Implementation of Quantum Key Distribution with Composable Security Against Coherent Attacks using Einstein-Podolsky-Rosen Entanglement

Tobias Gehring,[1,2] Vitus Händchen,[1] Jörg Duhme,[3] Fabian Furrer,[4] Torsten Franz,[3,5] Christoph Pacher,[6] Reinhard F. Werner,[3] and Roman Schnabel[1,7,*]

[1] *Max-Planck-Institut für Gravitationsphysik (Albert-Einstein-Institut) and Institut für Gravitationsphysik, Leibniz Universität Hannover, Callinstraße 38, 30167 Hannover, Germany*

[2] *Department of Physics, Technical University of Denmark, Fysikvej, 2800 Kgs. Lyngby, Denmark*

[3] *Institut für Theoretische Physik, Leibniz Universität Hannover, Appelstraße 2, 30167 Hannnover, Germany*

[4] *Department of Physics, Graduate School of Science, University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo, Japan, 113-0033*

[5] *Institut für Fachdidaktik der Naturwissenschaften, Technische Universität Braunschweig, Bienroder Weg 82, 38106 Braunschweig, Germany*

[6] *Digital Safety & Security Department, AIT Austrian Institute of Technology GmbH, 1220 Vienna, Austria*

[7] *Institut für Laserphysik und Zentrum für Optische Quantentechnologien, Universität Hamburg, Luruper Chaussee 149, 22761 Hamburg, Germany*

Secret communication over public channels is one of the central pillars of a modern information society. Using quantum key distribution (QKD)[1,2] this is achieved without relying on the hardness of mathematical problems which might be compromised by improved algorithms or by future quantum computers[3]. State-of-the-art QKD requires composable security against coherent attacks for a finite number of samples. Here, we present the first implementation of QKD satisfying this requirement and additionally achieving security which is independent of any possible flaws in the implementation of the receiver. By distributing strongly Einstein-Podolsky-Rosen entangled continuous variable (CV)[4,5] light in a table-top arrangement, we generated secret keys using a highly efficient error reconciliation algorithm. Since CV encoding is compatible with conventional optical communication technology, we consider our work to be a major promotion for commercialized QKD providing composable security against the most general channel attacks.

Using a QKD system the communicating parties employ a cryptographic protocol that cannot be broken, neither by todays nor by future technology. The security of the key distributed by such a system is guaranteed on the basis of quantum theory by a mathematical proof, which has to consider the most sophisticated (quantum) attacks on the quantum channel, so-called 'coherent attacks'. Furthermore, security has to be established in a 'composable' fashion, which means that if the distributed key is used in another secure protocol (like one-time-pad encryption), it remains secure in the composition of the two protocols. To make a security proof applicable to actual implementations, it also has to include all effects due to the finite number of distributed quantum states. Additionally, the security proof has to model the source and the detectors correctly. Since a completely correct model of a detector is difficult to achieve, the proof can be made 'measurement-device independent' instead, i.e. the proof does not include any detector implementation details at all. Thus, security cannot be compromised by any 'side-channels' of the detector's implementation, including those which may only be discovered in the future. To match the properties of actual implementations and the assumptions made in security proofs, intense theoretical as well as experimental research and development is ongoing.

Here, we report the first QKD implementation that generates a (finite) key which is secure against coherent attacks and whose security is composable as well as guaranteed independent of possible side channels of the receiver's detector. Theoretically, the security of our protocol has been established in Ref. 6. Following this work we use measurement variables with continuous spectra (continuous variables) and strongly Einstein-Podolsky-Rosen entangled light beams whose actual entanglement strength is a crucial parameter for achieving a positive key rate.

Our work was possible only after the security proof of Ref. 6 was found. Other proofs did also find composable security against coherent attacks[7,8] but only for an unrealistically large number of distributed quantum states. The security of previous experimental continuous-variable implementations, however, were restricted to the class of 'collective attacks'. While this class of attacks already allows an eavesdropper to possess a quantum memory, all quantum states are attacked identically using a collective Gaussian operation. Although collective attacks are in the limit of an infinite number of distributed quantum states as strong as coherent attacks, it is currently not known whether this holds for a realistic finite key length protocol. For collective attacks a transmission distance of 80 km was achieved with a finite number of distributed quantum states using Gaussian modulated coherent states[9,10].

In the discrete-variable regime, first security proofs providing composable security against coherent attacks were given in Refs. 11–13. However, all of them have in common that they require perfect single-photon sources, which are experimentally impractical. The recent experimental demonstration reported in Ref. 14 targeted the QKD protocol considered in Ref. 13 but it used weak coherent pulses and, thus, an imperfect single-photon source. To compensate for imperfect single-photon sources, the decoy state method has been developed[15,16]. This method was very recently proven composable secure against coherent attacks[17] and was implemented in Ref. 18, at around the same time as our CV QKD implementation. To also avoid possible side-channel attacks in future discrete-variable QKD implementations, for instance on the employed single photon detectors[19], the finite-key measurement-device-independent protocol very recently proven composable secure in Ref. 20 could be implemented in the future.

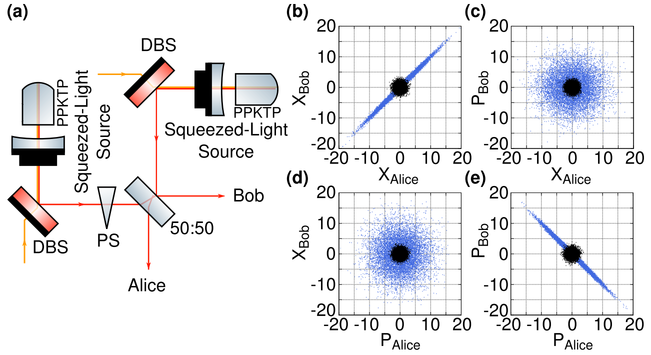

Figure 1. **Einstein-Podolsky-Rosen entanglement source for CV QKD.** (a) The source consists of two continuous-wave squeezed vacuum beams, generated by type I parametric down-conversion at 1550 nm (red), which are superimposed at a balanced beam splitter with a relative phase of $\frac{\pi}{2}$. Yellow beam: 775 nm pump field, DBS: Dichroic beam splitter, PS: Phase shifter. (b)-(e) Correlations between Alice's and Bob's data, measured by balanced homodyne detection in either the amplitude (X) or phase (P) quadrature. The data is normalized to the noise standard deviation of a vacuum state. Blue: Einstein-Podolsky-Rosen entangled state used for QKD. Black: Reference measurement of zero-point fluctuations of the ground state (vacuum).

Our implemented protocol uses two continuous-wave optical light fields which were produced by a source at one of the communicating parties (Alice) and whose amplitude and phase quadrature amplitude modulations were mutually entangled[21]. Using Einstein-Podolsky-Rosen entanglement as a resource makes our protocol a CV equivalent of the BBM92 protocol for discrete variables[22]. The schematic of the experimental setup is illustrated in Fig. 1(a). Two squeezed-light sources[23,24], each composed of a nonlinear PPKTP crystal and a coupling mirror, were pumped with a bright pump field at 775 nm (yellow) to produce two squeezed vacuum states at the telecommunication wavelength of 1550 nm (red). The two squeezed vacua, both exhibiting a high squeezing of more than 10 dB, were superimposed at a balanced beam splitter with a relative phase of $\pi/2$, thus generating Einstein-Podolsky-Rosen entanglement[21]. One of the outputs of the beam splitter was kept by Alice, while the other was sent to her communication partner (Bob). The technical details of the source, including the locking scheme, were characterized in Ref. 25.

Figures 1(b)-(e) show the distribution of measurement outcomes obtained by the two parties measuring either the amplitude (X) or phase (P) quadrature of their respective light field with balanced homodyne detection. Each measurement outcome is truly random since it stems from parametrically amplified zero-point fluctuations. When both parties simultaneously measure either X or P the strong correlations between their outcomes are clearly visible (Fig. 1 (b) and (e)). If the two parties measure different quadratures instead, the measurement outcomes are uncorrelated (Fig. 1(c) and (d)). The strength of the correlations of Alice's and Bob's measurement for the same quadratures, which is related to the initial squeezing strength, is a central parameter in our QKD protocol and enters the key length computation directly in the form of an *average distance* d_{pe}, introduced below.

The precise steps of the QKD protocol are as follows:[6]

Preliminaries Alice and Bob use a pre-shared key to authenticate the classical communication channel for post processing[26,27]. Furthermore, Alice and Bob negotiate all parameters needed during the protocol run and Alice performs a shot-noise calibration measurement by blocking the signal beam input of her homodyne detector.

Measurement Phase Alice prepares an entangled state using her Einstein-Podolsky-Rosen source and sends one of the outputs to Bob along with a local oscillator beam. Both Alice and Bob choose, randomly and independently from each other, a quadrature X or P, which they simultaneously measure by homodyne detection of their light fields. The outcome of this measurement is called a sample. This step is repeated until $2N$ samples have been obtained.

Sifting Alice and Bob announce their measurement bases and discard all samples measured in different quadratures.

Discretization The continuous spectrum of the measurement outcomes is discretized by the analog-to-digital converter (ADC) used to record the measurement. During the discretization step Alice and Bob map the fine grained discretization of their remaining samples caused by the ADC to a coarser one consisting of consecutive 2^d bins. In the interval $[-\alpha, \alpha]$ a binning with equal length is used, which is complemented by two bins $(-\infty, -\alpha)$ and (α, ∞). The parameter α is used to include the finite range of the homodyne detectors into the security proof.

Channel Parameter Estimation The secret key length is calculated using the average distance between Alice's and Bob's samples. To estimate it, the two parties randomly choose a common subset of length k from the sifted and discretized data, X_A^{pe} and X_B^{pe}, respectively, which they communicate over the public classical channel. Using these, they calculate

$$d_{\mathrm{pe}}(X_A^{\mathrm{pe}}, X_B^{\mathrm{pe}}) = \frac{1}{k}\sum_{\mu=1}^{k} |(X_A^{\mathrm{pe}})_\mu - (X_B^{\mathrm{pe}})_\mu| \ , \qquad (1)$$

and abort if it exceeds a threshold agreed on in the preliminaries step.

Error Reconciliation Bob corrects the errors in his data to match Alice's using the hybrid error reconciliation algorithm described below. Afterwards, Alice and Bob confirm that the reconciliation was successful.

Calculation of Secret Key Length Using the results from the channel parameter estimation and considering the number of published bits during error reconciliation, Alice and Bob calculate the secret key length ℓ according to Ref. 6. If the secret key length is negative, they abort the protocol.

Privacy Amplification Alice and Bob apply a hash function which is randomly chosen from a two-universal family[28], to their corrected strings to produce the secret key of length ℓ.

The key generated by the above protocol is proven to be ϵ-secure against coherent attacks in Ref. 6, where ϵ is the so-called composable security parameter. The security proof makes no assumptions on the attacks and only some on our implementation. First of all it assumes that Alice's measured quadrature angles are precisely adjusted to X and P, an assumption that can be overcome as the secure key length proves to be robust against small deviations[6]. Furthermore, the proof requires that Alice's station is inaccessible to the eavesdropper. This allows Alice to trust her source and to determine the probability for measuring a quadrature amplitude value exceeding the parameter α. There are no assumptions on Bob's measurement device (one-sided device independent) such that even attacks on his local oscillator are fully covered and a shot-noise calibration of his homodyne detector is not necessary.

Important for a high key rate is an error reconciliation protocol which has an efficiency close to the Shannon limit. Since in our CV QKD protocol the discretized sample values are non-binary and follow a Gaussian distribution, error reconciliation codes with high efficiency and low error rate are more difficult to achieve than for discrete-variable protocols with uniformly distributed binary outcomes[29]. To solve the problem, we designed a two-phase error reconciliation protocol which can exploit the non-uniform distribution efficiently. First the d_1 least significant bits of each sample are sent to Bob. Since these bits are only very weakly correlated this step works with an efficiency very close to the Shannon limit. In a second step Alice and Bob use a non-binary low density parity check (LDPC) code over the Galois field GF(2^{d_2}) to correct the $d_2 = d - d_1$ most significant bits. d_1, d_2, as well as the LDPC code were optimized for the different channel conditions and the actually employed code was determined using the k revealed samples from the channel parameter estimation. More details are given in the Methods.

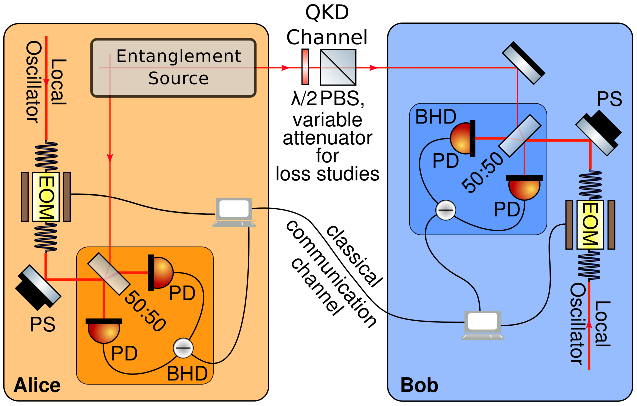

Figure 2. **Implementation of Alice's and Bob's QKD receivers**. Both parties used balanced homodyne detection (BHD) to measure their part of the quadrature entangled state. The measured quadrature angle was controlled by a computer via a fast fiber-coupled electro-optical modulator (EOM). To make sure that Alice and Bob switched between the same orthogonal quadratures, a phase shifter (PS) was employed to compensate slow phase drifts (see Methods). Optical losses of the transmission channel to Bob were modelled by a variable attenuator consisting of a half-wave plate ($\lambda/2$) and a polarizing beam splitter (PBS). The measurement rate was 100 kHz. PD: Photo Diode.

Figure 3 shows the experimental results. First we removed the variable attenuator in the transmission line to Bob and executed the protocol for different sample sizes to show the effect of the finite sample size on the secure key rate (Fig. 3 (a), blue points). For each sample size the number of samples k used for channel parameter estimation was optimized before each run of the QKD protocol to yield maximum key length. The hybrid error reconciliation had a total efficiency of $\beta = 94.6\,\%$ without a single frame error. While we achieved a positive secret key rate with already 5×10^6 samples, the secret key rate of 0.485 bit/sample achieved for 2×10^8 samples is close to saturation. The theoretical model, which is the solid line in the figure, is shown for comparison.

With the variable attenuator in place, we varied the optical loss of the channel to Bob between 0 % and 16 % (see Figure 3 (b)), which is equivalent to a fiber length of up to 2.7 km when standard telecommunication fibers with an attenuation of 0.2 dB/km are used and a coupling efficiency of 95 % is taken into account. By measuring a

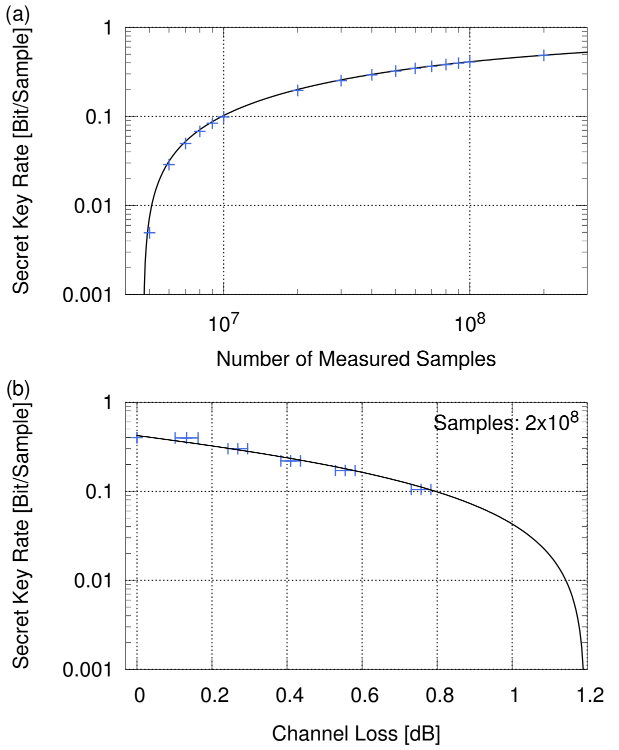

Figure 3. **Secure key rates achieved by our CV QKD system.** Common parameters: $\alpha = 61.6$, $d = 12$, $\epsilon = 2 \times 10^{-10}$. (a) Effect of the finite number of distributed quantum states on the secret key rate. The graph shows experimental results (blue points) obtained without the variable attenuator in Bob's arm. The theoretical model (solid line) is included for comparison and was calculated by reconstructing the covariance matrix for 10^8 samples. (b) Experimentally obtained secure key rate versus optical attenuation in the transmission line to Bob's detector for 2×10^8 measured samples (blue points). The error bars are due to the accuracy of the measurement of the optical attenuation. The theoretical model (solid line) was calculated by reconstructing the covariance matrix of the state corresponding to no attenuation (0 dB) and using a reconciliation efficiency of $\beta = 94.3\,\%$.

total of 2×10^8 samples we were still able to achieve a secret key rate of about 0.1 bit/sample at an equivalent fiber length of 2.7 km ($\approx$ 0.76 dB channel loss). This value, as well as the secret key sizes at the other attenuation values, were achieved by having a very high overall error reconciliation efficiency between $\beta = 94.3\,\%$ and 95.5 %, again without a single frame error. The theoretical model shown in the figure reveals that even an optical transmission loss of almost 1.2 dB between Alice and Bob should be possible. This corresponds to an equivalent distance of about 4.8 km, which is already enough to implement CV QKD links with composable security against coherent attacks between parties in, for instance, a city's central business district.

In conclusion, we have for the first time successfully implemented QKD with composable security against coherent attacks in a one-sided measurement-device independent manner. Along with the exploitation of strong Einstein-Podolsky-Rosen entanglement and a new highly efficient error reconciliation algorithm, the innovation of fast controlled random switching between the two measured quadrature angles made the implementation possible. Although attacks on the source of the quantum states are not covered by the security proof[6], these side-channel attacks can be avoided to arbitrarily low probabilities by adding optical isolators. While in our setup Alice and Bob were located on the same optical table, they could in principle be separated and connected by a standard telecommunication fiber (see Methods). Estimations show that our implementation is limited to about 4.8 km. Longer distances will be possible by using optical fibres with less loss, or by using reverse reconciliation[30].

Acknowledgements This research was supported by the Deutsche Forschungsgemeinschaft (projects SCH 77/5-1 and WE 1240/20-1), the Centre for Quantum Engineering and Space-Time Research (QUEST) and the Vienna Science and Technology Fund (WWTF) (project ICT10-067). TG and VH thank the IMPRS on Gravitational Wave Astronomy for support. FF acknowledges support from Japan Society for the Promotion of Science (JSPS) by KAKENHI grant No. 24-02793. CP would like to thank Gottfried Lechner for very helpful conversations. RFW acknowledges support from the European network SIQS.

METHODS

Experimental Details

The measurement rate of our implementation was 100 kHz. For each measurement, both Alice and Bob had to choose randomly between the X and P quadrature. The necessary relative phase shifts of $\pi/2$ of the local oscillator with respect to the signal beam were applied to the local oscillator beam by a high-bandwidth fiber-coupled electro-optical phase modulator driven by a digital pattern generator PCI-Express card. Since not only the orthogonality of the measurements is important but also that Alice and Bob measure the same set of quadratures, we compensated slow phase drifts by a phase shifter made of a piezo attached mirror. The error signal for this locking loop was derived by employing an 82 MHz single sideband from the entanglement generation[25] which was detected by the homodyne detector. By lowpass filtering the demodulated homodyne signal at 10 kHz with a sufficiently high order, the high frequency phase changes from the fiber-coupled phase modulator were averaged over. To make the average independent of the chosen sequence of quadratures we used the following scheme. For a choice of the X quadrature, the phase modulator was first set to a phase of $\pi/2$ during the first half of the 10 μs interval, and then to 0. For the P quadrature, the phase was first set to 0 and then to $\pi/2$. Thus, this scheme made sure that the phase did not stay in one quadrature for longer than 10 μs even in the case where one party chose by chance to measure only one quadrature for a while. The measurement was performed synchronously by Alice and Bob in the second half of the interval after 3 μs settling time.

The data acquisition was triggered by the pattern generator and performed by a two channel PCI-Express card at a rate of 256 MHz. The 200 acquired samples per channel were digitally mixed down at 8 MHz, lowpass filtered by a 200-tap finite impulse response filter with a cut-off frequency of 200 kHz and down-sampled to one sample. After the total number of samples were recorded the classical post processing of the QKD protocol was performed.

Alice and Bob both employed a local oscillator with a power of 10 mW, yielding a dark noise clearance of about 18 dB. The efficiency of both homodyne detectors was 98 % (quantum efficiency of the photo diodes 99 %, homodyne visibility 99.5 %). The pump powers for the two squeezed-light sources were 140 mW and 170 mW, respectively.

The optical attenuation of the variable attenuator used in Fig. 3(b) was measured by determining the strength of the 35.5 MHz phase modulation used to lock one of the squeezed-light sources[25] with Bob's homodyne detector. The error bars in the figure are due to the accuracy of this measurement.

The security of the protocol relies substantially on the use of true random numbers which are needed by Alice and Bob to choose between the X and P quadrature, and to determine a random hash function during privacy amplification. We implemented a quantum random number generator following a scheme of Ref. 31 which is based on vacuum state measurements performed by a balanced homodyne detector. For this purpose we implemented another balanced homodyne detector with blocked signal port using an independent 6 mW 1550 nm beam from a fiber-laser as local oscillator. The output of the homodyne detector circuit was anti-alias filtered by a 50 MHz fourth-order Butterworth filter and sampled with a sampling frequency of 256 MHz by a data acquisition card. The data was subsequently mixed down digitally at 8 MHz, lowpass filtered with a 200-tap finite-impulse-response filter with a cut-off frequency of 5 MHz and down-sampled to 2 MHz. The generation of the random numbers from the data stream followed the procedure in Ref. 31.

While in our implementation both parties were located on the same optical table and the quantum states including the local oscillator for Bob's homodyne detection were transmitted through free space, a separation is in principle possible by using standard telecommunication fibers. To send both the entangled state and the local oscillator to Bob, they could be, for instance, time multiplexed. Using a dedicated fiber for both beams would also be possible. To achieve synchronization between the two parties, a modulated 1310 nm beam could be employed which could be send along with the local oscillator by wavelength division multiplexing.

Classical Post Processing

The main post-processing is performed with the AIT QKD software. For the current protocol the following algorithms are combined: (i) the binning of the synchronized outcomes, (ii) the estimation algorithm for CV QKD, (iii) the reconciliation algorithm for CV QKD, (iv) the confirmation algorithm, and (v) the privacy amplification algorithm. All classical messages during the protocol are authenticated with a message authentication code using a pre shared secret key to select a random function from a set of (almost strongly two-universal) polynomial hash functions.

(i) First, Bob's samples in the P quadrature are multiplied by -1 to account for the anti-correlation. Alice and Bob then discretize their sifted samples into 2^d bins of equal size δ in the interval $[-\alpha, \alpha]$. The remaining outcomes associated to the intervals $(-\infty, -\alpha)$ and (α, ∞) are joined to $(-\alpha, -\alpha+\delta)$ and $(\alpha - \delta, \infty)$, respectively. The 2^d bins are identified with the key generation alphabet $\chi_{\mathrm{kg}} = \{0,1\}^d$ and each bin (symbol) has a unique binary representation of d bits. Alice and Bob obtain the binned sifted samples $X_A^{\mathrm{sift}} \in \chi_{\mathrm{kg}}^N$ and $X_B^{\mathrm{sift}} \in \chi_{\mathrm{kg}}^N$, respectively. Throughout the experiment we have used a key generation alphabet of size $|\chi_{\mathrm{kg}}| = 2^{12}$.

(ii) In the estimation module for CV QKD the average distance between Alice's and Bob's binned symbols is estimated. Alice chooses a random index set $\mathcal{E} \subset \{1, 2, \ldots, N\}$ of size $|\mathcal{E}| = k$ for estimation and communicates $\mathcal{E}$ together with the corresponding binned symbols $X_A^{\mathrm{pe}} := X_A^{\mathrm{sift}}(\mathcal{E})$ to Bob. Bob determines his corresponding binned raw key symbols $X_B^{\mathrm{pe}} := X_B^{\mathrm{sift}}(\mathcal{E})$, calculates the mean difference d_{pe} between X_A^{pe} and X_B^{pe} (see Eq. (1)), and checks that $d_{\mathrm{pe}} \leq d_{\mathrm{pe}}^0$. Here, d_{pe}^0 has been determined before the run of the protocol by a theoretical estimation given the characterization of the source, the fiber loss and excess noise. If the test passes they continue with the protocol and both parties remove the k estimation samples from their sifted samples to form their raw keys $X_A := X_A^{\mathrm{sift}} \setminus X_A^{\mathrm{pe}} \in \chi_{\mathrm{kg}}^{N-k}$ and $X_B := X_B^{\mathrm{sift}} \setminus X_B^{\mathrm{pe}} \in \chi_{\mathrm{kg}}^{N-k}$.

(iii) The reconciliation module for CV QKD implements the hybrid reconciliation protocol. As the security analysis assumes direct reconciliation, Bob has to correct his raw key X_B to match with Alice's X_A to generate a common raw key X. The hybrid reconciliation used to correct Bob's noisy raw key operates directly on the key generation alphabet χ_{kg}. In preparation for the hybrid reconciliation, two additional alphabets $\hat{\chi}$ and $\check{\chi}$ are introduced such, that $\chi_{\mathrm{kg}} = \hat{\chi} \times \check{\chi}$. Hence, each symbol $x \in \chi_{\mathrm{kg}}$ has a unique decomposition $x = (\hat{x}, \check{x})$ with $\hat{x} \in \hat{\chi}$ and $\check{x} \in \check{\chi}$. We take for $\hat{x}$ the d_2 most significant bits of the binary representation of x, and for $\check{x}$ the remaining $d_1 = d - d_2$ least significant bits of the binary representation of x. We thus decompose the raw keys as $X = (\hat{X}, \check{X})$, where $\hat{X}$ and $\check{X}$ denote the sequence of the d_2 most and the d_1 least significant bits of each key symbol, respectively. The reconciliation module performs the following steps:

(iii-a) Based on the variance of her binned raw key and the samples X_A^{pe} and X_B^{pe}, Alice determines d_1, d_2, and the code rate R such that the expected leakage is minimized w.r.t. the entropy in Bob's symbols, and transmits these parameters to Bob.

(iii-b) Then Alice communicates $\check{X}_A$ to Bob who reconciles $\check{X}_B$ simply by setting $\check{X}_B := \check{X}_A$. Hence, the errors which are left in Bob's key X_B are reduced to the errors in $\hat{X}_B$. Non-binary LDPC reconciliation is used to correct $\hat{X}_B$ as described in the next step.

(iii-c) Both Alice and Bob split their $\hat{X}_A$ and $\hat{X}_B$ into blocks $\hat{X}_A^{(\ell)}$ and $\hat{X}_B^{(\ell)}$, $\ell = 1, \ldots, \frac{N-k}{n}$, each with $n = 10^5$ elements of $\hat{\chi}$. For this step we identify $\hat{\chi}$ with $\mathrm{GF}(2^{d_2})$, the Galois field with 2^{d_2} elements. For each block $\hat{X}_A^{(\ell)}$, Alice uses the parity check matrix H of an LDPC code over $\mathrm{GF}(2^{d_2})$ and rate R to calculate the syndrome $s^{(\ell)} := H \cdot \hat{X}_A^{(\ell)}$. Alice sends the syndrome $s^{(\ell)}$ to Bob. For all elements $j \in GF(2^{d_2})$ and for all indices $i \in \{1, \ldots, n\}$ in the block Bob calculates the conditional probability that $(\hat{X}_A^{(\ell)})_i = j$, given that Bob has obtained $(\hat{X}_B^{(\ell)})_i$ and given Alice's value $(\check{X}_A^{(\ell)})_i$. Bob uses these probabilities to initialize a non-binary belief propagation decoder.

The non-binary belief propagation decoder operates in the probability domain using the multi-dimensional Hadamard transform to speed up the check node operations[32]. Using the syndrome $s^{(\ell)}$ and the conditional probabilities mentioned above, this decoder calculates Bob's estimate $\tilde{X}_A^{(\ell)}$ of Alice's block $X_A^{(\ell)}$.

We have constructed parity check matrices of non-binary LDPC codes over Galois fields of order 32, 64, 128, and 256 with code rates $R \in \{0.50, 0.51, \ldots, 0.95\}$. Each LDPC code has a variable-node degree of two, is check-concentrated, and has a block length of 10^5 symbols. We used the progressive edge-growth algorithm[33] to construct binary codes in a first step. Then each edge has been assigned a random non-zero element of the corresponding Galois field.[33] Alice and Bob have access to all non-binary parity check matrices.

In our proof-of-principle experiment the error reconciliation step took about 2 h on a single CPU core for the largest data set of 2×10^8 samples. Taking into account the about 30 min to measure the data, real-time error reconciliation could in principle be achieved by splitting the task to e.g. 5 CPU cores. Alternatively, to speed up the computation LDPC decoder algorithms with reduced complexity could be employed[34].

(iv) After each block has been corrected, a confirmation step establishes the correctness of the protocol using a family H of (almost) two-universal hash functions with $\mathrm{Prob}_{h \in_R H}(h(x_1) = h(x_2)) \leq \epsilon_c$ for all $x_1 \neq x_2$. For each block Alice chooses a hash function h randomly from H and communicates her choice to Bob. Alice and Bob apply this hash function to their blocks $X_A^{(\ell)}$ and $\tilde{X}_A^{(\ell)}$ and exchange the results. If their results agree the probability that Alice's and Bob's blocks are different is bounded from above by ϵ_c. If their results disagree their blocks are definitely different, and they discard them.

(v) Finally, Alice and Bob feed the sequence of all confirmed blocks into the privacy amplification module. Given the accumulated leakage ℓ_{LK} in bits from the previous protocol steps the secure key length is calculated according to Ref 6 as

$$\ell = (N-k)(\log \frac{1}{c(\delta)} - \log \gamma(d_{\mathrm{pe}}^0 + \mu)) - \ell_{\mathrm{LK}} - \log \frac{1}{\epsilon} \ , \quad (2)$$

where $c(\delta) \approx \delta^2/(2\pi)$ and γ is a bound on the correlation between Alice and Bob depending on the previously agreed average distance threshold d_{pe}^0 and statistical fluctuations μ. Alice chooses a hash function randomly from a two-universal hash family and communicates her choice to Bob. Then Alice and Bob both apply this hash function to the reconciled blocks and obtain the ϵ-secure key K_{sec}.

[*] corresponding author: roman.schnabel@aei.mpg.de

[1] Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H., Quantum Cryptography, Rev. Mod. Phys. **74**, 145 (2002).

[2] Scarani, V., et al., The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[3] Shor, P.W., Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM J. Comput. **26**, 1484 (1997).

[4] Cerf, N., Lévy, M., & Assche, G., Quantum distribution of Gaussian keys using squeezed states, Phys. Rev. A **63**, 052311 (2001).

[5] Weedbrook, C., et al., Gaussian quantum information, Rev. Mod. Phys. **84**, 621 (2012).

[6] Furrer, F., et al., Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security against Coherent Attacks, Phys. Rev. Lett. **109**, 100502 (2012).

[7] Renner, R. & Cirac, J., de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography, Phys. Rev. Lett. **102**, 110504 (2009).

[8] Leverrier, A., García-Patrón, R., Renner, R., & Cerf, N., Security of Continuous-Variable Quantum Key Distribution Against General Attacks, Phys. Rev. Lett. **110**, 030502 (2013).

[9] Leverrier, A., Grosshans, F., & Grangier, P., Finite-size analysis of a continuous-variable quantum key distribution, Phys. Rev. A, **81**, 062343 (2010).

[10] Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P., & Diamanti, E., Experimental demonstration of long-distance continuous-variable quantum key distribution, Nat. Photonics **7**, 378 (2013).

[11] Renner, R., Symmetry of large physical systems implies independence of subsystems, Nat. Phys. **3**, 645 (2007).

[12] Christandl, M., König, R., & Renner, R., Postselection Technique for Quantum Channels with Applications to Quantum Cryptography, Phys. Rev. Lett. **102**, 020504 (2009).

[13] Tomamichel, M., Lim, C.C.W., Gisin, N., & Renner, R., Tight finite-key analysis for quantum cryptography, Nat. Commun. **3**, 634 (2012).

[14] Bacco, D., Canale, M., Laurenti, N., Vallone, G., & Villoresi, P., Experimental quantum key distribution with finite-key security analysis for noisy channels, Nat. Commun. **4**, 2363 (2013).

[15] Wang, X.-B., Beating the photon-number-splitting attack in practical quantum cryptography, Phys. Rev. Lett., **94**, 230503 (2005).

[16] Lo, H.-K., Ma, X., & Chen, K., Decoy State Quantum Key Distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[17] Lim, C.C.W., Curty, M., Walenta, N., Xu, F., & Zbinden, H., Concise security bounds for practical decoy-state quantum key distribution, Phys. Rev. A **89**, 022307 (2014).

[18] Xu F., et al., Experimental quantum key distribution with source flaws and tight finite-key analysis, arXiv preprint, 1408.3667 (2014).

[19] Lydersen, L., Akhlaghi, M.K., Majedi, A.H., Skaar, J., & Makarov, V., Controlling a superconducting nanowire single-photon detector using tailored bright illumination, New J. Phys. **13**, 113042 (2011).

[20] Curty M., et al., Finite-key analysis for measurement-device-independent quantum key distribution, Nat. Commun. **5**, 3732 (2014).

[21] Furusawa, A., et al., Unconditional Quantum Teleportation, Science **282**, 706 (1998).

[22] Bennett, C.H., Brassard, G., Marim, N.D., Quantum Cryptography without Bell's Theorem, Phys. Rev. Lett. **68**, 557 (1992).

[23] Eberle, T., et al., Quantum Enhancement of the Zero-Area Sagnac Interferometer Topology for Gravitational Wave Detection, Phys. Rev. Lett. **104**, 251102 (2010).

[24] Mehmet, M., et al., Squeezed light at 1550 nm with a quantum noise reduction of 12.3 dB, Opt. Express **19**, 25763 (2011).

[25] Eberle, T., Händchen, V., & Schnabel, R., Stable Control of 10 dB Two Mode Squeezed Vacuum States of Light, Opt. Express **21**, 11546 (2013).

[26] Stinson, D.R., Universal hashing and authentication codes, Des. Codes Cryptogr. **4**, 369 (1994).

[27] Gemmell, P., & Naor, M., Codes for Interactive Authentication, Adv. Cryptol., CRYPTO'93 **773**, 355 (1994).

[28] Carter, J.L., & Wegman, M.N., Universal Classes of Hash Functions, J. Comput. System Sci., **18**, 143 (1979).

[29] Lodewyck, J., et al., Quantum key distribution over 25km with an all-fiber continuous-variable system, Phys. Rev. A **76**, 042305 (2007).

[30] Furrer F., Reverse-reconciliation continuous-variable quantum key distribution based on the uncertainty principle, Phys. Rev. A **90**, 042325 (2014).

[31] Gabriel, C., et al., A generator for unique quantum random numbers based on vacuum states, Nat. Photonics **4**, 711 (2010).

[32] Barnault, L., & Declercq, D., Fast decoding algorithm for LDPC over GF(2^q), IEEE Proceedings Information Theory Workshop 2003, 70-73 (2003).

[33] Hu, X.-Y., Eleftheriou, E., & Arnold, D.M., Regular and irregular progressive edge-growth tanner graphs, IEEE Trans. Inform. Theory **51**, 386 (2005).

[34] Voicila A., Declercq D., Verdier F., Fossorier M., & Urard, P., Low-Complexity Decoding for Non-Binary LDPC Codes in High Order Fields, IEEE Trans. Comm. **58**, 1365 (2010).