Erratum: Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security against Coherent Attacks [Phys. Rev. Lett. 109, 100502 (2012)]

F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner

An error in the numerical computation of the key rates secure against coherent attacks resulted in too pessimistic key rates and allowing only symmetric fiber losses up to 6%. The corrected computation shows that losses up to about 23% can be tolerated under the same conditions. The corrected plot for the key rate against coherent attacks updating Fig. 1 of the letter for now 0%, 10% and 20% of symmetric losses is given in Fig 1. The updated plot of Fig. 3 of the letter comparing the key rates for coherent attacks with the one secure against collective attacks and the optimal asymptotic value can be found in Fig. 2. The error did not affect the computation of the key rate secure against collective attacks.

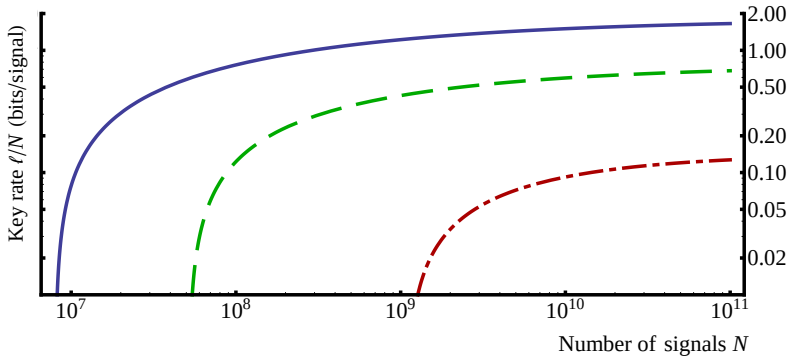

FIG. 1: Corrected version of Fig. 1. Key rate ℓ/N in bits per signal against coherent attacks for an input squeezing/antisqueezing of 11dB/16dB and additional symmetric losses of 0% (solid line), 10% (dashed line) and 20% (dash-dotted line). We assumed an error correction efficiency of 0.95 and set $\epsilon_s = \epsilon_c = 10^{-6}$.

The improved values for the key rates against coherent attacks also affect the conclusion drawn in the *Discussion and Outlook* section of the letter. In particular, the following sentences should be removed: *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 [25] for a proposal) is desirable.* Instead the conclusion should be the following: *The comparison with the finite-key rate against collective attacks shows that the gap is relatively small compared to the finite-size effects. This is due to the fact that the uncertainty relation is almost tight for the two-mode squeezed states. The reason that the key rates allow for only small amounts of losses is because of the direct reconciliation in the error correction protocol. Hence, an extension of the proof technique against coherent attacks to a reverse reconciliation error correction protocol would be desirable.*

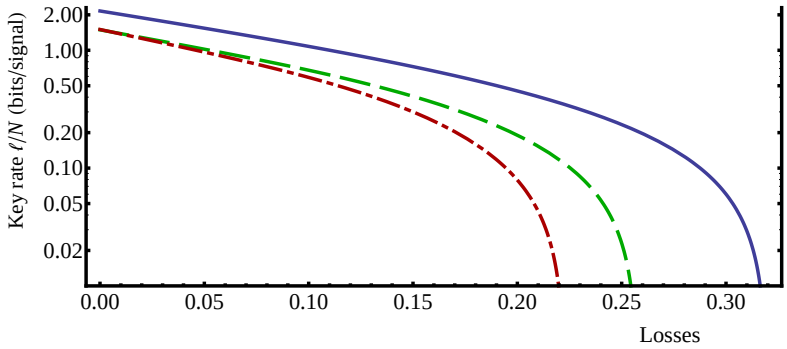

FIG. 2: Corrected version of Fig. 3. Key rate ℓ/N versus losses secure against coherent attacks at $N = 10^9$ (dot-dashed line), collective Gaussian attacks at $N = 10^9$ (dashed line), and the Devetak-Winter rate [7] for perfect information reconciliation (solid line). Squeezing strength, error correction efficiency and security parameters are chosen as in the case of coherent attacks.