Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security against Coherent Attacks - arXiv:1112.2179

F. Furrer,[1,*] T. Franz,[1] M. Berta,[2] V. B. Scholz,[1] M. Tomamichel,[2] and R. F. Werner[1]

[1] *Institut für Theoretische Physik, Leibniz Universität Hannover Appelstraße 2, 30167 Hannover, Germany*
[2] *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 composably 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.

The task in quantum key distribution (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 [1]. 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 [2].

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 ℓ 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.

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]. 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 task is often simplified by additional assumptions about the power of the eavesdropper. Instead of allowing the most general, coherent attack on the quantum communication 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 estimate the state they share, and using this knowledge, it is possible 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 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] . We are only aware of [8], where a finite-key analysis for specific protocols under the assumption of collective Gaussian attacks was provided. However, 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 [9], but only under the additional assumption of energy bounds [10]. It is often argued that, using these results, much of the DV theory can be transferred to CV systems. Unfortunately, this approach provides only very pessimistic key rate estimates for finite block lengths.

Recently, a more direct approach of proving security against coherent attacks was presented in [11], based on an entropic uncertainty relation with quantum side information for smooth entropies [12]. This allows to give a bound on Eve's information about Alice's measurement outcomes in terms of the correlation between Alice and Bob. Based on the extension of the smooth entropy formalism to the infinite-dimensional setting [13, 14], 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 bit 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

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

where ω_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

[*] fabian.furrer@itp.uni-hannover.de

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 $\omega^{\mathrm{id}}_{S_A E} = \tau_{S_A} \otimes \sigma_E$, with τ_{S_A} the uniform mixture of keys, and σ_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 no eavesdropper is present.

In reality we can only hope to achieve an almost ideal protocol. For small parameters ϵ_c, ϵ_s and an abortion probability p_{abort}, we require that the protocol is ϵ_c-correct, i.e. $\Pr[S_A \neq S_B] \leq \epsilon_c$, and that the protocol is ϵ_s-secret, i.e. $(1 - p_{\mathrm{abort}}) \inf_\sigma \frac{1}{2}\|\omega_{S_A E} - \tau_{S_A} \otimes \sigma_E\| \leq \epsilon_s$. Note that a protocol which always aborts is secure. Thus we may impose an additional requirement on the robustness, e.g., $p_{\mathrm{abort}} < 1$. 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 the security definition based on a small mutual information between the eavesdropper and the key [15].

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 $\mathrm{leak}_{\mathrm{EC}}$ 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 $O(\log \frac{1}{\epsilon_c})$ (see [11]).

In the privacy amplification step, two-universal hash functions are used to compress the raw key to a final length of ℓ bits. Roughly speaking, this reduces Eve's knowledge about Alice's key by $N - \ell$ bits. Hence, choosing ℓ sufficiently small ensures that Eve has no information about the resulting bit strings and the key is independent of E. Formally, Eve's uncertainty is measured in terms of the probability that she can guess Alice's raw key X_A, i.e. the conditional min-entropy $H_{\min}(X_A|E)$ [16]. In particular, the resulting key is ϵ_s-secret if [3, 14, 17]

$$\ell \lesssim H^{\epsilon}_{\min}(X_A|E)_\omega - \mathrm{leak}_{\mathrm{EC}} - O(\log \frac{1}{\epsilon_s \epsilon_c}) \ . \qquad (2)$$

Here, the smooth min-entropy $H^{\epsilon}_{\min}(X_A|E)$ is the optimization of the min-entropy over states which are $\epsilon(\epsilon_s, p_{\mathrm{abort}})$ 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 now lower bounds on the smooth min-entropy for the following protocol.

The Protocol.— We consider a 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. After a certain number of signals are measured, Alice and Bob execute a sifting and parameter estimation step. They first check if all quadrature measurements are below a certain threshold 2α ($\alpha > 0$, $\hbar = 1$) and abort the protocol otherwise. The measurement range $[-2\alpha, 2\alpha]$ is divided into intervals of equal length δ which are enumerated by $\mathcal{X} = \{1, ..., \lceil 4\alpha/\delta \rceil\}$. They reveal their measurement choices and discard the data in which they have measured different quadratures ending up with a string of N measurement results. Then, random samples of length k, $X^{pe}_A, X^{pe}_B \in \mathcal{X}^k$ are used for parameter estimation, checking that none of the absolute values of these quadrature measurements exceeds α and that the distance between X^{pe}_A and X^{pe}_B measured by $d(Y, Z) = \frac{1}{k}\sum_{i=1}^{k} |Y_k - Z_k|$ is smaller than d_0. If these tests fail the protocol is aborted. Otherwise, it proceeds with the classical post-processing on the remaining strings X_A and X_B.

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 [14], 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 $H^{\epsilon}_{\max}(X_A|X_B)$, which characterizes the amount of information Alice has to send Bob to retrieve X_A. This leads to the bound [16]

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

where ϵ' is equal to ϵ minus a correction term depending on p_{abort}, α, k, and N. The function $c(\delta)$ is the overlap of the two conjugated quadrature measurements on an interval of length δ which is well approximated by $c(\delta) \approx \delta^2/(2\pi)$ for sufficiently small δ [16]. Equation (3) assumes a uniformly random choice of measurement settings.

This reduces the problem to upper bounding the smooth max-entropy between X_A and X_B. In the limit of large n this can be done by $n \cdot \log \gamma(d(X_A, X_B))$, where γ is a function arising from a large deviation consideration. Using sampling theory, the quantity $d(X_A, X_B)$ can then, with high probability, be estimated by $d(X^{pe}_A, X^{pe}_B)$ plus a correction μ, which quantifies its statistical deviation to $d(X_A, X_B)$ and depends on α, k and n. Since the protocol aborts if $d(X^{pe}_A, X^{pe}_B) > d_0$, we obtain the following formula for the key length [16]. *For parameters*

k, α, δ, d_0, an ϵ_s-secret key of length

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

can be extracted.

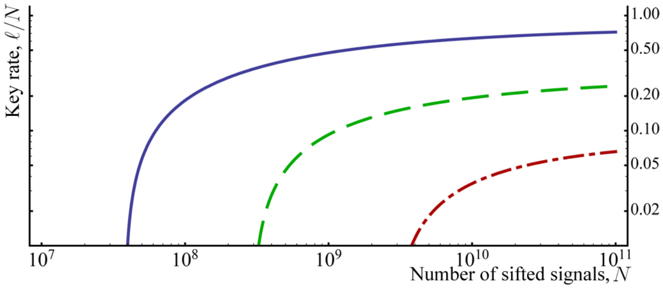

FIG. 1. Key rate ℓ/N against coherent attacks for an input squeezing/antisqueezing of 11dB/16dB and additional symmetric losses of 0% (solid line), 4% (dashed line) and 6% (dash-dotted line). For the chosen security parameters see the main text.

Note that the measurement device on Bob's side need not be trusted, except that measurements on different signals must commute. The only requirement is that Alice's measurement device is described by projections onto two canonical variable used in the computation of $c(\delta)$. Since the source is assumed to be located in Alice's lab, the additional reference signal (local oscillator) used for the homodyne detection on Alice's side is not subject to any attacks, and is therefore covered by our security analysis. The proof technique also applies to reverse reconciliation. However, the overlap has to be calculated for Bob's measurement which might be subjected to attacks on the reference signal. Since the estimate of the smooth min-entropy is symmetric in X_A and X_B only leak_{EC} would change.

We calculated the correlation between X_A and X_B under the assumption of an identically and independently distributed source producing states with an inputsqueezing of 11dB and antisqueezing of 16dB. Squeezing at this level has recently been realized in an experiment at 1550nm [18]. 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 and can in principle be reduced [16]. The leakage term is estimated assuming an error correction efficiency of 0.95 [19]. In Fig. 1 the resulting key rates ℓ/N are plotted for different symmetric losses. We have set security parameters $\epsilon_s = \epsilon_c = 10^{-13}$, and $\alpha = 30$ such that in the absence of any eavesdropper the protocol aborts with probability less than 0.01. The optimization over the other free parameters is done numerically for each N. Typical values for $N = 10^9$ are $k = 10^8$ and $\delta = 0.02$.

In Fig. 2, we compare the key rate for coherent attacks with an analysis against collective Gaussian attacks [16] and the Devetak-Winter rate for perfect error correction [7, 14].

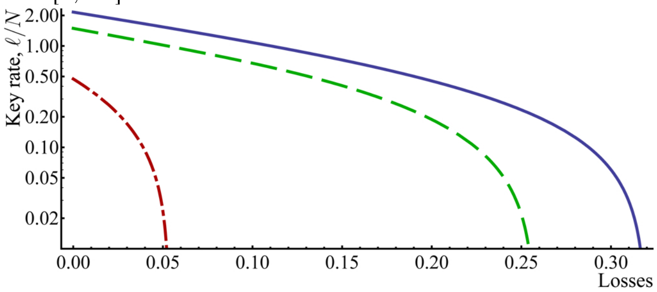

FIG. 2. Key rate versus losses secure against coherent attacks at $N = 10^9$ (dot-dashed line), collective Gaussian attacks at $N = 10^9$ (dashed line), and the Devetak-Winter rate [7, 14] for perfect information reconciliation (solid line). Squeezing strength and security parameters are chosen as before.

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. We compare it with key rates computed under the assumption of collective Gaussian attacks and find that they are significantly higher. This is because the applied entropic uncertainty relation, Eq. (3), is not tight for the considered state, which might be improved by a state dependent version thereof. Our results for collective attacks suggest that an extension of the post-selection technique to infinite-dimensional systems (see [20] for a proposal) is 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 [21, 22].

[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. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, arXiv:1110.3234v1 (2011).

[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] A. Leverrier, F. Grosshans, and P. Grangier, Phys. Rev. A **81**, 062343 (2010).

[9] M. Christandl, R. König, G. Mitchison, and R. Renner, Comm. Math. Phys. **273**, 473 (2007).

[10] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).

[11] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nat. Commun. **3**, 634 (2012).

[12] M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).

[13] F. Furrer, J. Aberg, and R. Renner, Comm. Math. Phys. **306**, 165 (2011).

[14] M. Berta, F. Furrer, and V. B. Scholz, arXiv:1107.5460v1 (2011).

[15] R. Renner and R. König, in *Proc. of TCC*, LNCS, Vol. 3378 (Springer, 2005) pp. 407–425.

[16] F. Furrer, T. Franz, M. Berta, V. B. Scholz, M. Tomamichel, and R. F. Werner, arXiv:1112.2179v1 (2011).

[17] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, IEEE Trans. Inf. Theory **57**, 8 (2011).

[18] T. Eberle, V. Händchen, J. Duhme, T. Franz, R. F. Werner, and R. Schnabel, Phys. Rev. A **83**, 052329 (2011).

[19] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, (2011), arXiv:1110.0100v1.

[20] A. Leverrier, E. Karpov, P. Grangier, and N. J. Cerf, New J. Phys. **11**, 115009 (2009).

[21] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).

[22] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).