Continuous-Variable Protocols in the Noisy-Quantum-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 a 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 assumes that the malicious party has only limited capabilities to store quantum information at one point during the protocol. The security is quantified by a trade-off relation between generated quantum uncertainty and the classical capacity of the memory channel. As our main technical tool, we study and derive uncertainty relations for continuous-variable systems that are essential to analyse security in the noisy-quantum-storage model.

Introduction. Quantum key distribution (QKD) offers security that rests only on the laws of quantum mechanics[1–3]. QKD is feasible with current technology, and implementations have already reached high maturity. 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 or 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 influence the outcome. Intuitively, what makes such tasks more difficult is that unlike in QKD where Alice and Bob trust each other and can hence work together to check on the eavesdropper, each party has to fend for itself.

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: First, one assumes that a particular problem such as factoring a large integer requires a large amount of computational resources. Second, one assumes that the adversary does not possess sufficient computational resources to solve that problem. Relying on such assumptions is difficult if one is interested in protocols that are fully future proof. Indeed, if a quantum computer is built in the future, any protocol whose security relies on the difficulty of factoring for example can retroactively be broken.

Instead of such computational assumptions, another line of research pursues physical assumptions on the adversary. Examples of such assumptions are that Alice and Bob are split into several space-like separated agents, a scenario that has been considered in classical cryptography[11] as well as relativistic quantum cryptography[12–16]. Security in such models demands such a space-like separation to exist in perpetuity, and security can retroactively be broken once the agents can communicate. This has severe consequences for our ability to use protocols based on relativistic assumptions as building blocks to solve more complicated cryptographic tasks.

Another physical assumption is the so-called bounded-storage model introduced classically[17,18], and later extended to the situation of bounded *quantum* storage[19,20], and *noisy quantum* storage[21]. Apart from classical storage being cheap and plentiful, the classical bounded storage model has the property that honest parties require a storage of $O(n)$ to execute a protocol in which n bits are sent, while the adversary can break the protocol using a mere $O(n^2)$ bits of classical storage. This is in sharp contrast to the quantum case, where the honest parties require *no* quantum memory at all to execute the protocol, while security is possible for any adversary who can store less than $n - O(\log n)$ qubits[22] when n qubits are sent in the protocol. This is essentially optimal.

Such bounds have been obtained using the more general perspective of noisy-quantum storage[21] in which the adversary can have an arbitrary noisy quantum storage device. In particular, this model can deal with devices that have even infinite degrees of freedom, but whose capacity for storing information is nevertheless limited. In 23 the security has been related to the classical capacity of the storage channel, in 24 to the entanglement cost and in 22 and 25 to the quantum capacity. Indeed, it has been shown that any assumption that leads to a limit of the adversary's entanglement leads to security[22,25]. The experimental feasibility of such protocols has been demonstrated in[26,27].

The assumption on the storage devices can be justified because they require advanced quantum information technologies that are assumed to be very challenging. However, any limit on the adversary's ability to store quantum information during a particular time period in the protocol, can in principle enable security: given a storage assumption we can compute the number of signals we need to send in order to obtain security. It is useful to realize that this assumption is fully future proof, in the sense that an adversary buying a much larger quantum storage device after this time period cannot retroactively break the protocol. As such, assumptions that limit the adversary's ability to store information are very appealing when it comes to building larger cryptographic protocols from basic primitives[28].

The protocols proposed so far[19,21,23,25,26,29,30] are based on discrete-variable systems that require single-photon sources and single-photon detectors. Despite recent improvements, both are still challenging technologies[31]. Here, we analyze the security in the noisy-storage model for protocols based on optical continuous-variable systems, where the informa-

tion is encoded in the quadrature of the electromagnetic field (see, e.g., 32). This information can then be read out efficiently using standard telecommunication technology such as homodyne detection. While discrete-variable protocols usually suffer from inefficient photon sources and detectors as well as photon losses, continuous-variable implementations suffer from lower fidelity, which, for instance, in cryptographic protocols result in more demanding classical post-processing[33–35].

Our main contribution is to derive uncertainty relations for CV systems, which are central ingredients to obtain security in the noisy-storage model. Moreover, we propose a practical protocol for implementing OT with CV systems and discuss its security in the noisy-storage model by applying the derived uncertainty relations. OT is particularly important as it is *universal* for two-party cryptography, i.e., any two-party primitive (such as bit commitment or password-based identification) can be generated from it by classical post-processing[36]. The security of our OT protocol is proven using techniques from[23], which enable us to relate the security in the noisy-storage model to the classical capacity of the quantum memory channel together with recent strong converse for the classical capacity of important bosonic channels[37–39].

Due to the non-perfect correlations that are unavoidable with a CV encoding at any finite squeezing strength, error-correction information (EC) has to be exchanged during the protocol. However, the amount of EC competes with the uncertainty that is generated by randomly choosing between maximally complementary measurements, i.e., observables satisfying the canonical commutation relation $[Q, P] = i$ ($\hbar = 1$). This has the consequence that very tight uncertainty relations are required to obtain a good trade-off. While we show an uncertainty relation that holds without any additional assumptions by using majorization techniques similar to 40, it turns out that it is not sufficient to obtain a good trade-off.

We overcome this technical problem by showing uncertainty relations under reasonable assumptions on the power of the malicious party. In particular, we show that if the encoding into the quantum memory is restricted to mixture of Gaussian operations, reasonable trade-offs can be achieved and implementations solely based on preparation and measurement of coherent states are possible. Moreover, if the encoding into the quantum memory can only act on a limited number of modes we still find a positive trade-off without any restriction to Gaussian operations. We then analyze the security of the OT protocol in both cases by assuming that the decoherence of the memory channel is modeled by a lossy and noisy bosonic Gaussian channel.

CV Uncertainty Relations for the Noisy Storage Model. The difficult case is security against the memory-bounded malicious Bob. In this case, we purify the protocol and consider a situation in which dishonest Bob is actually more powerful and can send a random n-mode state from an ensemble ρ^k, $k \in K$, to Alice who generates an outcome X by (honestly) measuring for any state randomly ($\theta \in_R \{0,1\}^n$) either quadrature Q ($\theta^i = 0$) or P ($\theta^i = 1$) (see, e.g., 23). The question is how much randomness can Alice extract, which is uncorrelated to Bob. Using privacy amplification and the left-over hash lemma[41], we know that this is determined by the smooth min-entropy $H_{\min}^{\epsilon}(X|\theta K)$. Hence, the goal is to give a bound $\lambda^{\epsilon}(n)$ on the entropy rate, that is, an uncertainty relation of the form

$$\frac{1}{n} H_{\min}^{\epsilon}(X|\theta K) \geq \lambda^{\epsilon}(n)\,. \tag{1}$$

A non-trivial bound only exists for coarse-grained quadrature measurements Q_δ and P_δ with a fixed binning δ.

We derive three different uncertainty bounds denoted by $\lambda_{\text{Maj}}^{\epsilon}$, $\lambda_{\text{Gauss}}^{\epsilon}$ and $\lambda_{\text{IID}}^{\epsilon}$. The first is valid without restrictions on the states ρ^k and is derived using majorization techniques similar to 40. The second, $\lambda_{\text{Gauss}}^{\epsilon}$, holds under the assumption that the states are mixtures of Gaussian states. Finally, the third, $\lambda_{\text{Gauss}}^{\text{IID}}$, applies under the assumption that the ensemble is given by an independent and identical distribution of m mode states ($m \ll n$). The three bounds are compared in Fig. 1.

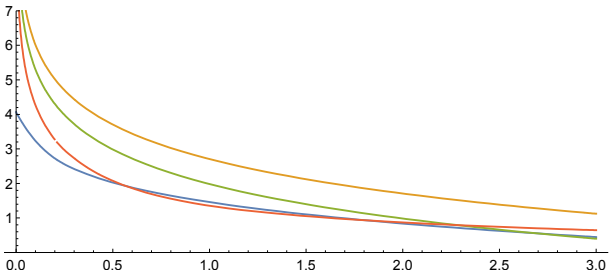

FIG. 1. The plot shows $\lambda_{\text{Maj}}^{\epsilon}$ (blue), $\lambda_{\text{Gauss}}^{\epsilon}$ (orange), $\lambda_{\text{IID}}^{\epsilon}$ (green) depending on δ. We have chosen $n = 10^8, \epsilon = 10^{-9}$, and for $\lambda_{\text{IID}}^{\epsilon}$ additionally $m = 10$. For security of OT in the noisy storage model the uncertainty bounds have to be larger than the error rate (red), which is plotted for an EPR state with variance $V = 3$ and one-sided losses of 0.05 and excess noise 0.001.

CV Protocol for OT in the Noisy Storage Model. We consider a randomized version of OT[23,30] in which Alice has no input and obtains as output two random strings $s_0, s_1 \in \{0,1\}^\ell$, and Bob has an input $c \in \{0,1\}$ and obtains a string $s_B \in \{0,1\}^\ell$. Correctness requires that the string s_B is equal to s_c. Security for Alice requires that a malicious Bob does not learn anything about the string s_{1-c}, and security for Bob requires that a malicious Alice does not learn c. See the technical version for the composable security definitions.

The CV protocol we propose goes roughly as follows (c.f. 30).

1) Alice distributes n EPR states with variance $V \geq 1$ (two-mode squeezed states). Alice and Bob measure in bases Q_δ or P_δ according to random independent basis strings $\theta_A, \theta_B \in \{0,1\}^n$ generating strings of outcomes X for Alice and Y for Bob, respectively.

2) They wait for a fixed time Δt.

3) Alice sends Bob her basis choice θ_A. Bob defines the sets $I_c = \{i \in [n] \mid \theta_A^i = \theta_B^i\}$ and $I_{\bar{c}} = [n] \backslash I_c$ and sends I_0, I_1 to Alice.

4) Alice forms the strings $X_k = (X^i)_{i\in I_k}$ for $k = 0, 1$, computes EC syndroms W_0, W_1 for X_0, X_1 using an EC protocol with rate r_{EC}, and sends it to Bob who corrects his string $Y_c = (Y^i)_{i\in I_c}$ according to W_c to obtain Y_c'.

5) Alice chooses random hash functions f_0, f_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 $s_B = f_c(Y_c')$.

Note that the above protocol can be implemented in a prepare-and-measure way. Correctness is ensured since the outcomes of Alice and Bob are correlated when measured in the same basis. By sending sufficient EC information, i.e., $\ell_{\text{EC}} \approx nH(X|Y)$, Bob can recover Alice's string. Security for Bob follows since he only sends the information I_0, I_1 which is independent of c. Security for Alice is more delicate to prove. In fact, if malicious Bob has a perfect quantum memory that can store the n modes over time Δt, he can wait until Alice sends her basis choice θ_A and measure accordingly. Thus, he obtains both s_0 and s_1.

However, if Bob's memory device is noisy, he will not have enough information to recover both of the strings. In a similar way as in[23,30] for a discrete variable protocol, we show a trade-off between security and the classical capacity of Bob's memory channel:

Assume that Bob has νn quantum memories $\mathcal{E}$ for which the success probability for sending classical information at a rate R bigger than the classical capacity $\mathcal{C}(\mathcal{E})$ is exponentially suppressed, i.e., $\mathcal{E}$ satisfies a strong converse. Then, we can obtain security for our OT protocol if

$$r_{\text{OT}} = \frac{1}{2}\left(\lambda^\epsilon - r_{\text{EC}}\right) - \nu\mathcal{C}(\mathcal{E}) > 0\,, \tag{2}$$

where λ^ϵ is a bound on the uncertainty rate of Alice's measurement (1)*. Moreover, the length of the string in the OT protocol is given by $\ell \approx nr_{OT}$ for sufficiently large n.*

We can now evaluate the above condition by using the different uncertainty bounds, $\lambda^\epsilon_{\text{Maj}}$, $\lambda^\epsilon_{\text{Gauss}}$ and $\lambda^\epsilon_{\text{IID}}$. As a necessary condition, we have that λ^ϵ has to be larger than the error correction rate. From Fig. 1, we see that without any constraints (i.e., $\lambda^\epsilon_{\text{Maj}}$) there exists only a very restricted region for which this is satisfied. Moreover, $\frac{1}{2}\left(\lambda^\epsilon - r_{\text{EC}}\right)$ is very small such that no good trade-off can be expected.

But we obtain a better trade-off if we restrict Bob's encoding operations, i.e., $\lambda^\epsilon_{\text{Gauss}}$ and $\lambda^\epsilon_{\text{IID}}$. Note that both constraints are reasonable from a practical point of view. For instance, implementations of efficient non-Gaussian operations are very challenging and often of non-deterministic nature[42]. Block encoding, i.e., $\lambda^\epsilon_{\text{IID}}$, can be justified since coherent encoding over all n modes is technologically demanding, and Bob has to wait until all modes arrive, which might already requires a short term memory device. Moreover, in the asymptotic limit this assumption is no restriction[43?] .

We plot in Fig. 2 the minimal constraints on Bob's quantum memory under Gaussian assumption (see 44 for more plots). Therein, the memory channel is assumed to be a thermal noise channel with transmissivity η and thermal number N_{th} plus Gaussian additive noise with variance V_N. For such a channel, a strong converse has recently been shown[39] under a maximal photon number constraint $N_{\max}$. We see that under additional bounds on the memory size $\nu \leq 1$, trade-offs are obtained even for optimistic assumptions on Bob's memory. While the plot is for realistic squeezing strengths, similar bounds are obtained for the coherent state protocols for $\nu = 1, 1/6, 1/12$. For similar assumptions but values $(\nu, m) = (1, 1), (1/8, 1), (1/8, 10)$ we obtain similar regions for $\lambda^\epsilon_{\text{IID}}$.

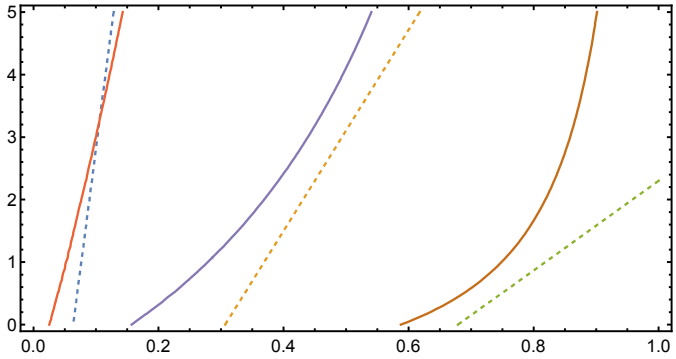

FIG. 2. The plots show when condition (2) is satisfied with equality for $\lambda^\epsilon_{\text{Gauss}}$ (i.e., left side of plots are secure regions). On the horizontal axis the transmissivity η is plotted and the vertical axis corresponds to the mean photon number N_{th} of the thermal noise channel (solid) and the noise variance V_N (dashed) for $N_{\max} = 30$ and $\nu = 1, 1/3, 1/5$ (from left to right). For the solid line we set $V_N = 2$ and for the dashed lines $N_{\text{th}} = 1$. The EPR state has variance $V = 3$ and for the transmission from Alice to Bob we assume transmissivity $\tau = 0.96$ and noise $\xi = 0.001$. Moreover, error correction efficiency is set to $\beta = 0.96$ (see, e.g., 34 and 35), $n = 10^8$ and $\epsilon = 10^{-9}$.

Conclusion We have presented an OT protocol for CV systems that provides security in the noisy storage model. The protocol is practical and uses similar resources as CV QKD. Under the constraint that Bob uses a Gaussian memory attack, an implementation with coherent states can provide security. As a key ingredient, we analyze and derive uncertainty relations for CV systems, which can be used along similar lines to analyze the security in the noisy-storage model for other protocols such as bit commitment or secure password-based identification[23,29,30]. We leave as open problem the task of finding optimal uncertainty relations without any further assumptions. It is possible such relations can be obtained by linking security again to the quantum capacity of the storage device[22,25], requiring however more sophisticated techniques. Such a result would also pose a challenge to find an explicit strong converse for the quantum capacity for bosonic channels.

[1] S. Wiesner. Conjugate coding. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984. Originally written c. 1970 but unpublished.

[2] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[3] A. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67:661–663, 1991.

[4]Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical review letters*, 78:3414, 1997.

[5]D. Mayers. The trouble with quantum bit commitment. 1996. arXiv:quant-ph/9603015v3.

[6]H-K. Lo and H. F. Chau. Is quantum bit commitment really possible? *Phys. Rev. Lett.*, 78:3410, 1997. arXiv:quant-ph/9603004v2.

[7]H-K. Lo and H.F. Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. In *Proceedings of PhysComp96*, 1996. arXiv:quant-ph/9605026v2.

[8]Hoi-Kwong Lo. Insecurity of quantum secure computations. *Physical Review A*, 56:1154, 1997.

[9]G. D'Ariano, D. Kretschmann, D. Schlingemann, and R.F. Werner. Quantum bit commitment revisited: the possible and the impossible. *Physical Review A*, 76:032328, 2007. arXiv:quant-ph/0605224v2.

[10]Harry Buhrman, Matthias Christandl, and Christian Schaffner. Complete insecurity of quantum protocols for classical two-party computation. *Physical review letters*, 109(16):160501, 2012.

[11]Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi Widgerson. Multi-Prover Interactive Proofs: How to Remove Intractability. In *Proc. ACM STOC*, pages 113–131, New York, New York, USA, 1988. ACM Press.

[12]Adrian Kent. Unconditionally secure bit commitment. *Phys. Rev. Lett.*, 83:1447–1450, Aug 1999.

[13]Sarah Croke and Adrian Kent. Security details for bit commitment by transmitting measurement outcomes. *Phys. Rev. A*, 86:052309, Nov 2012.

[14]Adrian Kent. Unconditionally secure bit commitment by transmitting measurement outcomes. *Phys. Rev. Lett.*, 109:130501, Sep 2012.

[15]J. Kaniewski, M. Tomamichel, E. Hänggi, and S. Wehner. Secure bit commitment from relativistic constraints. *IEEE Transactions on Information Theory (to be published)*, 2013.

[16]T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner, and H. Zbinden. Experimental bit commitment based on quantum communication and special relativity. *Phys. Rev. Lett.*, 111:180504, Nov 2013.

[17]U. Maurer. Conditionally-perfect secrecy and a provably-secure randomized cipher. *Journal of Cryptology*, 5:53–66, 1992.

[18]C. Cachin and U. M. Maurer. Unconditional security against memory-bounded adversaries. In *Proceedings of CRYPTO 1997*, Lecture Notes in Computer Science, pages 292–306, 1997.

[19]Ivan B Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Cryptography in the bounded-quantum-storage model. *SIAM Journal on Computing*, 37:1865–1890, 2008.

[20]Ivan B Damgård, Serge Fehr, Renato Renner, Louis Salvail, and Christian Schaffner. A tight high-order entropic quantum uncertainty relation with applications. In *Advances in Cryptology-CRYPTO 2007*, pages 360–378. Springer, 2007.

[21]Stephanie Wehner, Christian Schaffner, and Barbara M Terhal. Cryptography from noisy storage. *Physical Review Letters*, 100:220502, 2008.

[22]F. Dupuis, O. Fawzi, and S. Wehner. Entanglement sampling and applications. *Information Theory, IEEE Transactions on*, 61:1093–1112, 2015.

[23]Robert Konig, Stephanie Wehner, and Jürg Wullschleger. Unconditional security from noisy quantum storage. *IEEE Transactions on Information Theory*, 58:1962–1984, 2012.

[24]Mario Berta, Fernando GSL Brandao, Matthias Christandl, and Stephanie Wehner. Entanglement cost of quantum channels. *Information Theory, IEEE Transactions on*, 59:6779–6795, 2013.

[25]Mario Berta, Omar Fawzi, and Stephanie Wehner. Quantum to classical randomness extractors. In *Advances in Cryptology CRYPTO 2012*, volume 7417 of *Lecture Notes in Computer Science*, pages 776–793. 2012.

[26]Nelly Huei Ying Ng, Siddarth K Joshi, Chia Chen Ming, Christian Kurtsiefer, and Stephanie Wehner. Experimental implementation of bit commitment in the noisy-storage model. *Nature communications*, 3:1326, 2012.

[27]Chris Erven, N Ng, Nikolay Gigov, Raymond Laflamme, Stephanie Wehner, and Gregor Weihs. An experimental implementation of oblivious transfer in the noisy storage model. *Nature communications*, 5, 2014.

[28]Dominique Unruh. Concurrent composition in the bounded quantum storage model. In *Advances in Cryptology–EUROCRYPT 2011*, pages 467–486. Springer, 2011.

[29]S. Wehner, M. Curty, C. Schaffner, and H.-K. Lo. Implementation of two-party protocols in the noisy-storage model. *Physical Review A*, 81:052336, 2010. arXiv:0911.2302v2.

[30]Christian Schaffner. Simple protocols for oblivious transfer and secure identification in the noisy-quantum-storage model. *Phy. Rev. A*, 82:032308, 2010.

[31]Hoi-Kwong Lo, Marcos Curty, and Kiyoshi Tamaki. Secure quantum key distribution. *Nature Photonics*, 8:595–604, 2014.

[32]C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd. Gaussian quantum information. *Reviews of Modern Physics*, 84:621–669, 2012.

[33]Anthony Leverrier, Romain Alléaume, Joseph Boutros, Gilles Zémor, and Philippe Grangier. Multidimensional reconciliation for continuous-variable quantum key distribution. In *Information Theory, 2008. ISIT 2008. IEEE International Symposium on*, pages 1020–1024. IEEE, 2008.

[34]Paul Jouguet, David Elkouss, and Sébastien Kunz-Jacques. High-bit-rate continuous-variable quantum key distribution. *Physical Review A*, 90(4):042329, 2014.

[35]Tobias Gehring, Vitus Händchen, Jörg Duhme, Fabian Furrer, Torsten Franz, Christoph Pacher, Reinhard F Werner, and Roman Schnabel. Implementation of quantum key distribution with composable security against coherent attacks using einstein-podolsky-rosen entanglement. *arXiv:1406.6174*, 2014.

[36]Joe Kilian. Founding crytpography on oblivious transfer. In *Proceedings of the twentieth annual ACM symposium on Theory of computing*, pages 20–31. ACM, 1988.

[37]Mark M Wilde and Andreas Winter. Strong converse for the classical capacity of the pure-loss bosonic channel. *Problems of Information Transmission*, 50:117–132, 2014.

[38]Bhaskar Roy Bardhan and Mark M Wilde. Strong converse rates for classical communication over thermal and additive noise bosonic channels. *Physical Review A*, 89:022302, 2014.

[39]Bhaskar Roy Bardhan, Raul Garcia-Patron, Mark M Wilde, and Andreas Winter. Strong converse for the classical capacity of optical quantum communication channels. *arXiv preprint arXiv:1401.4161*, 2014.

[40]Łukasz Rudnicki. Majorization approach to entropic uncertainty relations for coarse-grained observables. *Physical Review A*, 91:032123, 2015.

[41]M. Tomamichel, C. Schaffner, A. Smith, and R. Renner. Leftover hashing against quantum side information. *Proceedings of IEEE Symposium on Information Theory*, pages 2703–2707, 2010. arXiv:1002.2436v1.

[42]Jérôme Wenger, Rosa Tualle-Brouri, and Philippe Grangier. Non-gaussian statistics from individual pulses of squeezed light. *Physical review letters*, 92:153601, 2004.

[43]R. Renner and J. I. Cirac. de Finetti representation theorem for infinite dimensional quantum systems and applications to quantum cryptography. *Physical Review Letters*, 102:110504, 2009. arXiv:0809.2243v1.

[44]S. Wehner F. Furrer, C. Schaffner. Continuous-variable protocols in the noisy-quantum-storage model. *Attached Technical Version*.

Continuous-Variable Protocols in the Noisy-Quantum-Storage Model

Technical Supplementary

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 a 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 assumes that the malicious party has only limited capabilities to store quantum information at one point during the protocol. The security is quantified by a trade-off relation between generated quantum uncertainty and the classical capacity of the memory channel. As our main technical tool, we study and derive uncertainty relations for continuous-variable systems that are essential to analyse security in the noisy-quantum-storage model.

I. INTRODUCTION

Quantum key distribution (QKD) offers security that rests only on the laws of quantum mechanics[1–3]. QKD is feasible with current technology, and implementations have already reached high maturity. 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 or 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 influence the outcome. Intuitively, what makes such tasks more difficult is that unlike in QKD where Alice and Bob trust each other and can hence work together to check on the eavesdropper, each party has to fend for itself.

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: First, one assumes that a particular problem such as factoring a large integer requires a large amount of computational resources. Second, one assumes that the adversary does not possess sufficient computational resources to solve that problem. Relying on such assumptions is difficult if one is interested in protocols that are fully future proof. Indeed, if a quantum computer is built in the future, any protocol whose security relies on the difficulty of factoring for example can retroactively be broken.

Instead of such computational assumptions, another line of research pursues physical assumptions on the adversary. Examples of such assumptions are that Alice and Bob are split into several space-like separated agents, a scenario that has been considered in classical cryptography[11] as well as relativistic quantum cryptography[12–16]. Security in such models demands such a space-like separation to exist in perpetuity, and security can retroactively be broken once the agents can communicate. This has severe consequences for our ability to use protocols based on relativistic assumptions as building blocks to solve more complicated cryptographic tasks.

Another physical assumption is the so-called bounded-storage model introduced classically[17,18], and later extended to the situation of bounded *quantum* storage[19,20], and *noisy quantum* storage[21]. Apart from classical storage being cheap and plentiful, the classical bounded storage model has the property that honest parties require a storage of $O(n)$ to execute a protocol in which n bits are sent, while the adversary can break the protocol using a mere $O(n^2)$ bits of classical storage. This is in sharp contrast to the quantum case, where the honest parties require *no* quantum memory at all to execute the protocol, while security is possible for any adversary who can store less than $n - O(\log n)$ qubits[22] when n qubits are sent in the protocol. This is essentially optimal.

Such bounds have been obtained using the more general perspective of noisy-quantum storage[21] in which the adversary can have an arbitrary noisy quantum storage device. In particular, this model can deal with devices that have even infinite degrees of freedom, but whose capacity for storing information is nevertheless limited. In 23 the security has been related to the classical capacity of the storage channel, in 24 to the entanglement cost and in 22 and 25 to the quantum capacity. Indeed, it has been shown that any assumption that leads to a limit of the adversary's entanglement leads to security[22,25]. The experimental feasibility of such protocols has been demonstrated in[26,27].

The assumption on the storage devices can be justified because they require advanced quantum information technologies that are assumed to be very challenging. However, any limit on the adversary's ability to store quantum information during a particular time period in the protocol, can in principle enable security: given a storage assumption we can compute the number of signals we need to send in order to obtain security. It is useful to realize that this assumption is fully future proof, in the sense that an adversary buying a much larger quantum storage device after this time period cannot retroactively break the protocol.

As such, assumptions that limit the adversary's ability to store information are very appealing when it comes to building larger cryptographic protocols from basic primitives[28].

The protocols proposed so far[19,21,23,25,26,29,30] are based on discrete-variable systems that require single-photon sources and single-photon detectors. Despite recent improvements, both are still challenging technologies[31]. Here, we analyze the security in the noisy-storage model for protocols based on optical continuous-variable systems, where the information is encoded in the quadrature of the electromagnetic field (see, e.g., 32). This information can then be read out efficiently using standard telecommunication technology such as homodyne detection. While discrete-variable protocols usually suffer from inefficient photon sources and detectors as well as photon losses, continuous-variable implementations suffer from lower fidelity, which, for instance, in cryptographic protocols result in more demanding classical post-processing[33–35].

Our main contribution is to derive uncertainty relations for CV systems, which are central ingredients to obtain security in the noisy-storage model. Moreover, we propose a practical protocol for implementing OT with CV systems and discuss its security in the noisy-storage model by applying the derived uncertainty relations. OT is particularly important as it is *universal* for two-party cryptography, i.e., any two-party primitive (such as bit commitment or password-based identification) can be generated from it by classical post-processing[36]. The security of our OT protocol is proven using techniques from[23], which enable us to relate the security in the noisy-storage model to the classical capacity of the quantum memory channel together with recent strong converse for the classical capacity of important bosonic channels[37–39].

Due to the non-perfect correlations that are unavoidable with a CV encoding at any finite squeezing strength, error-correction information (EC) has to be exchanged during the protocol. However, the amount of EC competes with the uncertainty that is generated by randomly choosing between maximally complementary measurements, i.e., observables satisfying the canonical commutation relation $[Q, P] = i$ ($\hbar = 1$). This has the consequence that very tight uncertainty relations are required to obtain a good trade-off. While we show an uncertainty relation that holds without any additional assumptions by using majorization techniques similar to 40, it turns out that it is not sufficient to obtain a good trade-off.

We overcome this technical problem by showing uncertainty relations under reasonable assumptions on the power of the malicious party. In particular, we show that if the encoding into the quantum memory is restricted to mixture of Gaussian operations, reasonable trade-offs can be achieved and implementations solely based on preparation and measurement of coherent states are possible. Moreover, if the encoding into the quantum memory can only act on a limited number of modes we still find a positive trade-off without any restriction to Gaussian operations. We then analyze the security of the OT protocol in both cases by assuming that the decoherence of the memory channel is modeled by a lossy and noisy bosonic Gaussian channel.

II. CONTINUOUS VARIABLE UNCERTAINTY RELATIONS FOR THE NOISY STORAGE MODEL

II.1. Setting and Notation

In the following we consider maximal complimentary quadrature observables, which are equivalent to position-momentum operators Q and P satisfying the canonical commutation relation $[Q, P] = i$ ($\hbar = 1$) (see, e.g., 32). They are uniquely represented on $\mathcal{H} = L^2(\mathbb{R})$ and act on smooth functions as multiplication and differential operator. We further denote by E_Q and E_P the projection-valued measure such that $Q = \int qE_Q(q)\mathrm{d}q$ and $P = \int pE_P(p)\mathrm{d}p$.

In the following we are mainly interested in coarse-grained measurements of Q and P given by projections onto a finite interval $I \subset \mathbb{R}$, i.e.,

$$Q[I] = \int_I E_Q(q)\mathrm{d}q \tag{1}$$

$$P[I] = \int_I E_P(p)\mathrm{d}p\,. \tag{2}$$

Let $\mathcal{P}_\delta = \{I_k\}_{k\in\mathbb{N}}$ be a partition of $\mathbb{R}$ into disjoint intervals I_k of length δ. We then define the positive operator-valued measure (POVM) with finite binning position and momentum measurements as $Q_\delta = \{Q_\delta^k\}$ and $P_\delta = \{P_\delta^k\}$ with $Q_\delta^k = Q[I_k]$ and $P_\delta^k = P[I_k]$ (see[41] for more details).

The situation of interest in the noisy- or bounded-storage model is given as follows[19,21,23]. One party referred to as Bob prepares an n-mode state ρ_A^k from an ensemble $\{\rho_A^k\}_{k\in K}$, which is correlated to a classical random variable K. He then sends the state to another party Alice who measures uniformly at random on each mode either quadrature Q or P. In the following, we denote the random variable corresponding to Alice's measurement choice by $\theta \in \{0,1\}^n$, where $\theta^i = 0$ refers to a Q measurement of the ith mode and $\theta^i = 1$ to a P measurement. Moreover, we denote the random variable describing Alice's measurement outcomes by X.

We are then interested how much randomness Alice can extract which is uncorrelated to Bob. Using privacy amplification

and the left-over hash lemma[42,43], we know that this is determined by the smooth min-entropy $H_{\min}^{\epsilon}(X|\theta K)_{\rho}$ of the state

$$\rho_{X^n\Theta^n K} = \frac{1}{2^n}\sum_{\vec{\theta},\vec{x},k} p_K(k)\,\mathrm{tr}(\rho_A^k \Pi_{\vec{x}}^{\vec{\theta}})|\vec{x}\rangle\langle\vec{x}| \otimes |\vec{\theta}\rangle\langle\vec{\theta}| \otimes |k\rangle\langle k|\,, \tag{3}$$

where $\Pi_x^0 = Q_{\delta q}^x$, $\Pi_x^1 = P_{\delta p}^x$ and $\Pi_{\vec{x}}^{\vec{\theta}} = \bigotimes_{i=1}^n \Pi_{x_i}^{\theta_i}$. For a definition and discussion of the smooth min-entropy we refer to[43,44] and references therein. Hence, we are interested to derive lower bounds on the smooth min-entropy, i.e.,

$$\frac{1}{n}H_{\min}^{\epsilon}(X|\theta K) \geq \lambda^{\epsilon}(n)\,. \tag{4}$$

This quantifies how well Bob can guess the outcome of two complementary measurements and is therefore an uncertainty relation. In the following, we derive three different bounds.

II.2. Uncertainty Relations for Renyi-Entropies

In order to derive tight bounds, we do not bound the smooth min-entropy directly. Instead, it is beneficial to use that they can be related to the conditional α-Renyi entropies

$$H_{\alpha}(A|B)_{\rho} = \frac{1}{1-\alpha}\,\mathrm{tr}[\rho_{AB}^{\alpha}(\mathrm{id}_A \otimes \rho_B)^{1-\alpha}]\,, \tag{5}$$

for bipartite state ρ_{AB} and α. In particular, it holds for $\alpha \in (1,2]$ and any two random variables X and Y that[45]

$$H_{\min}^{\epsilon}(X|Y) \geq H_{\alpha}(X|Y) - \frac{1}{\alpha-1}\log\frac{2}{\epsilon^2}\,, \tag{6}$$

where we present in Lemma 1 a simple generalization to unbounded classical variables X and Y. Hence, applied to the smooth min-entropy in (4) we obtain

$$\frac{1}{n}H_{\min}^{\epsilon}(X|\theta K) \geq \sup_{1<\alpha\leq 2}\Big(H_{\alpha}(X|\theta K) - \frac{1}{n(\alpha-1)}\log\frac{2}{\epsilon^2}\Big)\,. \tag{7}$$

Hence, for large n we obtain tight uncertainty relation for the smooth min-entropy by tight uncertainty relations for Renyi entropies of order $\alpha \in (1,2]$.

Since we are only interested in the situation where the side-information is classical it is sufficient to consider the situation for $n = 1$ and K trivial. Following the same arguments as in 46, we can show that if $H_{\alpha}(X|\theta) \geq \lambda$ holds for $n = 1$, then it holds that $H_{\alpha}(X|\theta K) \geq n\lambda$ for any n.

Hence, we focus in the following on 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 $\theta = 1$ correspond to Q_{δ} and P_{δ}. The goal is to derive a lower bound on $H_{\alpha}(X|\theta)$ independent on the sate.

II.2.1. Continuous Measurements.

For simplicity, consider first the case for $\delta \to 0$. Unfortunately, there exists no lower bound on the differential conditional Renyi-entropy $h_{\alpha}(X|\theta)$ is given as

$$2^{(1-\alpha)h_{\alpha}(X|\theta)_{\rho}} = \frac{1}{2}(\|\rho_Q\|_{\alpha}^{\alpha} + \|\rho_Q\|_{\alpha}^{\alpha})\,, \tag{8}$$

where $\rho_Q, \rho_P \in L^1(\mathbb{R})$ are the position and momentum distributions. Then there exists distributions in $L^1(\mathbb{R})$ that are not in $L^{\alpha}(\mathbb{R})$, i.e., the α-norm is unbounded. Thus, the right hand side of (8) is unbounded. The right hand side of (8) can even be made arbitrary large for Gausssian states. For a normal distribution with standard variance σ, the differential Renyi entropy is

$$h_{\alpha}(X) = \log[2\pi\sigma\alpha^{\frac{1}{2(\alpha-1)}}]\,. \tag{9}$$

Hence, we obtain that

$$2^{(1-\alpha)h_{\alpha}(X|\theta)_{\rho}} = (2\pi)^{(1-\alpha)/2}\alpha^{-1/2}\Big(\frac{1}{\sigma_Q^{\alpha-1}} + \frac{1}{\sigma_P^{\alpha-1}}\Big)\,. \tag{10}$$

This quantity can be made arbitrary large by taking a sufficiently small standard variance for either σ_Q or σ_P.

II.2.2. Coarse-grained Measurements.

However, the divergence of the entropy is not a problem for coarse-grained outcomes. Let us write

$$2^{(1-\alpha)H_\alpha(X|\theta)_\rho} = \frac{1}{2}(\sum_k q_k^\alpha + \sum_l p_l^\alpha)\,, \tag{11}$$

where q_k denotes the probability to measure a position in the interval I_k with $|I_k| = \delta$ and $\mathcal{P}_\delta = \{I_k\}_k$ a partition of $\mathbb{R}$ (and similar for p_l). Then, since both sums are smaller than 1, they are of course bounded. Moreover, the distributions $\{q_k\}$ and $\{p_l\}$ cannot be arbitrary. In particular it has been shown by Landau and Pollak[47] (see also 48, Section 2.9) that if $\psi \in L^2(\mathbb{R})$ with $\|\psi\|_2 = 1$ and $\hat{\psi}$ its Fourier transform, then the quantities

$$\alpha^2 = \int_{-a/2}^{a/2} |\psi(x)|^2 \mathrm{d}x \tag{12}$$

$$\beta^2 = \int_{-b/2}^{b/2} |\hat{\psi}(x)|^2 \mathrm{d}x \tag{13}$$

satisfy the inequality

$$\cos^{-1}(\alpha) + \cos^{-1}(\beta) \geq \cos^{-1}\left(\sqrt{c(a,b)}\right). \tag{14}$$

This condition can be reformulated in the following way:

- if $0 \leq \beta^2 \leq c(a,b)$, then all values for α are possible
- if $c(a,b) \leq \beta^2$, then

$$\alpha \leq \beta\sqrt{c} + \sqrt{(1-\beta^2)(1-c)}\,. \tag{15}$$

The same holds not only for pure states, but also for any mixed state.

Let us denote in the following the bound on α^2 from (15) by

$$g(q,a,b) := \sqrt{qc(a,b)} + \sqrt{(1-q)(1-c(a,b))}\,. \tag{16}$$

We further write for simplicity $g(q,a)$ if $a = b$ and simply $g(q)$ if a and b is clear from the context. The above condition imposes constraints on the possible probability distributions $\{q_k\}$ and $\{p_l\}$. For instance, if $(q_0, q_1, q_2, ...)$ is fixed and decreasingly ordered then we get the following set of constraints:

(1) for any k, it holds that

$$p_k \leq g(q,\delta,\delta) \text{ and } \forall l: \;\; p_k \leq g\big(\sum_{i=0}^{l} q_i, (l+1)\delta, \delta\big) \tag{17}$$

(2) for any k_1, k_2, it holds that

$$p_{k_1} + p_{k_2} \leq g(q,\delta,2\delta) \text{ and } \forall l: \;\; p_{k_1} + p_{k_2} \leq g\big(\sum_{i=0}^{l} q_i, (l+1)\delta, 2\delta\big) \tag{18}$$

(n) and in general for any $k_1, k_2, ..., k_n$, it holds for all l that

$$\sum_{j=1}^{n} p_{k_j} \leq g\big(\sum_{i=0}^{l} q_i, (l+1)\delta, n\delta\big)\,. \tag{19}$$

The question is now how to obtain a useful bound using these conditions.

II.2.3. Majorization Bound.

This bound follows an idea from 40. Let us denote by $r = (q \oplus p)_{\leq}$ the decreasingly ordered direct sum of the sequences $q = \{q_k\}$ and $p = \{p_l\}$. Since the function $r \mapsto \sum_k r_k^\alpha$ is Schur convex, we get an upper bound on (11) if we find a sequence w which majorizes any physically possible sequence r. Such an w can now be constructed in the following way[40].

First note that from equation (15) follows that

$$\alpha^2 + \beta^2 \leq 1 + \sqrt{c(a,b)}\,. \tag{20}$$

Assume now that the length of the interevals used for the discretization for position is δq and for momentum δp. We then easily find that for any n

$$\sum_{j=1}^{n} r_j \leq 1 + F_n(\delta q, \delta p)\,, \tag{21}$$

where

$$F_n(\delta q, \delta p) = \max_{1\leq k\leq n} \sqrt{c\big(k\delta q, (n-k)\delta p\big)}\,. \tag{22}$$

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

Hence, we can construct a majorizing sequence w by setting recursively

$$w_1 = 1, \text{ and } w_k = F_k - w_{k-1} \text{ for } k \geq 2\,. \tag{23}$$

The obtained bound on the Renyi-entropy is then

$$H_\alpha(X|\theta) \geq B^\alpha_{\text{Maj}} \tag{24}$$

where

$$B^\alpha_{\text{Maj}} = \frac{1}{1-\alpha} \log\big(\frac{1}{2}\sum_k w_k^\alpha\big)\,. \tag{25}$$

This then translates into a bound on the smooth min-entropy via (7)

$$\frac{1}{n} H^\epsilon_{\min}(X|\theta K) \geq \lambda^\epsilon_{\text{Maj}}\,, \tag{26}$$

with

$$\lambda^\epsilon_{\text{Maj}} = \sup_{1<\alpha\leq 2} \Big(B^\alpha_{\text{Maj}} - \frac{1}{n(\alpha-1)} \log\frac{2}{\epsilon^2}\Big)\,. \tag{27}$$

Since B^α_{Maj} depends on the recursevely defined sequence w in (23), there is no closed form and it can only be computed numerically. And for numerical calculations of a majorizing sequence one has to stop the recursion relation after a finite number of steps N setting $w_N = 1 - w_{N-1}$. But depending on $\delta q, \delta p$, we can always find a finite N such that $F_N \approx 1$, and the cut-off does not severely change the bound. Moreover, one can easily check that it is monotonically decreasing in α which is important in order to do the optimization in α needed for the bound on the smooth min-entropy (7). A plot of the uncertainty relation is shown in Figure 1. Unfortunately, the bound does not scale well for small δ.

II.2.4. Uncertainty Relation for Convex Combinations of Gaussian States.

In order to obtain an improved scaling in δ we consider the uncertainty relation under an additonal constraint. Since in general only Gaussian operations can efficiently been implemented, it is interesting to impose the constraint that the state is a classical mixture of Gaussian states. Here, it is important that we allow arbitrary and even continuous mixtures of Gaussian states. The reason is that a coarse-grained quadrature measurement on one mode of a multimode Gaussian state results in a continuous convex combination 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 $n > 1$ as in 46, this is crucial.

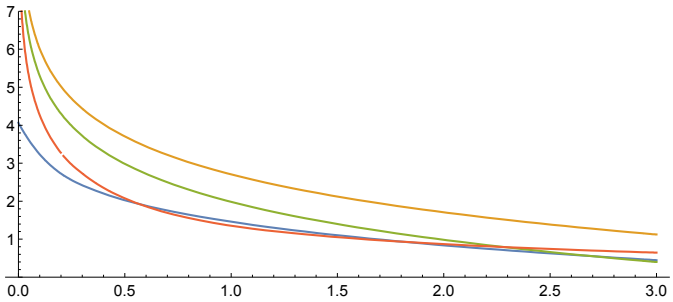

FIG. 1. The plot shows $\lambda^{\epsilon}_{\text{Maj}}$ (blue), $\lambda^{\epsilon}_{\text{Gauss}}$ (orange), $\lambda^{\epsilon}_{\text{IID}}$ (green) and the error correction rate (red) depending on δ for $n = 10^8$, $\epsilon = 10^{-9}$ and $m = 5$. We see that the bound under Gaussian constraint is the strongest. The error correction rate (63) is plotted for $\beta = 1$ and an EPR state with $V = 3$ and Bob's mode sent through a channel with transmissivity $\tau = 0.95$ and $\xi = 0.001$.

Theorem 1. *Let ρ_A be an arbitrary and possibly continuous convex combination of Gaussian states . It then holds that*

$$H_\alpha(X|\theta) \geq B^\alpha_{\textit{Gauss}}(\delta)\,, \tag{28}$$

where

$$B^\alpha_{\textit{Gauss}}(\delta) = \frac{1}{1-\alpha}\log\frac{1}{2}\left(1+\left(\frac{1}{\pi^2}\right)^{\frac{\alpha-1}{\alpha}}\frac{\delta^{2(\alpha-1)}}{\alpha}\right) \tag{29}$$

Proof. We first assume that ρ_A is a Gaussian state. Let us recall that

$$2^{(1-\alpha)H_\alpha(X|\theta)} = 1/2\left(\sum_k q_k^\alpha + \sum_k p_k^\alpha\right) \tag{30}$$

where we use the notation introduced in (11). Denoting the probability density function of the continuous Q measurement by $q(x)$, i.e., $q(x) = \mathrm{tr}(\rho_A E_Q(x))$. We then get that

$$q_k^\alpha = \left(\int_{I_k} q(x)dx\right)^\alpha \leq \delta^{\alpha-1}\int_{I_k} q(x)^\alpha dx \tag{31}$$

which follows directly from Jensen's inequality. Hence, we find for a normal distribution q with standard deviation σ that

$$\sum_k q_k^\alpha \leq \delta^{\alpha-1}\int q(x)^\alpha dx = \delta^{\alpha-1}\frac{1}{\sqrt{\alpha}(\sqrt{2\pi}\sigma)^{\alpha-1}}\,. \tag{32}$$

Note that the bound gets very bad if σ is much smaller than δ, in particular, exceeding the upper bound of 1 which holds trivially for $\sum_k q_k^\alpha$. We avoid that by simply bounding

$$\sum_k q_k^\alpha \leq \min\{\delta^{\alpha-1}\frac{1}{\sqrt{\alpha}(\sqrt{2\pi}\sigma)^{\alpha-1}}, 1\}\,. \tag{33}$$

Let us use that the standard deviations of the position and momentum distribution satisfy $\sigma_Q\sigma_P \leq 1/2$ ($\hbar = 1$). Without loss of generality, we can assume that $\sigma_Q \geq 1/\sqrt{2}$. A straightforward calculation then results in

$$\begin{aligned}\sum_k q_k^\alpha + \sum_k p_k^\alpha &\leq \min\{\frac{\delta^{\alpha-1}}{\sqrt{\alpha}(\sqrt{2\pi}\sigma_Q)^{\alpha-1}}, 1\} + \min\{\frac{\delta^{\alpha-1}}{\sqrt{\alpha}(\sqrt{2\pi}\sigma_P)^{\alpha-1}}, 1\} \\ &\leq \begin{cases} \frac{\delta^{\alpha-1}}{\sqrt{\alpha}(2\pi)^{\alpha-1}}\left(\frac{1}{\sigma_Q^{\alpha-1}} + (2\sigma_Q)^{\alpha-1}\right) & , \sigma_Q \leq \sqrt{\frac{\pi}{2}}\alpha^{\frac{1}{2(\alpha-1)}}/\delta \\ 1 + \frac{\delta^{\alpha-1}}{\sqrt{\alpha}(2\pi)^{\alpha-1}}\frac{1}{\sigma_Q^{\alpha-1}} & , \text{else} \end{cases}\end{aligned}$$

Maximizing the right hand side of the equation over all possible σ_Q, we find that the maximum is exactly attained for $\sigma = \sqrt{\pi/2}\alpha^{1/(2(\alpha-1))}/\delta$. Plugging this in we obtain that

$$\sum_k q_k^\alpha + \sum_k p_k^\alpha \leq 1 + (\frac{1}{2\pi^3})^{\frac{\alpha-1}{2}} \frac{\delta^{2(\alpha-1)}}{\alpha}\,, \tag{34}$$

which finishes the proof for Gaussian states.

Let us now assume that $\rho_A = \int_Y d\mu(y)p(y)\rho_A^y$ with $(Y, d\mu)$ a sigma-finite measure space, p a probability distribution over Y and ρ_A^y a Gaussian state for any y. It then follows that the Q measurement maps ρ_A 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_A^y. The same holds for the P measurement. It thus follows that

$$\sum_k \big(\int_{I_k} dx \int_Y d\mu(y)p(y)\rho_Q^y(x)\big)^\alpha = \sum_k \big(\int_Y d\mu(y)p(y)\int_{I_k} dx\rho_Q^y(x)\big)^\alpha \tag{35}$$

$$\leq \sum_k \int_Y d\mu(y)p(y)\big(\int_{I_k} dx\rho_Q^y(x)\big)^\alpha \tag{36}$$

$$= \int_Y d\mu(y)p(y)\sum_k \big(\int_{I_k} dx\rho_Q^y(x)\big)^\alpha \tag{37}$$

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 $x \mapsto x^\alpha$. Now, by the linearity of the integral we obtain the desired result. □

Similar to the majorization uncertainty relation, we get a bound on the smooth min-entropy via (7)

$$\frac{1}{n}H_{\min}^\epsilon(X|\theta K) \geq \lambda_{\text{Gauss}}^\epsilon(\delta)\,, \tag{38}$$

with

$$\lambda_{\text{Gauss}}^\epsilon(\delta) = \sup_{1<\alpha\leq 1}\Big(B_{\text{Gauss}}^\alpha(\delta) - \frac{1}{n(\alpha-1)}\log\frac{2}{\epsilon^2}\Big)\,. \tag{39}$$

It is easy to see that $B_{\text{Gauss}}^\alpha(\delta) \to 1/(\alpha-1)$ for $\delta \to 0$. Moreover, we get a significantly better scaling than $\lambda_{\text{Maj}}^\epsilon(\delta)$ especially for small δ, see Fig. **??**. As we will see later, that improvement is important to obtain security in the noisy-storage model.

II.3. Smooth Min-Entropy Uncertainty Relation under IID Assumption

Note that for the previous relations the n-mode states ρ_A^k can have arbitrary correlations between the n modes. Let us now 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 has the form $\rho_{A^nK^n} = (\sigma_{A^mK^m})^{\otimes n/m}$, where we assume that $n/m \in \mathbb{N}$.

This assumption simplifies the problem since it allows us to use the asymptotic equipartition property (AEP) of the smooth min-entropy for iid random variables or tensor product states in the quantum case[45,49,50]. The AEP says that for a state $\rho_{A^nB^n} = \rho_{AB}^{\otimes n}$ with $H(A)_\rho < \infty$, the smooth min-entropy can be approximated by the von Neumann entropy, i.e.,

$$\frac{1}{n}H_{\min}^\epsilon(A^n|B^n) \geq H(A|B)_\rho - \frac{4}{\sqrt{n}}\log(\tilde{\eta}(A|B)_\rho)^2\sqrt{\log\frac{2}{\epsilon^2}} \tag{40}$$

where $\tilde{\eta}(A|B)_\rho = 2^{-H_{\min}(A|B)_\rho/2} + 2^{H_{1/2}(A|B)_\rho/2} + 1$. Here, $H(A)_\rho = \operatorname{tr}\rho_A\log\rho_A$ is the von Neumann entropy and $H(A|B)_\rho = H(AB)_\rho - H(B)_\rho$ is the conditional von Neumann entropy.

Applying the above inequality to the setting described in Section II.1 under the assumption that $\rho_{A^nK^n} = (\sigma_{A^mK^m})^{\otimes n/m}$, we obtain that

$$\frac{1}{n}H_{\min}^\epsilon(X^n|\theta^nK^n) \geq \frac{1}{m}H(X^m|\theta^mK^m)_\sigma - 4\sqrt{\frac{m}{n}}\log(\eta(X^m)_\sigma)^2\sqrt{\log\frac{2}{\epsilon^2}}\,, \tag{41}$$

where $\eta(X^m)_\sigma = 2 + 2^{H_{1/2}(X)_\sigma} \geq \tilde{\eta}(X^m|\theta^mK^m)_\sigma$.

Now we can simply use the uncertainty relation for the von Neumann entropy with classical side information[51]

$$H(X^m|K\Theta=\theta)+H(X_\delta^m|K\Theta=\bar{\theta})\geq -m\log c(\delta)\,, \tag{42}$$

where $c(\delta)=\delta^2/(e\pi)$ and $\bar{\theta}=(\theta_i-1)_{i=1}^m$ denotes the complementary basis choice of $\theta=(\theta_i)_{i=1}^m$. This then implies that

$$H(X|\Theta K)=\frac{1}{2^m}\sum_\theta \frac{1}{2}\big(H(X^m|K\Theta=\theta)+H(X_\delta^m|K\Theta=\bar{\theta})\big)\geq -\frac{m}{2}\log c(\delta)\,. \tag{43}$$

Hence, we obtain the following uncertainty relation

$$\frac{1}{n}H_{\min}^\epsilon(X^n|\theta^n K^n)\geq \lambda_{\text{IID}}^\epsilon(\delta) \tag{44}$$

where

$$\lambda_{\text{IID}}^\epsilon(\delta)=-\frac{1}{2}\log c(\delta)-4\sqrt{\frac{m}{n}}\log(\eta(X^m)_\sigma)^2\sqrt{\log\frac{2}{\epsilon^2}}\,. \tag{45}$$

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

$$\lambda_{\text{IID}}^\epsilon(\delta)=-\frac{1}{2}\log c(\delta)-\mathcal{O}(m^2\sqrt{\frac{m}{n}})\,. \tag{46}$$

For comparison with the bound under Gaussian constraint, see Figure 1.

III. OBLIVIOUS TRANSFER

We consider a protocol that implements a randomized version of oblivious transfer (ROT) (see, e.g., 23 and 30). Alice has no input and obtains as output two random strings $s_0,s_1\in\{0,1\}^\ell$, and Bob has an input $c\in\{0,1\}$ and obtains a string $\tilde{s}_b=s_c$. This randomized OT protocol can then be turned into usual oblivious transfer by adding a simple classical communication step (see, e.g., 30). We start with a precise definition of the correctness and the security of ROT. In order to ensure composable security, we adopt the security definitions from 23, but allow our protocol to abort for clarity of exposition. However, it is straightforward to extend our protocol along the lines of 23 to deal with the general case.

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.

Definition 1. *A protocol between two parties Alice and Bob that takes input $c\in\{0,1\}$ from Bob and outputs on Alice's side two bit strings S_0,S_1 in $\{0,1\}^\ell$ and on Bob's side S_B is called an $(\epsilon_C,\epsilon_A,\epsilon_B)$-ROT protocol if the following holds.*

- *The protocol is ϵ_C-correct, that is, if the protocol does not abort and both parties follow the protocol, then the output of the protocol $\rho_{S_0S_1S_BC}$ satisfies*

$$\|\rho_{S_0S_1S_B|C=c}-\tau_{S_{\bar{c}}}\otimes\Omega_{S_cS_B}\|_1\leq\epsilon_C\,. \tag{47}$$

- *The protocol is ϵ_A-secure for Alice, that is, if the protocol does not abort and Alice follows the protocol, then for any strategy of Bob with output $\rho_{S_0S_1B'}$, where B' denotes Bob's register at the end of the protocol, holds that there exists a random variable D with range $\{0,1\}$ such that*

$$\|\rho_{S_{\bar{D}}S_DDB'}-\tau_{S_{\bar{D}}}\otimes\rho_{S_DDB'}\|_1\leq\epsilon_A\,. \tag{48}$$

- *The protocol is ϵ_B-secure for Bob, that is, if the protocol does not abort and Bob follows the protocol, then for any strategy of Alice with output $\rho_{A'S_BC}$ there exist random variables S_0',S_1' such that $\rho_{A'S_0'S_1'S_BC}$ satisfies that $\Pr[Y\neq S_c]\leq\epsilon_B$ and*

$$\|\rho_{A'S_0'S_1'|C=0}-\rho_{A'S_0'S_1'|C=1}\|_1\leq\epsilon_B\,. \tag{49}$$

III.1. CV ROT Protocol

We consider a generalization of the ROT protocol in 30 for continuous-variable encoding. But since the measurement outcomes of Alice and Bob do not perfectly match even if both chose the same basis, some error-correction information has to be exchanged. We first state the entanglement-based version of the protocol and then describe how this can equivalently be implemented as a prepare-and-measure scheme.

1) Alice (or Bob) distributes n EPR states (two-mode squeezed states) and sends from each one mode to Alice. Both then perform coarse-grained measurements in random independent basis choices $\theta_A, \theta_B \in \{0,1\}^n$ (see Section II.1 for the notation) obtaining measurement outcomes X and Y.

2) They wait for a fixed time Δt.

3) Alice sends Bob her basis choice θ_A. Bob defines the sets $I_c = \{i \in [n] | \theta_A^i = \theta_B^i\}$ and $I_{\bar{c}} = [n] \backslash I_c$ and sends I_0, I_1 to Alice. For simplicity we assume that $|I_0| = |I_1| = n/2$, as Alice aborts if this is not approximately true (see[23] for a rigorous treatment).

4) Alice forms the strings $X_k = (X^i)_{i \in I_k}$ for $k = 0, 1$. She then computes individually for X_0, X_1 error-correction syndromes W_0, W_1, and chooses random two-universal hash functions g_0, g_1 to a bit string of length $\log 1/\epsilon_C$. Alice then sends $W_0, W_1, g_0, g_1, g_0(X_0), g_1(X_1)$ to Bob who corrects his string $Y_c = (Y^i)_{i \in I_c}$ according to W_c to obtain Y_c'. He then checks that $g_c(X_c) = g_c(Y_c')$ and aborts otherwise.

5) Alice chooses random two-universal hash functions f_0, f_1 to an ℓ-bit string and outputs $s_k = f_k(X_k)$, $k = 1, 2$. She then sends f_0, f_1 to Bob who outputs $f_c(Y_c')$.

Let us first note that conditioned on the measurement of the sender, the state of the receiver is given by a squeezed state displaced according to a normal distribution. Hence, the above entanglement-based protocol is completely equivalent to a prepare-and-measure protocol in which the sender simply prepares the squeezed states and displaces them according to the corresponding normal distribution.

Intuitively, correctness is ensured since the outcomes of Alice and Bob are correlated when measured in the same basis. By sending sufficient error-correction (EC) information, i.e., $\ell_{\text{EC}} \approx nH(X|Y)$, Bob can recover Alice's string. Security for Bob follows since he only sends the information I_0, I_1 which is independent of c and can be formalized as in 23. Security for Alice is more delicate to prove. In fact, if malicious Bob has a perfect quantum memory that can store the n modes over the time Δt, he can wait until Alice sends her basis choice θ_A and measure accordingly. Thus, he obtains both s_0 and s_1. But as we show in the following, if Bob's memory device is noisy, he will not have enough information to recover both of the strings.

From a theoretical point of view, the protocols where Alice or Bob distributes the EPR pairs in step 1 are completely equivalent. Since, the amount of error-correcting information is smaller if Bob takes the role of the sender the theoretical trade-off turns out to be better. But from a practical point one can certainly argue that it is favorable if Alice distributes the states. The reason is simply that certain memories are probabilistic and Bob could distribute the states conditioned on successfully storing his mode.

III.2. Security Analysis

Correctness

ϵ_C-correctness follows directly from the definition of the protocol. Namely, if $g_c(X_c) = g_c(Y_c')$ is satisfied we know due to the properties of two-universal hash functions that the probability that $S_B = S_c$ is ϵ_C.

Security for Bob

The security for Bob follows from similar reasons as in[23].

Security for Alice

An arbitrary attack of Bob can be modeled as follows (see, e.g., 23). First, Bob applies an encoding strategy to his n modes B^n mathematically described by $\mathcal{M} = \{\mathcal{M}_k\}_k$, where $\mathcal{M}_k$ is a non-normalized quantum channel from the Hilbert space $L^2(\mathbb{R})^{\otimes n}$

to $\mathcal{H}_{Q_{\text{in}}}$ such that $\sum_k \mathcal{M}_k$ is a normalized quantum channel. We consider $\mathcal{M}$ as a map that takes a state ρ_{B^n} in B^n and outputs a classical quantum state

$$\rho_{KQ_{\text{in}}} = \sum_k |k\rangle\langle k| \otimes \mathcal{M}_k(\rho_{B^n}) \,, \tag{50}$$

on K and Q_{in}. Bob then stores the quantum part Q_{in} in a quantum memory described by a quantum channel $\mathcal{F} : \mathcal{S}(Q_{\text{in}}) \to \mathcal{S}(Q_{\text{out}})$. Here, $\mathcal{S}(Q_{\text{in}})$ denotes the state space corresponding to $\mathcal{H}_{Q_{\text{in}}}$, i.e., density operators on $\mathcal{H}_{Q_{\text{in}}}$ with unit trace. After time Δt, Bob obtains the basis information θ_A, and subsequently, the error correction syndromes $W = (W_0, W_1)$ together with the hash functions $H = (F_0, F_1, G_0, G_1)$ and the check values $C = (G_0(X_0), G_1(X_1))$. Hence, the state shared by Alice and Bob at the end of the protocol is given by $\rho_{S_0 S_1 Q_{\text{out}} B_{\text{cl}}}$, where $B_{\text{cl}} = \theta_A K W H C$ are Bob's classical registers.

The goal of the security analysis is to show that there exists a random variable D such that

$$\|\rho_{S_{\bar{D}} S_D D Q_{\text{out}} B_{\text{cl}}} - \tau_{S_{\bar{D}}} \otimes \rho_{S_D D Q_{\text{out}} B_{\text{cl}}}\|_1 \leq \epsilon_A. \tag{51}$$

The privacy amplification lemma[42] against infinite-dimensional quantum adversaries[43] tells us that (51) is satisfied if we choose ℓ equal or lower than

$$H_{\min}^{\epsilon_1}(X_D|S_{\bar{D}} D Q_{\text{out}} B_{\text{cl}}) - 2\log\frac{1}{\epsilon_A - 4\epsilon_1} \,, \tag{52}$$

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

Hence, we have to lower bound the smooth min-entropy. For this purpose we follow similar arguments as in[23,30]. Therein, a central ingredient is the connection between min-entropy of a state $\rho_{XZ\mathcal{F}(Q_{\text{in}})}$ with XZ classical and $\mathcal{F}$ a quantum channel from $\mathcal{Q}_{\text{in}}$ to $Q_{\text{out}} = \mathcal{F}(Q_{\text{in}})$, and the success rate R of classical coding sent through $\mathcal{F}$ given by

$$\mathcal{P}_{\text{succ}}^{\mathcal{F}}(nR) := \sup_{\rho_k, D_k} \frac{1}{2^{nR}} \sum_k \text{tr}(D_k \mathcal{F}(\rho_k)) \tag{53}$$

where the supremum runs over ensembles of code states $(\rho_k)_{k=1}^{nR}$ and POVM's $(D_k)_{k=1}^{nR}$ used to decode the classical information sent through the channel. It has been shown in 23 that (see Lemma 2)

$$H_{\min}^{\epsilon+\epsilon'}(X|\mathcal{F}(Q_{\text{in}})Z) \geq -\log \mathcal{P}_{\text{succ}}^{\mathcal{F}}\big(\lfloor H_{\min}^{\epsilon}(X|Z)_\rho - \log 1/\epsilon'^2 \rfloor\big) \,. \tag{54}$$

Applying the above inequality to the smooth entropy in (52) and using basic properties of the smooth min-entropy[44,52], we obtain

$$\begin{aligned} H_{\min}^{\epsilon_1}(X_D|S_D D Q_{\text{out}} B_{\text{cl}}) &\geq H_{\min}^{\epsilon_1}(X_D|D Q_{\text{out}} B_{\text{cl}}) - \log|S_{\bar{D}}| \\ &\geq -\log\Big(\mathcal{P}_{\text{succ}}^{\mathcal{F}}\big(\lfloor H_{\min}^{\epsilon_2}(X_D|DB_{\text{cl}}) - \log\frac{1}{(\epsilon_1-\epsilon_2)^2}\rfloor\big) \\ &\quad - \log|S_{\bar{D}}| \,. \end{aligned}$$

Using that $\log|S_{\bar{D}}| = \ell$, we obtain together with (52) that (51) is satisfied if we choose ℓ smaller or equal to

$$-\frac{1}{2}\log\Big(\mathcal{P}_{\text{succ}}^{\mathcal{F}}\big(\lfloor H_{\min}^{\epsilon_2}(X_D|DB_{\text{cl}}) - \log\frac{1}{(\epsilon_1-\epsilon_2)^2}\rfloor\big) - \log\frac{1}{\epsilon_A - 4\epsilon_1} \,. \tag{55}$$

The goal of the next part is to lower bound the smooth min-entropy $H_{\min}^{\epsilon_2}(X_D|DB_{\text{cl}})$. For that we use the min-entropy splitting theorem[20], (see also Lemma 3), which tells us that there exists a random variable D such that

$$H_{\min}^{\epsilon}(X_D|DB_{\text{cl}}) \geq \frac{1}{2} H_{\min}^{\epsilon}(X_0X_1|B_{\text{cl}}) - 1 \,. \tag{56}$$

Recall now that Bob's classical register B_{cl} is given by $\theta_A K W H C$ such that we can bound

$$\begin{aligned} H_{\min}^{\epsilon}(X_0X_1|B_{\text{cl}}) &\geq H_{\min}^{\epsilon}(X_0X_1|\theta_A K) - \log|W| - \log|C| \\ &\geq H_{\min}^{\epsilon}(X_0X_1|\theta_A K) - \ell_{\text{EC}} - 2\log\frac{1}{\epsilon_C} \,, \end{aligned}$$

where we defined ℓ_{EC} as the amount of bits sent in the error correction, and used that the hash functions are drawn independently at random and that C is the check information for error correction.

Now, we can bound the smooth min-entropy $H_{\min}^{\epsilon}(X_0X_1|\theta_A K)$ can be bounded by the uncertainty relations in Section II. In the following, we say that the measurement setup satisfies an uncertainty rate $\lambda_\epsilon(n)$ if under the given assumption the uncertainty relation

$$H_{\min}^{\epsilon}(X|K\theta) \geq n\lambda_\epsilon(n)\,, \tag{57}$$

where n stands for the number of rounds and $X = X_0X_1$.

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

Theorem 2. *Let Alice's measurement setup has an uncertainty rate $\lambda_\epsilon(n)$ and let us assume that the total number of bits for the error correction is ℓ_{EC}. Then an ϵ_C-correct protocol as defined in Section III.1 allows the oblivious transfer of ℓ bits with ϵ_A-security for Alice if*

$$\ell \geq -\frac{1}{2}\log \mathcal{P}_{succ}^{\mathcal{F}}\big(\lfloor\frac{1}{2}(n\lambda_{\epsilon_2}(n) - \ell_{EC} - 2\log\frac{1}{\epsilon_C}) - \log\frac{1}{(\epsilon_1-\epsilon_2)^2} - 1\rfloor\big) \tag{58}$$

$$- \log\frac{1}{\epsilon_A - 4\epsilon_1}\,, \tag{59}$$

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

Note that in the case that the left-hand side of (58) is negative, an implementation of the ROT protocol is not possible.

Let us now assume that $\mathcal{F} = \mathcal{E}^{\otimes \nu n}$ with $\nu \geq 0$, and that the classical capacity of $\mathcal{E}$ satisfies a strong converse. That is, the success probability $P_{\text{succ}}(nR)$ for sending classical information at a rate R bigger than the classical capacity $\mathcal{C}(\mathcal{E})$ is exponentially suppressed

$$\mathcal{P}_{\text{succ}}^{\mathcal{E}}(nR) \leq e^{-n(R-\mathcal{C}(\mathcal{E}))}\,. \tag{60}$$

Plugging this into (58), we find that in order to obtain a secure protocol for sufficiently large n the condition

$$1/2(\lambda_{\epsilon_2} - r_{\text{EC}}) \geq \nu\mathcal{C}(\mathcal{E}) \tag{61}$$

has to be satisfied, where where $r_{\text{EC}} = \ell_{\text{EC}}/n$ is the error correction rate.

A necessary condition is thus

$$1/2(\lambda_{\epsilon_2} - r_{\text{EC}}) > 0\,. \tag{62}$$

From the Slepian-Wolf theorem[53], we know that in the asymptotic limit the error-correction rate is given by the conditional Shannon entropy $H(X|Y)$, where Y denotes Bob's measurement outcomes measured in the same basis as Alice. In order to account for the correction due to a finite number of communication rounds, we introduce the error correction efficiency $\beta \leq 1$ and the corresponding rate as

$$r_{\text{EC}} = H(X) - \beta I(X:Y)\,. \tag{63}$$

Note that $\beta = 1$ corresponds to the asymptotic limit. Recent advances in error correction codes for correlated Gaussian variables allow for efficiencies $\beta \geq 0.95$[33–35].

Let us now analyze the quantity in (62) for the different uncertainty relations derived in Section II, which are plotted in Figure 2. In the following, we assume that the EPR state is distributed by Alice and that its covariance matrix is parametrized by the variance V, the transmissivity of Bob's mode τ and the excess noise ξ. The corresponding covariance matrix is then given by

$$\begin{pmatrix} VI & \sqrt{\tau(V^2-1)}Z \\ \sqrt{\tau(V^2-1)}Z & V_B(\tau,\xi)I \end{pmatrix} \tag{64}$$

with I the identity in $\mathbb{C}^2$, $Z = \text{diag}(1,-1)$ and $V_B(\tau,\xi) = \eta V + (1-\tau)1/2 + \tau\xi$. Since large distances are not particularly required for the usefulness of the OT protocol, we assume in Figure 2 that $\tau = 0.95$ and $\xi = 0.001$.

We then see that for the majorization uncertainty relation which holds without any additional assumptions, there is only a very limited range of δ for which (62) is positive and it is always smaller than 0.1. As this value has to be larger than the classical capacity of the memory channel, we have to assume a very low capacity of Bob's memory channel which is problematic especially for CV systems.

The situation looks better for the uncertainty relation obtained under additional assumptions. The best performance is obtained under the assumption that Bob's quantum memory can be described by (mixtures) of Gaussian operations, see Theorem 1.

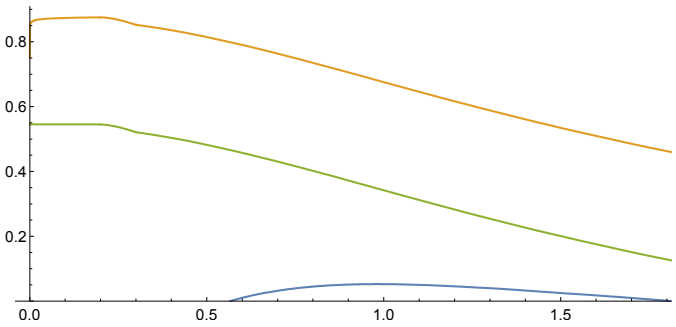

FIG. 2. The plot shows the difference (62) for $\lambda^{\epsilon}_{\text{Maj}}$ (blue), $\lambda^{\epsilon}_{\text{Gauss}}$ (orange), $\lambda^{\epsilon}_{\text{IID}}$ (green) depending on δ for $n = 10^8$, $\epsilon = 10^{-9}$ and $m = 1$. The error-correction rate (63) is plotted for $\beta = 1$ and an EPR state with $V = 3$ and Bob's mode sent through a channel with transmissivity $\tau = 0.95$ and $\xi = 0.001$.

Although not clearly seen in Figure 2, the difference goes to $-\infty$ in the limit $\delta \to 0$. Under the iid assumptin, Section II.3, we find a slightly smaller value for (62) than in under the Gaussian constraint. However, the quantity goes to a constant value for small enough δ since the error-correction rate scales similarly in δ as the bound $\lambda^{\epsilon}_{\text{IID}}(\delta)$, namely, like $-\log\delta$. In fact for sufficently small δ we can approximate the error correction rate as $r = H(X|Y) \approx h(X|Y) - \log\delta$, where $h(X|Y)$ is the differential conditional Shannon entropy and we set $\beta = 1$. Hence, for large n we find that

$$\begin{aligned} 1/2(\lambda^{\epsilon_2}_{\text{IID}} - r_{\text{EC}}) &\approx \log\sqrt{e\Pi} - h(X|Y) - \mathcal{O}(m^2\sqrt{\frac{m}{n}}) \\ &= \log\sqrt{e\Pi} - \log\left(\sqrt{2\pi e}\frac{V_X V_{X|Y}}{V_Y}\right) - \mathcal{O}(m^2\sqrt{\frac{m}{n}}) \\ &= \log\left(\frac{1}{\sqrt{2}}\frac{V_Y}{V_X V_{X|Y}}\right) - \mathcal{O}\left(m^2\sqrt{\frac{m}{n}}\right) . \end{aligned}$$

Thus, we need that the conditional variance is small enough such that

$$V_{X|Y}\frac{V_X}{V_Y} \leq \frac{1}{\sqrt{2}} . \tag{65}$$

III.3. Application to Bosonic Gaussian Memory Channels

Let us now consider the security of the ROT protocol if Bob's memory channel (or a part of it) can be modeled by a phase-insensitve Gaussian channel that acts on a single-mode covariance matrix as

$$\Gamma \mapsto T\Gamma T^T + N , \tag{66}$$

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

For phase-insensitive Gaussian channels a strong converse has recently been established[37–39]. Note first that the classical capacities for bosonic channels are only bounded under a mean-energy constraint, i.e., if the average photon number N_{av} of the average code state is finite. Then, the classical capacities are given by[54,55]

$$C(\mathcal{E}_{t,v}|N_{\text{av}}) = g\big(tN_{\text{av}} + (t+v-1)/2\big) - g\big((t+v-1)/2\big) , \tag{67}$$

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

A slightly stronger restriction than only an average-photon-number constraint has to be imposed in order for a strong-converse bound to hold[37]. Namely, a constraint on the maximal photon number has to hold. 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[37]

$$\text{tr}\left(\Pi_{nN_{\max}}\rho^n\right) \geq 1 - \delta(n) \tag{68}$$

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

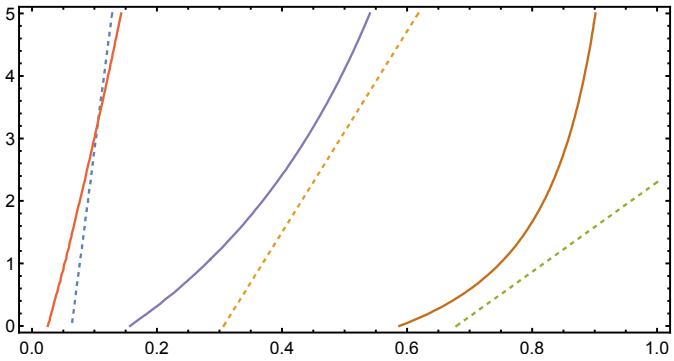

FIG. 3. The plots show when condition (71) is satisfied with equality for $\lambda^{\epsilon}_{\text{Gauss}}$. On the horizontal axis the transmissivity η is plotted and the vertical axis corresponds to the mean photon number N_{th} of the thermal noise channel (solid) and the noise variance V_N (dashed) for $N_{\max} = 30$ and $\nu = 1, 1/3, 1/5$ (from left to right). For the solid line we set $V_N = 2$ and for the dashed lines $N_{\text{th}} = 1$. The EPR state has variance $V = 3$ and Bob's mode is subjected to transmissivity $\tau = 0.96$ and $\xi = 0.001$. Moreover, error-correction efficiency is set to $\beta = 0.96$, $n = 10^8$ and $\epsilon = 10^{-9}$.

The strong converse theorem for any phase-insensitive channel $\mathcal{E}$ from 39 then says that the success probability for the transmission under the MPNC decays as

$$\mathcal{P}^{\mathcal{E}}_{\text{succ}}(nR|N_{\max}) \leq 2^{-n(R-C(\mathcal{E}|N_{\max})-\delta_1} + 2^{n\delta_2} + \delta_3(n)\,, \tag{69}$$

where δ_1, δ_2 are arbitrary small constants and $\delta_3(n) = \sqrt{\delta(n) + \sqrt{\delta(n)} + \delta_3(n)}$ with $\delta(n)$ given in (68) and $\delta_3(n)$ is exponentially decreasing in n.

In order to apply the above result to the noisy-storage model, we assume that Bob's memory channel is given by

$$\mathcal{F} = \mathcal{E}^{\otimes \nu n} \tag{70}$$

where $\mathcal{E}$ is a phase-insensitive Gaussian one-mode channel that works only properly if the channel input Q_{in} satisfies the MPNC with $N_{\max}$. Otherwise, we assume that the channel acts like a constant channel and the capacity is equal to 0.

We then obtain from Theorem 2 that if the condition

$$\frac{1}{2}(\lambda_{\epsilon_2}(n_0) - \ell_{\text{EC}}/n_0)) > \nu C(\mathcal{E}|N_{\text{in}}) \tag{71}$$

is satisfied for an n_0, we can find an appropriate $N_0 \geq n_0$ such that for any $n \geq N_0$, the length of the bit string in the ROT protocol scales like $\ell \approx n(\frac{1}{2}(\lambda_{\epsilon_2}(n_0) - \ell_{\text{EC}}/n_0)) - \nu C(\mathcal{E}|N_{\max})$.

III.3.0.1. Thermal Noise Channel with Additive Gaussian White Noise. The thermal channel can be modeled as 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 (66), it is expressed by $t = \eta$ and $v = (1-\eta)(1+2N_{\text{th}})$. And if we include additional additive Gaussian noise V_n, the parameters are $t = \eta$ and $v = (1-\eta)(1+2N_{\text{th}}) + V_n$.

In Figure 3, 4 and 5, we show when condition (71) is satisfied with equality. Hence, the left-hand side of the plots specifies the condition on Bob's memory for which security in the noisy-storage model can be obtained. We emphasize that security with coherent states can be achieved under Gaussian assumption, see Figure 4.

IV. CONCLUSION

We have presented an OT protocol for CV systems that provides security in the noisy storage model. The protocol is practical and uses similar resources as CV QKD. Under the constraint that Bob uses a Gaussian memory attack, an implementation with coherent states can provide security. As a key ingredient, we analyze and derive uncertainty relations for CV systems, which can be used along similar lines to analyze the security in the noisy-storage model for other protocols such as bit commitment or secure password-based identification[23,29,30]. We leave as open problem the task of finding optimal uncertainty relations without any further assumptions. It is possible such relations can be obtained by linking security again to the quantum capacity of the storage device[22,25], requiring however more sophisticated techniques. Such a result would also pose a challenge to find an explicit strong converse for the quantum capacity for bosonic channels.

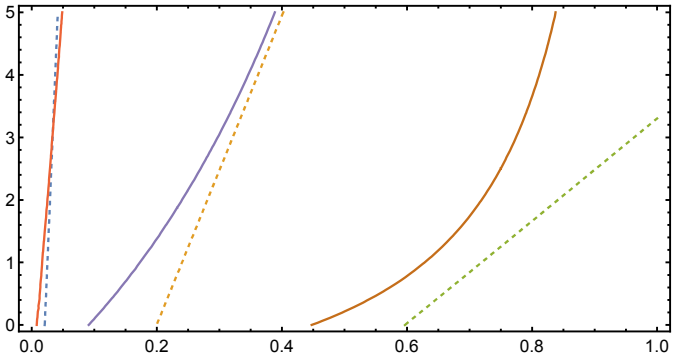

FIG. 4. The plots are exactly the same as in Figure 3 except that it is for coherent states ($V = 1/2$) and $\nu = 1, 1/6, 1/12$ (from left to right).

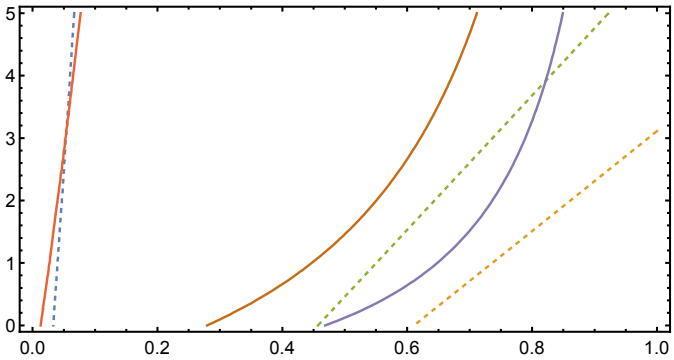

FIG. 5. The plots show when condition (71) is satisfied with equality for $\lambda^{\epsilon}_{\text{IID}}$. On the horizontal axis the transmissivity η is plotted and the vertical axis is the means photon number N_{th} of the thermal noise channel (solid) and the noise variance V_N for the additive Gaussian noise for $(\nu, m) = (1, 1), (1/8, 1), (1/8, 10)$ (from left to right). For the solid line we set $V_N = 2$ and for the dashed lines $N_{\text{th}} = 1$. The other parameters are as in Figure 3.

Acknowledgements

We would like to thank Anthony Leverrier, Loïck Magnin and Frédéric Grosshans for useful discussions about the continuous-variable world. FF is supported by the Japan Society for the Promotion of Science (JSPS) by KAKENHI grant No. 24-02793. CS is supported by a 7th framework EU SIQS grant.

Appendix A: Technical Lemmas

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

$$H^{\epsilon}_{\min}(X|Y) \geq H_{\alpha}(X|Y) - \frac{1}{\alpha - 1} \log \frac{2}{\epsilon^2} \,. \tag{A1}$$

Proof. The lemma has been shown for finite-dimensional systems in[45]. An easy way to show it in the infinite-dimensional case is by means of the approximation result from[50]. This allows us to obtain

$$H^{\epsilon}_{\min}(X|Y)_{\rho} \geq H^{\epsilon-\delta}_{\min}(X|Y)_{P_k \rho P_k} \tag{A2}$$

$$\geq H_{\alpha}(X|Y)_{P_k \rho P_k} - \frac{1}{\alpha - 1} \log \frac{2}{(\epsilon - \delta)^2} \tag{A3}$$

where $P_k = P^X_k \otimes P^Y_k$ is a projector onto a finite-dimension subspace such that $P_k \rho P_k$ is δ-close to ρ. Note that such a projection always exists for any δ. Next, we use that $H_{\alpha}(X|Y)_{P_k \rho P_k} \to H_{\alpha}(X|Y)_{\rho}$ for $k \to \infty$. This follows simply since all the sums involved in the definition of the α entropy converge absolutely, and thus, can be rearranged. This then leads to the

conclusion that

$$H_{\min}^{\epsilon}(X|Y)_{\rho} \geq H_{\alpha}(X|Y)_{\rho} - \frac{1}{\alpha - 1} \log \frac{2}{(\epsilon - \delta)^2} \tag{A4}$$

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

The following statement has been shown in[23] and generalizes straightforwardly to infinite dimensions using the same strategy as in the proof above based on the approximation theorem in[50].

Lemma 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}, and set $k_{\epsilon,\epsilon'} = \lfloor H_{\min}^{\epsilon}(X|K)_{\rho} - \log 1/\epsilon'^2 \rfloor$. Then, it holds that*

$$H_{\min}^{\epsilon+\epsilon'}(X|\mathcal{F}(Q_{in})K) \geq -\log \mathcal{P}_{succ}(k_{\epsilon}, \epsilon') \,. \tag{A5}$$

The technique of min-entropy splitting is due to[56], and used as the following Lemma in[20], which generalizes by a simple application of the approximation in[50] to arbitrary alphabet sizes.

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

$$H_{\min}^{\epsilon}(X_D|DY) \geq \frac{1}{2} H_{\min}^{\epsilon}(X_0 X_1|Y) - 1 \,. \tag{A6}$$

[1] S. Wiesner, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing pp. 175–179 (1984), originally written c. 1970 but unpublished.
[2] C. H. Bennett and G. Brassard, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing pp. 175–179 (1984).
[3] A. Ekert, Physical Review Letters **67**, 661 (1991).
[4] D. Mayers, Physical review letters **78**, 3414 (1997).
[5] D. Mayers (1996), arXiv:quant-ph/9603015v3.
[6] H.-K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997), arXiv:quant-ph/9603004v2.
[7] H.-K. Lo and H. Chau, in *Proceedings of PhysComp96* (1996), arXiv:quant-ph/9605026v2.
[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), arXiv:quant-ph/0605224v2.
[10] H. Buhrman, M. Christandl, and C. Schaffner, Physical review letters **109**, 160501 (2012).
[11] M. Ben-Or, S. Goldwasser, J. Kilian, and A. Widgerson, in *Proc. ACM STOC* (ACM Press, New York, New York, USA, 1988), pp. 113–131, ISBN 0897912640, URL http://portal.acm.org/citation.cfm?doid=62212.62223.
[12] A. Kent, Phys. Rev. Lett. **83**, 1447 (1999), URL http://link.aps.org/doi/10.1103/PhysRevLett.83.1447.
[13] S. Croke and A. Kent, Phys. Rev. A **86**, 052309 (2012), URL http://link.aps.org/doi/10.1103/PhysRevA.86.052309.
[14] A. Kent, Phys. Rev. Lett. **109**, 130501 (2012), URL http://link.aps.org/doi/10.1103/PhysRevLett.109.130501.
[15] J. Kaniewski, M. Tomamichel, E. Hänggi, and S. Wehner, IEEE Transactions on Information Theory (to be published) (2013).
[16] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner, and H. Zbinden, Phys. Rev. Lett. **111**, 180504 (2013), URL http://link.aps.org/doi/10.1103/PhysRevLett.111.180504.
[17] U. Maurer, Journal of Cryptology **5**, 53 (1992).
[18] C. Cachin and U. M. Maurer, in *Proceedings of CRYPTO 1997* (1997), Lecture Notes in Computer Science, pp. 292–306.
[19] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner, SIAM Journal on Computing **37**, 1865 (2008).
[20] I. B. Damgård, S. Fehr, R. Renner, L. Salvail, and C. Schaffner, in *Advances in Cryptology-CRYPTO 2007* (Springer, 2007), pp. 360–378.
[21] S. Wehner, C. Schaffner, and B. M. Terhal, Physical Review Letters **100**, 220502 (2008).
[22] F. Dupuis, O. Fawzi, and S. Wehner, Information Theory, IEEE Transactions on **61**, 1093 (2015).
[23] R. Konig, S. Wehner, and J. Wullschleger, IEEE Transactions on Information Theory **58**, 1962 (2012).
[24] M. Berta, F. G. Brandao, M. Christandl, and S. Wehner, Information Theory, IEEE Transactions on **59**, 6779 (2013).
[25] M. Berta, O. Fawzi, and S. Wehner, in *Advances in Cryptology CRYPTO 2012* (2012), vol. 7417 of *Lecture Notes in Computer Science*, pp. 776–793, ISBN 978-3-642-32008-8.
[26] N. H. Y. Ng, S. K. Joshi, C. C. Ming, C. Kurtsiefer, and S. Wehner, Nature communications **3**, 1326 (2012).
[27] C. Erven, N. Ng, N. Gigov, R. Laflamme, S. Wehner, and G. Weihs, Nature communications **5** (2014).
[28] D. Unruh, in *Advances in Cryptology–EUROCRYPT 2011* (Springer, 2011), pp. 467–486.
[29] S. Wehner, M. Curty, C. Schaffner, and H.-K. Lo, Physical Review A **81**, 052336 (2010), arXiv:0911.2302v2.
[30] C. Schaffner, Phy. Rev. A **82**, 032308 (2010).
[31] H.-K. Lo, M. Curty, and K. Tamaki, Nature Photonics **8**, 595 (2014).
[32] 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), URL http://link.aps.org/doi/10.1103/RevModPhys.84.621.
[33] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, in *Information Theory, 2008. ISIT 2008. IEEE International Symposium on* (IEEE, 2008), pp. 1020–1024.
[34] P. Jouguet, D. Elkouss, and S. Kunz-Jacques, Physical Review A **90**, 042329 (2014).
[35] T. Gehring, V. Händchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R. F. Werner, and R. Schnabel, arXiv:1406.6174 (2014).
[36] J. Kilian, in *Proceedings of the twentieth annual ACM symposium on Theory of computing* (ACM, 1988), pp. 20–31.
[37] M. M. Wilde and A. Winter, Problems of Information Transmission **50**, 117 (2014).
[38] B. R. Bardhan and M. M. Wilde, Physical Review A **89**, 022302 (2014).
[39] B. R. Bardhan, R. Garcia-Patron, M. M. Wilde, and A. Winter, arXiv preprint arXiv:1401.4161 (2014).

[40]Ł. Rudnicki, Physical Review A **91**, 032123 (2015).
[41]F. Furrer, M. Berta, M. Tomamichel, V. B. Scholz, and M. Christandl, Journal of Mathematical Physics **55**, 122205 (2014).
[42]M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, Proceedings of IEEE Symposium on Information Theory pp. 2703–2707 (2010), arXiv:1002.2436v1.
[43]M. Berta, F. Furrer, and V. B. Scholz, arXiv preprint arXiv:1107.5460 (2011).
[44]M. Tomamichel, Ph.D. thesis, ETH Zürich (2013).
[45]M. Tomamichel, R. Colbeck, and R. Renner, IEEE Transactions on Information Theory **55**, 5840 (2009).
[46]N. H. Y. Ng, M. Berta, and S. Wehner, Phys. Rev. A **86**, 042315 (2012), URL `http://link.aps.org/doi/10.1103/PhysRevA.86.042315`.
[47]H. J. Landau and H. O. Pollak, The Bell System Technical Journal **65**, 43 (1961).
[48]H. Dym and H. P. McKean, *Fourier Series and Integrals* (Academic, New York, 1972).
[49]R. Renner, Ph.D. thesis, ETH Zurich (2005), URL `http://arxiv.org/abs/quant-ph/0512258`.
[50]F. Furrer, J. Aberg, and R. Renner, Communications in Mathematical Physics **306**, 165 (2011).
[51]I. Bialynicki-Birula, Physics Letters **103**, 253 (1984).
[52]M. Berta, F. Furrer, and V. B. Scholz (2011), arXiv:1107.5460v1.
[53]D. Slepian and J. Wolf, IEEE Transactions on Information Theory **19**, 461 (1971).
[54]V. Giovannetti, A. Holevo, and R. Garcia-Patron, arXiv preprint arXiv:1312.2251 (2013).
[55]V. Giovannetti, R. Garcia-Patron, N. Cerf, and A. Holevo, arXiv preprint arXiv:1312.6225 (2013).
[56]J. Wullschleger, in *Advances in Cryptology EUROCRYPT* (Springer, 2007), Lecture Notes in Computer Science.