Realization of Finite-Size Continuous-Variable Quantum Key Distribution based on Einstein-Podolsky-Rosen Entanglement

Tobias Eberle,[1] Vitus Händchen,[1] Fabian Furrer,[2] Torsten Franz,[3]
Jörg Duhme,[3] Reinhard F. Werner,[3] and Roman Schnabel[1]

[1] *Max-Planck-Institut für Gravitationsphysik (Albert-Einstein-Institut) and Institut für Gravitationsphysik der Leibniz Universität Hannover, Callinstraße 38, 30167 Hannover, Germany*
[2] *Department of Physics, Graduate School of Science, University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo, Japan, 113-0033*
[3] *Institut für Theoretische Physik der Leibniz Universität Hannover, Appelstraße 2, 30167 Hannnover*

Continuous-variable quantum key distribution has made great progress during the last years. Recently, a security proof for a finite number of measurements with composable security against arbitrary attacks was published which employs Einstein-Podolsky-Rosen (EPR) entangled states. Here, we present a first implementation of this protocol, demonstrating the feasibility of secure key generation. The implementation relies on continuous-wave quadrature-entangled states at the telecommunication wavelength of 1550 nm with unprecedented EPR entanglement and homodyne detection with a random choice of quadrature for each measurement. We further present the generation of a key which is secure under collective attacks with 10^8 measurements.

Since its invention in 1984 [1], quantum key distribution (QKD) has developed to the probably most important application of quantum information [2, 3]. Discrete variable systems which employ the polarization state of single photons, have to rely on single photon sources and especially, single photon detectors. In 2001 Cerf et al. [4] came up with the first QKD protocol using the amplitude and phase quadratures of light fields which are continuous variables. These variables are usually measured by homodyne detection where a strong light field, a so-called *local oscillator*, is superimposed at a balanced beam splitter with a quantum state which carries the information used to distribute a key. Both output ports of this beam splitter are detected by PIN photo diodes which are standard telecommunication devices offering high bandwidth and low electronic dark noise. Most commonly prepare-and-measure schemes using Gaussian modulated coherent states are employed [5–8] and distances between the communicating parties, usually called Alice and Bob, of up to 80 km were reached using these states [9].

While prepare-and-measure schemes have to use random number generators to generate bit strings that are encoded to the quantum states, entangled states [10] do not need this side-information channel. For entangled states the randomness of the key is directly offered by the quantum measurement performed by Alice and Bob. In their famous Gedankenexperiment in 1935 Einstein, Podolsky and Rosen (EPR) employed states which were entangled in their position and momentum [11]. Using a criterion by Reid [12] for the counterpart of position and momentum in quantum optics, the amplitude and phase quadratures of light fields, Ou et al. [13] demonstrated the non-locality property of quantum mechanics and thus, the EPR paradox. Further implementations of EPR entangled states are for instance presented in [14–16]. Quadrature entangled states used for quantum key distribution are reported in [17, 18].

In the past the security analysis of continuous-variable protocols was performed in the asymptotic regime of infinite measurements [7, 19]. Recently, also effects caused by a finite number of exchanged quantum states were taken into account [20, 21]. While the finite-size Gaussian modulation protocol from Ref. [20] was implemented in [9], the protocols from Ref. [21] are based on EPR entangled states and provide composable security [22] for collective and arbitrary attacks, respectively. Indeed, their proof of the protocol for arbitrary attacks demands strongly entangled states, low optical loss and a large number of measurements to achieve positive secure key rates.

Here, we present the generation of EPR entangled states at the standard telecommunication wavelength of 1550 nm which are capable of fulfilling the requirements of the security proof under arbitrary attacks. Choosing the measured quadratures at random we recorded 2×10^8 samples in a table-top environment and demonstrated the feasibility of the secure key generation from the measured samples using a non-binary error correction code with more than 91 % efficiency. Furthermore, we generated a key which is secure under collective attacks using a post selection technique.

Figure 1 shows the experimental implementation of the QKD protocol. The EPR entanglement was generated by superimposing two 1550 nm continuous-wave squeezed vacuum modes at a balanced beam splitter. To achieve a stable operation all degrees of freedom were locked with active control loops. In particular, this included the phase of the squeezed modes at the balanced beam splitter, which is difficult to lock without introducing too much optical loss degrading the entanglement. The bipartite states were characterized using the EPR-Reid criterion [12]

$$\mathcal{E} = \min_g \mathrm{Var}(\hat{X}_A - g\hat{X}_B) \times \min_h \mathrm{Var}(\hat{P}_A - h\hat{P}_B) < 1 \ , \quad (1)$$

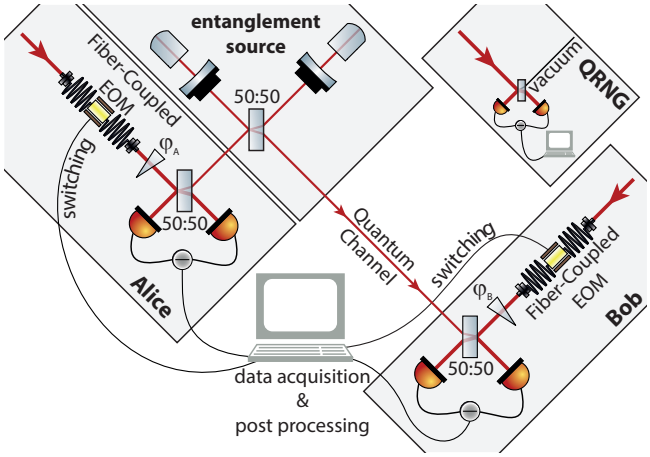

Figure 1. Experimental implementation of the QKD protocols. QRNG: Quantum Random Number Generation, EOM: Electro-Optical Modulator.

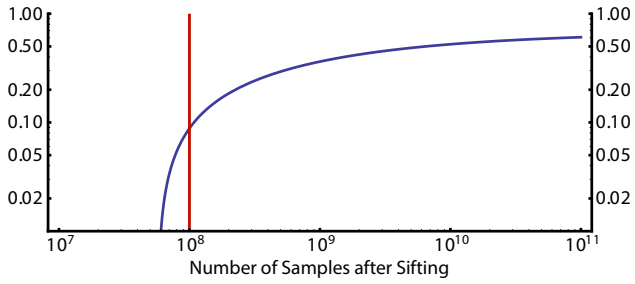

Figure 2. Secure key rate for arbitrary attacks versus the number of measured samples after sifting. The curve is simulated for our generated states. The red line indicates the number of samples we have measured.

where $\hat{X}$ denotes the amplitude quadrature, $\hat{P}$ denotes the phase quadrature and Var denotes the variance. Our states exhibited an EPR-value of $\mathcal{E} = 0.0309 \pm 0.0002$ [23] improving the previous record reported in Ref. [15], which was already outperforming all other experiments by almost an order of magnitude. The measured EPR-value could be achieved by using squeezed vacuum input modes with more than 10 dB nonclassical noise reduction in the squeezed quadrature in comparison to vacuum noise.

To generate a raw key Alice and Bob had to measure each sample either in amplitude or phase quadrature which was chosen at random. For this purposes we implemented fiber-coupled electro-optical modulators in the local oscillator beams which applied fast phase shifts to yield a measurement in the desired quadrature. The measurements were timed to perform at a rate of 100 kHz. The quantum random numbers used by Alice and Bob for choosing the quadrature were provided by homodyne measurements of a vacuum state [24].

Using 2×10^8 measurements we generated a raw key by checking the abort conditions and by performing sifting, parameter estimation and binning of the measurement outcomes to a finite alphabet according to the protocol from Ref. [21]. Assuming an error correction efficiency of 95 %, Fig. 2 shows a simulation of the key rate with security under arbitrary attacks versus the number of measured samples after sifting for the states generated by our entanglement source. The red line indicates the number of samples we have measured for which a secure key rate of 0.08 bits/sample could be achieved. A simulation revealed that for the number of measurements we have performed the secure key rate will be positive for an error correction efficiency larger than about 91 %.

Since a non-binary error correction was not available, we generated a secret key which is secure under collective attacks using the collective protocol from Ref. [21]. To be able to use a binary error correction algorithm instead, the error rate was reduced by post selection. For this purpose we used a 6 bit encoding of our measurements with the bins having an equal spacing. By discarding 6 bins from the middle we were able to reduce the bit error rate from about 13.2 % to 3.8 % which enabled use to distill a key.

In conclusion, we have demonstrated the feasibility of composable secure key generation with security against arbitrary attacks using a finite number of samples. The demanding requirements of the security proof on the EPR entangled states could be fulfilled by implementing a low loss setup with input squeezed vacuum states with more than 10 dB squeezing. We further demonstrated the successful secure key generation under collective attacks using a post selection technique. While for security against arbitrary attacks only table-top implementations are possible, the finite-size QKD protocol with security against collective attacks allows for distances between Alice and Bob in the order of several ten kilometers.

[1] C. H. Bennett, and G. Brassard, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore India **175**, (1984).

[2] V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, Reviews of Modern Physics **81**, 1301 (2009).

[3] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Review of Modern Physics **84**, 621 (2012).

[4] N. Cerf, M. Lévy, and G. Assche, Physical Review A **63**, 052311 (2001).

[5] F. Grosshans, and P. Grangier, Physical Review Letters **88**, 057902 (2002).

[6] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature **421**, 238 (2003).

[7] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier,

E. Karpov, E. Diamanti, T. Debuisschert, N. Cerf, R. Tualle-Brouri, S. McLaughlin, and P. Grangier, Physical Review A **76**, 042305 (2007).

[8] S. Fossier, E. Diamanti, T. Debuisschert, A Villing, R. Tualle-Brouri, and P. Grangier, New Journal of Physics **11**, 045023 (2009).

[9] P. Jouguet, A. Leverrier, P. Grangier, and E. Diamanti, arXiv 1210.6216 (2012).

[10] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Reviews of Modern Physics **81**, 865 (2009).

[11] A. Einstein, B. Podolsky, and N. Rosen, Physical Review **47**, 777 (1935).

[12] M. D. Reid, Physical Review **A** 40, 913 (1989).

[13] Z. Y. Ou, S. F. Pereira, H. J. Kimble, and K. C. Peng, Physical Review Letters **68**, 3663 (1992).

[14] W. P. Bowen, R. Schnabel, and P. K. Lam, Physical Review Letters **90**, 043601 (2003).

[15] S. Steinlechner, J. Bauchrowitz, T. Eberle, and R. Schnabel, Physical Review A **87**, 022104 (2013).

[16] V. Händchen, T. Eberle, S. Steinlechner, A. Samblowski, T. Franz, R. F. Werner, and R. Schnabel, Nature Photonics **6**, 596 (2012).

[17] X. Su, W. Wang, Y. Wang, X. Jia, C. Xie, and K. Peng, Europhysics Letters **87**, 20005 (2009).

[18] L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, and U. L. Andersen, Nature Communications **3**, 1083 (2012).

[19] I. Devetak, and A. Winter, Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **461**, 207 (2005).

[20] A. Leverrier, F. Grosshans, and P. Grangier, Physical Review A **81**, 062343 (2010).

[21] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. Scholz, M. Tomamichel, and R. Werner, Physical Review Letters **109**, 100502 (2012).

[22] R. Canetti, Proc. 42nd IEEE Symp. on Foundations of Computer Science 136 (2001).

[23] T. Eberle, V. Händchen, and R. Schnabel, Optics Express, accepted.

[24] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, Nature Photonics **4**, 711 (2010).