

# Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security against Coherent Attacks

F. Furrer,<sup>1,\*</sup> T. Franz,<sup>1</sup> M. Berta,<sup>2</sup> A. Leverrier,<sup>2</sup> V. B. Scholz,<sup>1</sup> M. Tomamichel,<sup>2</sup> and R. F. Werner<sup>1</sup>

<sup>1</sup>*Institut für Theoretische Physik, Leibniz Universität Hannover Appelstraße 2, 30167 Hannover, Germany*

<sup>2</sup>*Institut für Theoretische Physik, ETH Zürich, 8093 Zürich, Switzerland*

We provide a security analysis for continuous variable quantum key distribution protocols based on the transmission of two-mode squeezed vacuum states measured via homodyne detection. We employ a version of the entropic uncertainty relation for smooth entropies to give a lower bound on the number of secret bits which can be extracted from a finite number of runs of the protocol. This bound is valid under general coherent attacks, and gives rise to keys which are composable secure. For comparison, we also give a lower bound valid under the assumption of collective attacks. For both scenarios, we find positive key rates using experimental parameters reachable today.

Quantum key distribution (QKD) is one of the first ideas from quantum information theory for turning quantum paradoxes into applications, see [1] and references therein. The task in QKD is to generate a shared key, secret from any eavesdropper (Eve), between two distant parties (Alice and Bob) using communication over a public quantum channel and an authenticated classical channel. Many different implementations of QKD have been proposed, each one with individual strengths and weaknesses. Early proposals are based on exchanging qubits, and are part of the family of discrete variable (DV) QKD protocols. Continuous variable (CV) protocols have later been proposed and offer the possibility to use standard telecom technologies (see [2] and references therein), in particular, they do not require photon counters.

A generic QKD protocol starts with the distribution of, say,  $N$  quantum states between the honest parties which are then measured according to the rules of the protocol. A certain part of the measurement outcomes is then used to estimate Eve's information about the remaining data from which a key of length  $\ell$  is generated by classical post-processing. The goal of a finite-key security analysis is to prove that the key is secure against any wiretapping strategy of Eve, up to a small failure probability. This is in contrast to the study of asymptotic rates in which perfect security in the limit for  $N$  to infinity is considered.

Eve's knowledge can be bounded by the probability that she correctly guesses Alice's measurement outcomes. This is expressed by the conditional smooth min-entropy [3] of the data from which the key is generated given Eve's quantum system. This ensures composable security [4], i.e., the protocol can securely be combined with other composable secure cryptographic protocols. Since the actual state is not known, the smooth min-entropy has to be bounded for the worst case compatible with the observed measurement data. This is in general a hard task and often simplified by additional assumptions about the power of the eavesdropper. Instead of allowing the most general, *coherent* attack on the quantum com-

munication between Alice and Bob, the eavesdropper is often restricted to *collective* attacks, meaning that every signal is attacked with the same quantum operation. Under this assumption, Alice and Bob can employ state tomography to bound Eve's information and to ensure security. In the case of DV QKD, these security proofs can then often be lifted to security proofs against coherent attacks using the exponential de Finetti theorems [5] or the post-selection technique [6].

Most security analysis for CV protocols neglect finite-key effects and consider asymptotic rates by using the Devetak-Winter formula [7] (see [8] for an infinite dimensional version). We are only aware of [9], where a first finite-key analysis for specific protocols under the assumption of collective Gaussian attacks was provided. Security against coherent attacks was considered in [10, 11] based on entanglement purification protocols, but without a quantitative analysis. The transfer of the exponential de Finetti technique to the infinite-dimensional setting is very subtle. This is because exponential de Finetti theorems do in general not hold in infinite-dimensional systems [12], but only under additional assumptions [13]. It is often argued that, using these results, much of the DV theory can be transferred to CV systems. Unfortunately, this approach provides only pessimistic finite-key rate estimates.

Recently, a more direct approach to prove DV QKD secure against coherent attacks was presented in [14], which is based on an entropic uncertainty relation with quantum side information for smooth entropies [15]. This uncertainty relation gives a bound on Eve's information about Alice's measurement outcomes in terms of the correlation between Alice and Bob. The relation between security in QKD and uncertainty relations has also been employed in [16, 17]. Based on the recent extension of the smooth entropy formalism to the infinite-dimensional setting [8, 18], it is the objective of this letter to apply the above reasoning to an entanglement based CV protocol using two-mode squeezed vacuum states measured via homodyne detection.

*Security Definition and Key Rates.*—A generic QKD protocol between two honest parties, Alice (A) and Bob (B) either aborts or outputs a key which consists of

---

\*Electronic address: fabian.furrer@itp.uni-hannover.de

strings  $S_A$  and  $S_B$  on Alice's and Bob's side, respectively. We denote by  $E$  the information which is wiretapped during the run of the protocol by an attack on the quantum channel. For CV systems this is modeled on an infinite-dimensional Hilbert space. The state of  $S_A$  and  $E$  can be described as a classical quantum state

$$\omega_{S_A E} = \sum_s |s\rangle\langle s| \otimes \omega_E^s, \quad (1)$$

where  $\omega_E^s$  are states on Eve's system. Three requirements have to be fulfilled by an ideal protocol: correctness, secrecy and robustness. Correctness is achieved when the output on Alice's and Bob's side agree,  $S_A = S_B$ . Secrecy of a key means that  $S_A$  is uniformly distributed and independent of  $E$  and thus given by  $\omega_{S_A E}^{\text{id}} = \tau_{S_A} \otimes \sigma_E$ , with  $\tau_{S_A}$  the uniform mixture of keys, and  $\sigma_E$  an arbitrary state on the  $E$  system. A protocol is called secure if it is both correct and secret. Finally, we call an ideal protocol robust if it never aborts when Eve is passive.

In reality, we can only hope to achieve an almost ideal protocol. For small parameters  $\epsilon_c$ ,  $\epsilon_s$  and an abortion probability  $p_{\text{abort}}$ , we require that the protocol is  $\epsilon_c$ -correct, i.e.  $\Pr[S_A \neq S_B] \leq \epsilon_c$ , and that the protocol is  $\epsilon_s$ -secret, i.e.  $(1 - p_{\text{abort}}) \inf_{\sigma} \frac{1}{2} \|\omega_{S_A E} - \tau_{S_A} \otimes \sigma_E\| \leq \epsilon_s$ . Note that a protocol which always aborts is secure. Thus we may impose an additional requirement on the robustness, e.g.,  $p_{\text{abort}} < 1$ . This security definition also ensures that the protocol is secure in the framework of composable security [4], in which different cryptographic protocols can be combined without compromising the overall security. We note that this is not the case for security definitions that require only a small mutual information between the eavesdropper and the key [19].

The measurement step of a QKD protocol produces a pair of raw keys,  $X_A$  and  $X_B$ , held by Alice and Bob. If the protocol does not abort, the secret keys  $S_A$  and  $S_B$  are extracted using classical error correction and privacy amplification schemes. We do not discuss the error correction scheme here and simply assume that it will leak  $\text{leak}_{\text{EC}}$  bits of information about the key to the eavesdropper. The correctness is checked using a hash function evaluated on both resulting strings which leads to an additional leakage of order  $O(\log \frac{1}{\epsilon_c})$  [14].

In the privacy amplification step, two-universal hash functions are used to compress the raw key to a final length of  $\ell$  bits. Roughly speaking, this reduces Eve's knowledge about Alice's key by  $N - \ell$  bits. Hence, choosing  $\ell$  sufficiently small ensures that Eve has no information about the resulting bit strings and the key is independent of  $E$ . Formally, Eve's uncertainty (or lack of knowledge) is measured in terms of the probability that she can guess Alice's raw key  $X_A$ , i.e. the conditional min-entropy  $H_{\min}(X_A|E)$  (see Appendix A for a formal definition). In particular, the resulting key is  $\epsilon_s$ -secret if [3, 8, 20]

$$\ell \lesssim H_{\min}^{\epsilon}(X_A|E)_{\omega} - \text{leak}_{\text{EC}} - O\left(\log \frac{1}{\epsilon_s \epsilon_c}\right), \quad (2)$$

where  $\epsilon \propto \epsilon_s/p_{\text{abort}}$ . Here, the smooth min-entropy,  $H_{\min}^{\epsilon}(X_A|E)$ , is the optimization of the min-entropy over states which are  $\epsilon$  close to  $\omega_{X_A E}$ , where  $\omega_{X_A E}$  denotes the joint state prior to the classical post-processing conditioned on the event that the protocol does not abort. We derive lower bounds on this entropy for the following protocol.

*The Protocol.*— The analysis of coherent and collective attacks can widely be treated in parallel. We consider a trusted source located in Alice's lab that produces an entangled state by mixing two squeezed vacuum states on a balanced beam splitter. We assume that each beam consists of only one bosonic mode. Alice sends one beam to Bob whereupon both perform a homodyne measurement. They choose uniformly at random between two canonically conjugated quadrature observables, amplitude and phase, such that Alice's and Bob's outcomes are maximally correlated whenever their choice agree. In the case of collective attacks they additionally perform measurements to estimate the covariance matrix. We further assume that the states generated by the source have tensor product form and that the probability that Alice measures an amplitude or phase quadrature is larger than  $\alpha$  ( $\hbar = 1$ ) is bounded by  $p_{\alpha}$ . This is possible since the source is trusted and located in Alice's lab.

After all measurements are performed, the two parties reveal their measurement choices. In the case of coherent attacks, they discard the data in which they have measured different quadratures ending up with a string of  $N$  measurement results. Then, they divide the continuous outcome range of the quadrature measurements into intervals  $(-\infty, -\alpha + \delta]$ ,  $(-\alpha + \delta, -\alpha + 2\delta]$ ,  $\dots$ ,  $(\alpha - \delta, \infty)$  where we assume for simplicity that  $2\alpha/\delta \in \mathbb{N}$ . We denote the outcome alphabet by  $\mathcal{X} = \{1, 2, \dots, 2\alpha/\delta\}$ . A random sample  $X_A^{pe}, X_B^{pe} \in \mathcal{X}^k$  of length  $k$  are used for parameter estimation, in which they check the quality of their correlation by computing the average distance  $d(X_A^{pe}, X_B^{pe}) = \frac{1}{k} \sum_{i=1}^k |X_{A,i}^{pe} - X_{B,i}^{pe}|$  where  $X_A^{pe} = (X_{A,i}^{pe})_{i=1}^k$  and  $X_B^{pe} = (X_{B,i}^{pe})_{i=1}^k$ . If  $d(X_A^{pe}, X_B^{pe})$  is smaller than  $d_0$  they proceed and otherwise they abort the protocol. In case the test is passed, they use the remaining data  $X_A, X_B \in \mathcal{X}^n$  ( $n = N - k$ ) as the raw key and execute the error correction and privacy amplification protocol as discussed in the paragraph before. For collective attacks, the strings  $X_A \in \mathcal{X}^n$  and  $X_B \in \mathcal{X}^n$  are generated as for coherent attacks but the remaining data (before the binning) is used to estimate the covariance matrix. This also includes the one in which Alice and Bob measured different quadratures.

*Analysis for Coherent Attacks.*— The goal is to bound the smooth min-entropy conditioned on the event that the protocol does not abort. For that we use an infinite-dimensional version of the entropic uncertainty relation for smooth entropies with side information [8], combining the uncertainty principle for complementary measurements with monogamy of entanglement. It states that Eve's information about the measurement outcomes  $X_A$  can be bounded by using the the complementary of the

measurements and the correlation between  $X_A$  and  $X_B$ . In particular, if Alice and Bob are highly correlated after measuring e.g., the phase quadrature, then Eve’s knowledge about the outcome of the amplitude measurement is nearly zero, since the observables are maximally complementary. We measure this correlation strength by the smooth max-entropy  $H_{\max}^\epsilon(X_A|X_B)$ , which characterizes the amount of information Alice has to send Bob to retrieve  $X_A$ . This leads to the bound (see Appendix B)

$$H_{\min}^\epsilon(X_A|E)_\omega \geq n \log \frac{1}{c(\delta)} - H_{\max}^{\epsilon'}(X_A|X_B)_\omega, \quad (3)$$

where  $c(\delta)$  is the overlap of the two conjugated quadrature measurements on an interval of length  $\delta$  which is well approximated by  $c(\delta) \approx \delta^2/(2\pi)$  for small  $\delta$ . Equation (3) assumes a uniformly random choice of measurement settings. Since projectors onto intervals  $(-\infty, -\alpha]$  and  $[\alpha, \infty)$  would lead to a trivial state-independent uncertainty relation, the probability of this event has to be estimated using  $p_\alpha$ . In equation 3 this is included in the change of the smoothing parameter from  $\epsilon$  to  $\epsilon'$ .

This reduces the problem to upper bounding the smooth max-entropy between  $X_A$  and  $X_B$ , which can be done by  $n \cdot \log \gamma(d(X_A, X_B))$ , where  $\gamma$  is a function arising from a large deviation consideration (see Appendix C). Using sampling theory, the quantity  $d(X_A, X_B)$  can then, with high probability, be estimated by  $d(X_A^{pe}, X_B^{pe})$  plus a correction  $\mu$ , which quantifies its statistical deviation to  $d(X_A, X_B)$  and depends on  $p_\alpha$ ,  $k$  and  $n$ . Since the protocol aborts if  $d(X_A^{pe}, X_B^{pe}) > d_0$ , we obtain the following formula for the key length: For parameters  $k, p_\alpha, \delta, d_0$ , an  $\epsilon_s$ -secret key of length

$$\ell = n \left[ \log \frac{1}{c(\delta)} - \log \gamma(d_0 + \mu) \right] - \text{leak}_{\text{EC}} - O\left(\log \frac{1}{\epsilon_s \epsilon_c}\right).$$

can be extracted.

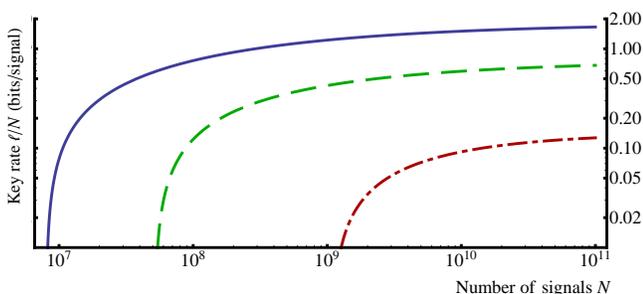


FIG. 1: Key rate  $\ell/N$  against coherent attacks for an input squeezing/antisqueezing of 11dB/16dB and additional symmetric losses of 0% (solid line), 10% (dashed line) and 20% (dash-dotted line). For the chosen security parameters see the main text.

We assume that the source in Alice’s lab is trusted and that her measurement device is described by projections onto two canonical variables. Note that the measurement device on Bob’s side need not to be trusted, except

that measurements on different signals commute. Hence, the additional reference signal (local oscillator) used by Bob for homodyne detection is covered by our security analysis. Placing the trusted source in Alice’s lab also implies that the analysis is not compatible with reverse reconciliation.

We calculate the correlation between  $X_A$  and  $X_B$  under the assumption of an identically and independently distributed source producing states with an input squeezing of 11dB and antisqueezing of 16dB. Squeezing at this level has been realized in an experiment at 1550nm [21]. Our noise model consists of loss and excess noise, where the latter is set to be 1% as it is mainly due to the classical data acquisition (see Appendix D). The leakage term is estimated assuming an error correction efficiency of 0.95 [22]. In Fig. 1 the resulting key rates  $\ell/N$  are plotted for different symmetric losses. We have set security parameters  $\epsilon_s = \epsilon_c = 10^{-6}$ . The optimization over the other free parameters is done numerically for each  $N$ . Typical values for  $N = 10^9$  are  $k = 10^8$ ,  $\alpha = 52$  and  $\delta = 0.01$ .

*Analysis for Collective Attacks*— Under the assumption of collective attacks, the state between Alice, Bob, and Eve has tensor product structure,  $\omega_{ABE}^{\otimes N}$ , enabling statistical estimations of the covariance matrix of  $\omega_{AB}$ . However, we do not cover the statistical details here and simply introduce confidence sets  $\mathcal{C}_{\epsilon_{pe}}$ , which ensure that whenever the protocol does not abort the covariance matrix  $\Gamma_{AB}$  of  $\omega_{AB}$  lies in  $\mathcal{C}_{\epsilon_{pe}}$  with probability at least  $1 - \epsilon_{pe}$ . Hence, we have to give a lower bound on the smooth min-entropy  $H_{\min}^\epsilon(X_A|E)_{\omega^{\otimes n}}$  over all states with a covariance matrix  $\Gamma_{AB} \in \mathcal{C}_{\epsilon_{pe}}$ . The smooth min-entropy is evaluated on the classical quantum state  $\omega_{X_A E}$  which is obtained from  $\omega_{AB}$  by taking a purification  $\omega_{ABE}$  and applying the discretized quadrature measurement on the  $A$  system.

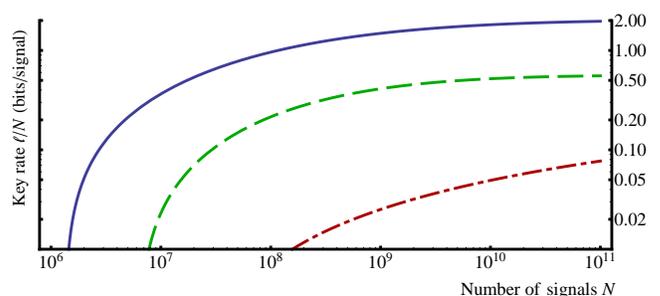


FIG. 2: Key rate  $\ell/N$  against collective Gaussian attacks for losses of 0% (solid line), 15% (dashed line), 25% (dash-dotted line). Squeezing strength and security parameters are chosen as in the case of coherent attacks.

We employ the quantum equipartition property of the smooth min-entropy [23] for infinite-dimensional systems [18], stating that for large  $n$ ,  $H_{\min}^\epsilon(X_A|E)_{\omega^{\otimes n}}$  approaches the conditional von Neumann entropy

$H(X_A|E)_\omega$ . More precisely, we have

$$H_{\min}^\epsilon(X_A|E)_{\omega^{\otimes n}} \geq n \cdot H(X_A|E)_\omega - \sqrt{n} \cdot \Delta, \quad (4)$$

where  $\Delta$  is a function of  $\epsilon$ ,  $\delta$  and  $\alpha$  (see Appendix E). Using that the minimum of  $H(X_A|E)_\omega$  over all states with a fixed covariance matrix  $\Gamma_{AB}$  is attained for the corresponding Gaussian state  $\omega^{\Gamma_{AB}}$  (see Appendix F and [24]), we get the following formula for the key length.

For parameters  $k, \alpha, \delta$ , an  $(\epsilon_s + \epsilon_{pe})$ -secret key of length

$$n \cdot \inf_{\Gamma \in \mathcal{C}_{\epsilon_{pe}}} H(X_A|E)_{\omega^\Gamma} - \sqrt{n} \cdot \Delta - \text{leak}_{\text{EC}} - O\left(\log \frac{1}{\epsilon_s \epsilon_c}\right)$$

can be extracted assuming collective attacks.

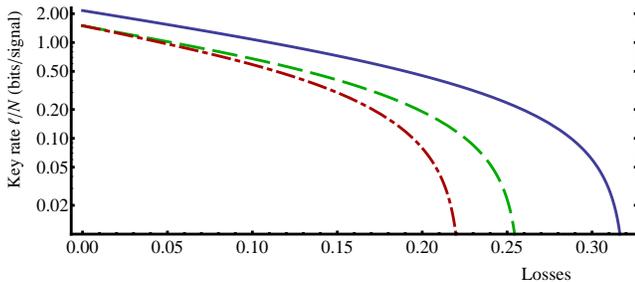


FIG. 3: Key rate versus losses secure against coherent attacks at  $N = 10^9$  (dot-dashed line), collective Gaussian attacks at  $N = 10^9$  (dashed line), and the Devetak-Winter rate [7] for perfect information reconciliation (solid line). Squeezing strength and security parameters are chosen as in the case of coherent attacks.

To evaluate this finite-key bound numerically, we need explicit expressions for the confidence sets. For this, we use results from [9], which assume collective Gaussian attacks. We computed the key rates  $\ell/N$  in Fig. 2 for the same squeezing strength and loss model as in the case of coherent attacks. The detailed calculation of  $H(X_A|E)_{\omega^\Gamma}$  can be found in Appendix G. For simplicity, we assumed a constant binning of  $\delta$  over the entire outcome range ( $\alpha = \infty$ ). In contrast to the case of coherent attacks, reverse reconciliation is possible and can increase the key rate essentially if asymmetric losses are assumed (which we do not discuss here). In Fig. 3, we plotted the key rate for coherent and collective Gaussian attacks in dependence of the losses, and compare them with the Devetak-Winter rate [7, 8] for perfect error correction.

*Discussion and Outlook.*— We provided a finite-key security analysis for a continuous variable QKD protocol and obtain a composable secure positive key rate against coherent attacks for experimentally feasible parameters. The comparison with the finite-key rate against collective attacks shows that the gap is relatively small compared to the finite-size effects. This is due to the fact that the uncertainty relation is almost tight for the two-mode squeezed states. The reason that the key rates allow for only small amounts of losses is because of the direct

reconciliation in the error correction protocol. Hence, an extension of the proof technique against coherent attacks to a reverse reconciliation error correction protocol would be desirable. In order to relax the assumptions in the security proof against coherent attacks, it would be interesting to study the overlap for more realistic models of the quadrature measurements, which may include a continuum of modes. Moreover, our arguments might also be applicable to other CV QKD schemes [25, 26].

*Acknowledgments.*— We thank R. Renner for suggesting this work, and R. García-Patrón and I. Cirac for helpful discussions. F.F acknowledges support from the LUH GRK 1463. T.F, V.B.S, and R.F.W acknowledge support from the DFG (grant WE-1240/12-1), BMBF project QuORep, EU project Q-ESSENCE, and the research cluster QUEST. M.B is supported by the SNF (grant PP00P2-128455), and the DFG (grants CH 843/1-1 and CH 843/2-1). A.L., M.B, V.B.S and M.T are supported by the SNF through the National Centre of Competence in Research ‘Quantum Science and Technology’.

## Appendix A: Smooth Min- and Max-Entropies

For the sake of completeness, we give here a formal definition of the smooth conditional min- and max-entropies and present the basic properties used in the following. For a detailed discussion consult e.g. [23, 27, 28] for the finite-dimensional case and [8, 18] for the infinite-dimensional case. In the following,  $\mathcal{H}$  always denotes a separable Hilbert space and  $\mathcal{S}(\mathcal{H})$  the state space associated to  $\mathcal{H}$ , which consists of all positive semi-definite trace class operators on  $\mathcal{H}$  with trace 1. Furthermore, we define  $\mathcal{S}_{\leq}(\mathcal{H})$  to be the set of all non-normalized states, that is, positive semi-definite trace class operators with trace smaller or equal to 1. We indicate different subsystems by labels and denote a state on  $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$  by  $\omega_{AB}$  and its reduced state on  $\mathcal{H}_A$  simply by  $\omega_A$ . Classical systems are denoted by  $X, Y, Z$  and are described by embedding the classical degrees of freedom into a Hilbert space w.r.t. a fixed orthonormal basis. This allows to read the following definitions for quantum as well as classical systems.

**Definition 1.** For  $\omega_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$ , we define the min-entropy of  $A$  conditioned on  $B$  as

$$H_{\min}(A|B)_\omega = \sup_{\sigma_B \in \mathcal{S}(B)} \sup\{\lambda \in \mathbb{R} | \omega_{AB} \leq 2^{-\lambda} \mathbb{1}_A \otimes \sigma_B\}.$$

The min-entropy of a classical-quantum state  $\omega_{XB}$  characterizes the optimal guessing probability of the classical variable  $X$  given the quantum system  $B$  [27].

The purified distance between two states  $\omega, \rho \in \mathcal{S}_{\leq}(\mathcal{H})$  is defined [28] as  $\mathcal{P}(\omega, \rho) = \sqrt{1 - F(\omega, \rho)}$  where  $F(\omega, \rho) = (\text{tr}(|\sqrt{\omega}\sqrt{\rho}|) + \sqrt{(1 - \text{tr}[\sigma])(1 - \text{tr}[\rho])})^2$  denotes the generalized fidelity.

**Definition 2.** For  $\omega_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$  and  $\epsilon \geq 0$ , we define the  $\epsilon$ -smooth min-entropy of  $A$  conditioned on  $B$  as

$$H_{\min}^{\epsilon}(A|B)_{\omega} = \sup H_{\min}(A|B)_{\tilde{\omega}}. \quad (\text{A1})$$

where the supremum is taken over all  $\tilde{\omega}_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$  with  $\mathcal{P}(\omega_{AB}, \tilde{\omega}_{AB}) \leq \epsilon$ . The  $\epsilon$ -smooth max-entropy of  $A$  conditioned on  $B$  is defined as

$$H_{\max}^{\epsilon}(A|B)_{\omega} = -H_{\min}^{\epsilon}(A|C)_{\omega}. \quad (\text{A2})$$

where  $\omega_{ABC}$  is an arbitrary purification of  $\omega_{AB}$ .

One can show that the definition of the smooth max-entropy is independent of the choice of the purification. As for the min-entropy, we denote the non-smoothed version ( $\epsilon = 0$ ) of the max-entropy simply by  $H_{\max}(A|B)_{\omega}$ . The smooth max-entropy can also be expressed as the optimization of the max-entropy over  $\epsilon$ -close states, that is,

$$H_{\max}^{\epsilon}(A|B)_{\omega} = \inf H_{\max}(A|B)_{\tilde{\omega}}, \quad (\text{A3})$$

where the infimum is taken over all  $\tilde{\omega}_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$  with  $\mathcal{P}(\omega_{AB}, \tilde{\omega}_{AB}) \leq \epsilon$ . These entropies satisfy the data processing inequality saying that whenever the system  $B$  is manipulated with a quantum operation  $\mathcal{E} : \mathcal{S}(\mathcal{H}_B) \rightarrow \mathcal{S}(\mathcal{H}_C)$ , the entropy can only increase

$$H_{\min}^{\epsilon}(A|B)_{\omega} \leq H_{\min}^{\epsilon}(A|C)_{\text{id}_A \otimes \mathcal{E}(\omega)} \quad (\text{A4})$$

$$H_{\max}^{\epsilon}(A|B)_{\omega} \leq H_{\max}^{\epsilon}(A|C)_{\text{id}_A \otimes \mathcal{E}(\omega)}. \quad (\text{A5})$$

## Appendix B: Derivation of the Uncertainty Relation

Let us assume that the protocol parameters  $\alpha$  and  $\delta$  are fixed. For simplicity, we further assume that  $M := 2\alpha/\delta$  is in  $\mathbb{N}$ . In the protocol Alice and Bob both measure the projectors of the quadrature measurements on the intervals  $I_1 = (-\infty, -\alpha + \delta]$ ,  $I_2 = (-\alpha + \delta, -\alpha + 2\delta]$ , ...,  $I_M = (\alpha - \delta, \infty)$ . Let us denote the corresponding outcome alphabet by  $\mathcal{X} = \{1, 2, \dots, M\}$ , which by definition is of size  $|\mathcal{X}| = 2\alpha/\delta$ . Let us introduce another partition of  $\mathbb{R}$  into intervals  $\{\tilde{I}_k\}_{k \in \mathbb{N}}$  of equal length  $\delta$  such that  $\tilde{I}_k = I_k$  for  $k \in \mathcal{X} \setminus \{1, M\}$ . In the following we denote the projection onto the interval  $I$  of the spectrum of the phase and amplitude operator of Alice by  $Q_A(I)$  and  $P_A(I)$ .

We can assume that they first distribute all the subsystems on which they perform the measurements. Let us denote the state shared between Alice, Bob and Eve on which they produce the sifted  $N$  measurements by  $\omega_{A^N B^N E}$ , where  $N$  denotes the number of subsystems. In the parameter estimation step they check that the average distance of the random sample of  $k$  measurements  $X_A^{pe}, X_B^{pe} \in \mathcal{X}^k$  satisfies

$$d(X_A^{pe}, X_B^{pe}) \leq d_0. \quad (\text{B1})$$

Note that this test can be written as a projector  $\Pi_k^{\text{pass}}$  which only acts non-trivially on the  $k$  subsystems used

in the parameter step. If this condition holds, they pursue with the protocol otherwise they abort. Let us denote by  $\omega_{A^N B^N E}$  the quantum state on the remaining  $n$  subsystems conditioned on the event that the parameter estimation test passes.

Alice chooses now for each subsystem uniform at random between phase and amplitude measurements. This can be modeled by introducing a random variable  $Z^n = (Z_1, \dots, Z_n)$  independently and identically distributed according to the uniform distribution, where  $Z_i$  takes values 0 or 1 depending on whether Alice measures phase or amplitude in the  $i$ th run. Let us denote the uniform distribution over  $\mathcal{Z}^n = \{0, 1\}^n$  by  $u$  and by  $\{|z^n\rangle\}_{z^n \in \mathcal{Z}^n}$  an orthonormal basis of a Hilbert space. The random measurement choice of Alice can now be modeled by introducing the state

$$\omega_{Z^n A^n B^n E} = \sum_{z^n \in \mathcal{Z}^n} u(z^n) |z^n\rangle\langle z^n| \otimes \omega_{A^n B^n E}, \quad (\text{B2})$$

and the positive operator valued measure (POVM)  $\{\Pi_A^{l^n}(z^n) \otimes |z^n\rangle\langle z^n|\}_{z^n \in \mathcal{Z}^n, l^n \in \mathcal{X}^n}$  acting on  $A^n$  and  $Z^n$ , where

$$\Pi_A^{l^n}(z^n) = \bigotimes_i \Pi_A^{l_i}(z_i), \quad (\text{B3})$$

with  $\Pi_A^i(0) = Q_A(I_i)$  and  $\Pi_A^i(1) = P_A(I_i)$  for  $i \in \mathcal{X}$ . Hence,  $z_i^n$  determines whether phase or quadrature is measured. Let us denote the post-measurement state obtained by measuring the state  $\omega_{A^n B^n E Z^n}$  by the POVM  $\{\Pi_{k^n}(z^n) \otimes |z^n\rangle\langle z^n|\}$  by  $\omega_{X_A^n B^n E Z^n}^n$ . Here,  $X_A$  takes values in  $\mathcal{X}^k$  and denotes the random variable which describes the distribution of the keys. Note that all parties are assumed to hold a copy of the variable  $Z$  since the measurement choices have been revealed in the sifting phase. Additionally, we introduce a similar POVM for the projections onto the spectrum of Alice's phase and amplitude measurements onto the intervals  $\{\tilde{I}_i\}_{i \in \mathbb{N}}$  and denote them by

$$\tilde{\Pi}_A^{l^n}(z^n) = \bigotimes_i \tilde{\Pi}_A^{l_i}(z_i), \quad (\text{B4})$$

where  $\tilde{\Pi}_A^i(0) = Q_A(\tilde{I}_i)$  and  $\tilde{\Pi}_A^i(1) = P_A(\tilde{I}_i)$  for  $i \in \mathbb{N}$ . The corresponding post-measurement state is denoted by  $\tilde{\omega}_{X_A^n B^n E Z^n}^n$ . Note that here the distribution over  $X_A$  can take values in  $\mathbb{N}^n$ .

The main idea in the security proof is to apply an uncertainty relation with quantum side information for the smooth min- and max-entropy [15]. For that, it is important that the measurements are maximally complementary. In the case of the POVM  $\{\Pi_{k^n}(z^n) \otimes |z^n\rangle\langle z^n|\}$  this is a problem since the projectors of the phase and amplitude measurements onto the big intervals  $I_1$  for  $i = 1, M$  almost commute. The idea is now that by trusting the source, we can estimate the (purified) distance between the states  $\omega_{X_A^n B^n E Z^n}^n$  and  $\tilde{\omega}_{X_A^n B^n E Z^n}^n$ . For the state  $\tilde{\omega}_{X_A^n B^n E Z^n}^n$ , we can then obtain a non-trivial uncertainty relation since all projectors have only support

on an interval of length  $\delta$ . In particular, it follows that

$$H_{\min}^{\epsilon}(X_A|EZ^n)_{\tilde{\omega}} \geq -n \log c - H_{\max}^{\epsilon}(X_A|B^n Z^n)_{\tilde{\omega}} \quad (\text{B5})$$

where  $c = \sup_{i,j} \|\sqrt{Q_A(\tilde{I}_i)}\sqrt{P_A(\tilde{I}_j)}\|^2$ . The inequality in this form is proven for the finite-dimensional case in [29, Corollary 7.6]. The generalization to infinite dimensions is straightforward by using the techniques from [8]. It turns out the the overlap  $c$  only depends on the length of the intervals and is given by

$$c(\delta) = \frac{\delta^2}{2\pi} \cdot S_0^{(1)}\left(1, \frac{\delta^2}{4}\right)^2,$$

where  $S_n^{(1)}(\cdot, u)$  denotes the radial prolate spheroidal wave function of the first kind (see [30] and references therein).

In a next step, we estimate the distance between  $\omega_{X_A B E Z}^n$  and  $\tilde{\omega}_{X_A B E Z}^n$ . According to the main text, we assume that the source produces a state which is independently and identically for each run. That is, the state has tensor product form  $\omega_{A^N} = \omega_A^{\otimes N}$ . Furthermore, if we set  $\bar{p}_\alpha = 1 - p_\alpha$  we have by assumption that the source satisfies

$$\text{tr} \left[ \omega_A Q_A([-\alpha, \alpha]) \right] \geq \bar{p}_\alpha, \quad (\text{B6})$$

as well as  $\text{tr} [\omega_A P_A([-\alpha, \alpha])] \geq \bar{p}_\alpha$ . Let us now define  $\Lambda = \mathbb{N} \setminus \mathcal{X}$  and for every  $z^n \in [0, 1]^n$  the projector

$$\Pi_A^\Lambda(z^n) = \sum_{l^n \in \Lambda} \tilde{\Pi}_A^{l^n}(z^n) \quad (\text{B7})$$

which corresponds to the event where at least one of the quadrature measurements exceeds  $\alpha$ . Since

$$\omega_{A^n} = \frac{1}{p_{\text{pass}}} \text{tr}_{A^k B^N} \left( \Pi_k^{\text{pass}} \omega_{A^N B^N} \right) \leq \frac{1}{p_{\text{pass}}} \omega_A^{\otimes n}$$

with  $p_{\text{pass}} = 1 - p_{\text{abort}}$ , we obtain for every  $z^n \in \mathcal{Z}^n$

$$\text{tr} \left[ \omega_{A^n} \Pi_A^\Lambda(z^n) \right] \leq \frac{1 - \bar{p}_\alpha^n}{p_{\text{pass}}}. \quad (\text{B8})$$

We can now bound the fidelity for a fixed  $z^n \in \mathcal{Z}^n$  by

$$\begin{aligned} F(\omega_{X_A B^n E}^{z^n}, \tilde{\omega}_{X_A B^n E}^{z^n}) &\geq (1 - \text{tr} [\omega_{A^n} \Pi_A^\Lambda(z^n)])^2 \\ &\geq 1 - 2 \text{tr} [\omega_{A^n} \Pi_A^\Lambda(z^n)] \\ &\geq 1 - 2 \frac{1 - \bar{p}_\alpha^n}{p_{\text{pass}}}, \end{aligned}$$

where  $\omega_{X_A B^n E}^{z^n}$  and  $\tilde{\omega}_{X_A B^n E}^{z^n}$  denote the normalized states conditioned on the event  $z^n$ . Since now the fidelity between  $\omega_{X_A B^n E Z^n}^n$  and  $\tilde{\omega}_{X_A B^n E Z^n}^n$  is just the average over  $z^n \in \mathcal{Z}^n$ , we obtain by the definition of the purified distance (see Section A)

$$\mathcal{P}(\omega_{X_A B^n E Z^n}^n, \tilde{\omega}_{X_A B^n E Z^n}^n) \leq \frac{f(n, p_\alpha)}{\sqrt{p_{\text{pass}}}}, \quad (\text{B9})$$

where  $f(p_\alpha, n) = \sqrt{2(1 - (1 - p_\alpha)^n)}$ .

The bound in (B9) can now be used to bound the smooth min- and max-entropy by

$$\begin{aligned} H_{\min}^{\epsilon+\tilde{\epsilon}}(X_A|EZ^n)_\omega &\geq H_{\min}^{\epsilon}(X_A|EZ^n)_{\tilde{\omega}} \\ -H_{\max}^{\epsilon+\tilde{\epsilon}'}(X_A|B^n Z^n)_{\tilde{\omega}} &\geq -H_{\max}^{\epsilon}(X_A|B^n Z^n)_\omega, \end{aligned}$$

where  $\tilde{\epsilon} = f(p_\alpha, n)/\sqrt{p_{\text{pass}}}$ . We simply used the Definition 2 and the fact that the purified distance can only decrease by tracing out a subsystem. In combination with the uncertainty relation in (B5), we arrive at

$$H_{\min}^{\epsilon+2\tilde{\epsilon}}(X_A|EZ^n)_\omega \geq -n \log c(\delta) - H_{\max}^{\epsilon}(X_A|B^n Z^n)_\omega.$$

Applying the data processing inequality to the max-entropy  $H_{\max}^{\epsilon}(X_A|B^n Z^n)_\omega \leq H_{\max}^{\epsilon}(X_A|X_B)_\omega$ , we obtain the final uncertainty relation used in Equation (3) in the main text. Note that we assumed in the main text that  $Z^n$  is included in  $E$ .

### Appendix C: Statistical Analysis for Coherent Attacks

The goal is to show that if the protocol does not abort and thus, satisfies  $d(X_A^{pe}, X_B^{pe}) \leq d_0$ , the smooth max-entropy in Equation (3) can be bounded by

$$H_{\max}^{\epsilon'}(X_A|X_B)_\omega \leq n \log \gamma(d_0 + \mu_0), \quad (\text{C1})$$

where

$$\gamma(t) = (t + \sqrt{1+t^2}) \left( \frac{t}{\sqrt{1+t^2}-1} \right)^t,$$

and

$$\mu_0 = |\mathcal{X}| \sqrt{\frac{N(k+1)}{nk^2} \log \frac{1}{\epsilon_s/4 - 2f(p_\alpha, n)}}. \quad (\text{C2})$$

Note that the alphabet  $\mathcal{X}$  satisfies  $|\mathcal{X}| = \lceil 2\frac{\alpha}{\delta} \rceil$  and  $\epsilon' = \epsilon_s/(4p_{\text{pass}}) - 2f(p_\alpha, n)/\sqrt{p_{\text{pass}}}$  [37]. The proof is divided into two steps and follows closely the arguments in [14]. First we derive a bound on the smooth max-entropy, and then we estimate the probability that  $d(X_A, X_B) \geq d(X_A^{pe}, X_B^{pe}) + \mu$ .

**Proposition 1.** *Let  $\mathcal{X}$  be a finite alphabet,  $\mathbb{P}(x, x')$  a probability distribution on  $\mathcal{X}^n \times \mathcal{X}^n$  for some  $n \in \mathbb{N}$ ,  $d_0 > 0$  and  $\epsilon > 0$ . If  $\mathbb{P}$  satisfies  $\Pr_{\mathbb{P}}[d(x, x') \geq d_0] \leq \epsilon^2$ , then*

$$H_{\max}^{\epsilon}(X|X')_{\mathbb{P}} \leq n \log \gamma(d_0),$$

where

$$\gamma(t) = (t + \sqrt{1+t^2}) \left( t/[\sqrt{1+t^2}-1] \right)^t.$$

*Proof.* We first note that the smooth max-entropy is obtained by taking the infimum over non-smooth max-entropies of all states which are  $\epsilon$ -close in purified distance (A3). Let us define the probability distribution

$$\mathbb{Q}(x, x') = \begin{cases} \frac{\mathbb{P}(x, x')}{\Pr_{\mathbb{P}}[d(x, x') \leq d_0]}, & \text{if } d(x, x') \leq d_0 \\ 0, & \text{else} \end{cases}$$

and note that  $F(\mathbb{P}, \mathbb{Q}) = \Pr_{\mathbb{P}}[d(x, x') \leq d_0]$ . Hence, it follows that  $\mathcal{P}(\mathbb{P}, \mathbb{Q}) = \sqrt{\Pr_{\mathbb{P}}[d(x, x') \geq d_0]} \leq \epsilon$ . Using that the 0-Rényi-entropy is bigger than the max-entropy [20], we obtain

$$H_{\max}^{\epsilon}(X|X')_{\mathbb{P}} \leq H_{\max}(X|X')_{\mathbb{Q}} \leq H_0(X|X')_{\mathbb{Q}}.$$

The conditional 0-Rényi entropy of the distribution  $\mathbb{Q}$  is then given by [3, Remark 3.1.4]

$$\begin{aligned} H_0(X|X')_{\mathbb{Q}} &= \max_{x'} \log |\{x \in \mathcal{X}^n ; \mathbb{Q}(x, x') \neq 0\}| \\ &\leq \log |\{x \in \mathbb{Z}^n ; \sum_{i=1}^n |x_i| \leq nd_0\}|. \end{aligned}$$

For any  $\lambda > 0$  we estimate

$$\begin{aligned} |\{x \in \mathbb{Z}^n ; \sum_{i=1}^n |x_i| \leq nd_0\}| &\leq \sum_{x \in \mathbb{Z}^n} \exp[\lambda(nd_0 - \sum_{i=1}^n |x_i|)] \\ &= e^{\lambda nd_0} \left( \sum_{z \in \mathbb{Z}} e^{-\lambda |z|} \right)^n \\ &= \left( e^{\lambda d_0} \frac{1 + e^{-\lambda}}{1 - e^{-\lambda}} \right)^n. \end{aligned}$$

By optimizing over  $\lambda > 0$ , one finds that  $|\{x \in \mathbb{Z}^n ; \sum_{i=1}^n |x_i| \leq nd_0\}| \leq \gamma(d_0)^n$ . This completes the proof.  $\square$

Now, we have to estimate the probability that  $d(X_A, X_B) \geq d(X_A^{pe}, X_B^{pe}) + \nu$  conditioned on the event that the protocol does not abort. Since the probability that the protocol passes is  $p_{\text{pass}}$ , we find according to Bayes' theorem that

$$\begin{aligned} \Pr[d(X_A, X_B) \geq d(X_A^{pe}, X_B^{pe}) + \nu | \text{"pass"}] \\ \leq \frac{1}{p_{\text{pass}}} \Pr[d(X_A, X_B) \geq d(X_A^{pe}, X_B^{pe}) + \nu]. \end{aligned}$$

Deriving a bound on  $\Pr[d((X_A, X_B) \geq d(X_A^{pe}, X_B^{pe}) + \nu]$  is a standard problem from random sampling without replacement. We have that  $X_A^{pe}, X_B^{pe} \in \mathcal{X}^k$  is a random sample of all measurements  $X_A^{tot}, X_B^{tot} \in \mathcal{X}^N$ . The quantity of interest is  $|x_A^i - x_B^i|$ , where  $x_A^i \in X_A^{tot}$  and  $x_B^i \in X_B^{tot}$ . For this we denote the population mean by  $d_{tot} = d(X_A^{tot}, X_B^{tot})$ , the sample mean by  $d_{pe} = d(X_A^{pe}, X_B^{pe})$ , and for the raw key  $d_{key} = d(X_A, X_B)$ . Note that these are related via

$$Nd_{tot} = kd_{pe} + nd_{key}. \quad (\text{C3})$$

We consider the runs of the protocol as a probabilistic process and treat  $d_{tot}$  as a random variable. We first use the bound from [31] to obtain

$$\Pr[d_{key} \geq a + \nu | d_{tot} = a] \leq e^{-2\nu^2 \frac{N}{|\mathcal{X}|^2(k+1)}},$$

which is independent of  $a$ . Here, we used that the maximal value of  $|x_A^i - x_B^i|$  is given by  $|\mathcal{X}|$ . Using Eq. (C3), we can compute

$$\begin{aligned} \Pr[d_{key} \geq d_{pe} + \nu] &= \Pr[d_{key} \geq d_{tot} + \frac{k}{N}\nu] \\ &= \sum_a \Pr[d_{tot} = a] \cdot \Pr[d_{key} \geq a + \frac{k}{N}\nu | d_{tot} = a] \\ &\leq e^{-2\nu^2 \frac{nk^2}{|\mathcal{X}|^2 N(k+1)}}. \end{aligned}$$

Hence, together with Proposition 1 and the fact that the protocol aborts for  $d(X_A^{pe}, X_B^{pe}) > d_0$ , we arrive at

$$H_{\max}^{\epsilon}(X|X')_{\mathbb{P}} \leq n \log \gamma(d_0 + \nu)$$

for

$$\nu = |\mathcal{X}| \sqrt{\frac{N(k+1)}{nk^2} \log \frac{1}{\epsilon \cdot \sqrt{p_{\text{pass}}}}}.$$

In the protocol, we have to bound the smooth max-entropy for a smoothing parameter  $\epsilon' = \epsilon = \frac{\epsilon_s}{4p_{\text{pass}}} - 2f(p_{\alpha}, n)/\sqrt{p_{\text{pass}}}$ . Since  $p_{\text{pass}} \leq 1$ , we can bound  $\nu \leq \mu$  and obtain the bound in Equation (C1).

## Appendix D: The Error Model

We consider a symmetric two parameter error model, using the loss  $\mu_{\text{loss}}$  and excess noise  $\mu_{\text{en}}$ . The loss is our main source of noise and is equivalent to replacing a certain amount of signal by vacuum. The excess noise corresponds to a classical noise added by the data acquisition system and can in principle be made arbitrary small by using appropriate equipment. Both effects are gaussian noise sources and are expressed as action on the covariance matrix by  $\Gamma \rightarrow (1 - \mu_{\text{loss}})\Gamma + (\mu_{\text{loss}} + \mu_{\text{en}})\Gamma_{\text{vac}}$ , where  $\Gamma_{\text{vac}}$  denotes the covariance matrix of the vacuum state.

## Appendix E: Asymptotic Equipartition Property

We use [18, Proposition 8], which states that for  $\epsilon > 0$ ,  $n \geq \frac{8}{5} \log \frac{2}{\epsilon^2}$ , and any quantum state  $\omega_{AB}$  for which  $H(A)_{\omega}$  is finite, we have

$$H_{\min}^{\epsilon}(A|B)_{\omega^{\otimes n}} \geq n \cdot H(A|B)_{\omega} - \sqrt{n}.$$

$$4 \log(2^{-\frac{1}{2} H_{\min}(A|B)_{\omega}} + 2^{\frac{1}{2} H_{\max}(A|B)_{\omega}} + 1) \sqrt{\log \frac{2}{\epsilon^2}}.$$

In our case, we are interested in the classical quantum state  $\omega_{X_A E}$  for which  $H(X_A)_\omega$  is finite and the formula applies. Let us now simplify the last term in the above inequality. Let  $\omega_{X_A E C}$  be an arbitrary purification of  $\omega_{X_A E}$ , we have according to the definition of the max-entropy (A2)

$$-H_{\min}(X_A|E)_\omega = H_{\max}(X_A|C)_\omega \leq H_{\max}(X_A)_\omega$$

where the last inequality is due to the data processing inequality (A5). Furthermore, we can also use the data processing inequality (A5) to bound the max-entropy  $H_{\max}(X_A|E)_\omega \leq H_{\max}(X_A)_\omega$ . Using this two estimations, we obtain

$$2^{-\frac{1}{2}H_{\min}(X_A|E)_\omega} + 2^{\frac{1}{2}H_{\max}(X_A|E)_\omega} \leq 2^{\frac{1}{2}H_{\max}(X_A)_\omega + 1}.$$

Hence, we finally arrive at  $H_{\min}^\epsilon(X_A|E)_{\omega^{\otimes n}} \geq n \cdot H(X_A|E)_\omega - \sqrt{n} \cdot \Delta$  with

$$\Delta = 4 \log(2^{\frac{1}{2}H_{\max}(X_A)_\omega + 1} + 1) \sqrt{\log \frac{2}{\epsilon^2}}, \quad (\text{E1})$$

which is used in (4) of the main paper. Note that  $\Delta$  only depends on  $\epsilon$  and the measurement distribution on Alice's side. Since we assume in our setup a known source in Alice's lab this can be directly calculated.

## Appendix F: Gaussian Extremality

In the following we show that the infimum  $\inf_\omega H(X_A|E)_\omega$  taken over all states  $\omega_{AB}$  with covariance matrix  $\Gamma$  is attained for the Gaussian representative. Even though the argument is in analogy to [24], we give it here for the sake of completeness. See also [32] for a similar result.

The main tool is the result from [33] which classifies functions which are optimized by Gaussian states. In particular, if one can show that a function  $f(\omega_{AB})$  is (i) lower semi-continuous in trace norm, (ii) invariant under local unitary transformations, and (iii) strongly superadditive, i.e.  $f(\omega_{ABA'B'}) \geq f(\omega_{AB}) + f(\omega_{A'B'})$  where equality holds if  $\omega_{ABA'B'} = \omega_{AB} \otimes \omega_{A'B'}$ , then it follows that  $f(\omega_{AB}) \geq f(\omega_{AB}^\Gamma)$ . Here,  $\omega_{AB}^\Gamma$  denotes the Gaussian representative of the family of states with same covariance matrix  $\Gamma$ .

Consider now the function  $f(\omega_{AB}) = H(X|E)_\omega$  where  $\omega_{ABE}$  is a purification of  $\omega_{AB}$  and  $\omega_{XBE}$  is obtained by applying the measurement used in our protocol on the A system. The conditional von Neumann entropy is defined in accordance with [34], that is,  $H(A|B)_\rho = H(A)_\rho - H(\rho_{AB} || \rho_A \otimes \rho_B)$  where  $H(\rho || \sigma)$  denotes the relative entropy. In this definition we require that  $H(A)_\rho$  is finite. Note that the classical alphabet  $\mathcal{X}$  on which  $\omega_X$  is defined is finite such that  $H(X)_\omega$  is always finite and the conditional entropy is well-defined. Because  $0 \leq H(X|B)_\rho \leq H(X)_\rho \leq \log |\mathcal{X}|$  holds for any

finite-dimensional B systems, we obtain the same result for infinite-dimensional Hilbert spaces via the finite-dimensional approximation property of the conditional von Neumann entropy as shown in [34].

We show now that  $f(\omega_{AB}) = H(X|E)_\omega$  satisfies the properties (i)-(iii) from which the extremality of the Gaussian state follows. The properties (i) and (ii) are obtained in a similar way as in [24]. In order to show property (iii) one takes a purification  $\omega_{ABA'B'E}$  of  $\omega_{ABA'B'}$ , which is of course also a purification of  $\omega_{AB}$  and  $\omega_{A'B'}$ . The following chain of inequalities for the von Neumann entropies

$$\begin{aligned} H(XX|E)_\omega &= H(X|X'E)_\omega + H(X'|XE)_\omega \\ &\quad + I(X : X'|E)_\omega \\ &\geq H(X|A'B'E) + H(X|ABE) \end{aligned}$$

holds for finite-dimensional systems due to  $I(X : X'|E)_\omega \geq 0$  and since  $X$  ( $X'$ ) is obtained from  $AB$  ( $A'B'$ ) via a trace preserving completely positive map. But this can be lifted to infinite-dimensions via the finite-dimensional approximation property [34] as the entropies are all finite. Hence, we obtain the strong superadditivity

$$\begin{aligned} f(\omega_{ABA'B'}) &= H(XX|E)_\omega \\ &\geq H(X|A'B'E) + H(X|ABE) \\ &= f(\omega_{AB}) + f(\omega_{A'B'}). \end{aligned}$$

The equality in the case of  $\omega_{AB} \otimes \omega_{A'B'}$  follows from the additivity of the von Neumann entropy.

## Appendix G: Calculation of $H(X_A|E)$ for Discretized Measurements

In order to compute the bound on the key length secure against collective attacks as given in the main paper, we have to calculate  $H(X_A|E)_\omega$  for a two mode squeezed Gaussian state  $\omega_{AB}$ . For the proper definition and the properties of conditional von Neumann entropies for infinite-dimensional systems, we refer to [34]. Let  $\omega_{ABC}$  be a Gaussian purification of  $\omega_{AB}$  with  $\omega_E$  a two mode Gaussian state. We first rewrite the entropy as

$$\begin{aligned} H(X_A|E)_\omega &= H(X_A E)_\omega - H(E)_\omega \\ &= H(E|X_A)_\omega + H(X_A)_\omega - H(AB)_\omega, \end{aligned}$$

where we used that  $\omega_{ABE}$  is pure and therefore  $H(E) = H(AB)$ . Note also that in our case the alphabet  $\mathcal{X}$  is finite. Since  $\omega_{AB}$  is a two mode Gaussian state the entropy  $H(AB)_\omega$  is just a function of the symplectic invariants and can be calculated [35].

For the computation of the other entropies, we assume for simplicity that the correlations in amplitude and phase are symmetric, and do the calculation for the amplitude measurement with corresponding operator denoted by  $X$ . The measurement operators for a projection onto the interval  $I_k$ ,  $k \in \mathcal{X}$ , are described

by  $E_k = \mu_x(I_k)$ , where  $\mu_x$  is the spectral measure of  $X$ . The post-measurement states are then given by  $\omega_{ABE}^k = 1/p_k(E_k\omega_{ABE}E_k^\dagger)$ , where  $p_k = \text{tr}[\omega_{ABE}E_k]$ . The entropy  $H(X_A)_\omega$  is the Shannon entropy of the classical distribution  $\{p_k\}$ .

Let us turn to the estimation of  $H(E|X_A)_\omega$ . First, we note that

$$H(E|X_A)_\omega = \sum_k p_k H(E)_{\omega^k},$$

which reduces the problem to calculate  $H(E)_{\omega^k}$  for every  $k \in \mathcal{X}$ . For that we introduce the normalized post measurement state  $\omega_{BE}(x)$  conditioned that Alice measures the amplitude  $x \in \mathbb{R}$ . Furthermore, we denote by  $p(x)$  the probability that Alice measures  $x$ . Since  $\omega_{AE}$  is a Gaussian state, one can show that  $\omega_E(x) = U(v(x))\omega_E(0)U(v(x))^\dagger$ , where  $U(v)$  denotes the Weyl operator which corresponds to a phase space translation and  $v$  is a continuous function which depends on  $\Gamma_{AE}$ . Hence, we obtain that  $H(E)_{\omega(x)} = H(E)_{\omega(0)}$  for all  $x$ .

**Proposition 2.** *Let  $\omega_{AB}$  be a two mode squeezed Gaussian state,  $\omega_{ABE}$  a Gaussian purification, and  $\omega_{BE}(x)$  and  $\omega_{BE}^k$  as defined above. Then, it follows that  $H(E)_{\omega^k} \geq H(E)_{\omega(0)}$  and, thus,  $H(E|X_A)_\omega \geq H(E)_{\omega(0)}$ .*

*Proof.* The proof exploits the concavity of the von Neumann entropy and the fact that the state  $\omega_E^k$  can be approximated in trace class by a finite convex combination of states  $\omega_E(x)$ . Note that we can write  $\omega_E^k = 1/p_k \int_{I_k} p(x)\omega_E(x)dx$  where the integral converges weakly. As discussed above we also have the relation  $\omega_E(x) = U(v(x))\omega_E(0)U(v(x))^\dagger$ . Since  $U(v)$  is strongly continuous in  $v$ , we have  $x \mapsto \omega_{BE}(x)$  and, thus,  $x \mapsto \omega_E(x)$  are trace class continuous. Hence, we know that the Lebesgue integral  $\int_{I_k} p(x)\omega_E(x)dx$  converges even in

trace norm, and furthermore, it is equal to the Riemann integral. So we can approximate  $\omega_E^k$  in trace norm via step functions

$$\rho_E^l = \frac{1}{p_k} \sum_{j=1}^{N_l} p(x_j^l) |J_j^l| \omega_E(x_j^l),$$

where it holds for all  $l$  that  $I_k = \bigcup_j J_j^l$ , the  $x_j^l \in J_j^l$  are chosen such that  $\sum_{j=1}^{N_l} p(x_j^l) |J_j^l| = p_k$ , and  $\sup_j |J_j^l| \rightarrow 0$  for  $l \rightarrow \infty$ . Furthermore, as  $\omega_E(x)$  is a Gaussian state, we have that for  $H = Q_E^2 + P_E^2$  the expectation value  $\text{tr}[\omega_E(x)H]$  is bounded and continuous in  $x$ , so  $\text{tr}[\rho_E^l H] \rightarrow \text{tr}[\omega_E^k H]$  for  $l \rightarrow \infty$  [38]. Using that the von Neumann entropy is continuous for sequences of states with finite energy [36], we find that  $H(E)_{\omega^k} = \lim_{l \rightarrow \infty} H(\rho_E^l)$ , and thus,

$$\begin{aligned} H(\omega_E^k) &= \lim_{l \rightarrow \infty} H(\rho_E^l) \\ &\geq \lim_{l \rightarrow \infty} \frac{1}{p_k} \sum_{j=1}^{N_l} p(x_j^l) |J_j^l| H(\omega_E(x_j^l)) = H(\omega_E(0)). \end{aligned}$$

The inequality is due to the concavity of the von Neumann entropy [36] and the last equality holds because  $H(\omega_E(x))$  is independent of  $x$ .  $\square$

Using this proposition we finally get

$$H(X_A|E)_\omega \geq H(E)_{\omega(0)} + H(X_A)_\omega - H(AB)_\omega,$$

where the right-hand side can be calculated since  $\omega_E(0)$  and  $\omega_{AB}$  are Gaussian states (see [35]). Note that the only dependence on the interval length  $\delta$  in this formula is due to  $H(X_A)_\omega$ .

- 
- [1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *Rev. Mod. Phys.* **81**, 1301 (2009).
- [2] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, *Rev. Mod. Phys.* **84**, 621 (2012).
- [3] R. Renner, *Security of Quantum Key Distribution*, Ph.D. thesis, ETH Zurich (2005).
- [4] R. Canetti, in *Proc. IEEE Int. Conf. on Cluster Comput.* (IEEE, 2001) pp. 136–145.
- [5] R. Renner, *Nat. Phys.* **3**, 645 (2007).
- [6] M. Christandl, R. König, and R. Renner, *Phys. Rev. Lett.* **102**, 020504 (2009).
- [7] I. Devetak and A. Winter, *Proc. Roy. Soc. A* **461**, 207 (2005).
- [8] M. Berta, F. Furrer, and V. B. Scholz, arXiv:1107.5460v1 (2011).
- [9] A. Leverrier, F. Grosshans, and P. Grangier, *Phys. Rev. A* **81**, 062343 (2010).
- [10] D. Gottesman and J. Preskill, *Phys. Rev. A* **63**, 022309 (2001).
- [11] G. Van Assche, S. Iblisdir, and N. J. Cerf, *Phys. Rev. A* **71**, 052304 (2005).
- [12] M. Christandl, R. König, G. Mitchison, and R. Renner, *Comm. Math. Phys.* **273**, 473 (2007).
- [13] R. Renner and J. I. Cirac, *Phys. Rev. Lett.* **102**, 110504 (2009).
- [14] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, *Nat. Commun.* **3**, 634 (2012).
- [15] M. Tomamichel and R. Renner, *Phys. Rev. Lett.* **106**, 110506 (2011).
- [16] F. Grosshans and N. Cerf, *Phys. Rev. Lett.* **92**, 047905 (2004).
- [17] M. Koashi, *J. Phys.: Conf. Ser.* **36**, 98 (2006).
- [18] F. Furrer, J. Aberg, and R. Renner, *Comm. Math. Phys.* **306**, 165 (2011).
- [19] R. Renner and R. König, in *Proc. of TCC*, LNCS, Vol. 3378 (Springer, 2005) pp. 407–425.
- [20] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, *IEEE Trans. Inf. Theory* **57**, 8 (2011).

- [21] T. Eberle, V. Händchen, J. Duhme, T. Franz, R. F. Werner, and R. Schnabel, *Phys. Rev. A* **83**, 052329 (2011).
- [22] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, *Phys. Rev. A* **84**, 062317 (2011).
- [23] M. Tomamichel, R. Colbeck, and R. Renner, *IEEE Trans. Inf. Th.* **55**, 5840 (2009).
- [24] R. García-Patrón and N. J. Cerf, *Phys. Rev. Lett.* **97**, 190503 (2006).
- [25] F. Grosshans and P. Grangier, *Phys. Rev. Lett.* **88**, 057902 (2002).
- [26] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, *Phys. Rev. Lett.* **93**, 170504 (2004).
- [27] R. König, R. Renner, and C. Schaffner, *IEEE Trans. Inf. Theory* **55**, 4674 (2009).
- [28] M. Tomamichel, R. Colbeck, and R. Renner, *IEEE Trans. Inf. Th.* **56**, 4674 (2010).
- [29] M. Tomamichel, *A Framework for Non-Asymptotic Quantum Information Theory*, Ph.D. thesis, ETH Zurich (2012).
- [30] J. Kiukas and R. F. Werner, *J. Math. Phys.* **51**, 072105 (2010).
- [31] R. J. Serfling, *Ann. Stat.* **2**, 39 (1974).
- [32] M. Navascués, F. Grosshans, and A. Acín, *Phys. Rev. Lett.* **97**, 190502 (2006).
- [33] M. M. Wolf, Giedke, Geza, and J. I. Cirac, *Phys. Rev. Lett.* **96**, 080502 (2006).
- [34] A. A. Kuznetsova, *Theory Probab. Appl.* **55**, 709 (2011).
- [35] A. Serafini, F. Illuminati, and S. De Siena, *J. Phys. B: At. Mol. Opt. Phys.* **37**, L21 (2004).
- [36] A. Wehrl, *Rev. Mod. Phys.* **50**, 2 (1978).
- [37] The value of  $\epsilon$  in Equation (4) can be chosen as  $\epsilon_s/(4p_{\text{pass}})$  and that the other term  $2f(p_\alpha, n)/\sqrt{p_{\text{pass}}}$  comes from the uncertainty relation derived in Section B.
- [38] We also use that  $x < \infty$  for  $x \in I_k$  since  $I_k \subset \mathbb{R}$  for all  $k$ .