leq \epsilon_H.$$
(C1)

- *The protocol is ϵ_B-binding. That is, if Alice is honest, then for any strategy of Bob, there exists after the commitment phase a random variable D in $\{0, 1\}$ such that for any value D' that Bob wants to convince Alice to accept, it holds that*

$$\Pr[D' \neq D \mid F = accept] \leq \epsilon_B.$$
(C2)

2. Security analysis for bit commitment

It is easy to see that the BC protocol is correct. The first condition $\Pr[\tilde{C} \neq C \mid F = accept] \leq \epsilon_C$ is satisfied due to the definition of the protocol. The second condition holds for sufficiently large n due to the properties of typical sets. The protocol is perfectly hiding as Bob does not send any information to Alice during the commitment phase. So, the interesting case is to show that the protocol is binding as long as Bob's quantum memory satisfies some constraints. We start with a lemma.

Lemma C.2. *Let ρ_{XU} be an arbitrary state on X and U, where X is a classical system with alphabet $\mathcal{X}$ and U is arbitrary (possibly quantum). Moreover, let $B(x) \subset \mathcal{X}$ for $x \in \mathcal{X}$. Then for all $\epsilon \geq 0$, the optimal probability to correctly guess Y in $B(X)$ given the system U is upper bounded by*

$$\sup_{\mathcal{E}} \mathbb{P}_\rho[\mathcal{E}(U) \in B(X)] \leq \max_y |B^{-1}(y)| 2^{-H_{\min}^\epsilon(X|U)} + 2\epsilon,$$
(C3)

where $B^{-1}(y) = \{x \,|\, y \in B(x)\}$ and the supremum runs over all channels $\mathcal{E}$ that map U to $\mathcal{X}$.

Proof. We consider first the case $\epsilon = 0$. Let $Y = \mathcal{E}(U)$ for an arbitrary channel $\mathcal{E}$ with range $\mathcal{X}$, and $p(x, y)$ the corresponding joint distribution of X and Y. We then compute

$$\begin{aligned}
&\mathbb{P}_\rho[Y \in B(X)] \\
&= \sum_{x,y} \delta(y \in B(x))p(x,y) \\
&= \sum_y p(y) \sum_x \delta(y \in B(x))p(x|y) \\
&\leq \sum_y p(y) \max_{x'} p(x'|y) \max_{y'} \sum_x \delta(y' \in B(x)) \\
&= \max_{y'} |B^{-1}(y')| \sum_y p(y) 2^{-H_{\min}(X|Y=y)} \\
&= \max_y |B^{-1}(y)| 2^{-H_{\min}(X|Y)_\rho} \\
&\leq \max_y |B^{-1}(y)| 2^{-H_{\min}(X|U)_\rho} .
\end{aligned}$$

In the third equality, we used that the min-entropy of a distribution $q(x)$ is $-\log \max_x q(x)$, the forth equality uses a basic property of the classical conditional min-entropy, and the last inequality is due to the data-processing inequality $H_{\min}(X|U) \leq H_{\min}(X|\mathcal{E}(U))$ (see e.g. [50]). Since the upper bound holds for any $\mathcal{E}$ and is independent of $\mathcal{E}$, we can also take the supremum over all $\mathcal{E}$ concluding the result for $\epsilon = 0$.

In order to generalize the above estimate to $\epsilon > 0$, we take an arbitrary state $\tilde{\rho}_{XU}$ such that $\mathcal{P}(\rho_{XU}, \tilde{\rho}_{XU}) \leq \epsilon$. We denote the joint probability distribution obtained by applying an arbitrary strategy $\mathcal{E}$ on ρ_{XU} and $\tilde{\rho}_{XU}$ by $p(x, y)$ and $\tilde{p}(x, y)$, respectively. We then compute that

$$\begin{aligned}
\mathbb{P}_\rho[Y \in B(X)] &= \sum_{x,y} \delta(y \in B(x))p(x,y) \\
&= \sum_{x,y} \delta(y \in B(x))\tilde{p}(x,y) \\
&\quad + \sum_{x,y} \delta(y \in B(x))(p(x,y) - \tilde{p}(x,y)) \\
&\leq \max_y |B^{-1}(y)| 2^{-H_{\min}(X|U)_{\tilde{\rho}}} \\
&\quad + \|\rho_{XY} - \tilde{\rho}_{XY}\|_1 ,
\end{aligned}$$

where the last inequality follows from the result for $\epsilon = 0$ applied to $\tilde{\rho}_{XU}$, and $\rho_{XY} = \mathcal{E}(\rho_{XU})$ and similar for $\tilde{\rho}_{XY}$. Due to the monotonicity of the trace norm under channels, we

have that $\|\rho_{XY} - \tilde{\rho}_{XY}\|_1 \leq \|\rho_{XU} - \tilde{\rho}_{XU}\|_1$. Finally, by using that for any two states σ and η, the purified distance satisfies $\|\sigma - \eta\|_1 \leq 2\mathcal{P}(\sigma, \eta)$, and by taking the minimum over all states $\tilde{\rho}_{XU}$ with $\mathcal{P}(\rho_{XU}, \tilde{\rho}_{XU}) \leq \epsilon$, we arrive at the desired inequality. □

In the following, additional to (Q1)-(Q3) and (BC1), we assume that Alice sets F=reject also if the condition $n/2 - \varepsilon' \leq |I| \leq n/2 + \varepsilon'$ is violated. Moreover, we define a general verification set $B_{\epsilon_C}^m(Z_I)$, where $m = |Z_I|$ indicates the length of the string and ϵ_C the probability that Y_I is in $B_{\epsilon_C}^m(Z_I)$. We discuss the proper choice of the verification set $B_{\epsilon_C}^m(Z_I)$ as the set of typical subsequences after the proof of the following theorem.

Theorem C.3. *Let us assume that $H_{\min}^\epsilon(Z|K\theta) \geq n\lambda_\epsilon(n)$ and Bob's memory channel is given by $\mathcal{M}$. Then, the BC protocol with verification set $B_{\epsilon_C}^m(z)$, $z \in \mathcal{X}^m$, is ϵ_B-binding with*

$$\epsilon_B \leq V_{\epsilon_C}^{\varepsilon'} \mathcal{P}_{succ}^{\mathcal{M}} \left(\left\lfloor \frac{n}{2}\lambda_{\epsilon_1}(n) - \log \frac{1}{(\epsilon_2 - \epsilon_1)^2} - 1 \right\rfloor \right) + 2\epsilon_2$$
(C4)

where $V_{\epsilon_C}^{\varepsilon'} := \max_y |[B_{\epsilon_C}^{n/2+\varepsilon'}]^{-1}(y)|$ and $\epsilon_B/2 > \epsilon_2 > \epsilon_1 \geq 0$ arbitrary.

Proof. We use the same notation as in the proof for OT and denote Bob's system after the commitment phase by $B' = Q_{out}K$ where K is a classical register and $Q_{out} = \mathcal{M}(Q_{in})$. Let us denote by Z_0 and Z_1 the substrings of Z in which Alice chose basis 0 and 1, respectively. According to (C2), we have to show that there exists a random variable D such that the probability that Bob convinces Alice that his commitment was $\bar{D}$ is smaller than ϵ_B. Let us denote Bob's system after the commitment phase by B' and his opening strategy by $\mathcal{E}$ from B' to $\mathcal{Z}$. Since Alice accepts only if Bob can answer correctly with a string $Y = \mathcal{E}(B')$ in $B_{\epsilon_C}(Z_{\bar{D}})$, the probability can be bounded by Lemma C.2 as

$$\begin{aligned}
\mathbb{P}[\mathcal{E}(B') \in B_{\epsilon_C}(X_{\bar{D}})|F = \text{accept}] &\leq V_{\epsilon_C}^{\varepsilon'} 2^{-H_{\min}^\epsilon(X_{\bar{D}}|B'D)} \\
&\quad + 2\epsilon ,
\end{aligned}$$

where we used that $V_{\epsilon_C}^{\varepsilon'} \geq \max_y |[B_{\epsilon_C}^{|Z_D|}]^{-1}(y)|$. Hence, it remains to find a lower bound on $H_{\min}^\epsilon(Z_{\bar{D}}|B'D)$. For that we follow a similar strategy as in the proof of OT.

In order to define the random variable D, we use the min-entropy splitting theorem (Lemma F.3). This lemma tells us that there exists a random variable D such that

$$H_{\min}^\epsilon(Z_{\bar{D}}|DK\theta_A) \geq \frac{1}{2} H_{\min}^\epsilon(Z_0 Z_1|K\theta_A) - 1 . \quad \text{(C5)}$$

This technique allows us to define a state $\rho_{Z_D K Q_{out} D}$ such that $\rho_{Z_D K Q_{out}(D=d)} = \rho_{Z_d K Q_{out}}$. We then bound the smooth min-entropy of this state by using (B7) (see also Lemma F.2)

$$\begin{aligned}
&H_{\min}^\epsilon(Z_{\bar{D}}|K\mathcal{M}(Q_{in})\theta_A D) \\
&\geq -\log\left(\mathcal{P}_{succ}^{\mathcal{M}} \left(\left\lfloor H_{\min}^{\epsilon_1}(Z_{\bar{D}}|K\theta_A D) - \log \frac{1}{(\epsilon - \epsilon_1)^2} \right\rfloor \right) \right) ,
\end{aligned}$$

which concludes the proof by setting $\epsilon = \epsilon_2$. □

Let us assume that the memory channel satisfies a strong converse similar to (B11) given by

$$\mathcal{P}_{\mathrm{succ}}^{\mathcal{F}^{\otimes \nu n}}(nR) \leq 2^{-n\xi(R-\nu C(\mathcal{F}))}. \qquad (C6)$$

According to Theorem C.3, we obtain an ϵ_B-binding protocol if $\epsilon_B - 2\epsilon_2$ is smaller than

$$2^{-n\left[(\xi/2)(\lambda_{\epsilon_1}(n)-(1/n)\log\frac{1}{(\epsilon_1-\epsilon_2)^2}-1/n)-\log V_\varepsilon^{\varepsilon'}/n-C(\mathcal{F})\right]}.$$

Hence, the necessary condition for obtaining security for sufficiently large n is given by

$$\frac{\xi}{2}\lambda_{\epsilon_1}(n)(\delta_x) - \frac{\log V_\varepsilon^{\varepsilon'}}{n} - \nu C(\mathcal{F}) \qquad (C7)$$

$$-\frac{1}{n}(\log\frac{1}{(\epsilon_B-2\epsilon_2)(\epsilon_1-\epsilon_2)^2}+1) > 0, \qquad (C8)$$

where ϵ_1, ϵ_2 can be chosen arbitrarily according to $\epsilon_B/2 > \epsilon_2 > \epsilon_1 \geq 0$.

The canonical choice for the verification set $B_\varepsilon^m(z)$ is the set of ε-typical sequences corresponding to the output on Bob's side if Alice's outcome is z. Let us now assume that the state shared by Alice and Bob is given by an EPR state where Bob's mode is sent through a fiber with transmissivity τ. Thus, it is of form (D1). Then the outcome X^A of a continuous X measurement on Alice's side relates to Bob's outcome X^B of an X measurement by

$$X^B = \sqrt{\tau}X^A + \mathcal{N}(V_{B|A}), \qquad (C9)$$

where $V_{B|A}$ denotes the conditional variance of X^B given X^A (which is independent of X^A for (D1)), and $\mathcal{N}(V)$ denotes the normal distribution centered at 0 with variance V. It follows that $1/\sqrt{\tau}X^B - X^A$ is distributed according to $\mathcal{N}(V_{B|A}/\tau)$. Hence, in the case of continuous measurements, the typical set corresponds to the typical set of the normal distribution $\mathcal{N}(V_{B|A}/\tau)$. Note that the state considered here is symmetric in X and P.

Alice and Bob measure coarse-grained versions of X_A and X_B. In order to re-scale Bob's outcome directly, it is convenient to choose different discretizations for Alice and Bob given by $\delta_A = \delta$ and $\delta_B = \sqrt{\tau}\delta$. Then Bob's discretized outcome is distributed according to the discretization of $X_A + \mathcal{N}(V_{B|A}/\tau)$ with binning δ. Hence, the verification set is translation invariant and given by $B_\varepsilon^m(z) = z + T_\varepsilon^m(V_{B|A}/\tau, \delta)$, where $T_\varepsilon^m(V_{B|A}/\tau, \delta)$ denotes the ε-typical sequences of length m sampled according to the discretized normal distribution $\mathcal{N}(V_{B|A}/\tau)$ with binning δ.

We are interested in the inverse set $[B_\varepsilon^m]^{-1}(y)$, which due to the appropriate scaling of Bob's outcome is equal to $B_\varepsilon^m(z)$. Note that the size of the set of ε-typical sequences of length m of a random variable W is upper bounded by $2^{n(H(W)+\varepsilon)}$. Since the distribution of $X_{\sqrt{\tau}\delta}^B$ conditioned on X_δ^A is independent of the value of X_δ^A, we have that the entropy of the conditional distribution for a fixed value of X_δ^A is equal to the average over all values of X_δ^A. This then implies that $\log T_\varepsilon^m(V_{B|A}/\tau, \delta) = n(H(X_{\sqrt{\tau}\delta}^B|X_\delta^A)+\varepsilon)$, which

yields

$$V_\varepsilon^{\varepsilon'} = (\frac{n}{2} + \varepsilon')(H(X_{\sqrt{\tau}\delta}^B|X_\delta^A) + \varepsilon). \qquad (C10)$$

As in the case of OT, let us consider condition (C7) in the asymptotic limit, i.e., taking $\lambda_{\mathrm{as}}(\delta)$. For simplicity, we again assume that $\sqrt{\tau}\delta \ll V_{A|B}$ such that we can approximate $H(X_{\sqrt{\tau}\delta}^B|X_\delta^A) \approx h(X^B|X^A) - \log\sqrt{\tau}\delta$. Then, we find that in the asymptotic limit the condition for security is given by

$$\xi\lambda_{\mathrm{as}}(\delta) - H(Y_{\sqrt{\tau}\delta}|X_\delta) \approx \xi\log\sqrt{e\pi} - h(Y|X) + \log\tau$$
$$+ (\xi - 1)\log\frac{1}{\delta}.$$

The last term shows that the value of ξ is very crucial, in the sense that if $\xi > 1$, we can increase the value arbitrarily by making δ small. Unfortunately, in the case of bosonic channels $\xi = 1$. For $\xi = 1$ and a state given in (D1), the condition $\xi\lambda_{\mathrm{as}}(\delta) - H(Y_{\sqrt{\tau}\delta}|X_\delta) > 0$ translates to ($\hbar = 2$)

$$\frac{(1-\tau)V + \tau}{\tau V} < 1 \qquad (C11)$$

which is satisfied if $\tau > V/(2V - 1)$. Hence, a non-trivial squeezing is required and $\tau > 1/2$ in the limit $V \to \infty$.

Appendix D: Model of the EPR source

For the simulations used to generate Fig. 2 and 3, we assume an EPR state with variance $V = \hbar\cosh 2r$ with r the squeezing parameter (see, e.g., [25]). Alice's mode is loss-free and Bob's mode is sent through a fiber with transmissivity τ. We further assume in some cases a non-zero excess noise ξ. Then, the covariance matrix of the Gaussian state shared between Alice and Bob is given by

$$\begin{pmatrix} VI & \sqrt{\tau(V^2-1)}Z \\ \sqrt{\tau(V^2-1)}Z & V_B(\tau,\xi)I \end{pmatrix} \qquad (D1)$$

with I the identity in $\mathbb{C}^2$, $Z = \mathrm{diag}(1,-1)$ and $V_B(\tau,\xi) = \tau V + (1-\tau)\hbar/2 + \tau\xi$. Since large distances are not particularly required for the usefulness of OT and BC, we assume in the plots that $\tau = 0.94$ and $\xi = 0.0005\hbar$. Moreover, we use a variance of $V = 3\hbar$ which corresponds to a squeezing strength of about 10.8dB.

Appendix E: Bosonic Gaussian memory channels

Let us consider the security conditions for the OT and BC protocol if Bob's memory channel (or a part of it) can be modelled by a phase-insensitive Gaussian channel that acts on a single-mode covariance matrix as

$$\Gamma \mapsto T\Gamma T^T + N, \qquad (E1)$$

where $T = \mathrm{diag}(\sqrt{t}, \sqrt{t})$ and $N = \mathrm{diag}(v,v)$ such that $v \geq 0$ and $v \geq (t-1)$. In the following, we denote the corresponding quantum channels by $\mathcal{F}_{t,v}$.

For phase-insensitive Gaussian channels a strong converse has recently been established [48, 61, 62]. Note first that the classical capacities for bosonic channels are only bounded under a mean-energy constraint, i.e., if the mean photon number N_{av} of the average code state is finite. Then, the classical capacities are given by [46, 47]

$$C(\mathcal{F}_{t,v}|N_{av}) = g\left(tN_{av} + (t+v-1)/2\right) - g\left(\frac{t+v-1}{2}\right),$$
(E2)

where $g(x) = (x+1)\log(x+1) - x\log x$.

For a strong converse bound to hold, a mean-photon number constraint is not sufficient and one has to impose a maximal-photon-number constraint. More precisely, let ρ^n be the average channel input for n channel uses of $\mathcal{E}_{t,v}$. Then we say that a family of codes $\{\rho^n\}_n$ satisfies a maximal-photon-number constraint (MPNC) with N_{max} if [48]

$$\text{tr}\left(\Pi_{nN_{max}}\rho^n\right) \geq 1 - \delta(n)$$
(E3)

where $\Pi_{nN_{max}}$ denotes the projector onto the subspace with at most nN_{max} photons and $\delta(n)$ decays exponentially in n.

The strong converse theorem for any phase-insensitive channel $\mathcal{F}$ from [62] then says that the success probability for the transmission under the MPNC decays as

$$\mathcal{P}_{succ}^{\mathcal{F}^{\otimes n}}(nR|N_{max}) \leq 2^{-n(R-C(\mathcal{F}|N_{max})-\delta_1} + 2^{n\delta_2} + \delta_3(n),$$
(E4)

where δ_1, δ_2 are arbitrary small constants and $\delta_3(n) = \sqrt{\delta(n) + \sqrt{\delta(n)}} + \delta_4(n)$ with $\delta(n)$ given in (E3) and $\delta_4(n)$ is exponentially decreasing in n. Hence, we have a strong converse of the form (B11) with $\xi = 1$, and we can analyse the security conditions for OT and BC given in (4) and (5) in the main text.

For the plots in the main text we consider the most common phase-insensitive channel given by a thermal-loss channel with additive noise. A thermal-loss channel can be modeled by mixing the mode by a beam splitter with transmissivity η with a thermal state with average photon number N_{th}. In terms of the parameters t, v in (E1), it is expressed by $t = \eta$ and $v = (1 - \eta)(1 + 2N_{th})$. Moreover, if we include additional additive Gaussian noise V_n, the parameters are $t = \eta$ and $v = (1 - \eta)(1 + 2N_{th}) + V_n$.

Appendix F: Technical lemmas

Lemma F.1. *Let X and Y be possibly infinite discrete classical systems. It then holds for any $1 < \alpha \leq 2$ that*

$$H_{min}^\epsilon(X|Y) \geq H_\alpha(X|Y) - \frac{1}{\alpha - 1}\log\frac{2}{\epsilon^2}.$$
(F1)

Proof. The lemma has been shown for finite-dimensional systems in [52]. An easy way to show it in the infinite-dimensional case is by means of a finite-dimensional approximation result shown in [45]. This approximation allows us to obtain

$$H_{min}^\epsilon(X|Y)_\rho \geq H_{min}^{\epsilon-\delta}(X|Y)_{P_k\rho P_k}$$
(F2)

$$\geq H_\alpha(X|Y)_{P_k\rho P_k} - \frac{1}{\alpha - 1}\log\frac{2}{(\epsilon - \delta)^2}$$
(F3)

where $P_k = P_k^X \otimes P_k^Y$ is a projector onto a finite-dimensional subspace such that $P_k\rho P_k$ is δ-close to ρ, for some $\delta > 0$. Note that such a projection always exists for any δ. Next, we use that $H_\alpha(X|Y)_{P_k\rho P_k} \rightarrow H_\alpha(X|Y)_\rho$ for $k \rightarrow \infty$. This limit follows simply since all the sums involved in the definition of the α entropy converge absolutely, and thus, can be rearranged. We get as conclusion that

$$H_{min}^\epsilon(X|Y)_\rho \geq H_\alpha(X|Y)_\rho - \frac{1}{\alpha - 1}\log\frac{2}{(\epsilon - \delta)^2}$$
(F4)

holds for any $\delta > 0$. And thus in the limit δ to 0 we obtain the desired result. $\square$

The following statement has been shown in [16] and generalizes straightforwardly to infinite dimensions using the same strategy as in the proof above based on the approximation theorem in [45].

Lemma F.2. *Let $\rho_{XKQ_{in}}$ be a state of classical random variables XK correlated with a quantum system Q_{in} and $\mathcal{F}$ a quantum channel from Q_{in} to Q_{out}. Then, it holds that*

$$H_{min}^{\epsilon+\epsilon'}(X|\mathcal{F}(Q_{in})K) \geq -\log\mathcal{P}_{succ}(k_{\epsilon,\epsilon'}),$$
(F5)

where $k_{\epsilon,\epsilon'} = \lfloor H_{min}^\epsilon(X|K)_\rho - \log 1/\epsilon'^2 \rfloor$.

The technique of min-entropy splitting is due to [35], and used as the following Lemma in [14, 23], which generalizes by a simple application of the approximation in [45] to arbitrary alphabet sizes.

Lemma F.3. *Let X_0, X_1, Y be classical random variables. Then there exists a random variable D with range $\{0, 1\}$ such that*

$$H_{min}^\epsilon(X_D|DY) \geq \frac{1}{2}H_{min}^\epsilon(X_0X_1|Y) - 1.$$
(F6)

[1] S. Wiesner, SIGACT News **15**, 78 (1983).
[2] C. H. Bennett and G. Brassard, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing , 175 (1984).
[3] A. Ekert, Physical Review Letters **67**, 661 (1991).
[4] D. Mayers, Physical Review Letters **78**, 3414 (1997).

[5] D. Mayers, arXiv preprint, arxiv:quant-ph/9603015 (1996).

[6] H.-K. Lo and H. F. Chau, Physical Review Letter **78**, 3410 (1997).

[7] H.-K. Lo and H. F. Chau, Physica D: Nonlinear Phenomena **120**, 177 (1998).

[8] H.-K. Lo, Physical Review A **56**, 1154 (1997).

[9] G. D'Ariano, D. Kretschmann, D. Schlingemann, and R. Werner, Physical Review A **76**, 032328 (2007).

[10] H. Buhrman, M. Christandl, and C. Schaffner, Physical Review Letters **109**, 160501 (2012).

[11] U. Maurer, Journal of Cryptology **5**, 53 (1992).

[12] C. Cachin and U. M. Maurer, in *Proceedings of CRYPTO 1997*, Lecture Notes in Computer Science (1997) pp. 292–306.

[13] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner, SIAM Journal on Computing **37**, 1865 (2008).

[14] I. B. Damgård, S. Fehr, R. Renner, L. Salvail, and C. Schaffner, in *Advances in Cryptology-CRYPTO 2007* (Springer, 2007) pp. 360–378.

[15] S. Wehner, C. Schaffner, and B. M. Terhal, Physical Review Letters **100**, 220502 (2008).

[16] R. Konig, S. Wehner, and J. Wullschleger, IEEE Transactions on Information Theory **58**, 1962 (2012).

[17] M. Berta, O. Fawzi, and S. Wehner, in *Advances in Cryptology CRYPTO 2012*, Lecture Notes in Computer Science, Vol. 7417 (2012) pp. 776–793.

[18] M. Berta, F. G. Brandao, M. Christandl, and S. Wehner, IEEE Transactions on Information Theory **59**, 6779 (2013).

[19] F. Dupuis, O. Fawzi, and S. Wehner, IEEE Transactions on Information Theory **61**, 1093 (2015).

[20] N. H. Y. Ng, S. K. Joshi, C. C. Ming, C. Kurtsiefer, and S. Wehner, Nature Communications **3**, 1326 (2012).

[21] C. Erven, N. H. Y. Ng, N. Gigov, R. Laflamme, S. Wehner, and G. Weihs, Nature Communications **5** (2014).

[22] S. Wehner, M. Curty, C. Schaffner, and H.-K. Lo, Physical Review A **81**, 052336 (2010), arXiv:0911.2302v2.

[23] C. Schaffner, Physical Review A **82**, 032308 (2010).

[24] H.-K. Lo, M. Curty, and K. Tamaki, Nature Photonics **8**, 595 (2014).

[25] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Reviews of Modern Physics **84**, 621 (2012).

[26] G. Masada, K. Miyata, A. Politi, T. Hashimoto, J. L. O'Brien, and A. Furusawa, Nature Photonics **9**, 316 (2015).

[27] Ł. Rudnicki, Physical Review A **91**, 032123 (2015).

[28] J. Kilian, in *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing* (ACM, 1988) pp. 20–31.

[29] A. Einstein, B. Podolsky, and N. Rosen, Physical Review Letters **47**, 777 (1935).

[30] F. Furrer, M. Berta, M. Tomamichel, V. B. Scholz, and M. Christandl, Journal of Mathematical Physics **55**, 122205 (2014).

[31] Note that due to transmission losses in Bob's mode, he scales his outcomes with $1/\sqrt{\tau}$, where τ is the transmissivity.

[32] Note that we could introduce an additional step that Bob can check if the error correction worked properly, namely, by Alice sending a hash of Z_0, Z_1. However, Bob is not allowed to tell Alice whether the test was passed or not, since Alice could design attacks which lead to pass or failure of the test depending on his choice t.

[33] R. Renner, *Security of Quantum Key Distribution*, Ph.D. thesis, ETH Zurich (2005).

[34] R. König, R. Renner, and C. Schaffner, IEEE Transactions on Information Theory **55**, 4674 (2009).

[35] J. Wullschleger, in *Advances in Cryptology EUROCRYPT*, Lecture Notes in Computer Science (Springer, 2007) pp. 555–572.

[36] T. Vidick and S. Wehner, Physical Review Letters **030401** (2011).

[37] In information theory this is referred to as a strong converse for the classical capacity and has been shown for many channels.

[38] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Physical Review A **84**, 062317 (2011).

[39] P. Jouguet, D. Elkouss, and S. Kunz-Jacques, Physical Review A **90**, 042329 (2014).

[40] T. Gehring, V. Händchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R. F. Werner, and R. Schnabel, arxiv preprint, arXiv:1406.6174 (2014).

[41] N. H. Y. Ng, M. Berta, and S. Wehner, Phys. Rev. A **86**, 042315 (2012).

[42] E. Kennard, Zeitschrift für Physik **44**, 326 (1927).

[43] I. Bialynicki-Birula, Physics Letters **103**, 253 (1984).

[44] H. J. Landau and H. O. Pollak, The Bell System Technical Journal **65**, 43 (1961).

[45] F. Furrer, J. Aberg, and R. Renner, Communications in Mathematical Physics **306**, 165 (2011).

[46] V. Giovannetti, A. Holevo, and R. Garcia-Patron, arXiv preprint, arXiv:1312.2251 (2013).

[47] V. Giovannetti, R. Garcia-Patron, N. Cerf, and A. Holevo, arXiv preprint, arXiv:1312.6225 (2013).

[48] M. M. Wilde and A. Winter, Problems of Information Transmission **50**, 117 (2014).

[49] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Transactions on Information Theory **56**, 4674 (2010).

[50] M. Tomamichel, *A Framework for Non-Asymptotic Quantum Information Theory*, Ph.D. thesis, ETH Zürich (2013).

[51] M. Berta, F. Furrer, and V. B. Scholz, arXiv preprint, arXiv:1107.5460 (2011).

[52] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Transactions on Information Theory **55**, 5840 (2009).

[53] H. Dym and H. P. McKean, *Fourier Series and Integrals* (Academic, New York, 1972).

[54] I. Bialynicki-Birula and J. Mycielski, Communications in Mathematical Physics **44**, 129 (1975).

[55] W. Beckner, Annals of Mathematics **102**, 159 (1975).

[56] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, Proceedings of IEEE Symposium on Information Theory , 2703 (2010).

[57] R. Renner and J. I. Cirac, Physical Review Letters **102**, 110504 (2009).

[58] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, Physical Review Letters **110**, 030502 (2013).

[59] D. Slepian and J. Wolf, IEEE Transactions on Information Theory **19**, 461 (1971).

[60] If the covariance matrix of two Gaussian random variables X and Y is denoted by Γ_{XY}, then $V_{X|Y} = \det \Gamma_{XY}/V_Y$.

[61] B. R. Bardhan and M. M. Wilde, Physical Review A **89**, 022302 (2014).

[62] B. R. Bardhan, R. Garcia-Patron, M. M. Wilde, and A. Winter, arXiv preprint, arXiv:1401.4161 (2014).