Composably secure time-frequency quantum key distribution

Nathan Walk[1]* and Jonathan Barrett[1] and Joshua Nunn[2]
[1]*Department of Computer Science, University of Oxford, Wolfson Building, Parks Road, Oxford OX1 3QD, United Kingdom*
[2]*Clarendon Laboratory, University of Oxford, Oxford OX1 3PU, United Kingdom*
(Dated: April 1, 2017)

We present a composable security proof, valid against arbitrary attacks and including finite-size effects, for a high dimensional time-frequency quantum key distribution (TFQKD) protocol based upon spectrally entangled photons. Such schemes combine the impressive loss tolerance of single-photon QKD with the large alphabets of continuous variable (CV) schemes, but finite-size security has previously only been proven under the assumption of collective Gaussian attacks. Here, we derive a composable security proof that predicts key rates on the order of Mbits/s over metropolitan distances (40 km or less) and maximum transmission distances of up to 140 km.

Most photonic QKD implementations fall into one of two regimes. Traditional discrete variable (DV) schemes encode the secret key in a two-dimensional Hilbert space such as the polarisation of a single photon. Such protocols now enjoy general, *composable* security proofs [1] that function with reasonably small finite-size data blocks, and converge to the ideal Devetak-Winter rates [2] in the asymptotic limit. Continuous variable (CV) schemes instead utilise an infinite-dimensional Hilbert space, commonly the quadratures of the optical field. Whilst the finite range and precision of real-life detectors ensures the key is never perfectly continuous, CVQKD nevertheless has the capability to achieve greater than one bit per transmission and hence potentially much higher rates. Furthermore, composable, general, finite-size CVQKD security proofs have also appeared, although the present results either require extremely large block sizes [3], or are very sensitive to losses [4] and fail to converge to the Devetak-Winter rates.

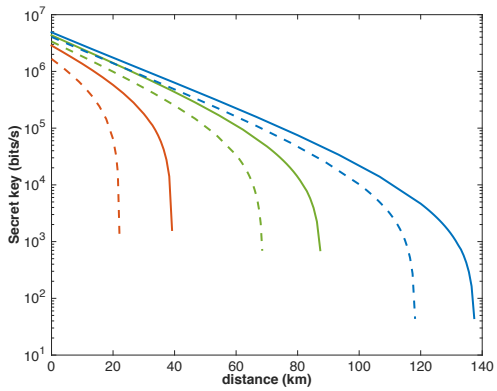

FIG. 1: Secret key rate as a function of transmission distance for protocols where the key is generated from frequency (dashed) or time (solid) variables. Sample sizes are $N = \{10^9, 10^{10}, 10^{11}\}$ in red, green and blue respectively with a security parameter of 10^{-10}.

An alternative approach is to encode the key in the continuous degrees of freedom of single photons, inheriting both the loss tolerance of DVQKD and the larger encoding space of CV protocols [5]. These time-frequency schemes are primarily pursued via the temporal and spectral correlations of single photons emitted during spontaneous parametric down conversion (SPDC) and the security stems from the conjugate nature of frequency and arrival time measurements. Significant progress has been made in security analysis [6], particularly identifying analogies between the time and frequency observables of a single photon and the canonical quadrature observables. However, a general composable security proof is lacking. In this work we present such a proof by combining the entropic uncertainty proofs for CVQKD [4] with efficient, finite-size decoy-state analysis [7] for DVQKD which allows us to rigorously determine the number of single photon events. The resultant proofs allow for high rates key rates over urban and inter-city distances with reasonable block sizes. Detailed proofs, calculations and simulation parameters can be found in [8].

Note added: During the writing up of this work the authors became aware of similar results obtained independently by Niu et al. [9].

References

[1] R. Renner, arXiv:0512258 (2005); M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nature Communications **3**, 634 (2012).
[2] I. Devetak and A. Winter, Proceedings of the Royal Society **461**, 207 (2005).
[3] A. Leverrier, Physical Review Letters **114**, 070501 (2015).
[4] F. Furrer et al., Physical Review Letters **109**, 100502 (2012).
[5] B. Qi, Optics Letters **31**, 2795 (2006).
[6] J. Nunn et al., Optics Express **21**, 15959 (2013); Z. Zhang et al., Physical Review Letters **112**, 120506 (2014); C. Lee et al., Quantum Information Processing **14**, 1005 (2015); D. Bunandar et al., Physical Review A **91**, 022336 (2015); H. Bao et al., Journal of Physics A: Mathematical and Theoretical **49**, 205301 (2016).
[7] C. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Physical Review A **89**, 022307 (2014).
[8] N. Walk, J. Barrett, and J. Nunn, arXiv:1609.09436 (2016).
[9] M. Y. Niu, F. Xu, F. Furrer, and J. H. Shapiro, arXiv:1606.08394, (2016).