Shaped Constellation Continuous Variable Quantum Key Distribution: Concepts, Methods and
Experimental Validation

Francois Roumestan, Amirhossein Ghazisaeidi, Member, IEEE, Jeremie Renaudier, Senior Member, IEEE,
Luis Trigo Vidarte, Anthony Leverrier, Eleni Diamanti, and Philippe Grangier

Abstract—Quantum key distribution (QKD) enables the establishment of secret keys between users connected via a channel vulnerable to eavesdropping, with information-theoretic security, that is, independently of the power of a malevolent party (Scarani et al., 2009). QKD systems based on the encoding of the key information on continuous variables (CV), such as the values of the quadrature components of coherent states (Weedbrook et al., 2012), (Diamanti and Leverrier, 2015), present the major advantage that they only require standard telecommunication technology. However, the most general security proofs for CV-QKD required until now the use of Gaussian modulation by the transmitter, complicating practical implementations (Jouguet et al., 2013), (Zhang et al., 2020), (Jain et al., 2022). Here, we experimentally implement a protocol that allows for arbitrary, Gaussian-like, discrete modulations, whose security is based on a theoretical proof that applies generally to such situations (Denys et al., 2021). These modulation formats are compatible with the use of powerful tools of coherent optical telecommunication, allowing our system to reach an estimated performance of tens of megabit per second secret key rates over 25 km.

Index Terms—Coherent detection, modulation formats, quantum key distribution.

I. INTRODUCTION

Driven by the pressing need for high-security solutions to address risks to cybersecurity posed by rapid technological progress, the development of quantum key distribution (QKD) systems has advanced significantly in recent years [8], [9], [10].

Manuscript received 2 November 2023; revised 5 February 2024 and 27 March 2024; accepted 2 April 2024. Date of publication 18 April 2024; date of current version 2 August 2024. The work of Francois Roumestan was supported by a CIFRE PhD grant. This work was supported by the E.C. projects CiViQ and OpenQKD, with a contribution by the Paris Region Project ParisRegionQCL. (Corresponding author: Amirhossein Ghazisaeidi.)

Francois Roumestan was with Nokia Bell Labs, 93100 Massy, France. He is currently self employed.

Amirhossein Ghazisaeidi and Jeremie Renaudier are with Nokia Bell Labs, 93100 Massy, France.

Luis Trigo Vidarte is with the ICFIO - Institut de Ciències Fotòniques, The Barcelona Institute of Science and Technology, 08860 Barcelona, Spain.

Anthony Leverrier is with Inria Paris, F-75589 Paris, France.

Eleni Diamanti is with Sorbonne Université, CNRS, LIP6, F-75005 Paris, France.

Philippe Grangier is with Université Paris-Saclay, IOGS, CNRS, Laboratoire Charles Fabry, F-91127 Palaiseau, France.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/JLT.2024.3391168.

Digital Object Identifier 10.1109/JLT.2024.3391168

A major challenge in this direction is to leverage the high potential of techniques that have been developed with great success for the classical telecommunication industry, with the goal of both enhancing the performance of QKD systems and assuring their smooth integration into deployed fibre optic network infrastructures. Continuous-variable (CV) QKD schemes [3], [11] are particularly well suited for this purpose. The key feature of such schemes is that dedicated photon-counting technology required in standard single-photon based schemes can be replaced by coherent detection techniques that are widely used in classical optical communications. This hardware simplification, however, comes at the price of a more involved theoretical analysis, and security proofs typically require the transmitter, commonly called Alice, to prepare coherent states with a Gaussian modulation to be sent to the receiver, Bob. Such a modulation has been used for advanced experimental implementations [4], [5], [6], but is not a common industrial practice; a more practical approach is to send coherent states chosen from a finite constellation in phase space. Although such discrete modulations were considered early in CV-QKD [12], [13], [14], sound security proofs have been developed only recently, for protocols with either very large constellation sizes [15] or very small ones [16], [17], [18], [19], with some experimental implementations in the latter case [20], [21]. But the most interesting format of medium-size quadrature amplitude modulation (QAM) used in classical optical communications remained out of reach for these methods, which rely on solving huge convex optimization problems. This outstanding issue was solved in [7], which provided an analytical bound for the asymptotic secret key rate of protocols with arbitrary modulation schemes, including probabilistic constellation shaping (PCS) QAM [23]. In practice, one needs also to take into account finite size effects, that are not included in [7]. We will therefore use an approach similar to the one of [24], that provides worst-case estimators of the secret key rate under reasonable assumptions.

Here, we experimentally demonstrate the feasibility of CV-QKD with PCS 64-QAM and 256-QAM that can reach very high peak secret key rate (SKR) with standard hardware and software compatible with current telecommunication systems [25], [26]. We emphasize that our choice of modulation format presents a number of advantages in practice: the use of QAM ensures the need for a smaller number of random numbers and leads
in principle to more efficient post-processing, pulse shaping requires a smaller bandwidth, and PCS optimizes the mutual information bringing it closer to Shannon channel capacity. Our results thus open the way towards integrating CV-QKD in standard optical communication systems, in an efficient, transparent, and cost-efficient way.

The paper is structured as follows: in Section II we overview the main concepts used in our work, namely the CV-QKD protocol and the PCS modulation formats. Section III discusses the experimental setup and methods, and in Section IV we present our experimental results. We conclude the paper in Section V, while in the Appendix we provide theoretical details regarding the security proofs for the derivation of the secret key rate.

II. CONCEPTS

A. CV-QKD Protocol and Security Proof

In the Prepare-and-Measure (PM) coherent state CV-QKD protocol with discrete modulation, Alice prepares coherent states $|\alpha\rangle = (|p + iq\rangle/2)$, chosen at random from a discrete constellation. She sends them through an optical link to Bob who measures them using coherent detection. This quantum transmission phase is followed by classical post-processing, in which Alice and Bob compare a randomly chosen fraction of their data to estimate the channel parameters and thus the length of the final key. Then they correct errors through a reconciliation step and finally turn their identical data set into a shorter secret key via privacy amplification.

The security of this PM protocol is analyzed through an equivalent Entanglement-Based (EB) protocol [3], where Alice (virtually) prepares an initial entangled state, measures one mode and transmits the second mode to Bob through the quantum channel. Exploiting the property that Gaussian states maximize the Holevo information between Bob’s measurement outcome and the eavesdropper quantum memory [27], [28], [29], it is sufficient to compute the covariance matrix of the bipartite state shared by Alice and Bob before measurement. The difficulty is that this virtual state is never prepared nor measured in the true PM protocol. Rather, the goal is for Alice and Bob to infer this covariance matrix from the data they observe in the PM protocol. While this task is straightforward when the modulation is Gaussian [4], [6], [11], it is more involved in the case of a discrete modulation. There, one needs to solve a semidefinite program whose dimension scales both with the constellation size and the dimension of the relevant Hilbert space — infinite for CV protocols. Even if it is possible to truncate the Fock space during the noise calibration process, and calculate worst-case estimators to take into account experimental finite-size effects, as explained below and in more details in [31] (In particular see Appendix B thereof for finite-size estimators). The main point that we want to make in this work is that our claims are based on the most recent theory, which is rigorous in the asymptotic regime. The calculation is made under minimal assumptions on the channel, and it is expected to provide conservative bounds; however, the present results cannot be considered as definitive, since the rigorous theory including the finite-size effect does not exist to-date. An overview of the CV-QKD protocol and the main results of [7] that are used in this work to compute the secret key rates are given in the Appendix.

B. Probabilistic Constellation Shaping for CV-QKD

The probabilistic constellation shaping with quadrature amplitude modulation (PCS-QAM) has been recently proposed [22], [23] as an efficient signaling technique for coherent optical communication. PCS-QAM builds on standard square M2-QAM modulation [32], but contrary to standard QAM, the frequency of occurrence of the constellation points follows Maxwell-Boltzmann probability mass function, parametrized by a single positive real parameter $\nu$, called the shaping parameter (see Appendix). In fact we can consider the PCS-QAM as a family of discrete modulation formats labeled by $(M, \nu)$, with cardinality $M^2$, and with the source entropy continuously depending on $\nu$. By providing an adjustable discrete approximation of the complex circular Gaussian distribution required by the Shannon classical information theory, PCS-QAM allows us tailoring the constellation and avoiding the shaping loss of the standard QAM, thus closing the gap to the capacity for a given channel by optimizing $M$ and $\nu$, cf. (3) and (4) in the Appendix.

Due to its property of offering efficient and flexible discrete approximations of Gaussian distributions, which are also required by the quantum information theory underlying the CV-QKD with coherent states, PCS-QAM is an attractive candidate for future implementations of such systems, and in the current work we present experimental proof of concept of such an approach. In order to design the system architecture for a given channel, i.e., a given fiber type and reach, first the total channel transmittance $T$ is determined, then the transmitter TX and receiver RX are characterized in terms of bandwidth, noise, loss and detection efficiency, and a target symbol rate $R_s$ is selected. Based on these characterizations and the theory of secret key rate (see Appendix), the optimum values of $M$ and $\nu$ are determined and the constellation design is achieved. The fine tuning and joint optimization of all parameters may require several iterations in the lab to maximize the secret key rate for a given system.

In our first demonstration of CV-QKD with discrete modulation, we worked with shaped 1024 QAM ($M = 32$) [33], considered as large enough to use Gaussian security proofs (see Appendix). Later on, and armed with the theory of [7], we found out that when $\nu$ (equivalently the variance of Alice normalized to the shot noise unit, denoted by $V_{\nu}$) is optimized, PCS 256-QAM ($M = 16$) theoretically approaches the maximal Gaussian limit of secret key rate. We then demonstrated, for the first time to our knowledge, shaped constellation CV-QKD implementations
with both PCS 256 and 64-QAM [25]. Following this result, further work was devoted to optimizing digital signal processing (DSP, see below). New measurements with both PCS 64-QAM and 256-QAM were performed and will be presented below for the first time. We have also demonstrated a multi-carrier quad-sub-carrier CV-QKD system, which has been already published elsewhere [34]. Fig. 1 illustrates the designed constellations used in the present work.

III. METHODS

A. Experimental Testbed

We use commercially available optical telecommunication equipment in order to provide practical and cost-efficient solutions. Important requirements that we sought for were high resolution, low noise and a bandwidth of at least 1 GHz. The setup is shown in Fig. 2. Alice generates coherent states using a 1550 nm tunable laser source with nominal 10 kHz linewidth. A dual polarization (DP) in-phase-and-quadrature (IQ) modulator is used to modulate the phase and amplitude of the laser beam. The analog inputs of the DP-IQ modulator are fed with the output of an Arbitrary Waveform Generator (AWG) with 5 GS/s sampling rate and 12 bits nominal resolution. The AWG outputs four 600 MBaud signals with Root Raised Cosine (RRC) pulse shape [32]. At the output of Alice’s lab, an optical power meter and an optical attenuator are used to monitor $V_A$. Bob uses a polarization-diverse 90-degrees hybrid to interfere the signal with the phase reference (or local oscillator, LO), which is generated with a laser identical to Alice’s. Four amplified balanced photodetectors convert the received optical signal to an analog electronic signal, which is then sampled using a 1 GHz real-time oscilloscope with 5 GS/s sampling rate and 12 bits nominal resolution. The sampled waveforms are stored for offline digital signal processing (DSP, see below). In the present experiment, parameter estimation and noise calibration are performed by offline DSP processing, and the frequency of alternative noise calibration is not optimized, but in a full-scale implementation the oscilloscope and offline DSP would be replaced by a continuously running receiver with real-time DSP, and careful system optimization should allow for a minimal overhead due to noise calibration. Also, a quantum device would be used for random number generation.

B. Digital Signal Processing

The implementation of the DSP suitable for CV-QKD was one of the main challenges of this work. The main building blocks shown in Fig. 3 are based on [23], but the adjustment of working parameters is critical. The algorithm inputs four sampled waveforms $y_1(k)$, $y_2(k)$, $y_3(k)$, $y_4(k)$, with an average number of samples per transmitted symbol $\bar{n}_{spr} = 8.3$ (calculated by dividing the 5 GS/s sampling rate with the 600 Mbaud symbol rate). The waveforms are then assembled into two complex waveforms $y_H(k) = y_1(k) + jy_2(k)$ and $y_V(k) = y_3(k) + jy_4(k)$. If the signal is single-side band, it is converted into a baseband signal by a digital frequency shift (bandwidth conversion), and a digital filter matching the pulse shape is applied; a root raised cosine (RRC) filter in our case. Then, we use a constant amplitude zero autocorrelation waveform (CAZAC) sequence [35] to compute the auto-correlation on the signal in order to retrieve the beginning of the time-multiplexed pilot sequence used in our implementation. The next steps are to correct linear impairments using a pilot-aided CMA adaptive equalizer [36], and to apply carrier frequency and carrier phase estimation algorithms. Finally, using the noise calibration symbols, denoted as $n_H$, $n_V$ in Fig. 3, which undergo the same DSP operations, QKD parameters are estimated to compute the achievable secret key rate.

These combined residual error of DSP algorithms contribute to the excess noise, which is the noise exceeding the fundamental shot noise of coherent states, and the electrical noise; see (1) below. Therefore it is crucial to optimize the various DSP parameters to minimize excess noise, ideally for each individual run of the experiment producing a block of data. In this work, the
optimization procedure has been performed offline, after signal acquisition, and is described in the following.

1) Pilot Amplitude and Rate: To correctly retrieve the low signal-to-noise ratio QKD symbols, the DSP relies on QPSK (that is 4-QAM) pilot symbols with a higher power, which needs to be optimized before signal acquisition. This is done by acquiring QKD signals with various values of the pilot amplitude, and applying the DSP to estimate the excess noise. Using such experimental tests, the pilot over QKD symbol power ratio was adjusted to 14 dB. The same optimization should be performed for the pilot rate. Contrary to pilot amplitude, the criterion to optimize the pilot rate is not the excess noise. In fact, if an increase of the pilot rate decreases the excess noise, it also decreases the rate of QKD symbols. Hence, we need to optimize directly the SKR. Using again an experimental optimization, we fixed the pilot rate to 4 pilots over 8 symbols, i.e., half of the transmitted symbols are actually pilots.

2) Adaptive Equalizer: For each experiment, we want to find the DSP parameters that minimize the excess noise. Since the DSP is performed offline, we can do a brute force optimization for the most relevant parameters, on a few acquisitions. To start with, we jointly optimize two parameters of the adaptive equalizer for polarization demultiplexing [40]: \( n_{\text{taps}} \), number of taps, and \( \mu \), the step size. For each couple \( (n_{\text{taps}}, \mu) \) under test, the DSP is applied to 12 different acquisitions. Fig. 4 shows the average excess noise for all the tested \( (n_{\text{taps}}, \mu) \), for experimental PCS 256-QAM data obtained in conditions slightly different than those presented in the main text. We observe that the lowest values of excess noise are achieved with 97 taps and a step size \( \mu \) of 10\(^{-6}\).

3) Signal Conditioning: We observed the presence of low frequency components of the excess noise, below 20 MHz, that we attribute to cutoff frequencies of the hardware as well as additive noise stemming from the electrical line. To avoid these perturbations, the outputs of the AWG are digitally upshifted such that the signal has no frequency component in the noisy region. In particular, the 600 Mbaud signal with RRC pulse shape and roll-off factor 0.4, corresponding to a bandwidth of 840 MHz, is upshifted by 500 MHz such that the useful bandwidth extends from 80 MHz to 920 MHz. The baudrate and roll-off factor have to be jointly optimized to minimize the excess noise. Furthermore, as noted above, the ratio of the QPSK pilots power relatively to the QAM symbols power has to be optimized to minimize the excess noise.

4) Signal Averaging: Our use of a worst-case estimator is justified if the fluctuations observed on the parameters are of a statistical nature. Given that all 5 \( \times \) 10\(^6\) data points within a data block are very close in time (total acquisition time 20 ms), the population variance can be considered sufficiently close to the theoretical variance to assume that fluctuations on the excess noise measurement are essentially of statistical nature. Therefore, the use of the worst-case estimator for the excess noise can be considered acceptable to take into account finite-size effects on the security of the protocol, although a more rigorous theoretical treatment of finite-size issues certainly remains desirable.

C. Noise Calibration Measurements

Most of the CV-QKD parameters are expressed in SNU. However, Bob effectively measures samples \( U \) of an electrical tension expressed in volts and obtains variances \( \text{Var}(U) \) in V\(^2\), thus he needs to estimate the quantity \( N_0 \), namely the variance of the shot noise expressed in V\(^2\). When disconnecting the signal input of the receiver, the output of the receiver is the sum of the shot noise and the electronic noise; therefore Bob can measure \( \text{Var}(U) = N_0(1 + V_\text{el}) \), where \( V_\text{el} \) is the variance of the receiver’s electronic noise in SNU. Then, disconnecting the LO input, Bob measures only the electronic noise, \( \text{Var}(U') = N_0 V_\text{el} \), and \( N_0 = \text{Var}(U) - \text{Var}(U') \).

This procedure gives four different values \( N_0^{(1)}, N_0^{(2)}, N_0^{(3)}, \) and \( N_0^{(4)} \), one for each channel of the oscilloscope. In practice, the samples measured on a channel are a mixture of the quadratures of the coherent states sent by Alice, that are recovered only after the DSP. This comes from several channel impairments such as polarization rotation or carrier phase noise. As a consequence, if the \( N_0^{(i)} \) are not all equal, they do not correspond to the variances of the shot noise on the quadratures effectively transmitted by Alice. To tackle this issue, we apply to the shot noise samples the same DSP correction as to the signal itself, and estimate the variances afterwards. In other words, the DSP operations applied to the signal samples are simultaneously applied to the noise samples.

We then note that the LO intensity and thus the shot noise may vary during the experiment, making it necessary to periodically reiterate the procedure of recording shot noise samples as often as possible. For this purpose, Bob’s setup includes an optical switch used to turn on and off the signal light coming from Alice. This procedure is repeated once every minute. Finally, the normalized value \( V_{BO} \) of Bob’s variance can be written as

\[
V_{BO} = 1 + \eta TV_A/2 + V_{el} + \xi_B,
\]

where \( T \) is the channel transmission efficiency, and \( \xi_B \) is the excess noise [3], [4] measured at Bob’s site, to be evaluated by Alice and Bob. The quantum efficiency and electronic noise of Bob’s detectors, which in our experiment take the values \( \eta = 0.65 \) and \( V_{el} = 0.1 \), respectively, are supposed here to be known to the legitimate users and cannot be modified by Eve.
TABLE I

| Fiber  | Modulation | V_A [SNU] | ξ_B [mSNU] | SKR [Mbps] |
|--------|------------|-----------|------------|------------|
| 9.5 km SMF-28 | 64-QAM | 0.0688 | 5.32 | 0.197 | 60.2 |
| 25 km EX3000 | 256-QAM | 0.0380 | 6.53 | 0.900 | 24.0 |

Indicative excess noise ξ_B (in mSNU) and estimated SKR (in Mbps) calculated using the security proof of [7] including finite-size effects, for PCS 64-QAM and PCS 256-QAM, during 1 hour of experiment, with 9.5 km of SMF-28 and 25 km of EX3000 fiber. The block size is N = 5 \times 10^6.

D. Non-Gaussian Attacks

Since our protocol follows the security proof of [7], Alice and Bob should not in fact evaluate \( T \) and \( ξ_B \) from the data, but rather three parameters denoted as \( c_1, c_2 \) and \( n_B \), as detailed in the Appendix; as a consequence, the SKR is a function of these three measured parameters. The quantity \( n_B \) denotes the average number of photons received by Bob, while \( c_1 \) and \( c_2 \) are two measures of correlation between transmitted symbols by Alice and received symbols by Bob, and are given by (10) and (11) in the Appendix. These two coefficients arise as the result of the analysis presented in [7]. Nevertheless, it is worth noticing that under our experimental conditions we found that the key rate calculated as a function of \( c_1, c_2, n_B \) is very close to the one calculated from \( T \) and \( ξ_B \) [31], meaning that the effective channel is well described by a Gaussian model. But we emphasize that this is an a posteriori observation, and not an a priori assumption, since the proof we are using is not restricted to Gaussian attacks.

Another issue is that the use of asymptotic formulas ignores finite-size effects in the actual measurements. In order to take them into account, we introduce worst-case estimators, following [24]. Although this approach does not apply strictly to discrete modulations, it provides a meaningful way to evaluate worst-case estimators [24]. Therefore we compute the SKR from \( c_{1\text{ min}}, c_{2\text{ min}}, n_{\text{ max}} \), which yields a reduced value with respect to the previous asymptotic rates. This procedure provides the results displayed in Table I, which correspond to a best-shot implementation of the protocol for a discrete modulation [31], given the available security proofs.

IV. RESULTS

Our experiment was performed with either 9.5 km of SMF-28 or 25 km of EX3000 fiber. The 25 km fiber link has a total loss of 4.3 dB. In each case the most critical DSP parameters are optimized to minimize the excess noise. In the present implementation the system operates with acquisitions of length 20 ms from which, after processing, \( N = 5 \times 10^6 \) QKD symbols are all used for parameter estimation, and no actual key is post-processed. Finally, the DSP optimization process is performed on a subset of 12 acquisitions.

Fig. 5 shows the estimated SKR for the 9.5 km SMF-28 fiber, for PCS 64 and 256-QAM. The estimation is based on the proof for an arbitrary modulation protocol [7], assuming \( \beta = 0.95 \) [37], and using worst-case estimators with \( N = 5 \times 10^6 \) and security parameter \( \epsilon = 10^{-10} \), following [24], [38], [39].

Table I summarizes the experimental results with modulation variance \( V_A \) values, excess noise \( ξ_B \) values, which are included as an indication of system performance, and SKR (in Mbps) calculated following the aforementioned procedure.

We can achieve a secret key rate of \( \sim 92 \) Mbps over 9.5 km and 24 Mbps over 25 km, using PCS 256-QAM format, averaged over 100 transmission blocks of \( N = 5 \times 10^6 \) QKD symbols. PCS 64-QAM gives lower performance, as theoretically expected. The expected behavior as a function of distance is shown in Fig. 6. Two modulation formats (PCS-64 and PCS-256) and two fibers have been used in this experiment; a 9.5 km standard single mode fiber (SMF-28) with attenuation coefficient 0.2 dB/km and a 25 km EX3000 fiber with attenuation coefficient 0.172 dB/km. PCS-64 modulation at 25 km does not yield a positive key rate. The expected SKR of a setup with Gaussian modulation in the asymptotic regime is plotted for comparison, assuming the same repetition rate \( R = 600 \) MBaud, \( ξ_B = 0.5 \) mSNU, and Alice using the optimal \( V_A \). The block size is \( N = 5 \times 10^6 \) [31]. By comparison with the current state of the art [5], [6], [9], [10], [26], these results confirm the high performance reached by our system by adopting techniques from standard optical communication and following the security proof for discrete modulation, including finite-size effects within a meaningful working hypothesis on optimal attacks. Finally, please note that [7] does not consider a specific implementation and is agnostic to DSP protocols. In practice this means that the output data from the DSP is taken as input data for the security proof, under the usual assumption that Bob’s detectors...
and subsequent data processing are private, so that we can apply the developed theoretical techniques to our implementation.

V. Conclusion

The laboratory experiment presented in this work opens interesting avenues towards faster and more flexible implementations of CV-QKD, within the standard environment of high bit rate coherent telecommunication. It leverages in particular industry-grade digital signal processing techniques that have been minimally modified for the CV-QKD implementation. To take full advantage of these improvements, it would be necessary to implement post-processing to extract the key from a non-disclosed fraction of the data. The speed of this data post-processing should be facilitated by the use of discrete constellations [7]. Finally, a better overall integration and stability of the whole setup will be ultimately required for advanced quantum communication networks [41, 42].

In future work, we plan to address the issue of finite-size effects and obtain a complete statistical treatment of the data based on a rigorous theoretical analysis. In this respect, we note that the analysis of [7] shows that for large constellations, the asymptotic SKR is essentially indistinguishable from that of a Gaussian modulation. We expect that the same will hold for finite-size corrections to the asymptotic SKR. We emphasize again that a full treatment of finite-size effects is a major open question in the theory of CV-QKD, and goes beyond the scope of our present work.

APPENDIX

Our goal in this appendix is to put forth the definitions and results that underlie the computation of the secret key rates presented in the main text. We do not aim to provide a tutorial on CV-QKD in general, since this is a vast subject whose proper expounding goes well beyond the scope of this paper. Readers are invited to consult [43] for fundamentals of quantum optics, [9] for a comprehensive overview of the field of QKD, [3], [31] and [44] for accessible introductions to CV-QKD, [2] for advanced material on Gaussian states and continuous variable quantum optics in phase space, [45] for advanced theoretical treatment of the security proofs of CV-QKD protocols, and [46] for implementation aspects of classical post-processing steps of the CV-QKD protocols.

Expression of the secret key rate (SKR): In our case the value $R$ of the SKR, in [bits/sec] is given by the formula

$$ R = 2R_s \times (1 - r_p) (I_{AB} - \beta \chi_{EB}). \tag{2} $$

This formula derives from the well-known Devetak-Winter theorem together with various practical overheads. The pre-factor 2 accounts for dual-polarizations, $R_s$ is the symbol-rate, $r_p$ is the DSP time-domain pilot rate (in our work $r_p = 0.5$), $I_{AB}$ is the standard classical mutual information between Alice and Bob in bits/channel-use, $\beta$ is the reconciliation efficiency, and $\chi_{EB}$ is the Holevo bound on the quantum-classical information between Eve and Bob, also in bits/channel-use.

The present work focuses on the experimental use of shaped constellation CV-QKD, and all symbols are revealed for parameter estimation. We did not implement classical post-processing, and we estimate the SKR assuming $\beta = 0.95$, as it is a standard value in the literature. Other parameters such as the frame error rate or the revealed fraction $r_{pe}$ may be included if needed.

General protocol: A CV-QKD protocol assumes the presence of an insecure quantum channel and an authenticated error-free public classical channel between two parties Alice and Bob. Alice generates a sequence of random bits, for instance via a quantum random number generator, and maps the bits to symbols using a suitable modulation format. Then she sends quantum coherent states based on those symbols over the quantum channel to Bob, who measures the coherent states. After a block of $N$ symbols has been prepared and transmitted by Alice and measured by Bob, Alice and Bob reveal $r_{pe} N$ symbols through the public classical channel, estimate parameters (as described below), then do reconciliation and privacy amplification on the $(1 - r_{pe}) N$ remaining symbols in order to jointly distill a shared secure bit string, the final secret key. Reconciliation is implemented using low density parity check codes, and has impact on the net rate through $\beta$ (2) and possibly a frame error rate. Privacy amplification is a standard technique from classical cryptography based on hash functions. In the following we report on the results concerning the achievable secret key rates of discrete modulation formats in the asymptotic regime, i.e., in the limit $N \to \infty$, and then comment on how we handled the finite-size effects. To simplify the presentation, we consider hereon single-polarization transmission and heterodyne coherent detection.

Constellation: An $M^2$-QAM constellation is a finite set $C$

$$ C = \{c_{mn} \mid m, n = 0, \ldots, M - 1\}, \tag{3} $$

consisting of $M^2$ complex numbers $c_{mn}$ called constellation points, $c_{mn} = 2(m + in) - (M - 1)(1 + i)$, where $m, n = 0, \ldots, M - 1$, and $i = \sqrt{-1}$. The Probabilistic Constellation Shaped (PCS) $M^2$-QAM modulation format with shaping parameter $\nu$ is a discrete source which maps the input bits to output symbols such that symbols are constellation points of $C$ selected with the Maxwell-Boltzmann probability mass function with parameter $\nu$ given by

$$ p_{mn}(M, \nu) = \frac{\exp \left( -\nu |c_{mn}|^2 \right)}{\sum_{k,l=0}^{M-1} \exp \left( -\nu |c_{kl}|^2 \right)}. \tag{4} $$

In the following, we order the $M^2$ symbols in a given way, and denote as $p_k$, $k = 1, \ldots, M^2$ the fixed probability associated with the $k$-th symbol.

Exchange of quantum data: For each channel use, symbols are chosen at random from a PCS $M^2$-QAM modulation. The symbols are multiplied by a constant factor to set the modulation variance of Alice to a given value $V_A$. Let $\alpha_i$ denote the symbol of the $i$-th channel use, and $|\alpha_i\rangle$ be the corresponding coherent state, for $i = 1, \ldots, N$. The coherent states, i.e., the states of the modulated laser field, are transmitted through a quantum channel, which is assumed to be fully controlled by Eve. The
Covariance matrix: The computation of the Holevo bound involves the $4 \times 4$ covariance matrix between position and momentum operators of the state shared by Alice and Bob, denoted $\Gamma_{AB}$. This matrix has the following form

$$
\Gamma_{AB} = \begin{bmatrix}
V & I_2 & Z & \sigma_x \\
Z & I_2 & W & \sigma_y \\
\sigma_z & W & I_2 & Z \\
\sigma_x & Z & \sigma_y & V
\end{bmatrix},
$$

where $I_2$ is the $2 \times 2$ identity matrix, and $\sigma_z$ is the third Pauli matrix

$$
\sigma_z = \begin{pmatrix}
1 & 0 \\
0 & -1
\end{pmatrix}.
$$

In (5) the quantities $V = V_A + 1$ and $W = TV_A + 1 + T\xi_A$ can be directly estimated using Alice’s and Bob’s symbols. However, the cross-correlation coefficient $Z$ is more delicate to infer from the experimental data, as explained below. Once the covariance matrix is estimated the Holevo bound and the achievable secret key rate can be computed using the well-known results described in Chapter 2 and the Appendix A.2 of [31] and the references therein.

Gaussian vs non-Gaussian modulation: For very large constellations, typically $M^2 \geq 4096$ [6], the modulation can be considered as Gaussian and it is possible to use the Gaussian optimality theorem to conclude that the best possible attack by Eve is also Gaussian (that is, it keeps the Gaussian character of an input state). Then the expression of $Z$ is well known, and can be used to compute the Holevo information $\chi_{EB}$ using standard methods [4], hence the secret key rate using (2).

For smaller constellations such as $M^2 = 64$ or 256 used in the present paper, the modulation differs significantly from a Gaussian modulation, and it is not possible to directly compute $Z$ from the data obtained by Alice and Bob. One can only infer a lower bound on its value. The main contribution of [7] is to provide a simple analytical formula for such a bound given the physical constraints; let us denote it by $Z^*$. This is achieved by first casting the problem into a semi-definite program, and then analytically solving it using a technique from convex optimization called sum-of-squares. Then as before the value of $Z^*$ is used to compute $\chi_{EB}$ and the SKR [7]. The explicit analytical formula for the lower bound of the cross-correlation coefficient (which corresponds to the maximum Holevo information) is

$$
Z^* := 2c_1 - 2\sqrt{w(n_B - 2c_2/V_A)}
$$

(7)

where the scalar $w$ only depends on the sequence of transmitted symbols and is given as

$$
w := \sum_k p_k \left( |\alpha_k| \hat{a}_\tau \hat{a}_\tau^* |\alpha_k\rangle - |\alpha_k\rangle \langle \alpha_k| \right)^2,
$$

(8)

using the Fock space operator $a_\tau := \tau^{1/2} a \tau^{-1/2}$, where $a$ is the annihilation operator corresponding to Alice’s mode, and $\tau$ is the density matrix of the emitted state [7], given by

$$
\tau = \sum_{k=1}^{M^2} p_k |\alpha_k\rangle \langle \alpha_k|.
$$

(9)

On the other hand the numbers $c_1$, $c_2$, and $n_B$ depend on both transmitted and received symbols and are computed during the parameter estimation. Denoting as $\beta_k$ the average values of Bob’s measurements corresponding to the (revealed) symbol $k$, and using over bars for complex conjugation, the explicit formulas are:

$$
c_1 := \text{Re} \left( \sum_k p_k \langle \alpha_k | \hat{a}_\tau | \alpha_k \rangle \beta_k \right)
$$

(10)

$$
c_2 := \text{Re} \left( \sum_k p_k \bar{\alpha}_k \beta_k \right)
$$

(11)

and $n_B$ is the average number of photons detected by Bob, also evaluated from the heterodyne data [7]. Given $Z^*$ from (7), the SKR can be calculated as previously. We note that in our fiber-based experimental setup (with no Eve!), the expected quantum channel between Alice and Bob can be modeled as a phase-insensitive Gaussian channel characterized by transmittance $T$ and the excess noise $\xi$, i.e., $\beta_k = \sqrt{T} \alpha_k + \gamma_k$, where $\gamma_k$ is a zero-mean Gaussian random variable with variance normalized to one in the SNU; hence for our experiments (7) may be reduced to (see (14) in [7])

$$
Z^*(T, \xi_A) := 2c_1 - \sqrt{T} \xi_A w
$$

(12)

but the general formula [7] we use makes no hypotheses on the channel.

Additional effects: In order to obtain actual experimental predictions, two more effects must be taken into account: (i) the imperfection of Bob’s detector, and (ii) finite size effects.

i) As indicated in the main text, the imperfections of Bob’s detector are taken into account by introducing a quantum efficiency $\eta$, and an electronic noise $V_{el}$. This can be done by standard methods, as described, e.g., in [31], [37].

ii) The previous results concern the asymptotic regime, where the total number of transmitted and received symbols $N$ tends to infinity. However, in practice $N$ is inevitably a finite number, therefore the parameters $c_1$, $c_2$, and $n_B$ in the above calculations should be given their actual observed values, which are themselves random variables, and fluctuate statistically. Developing rigorous proofs including such finite-size effects for non-Gaussian modulation (as defined above) is still an open problem to-date. In the absence of the rigorous theory, we make the reasonable assumption of Gaussian statistics for $c_1$, $c_2$, and $n_B$, that is actually in agreement with experimental data. Although this is not a proof, this allows us to compute confidence intervals, and to consider the worst-case estimators corresponding to the lowest SKR from these confidence intervals. Let us emphasize once again that no Gaussian assumption is made for calculating the asymptotic SKR, which is obtained directly from $c_1$, $c_2$, and $n_B$.

REFERENCES

[1] V. Scarani et al., “The security of practical quantum key distribution,” Rev. Modern Phys., vol. 81, 2009, Art. no. 1301.

[2] C. Weedbrook et al., “Gaussian quantum information,” Rev. Modern Phys., vol. 84, 2012, Art. no. 621.
[3] E. Diamanti and A. Leverrier, “Distributing secret keys with quantum continuous variables: Principle, security and implementations,” Entropy, vol. 17, pp. 6072–6092, 2015.

[4] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, “Experimental demonstration of long-distance continuous-variable quantum key distribution,” Nature Photon., vol. 7, pp. 378–381, 2013.

[5] Y. Zhang et al., “Long-distance continuous-variable quantum key distribution over 202.81km of fiber,” Phys. Rev. Lett., vol. 125, 2020, Art. no. 010502.

[6] N. Jain et al., “Practical continuous-variable quantum key distribution with composable security,” Nature Commun., vol. 13, 2022, Art. no. 4740.

[7] A. Denys, P. Brown, and A. Leverrier, “Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation,” Quantum, vol. 5, 2021, Art. no. 540.

[8] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, “Practical challenges in quantum key distribution,” npj Quantum Inf., vol. 2, 2016, Art. no. 16025.

[9] S. Pirandola et al., “Advances in quantum cryptography,” Adv. Opt. Photon., vol. 12, pp. 1012–1236, 2020.

[10] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, “Secure quantum key distribution with realistic devices,” Rev. Mod. Phys., vol. 92, 2020, Art. no. 025002.

[11] F. Grosshans, G. V. Asche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, “Quantum key distribution using Gaussian-modulated coherent states,” Nature, vol. 421, pp. 238–241, 2003.

[12] S. Lorenz, J. Rigas, M. Heid, U. L. Andersen, N. Lütkenhaus, and G. Leuchs, “Witnessing effective entanglement in a continuous variable prepare-and-measure setup and application to a quantum key distribution scheme using postselection,” Phys. Rev. A, vol. 74, 2006, Art. no. 042306.

[13] A. Leverrier and P. Grangier, “Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation,” Phys. Rev. Lett., vol. 102, 2009, Art. no. 180504.

[14] A. Leverrier and P. Grangier, “Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation,” Phys. Rev. A, vol. 83, 2011, Art. no. 042312.

[15] E. Kaur, S. Guha, and M. M. Wilde, “Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution,” Phys. Rev. A, vol. 103, 2021, Art. no. 012412.

[16] S. Ghoriai, P. Grangier, E. Diamanti, and A. Leverrier, “Asymptotic security of continuous-variable quantum key distribution with a discrete modulation,” Phys. Rev. X, vol. 9, 2019, Art. no. 021059.

[17] J. Lin, T. Upadhyaya, and N. Lütkenhaus, “Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution,” Phys. Rev. X, vol. 9, 2019, Art. no. 041064.

[18] J. Lin and N. Lütkenhaus, “Trusted detector noise analysis for discrete modulation schemes of continuous-variable quantum key distribution,” Phys. Rev. Appl., vol. 14, 2020, Art. no. 064030.

[19] T. Matsura, K. Maeda, T. Sasaki, and M. Koashi, “Finite-size security of continuous-variable quantum key distribution with digital signal processing,” Nature Commun., vol. 12, 2021, Art. no. 252.

[20] T. Hirano et al., “Implementation of continuous-variable quantum key distribution with digital modulation,” Quantum Sci. Technol., vol. 2, 2017, Art. no. 024010.

[21] P. Wang, Y. Zhang, Z. Lu, X. Wang, and Y. Li, “Discrete-modulation continuous-variable quantum key distribution with a high key rate,” New J. Phys., vol. 25, 2023.

[22] F. Buchali, F. Steiner, G. Böcherer, L. Schmalen, P. Schulte, and W. Idler, “Rate adaptation and reach increase by probabilistically shaped 64-QAM: An experimental demonstration,” J. Lightw. Technol., vol. 34, no. 7, pp. 1599–1609, Apr. 2016.

[23] A. Ghazisaeidi et al., “Advanced C+ L-band transoceanic transmission systems based on probabilistically shaped PDM-64QAM,” J. Lightw. Technol., vol. 35, no. 7, pp. 1291–1299, Apr. 2017.

[24] A. Leverrier, F. Grosshans, and P. Grangier, “Finite-size analysis of a continuous-variable quantum key distribution,” Phys. Rev. A, vol. 81, 2010, Art. no. 062343.

[25] F. Roumestan, A. Ghazisaeidi, J. Renaudier, L. T. Vidarte, E. Diamanti, and P. Grangier, “High-rate continuous variable quantum key distribution based on probabilistically shaped 64 and 256-QAM,” in Proc. IEEE Eur. Conf. Opt. Commun., 2021, pp. 1–4.

[26] Y. Pan et al., “Experimental demonstration of high-rate discrete-modulated continuous-variable quantum key distribution system,” Opt. Lett., vol. 47, pp. 3307–3310, 2022.

[27] M. M. Wolf, G. Giedke, and J. J. Cirac, “Extremality of Gaussian quantum states,” Phys. Rev. Lett., vol. 96, 2006, Art. no. 080502.

[28] R. García-Patrón and N. J. Cerf, “Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution,” Phys. Rev. Lett., vol. 97, 2006, Art. no. 190503.

[29] M. Navascués, F. Grosshans, and A. Acín, “Optimality of Gaussian attacks in continuous-variable quantum cryptography,” Phys. Rev. Lett., vol. 97, 2006, Art. no. 190502.

[30] T. Upadhyaya, T. v. Himbeeck, J. Lin, and N. Lütkenhaus, “Dimension reduction in quantum key distribution for continuous- and discrete-variable protocols,” PRX Quantum, vol. 2, 2021, Art. no. 020325.

[31] F. Roumestan, “Advanced signal processing techniques for optical fiber continuous-variable quantum key distribution systems,” Ph.D. dissertation, Sorbonne Univ., 2022.

[32] J. Proakis and M. Salehi, Digital Communications. New York, NY, USA: McGraw-Hill, 2007.

[33] F. Roumestan et al., “Demonstration of probabilistic constellation shaping for continuous variable quantum key distribution,” in Proc. Opt. Fiber Commun. Conf., 2021, Paper F4E1.

[34] F. Roumestan, A. Ghazisaeidi, H. Mardoyan, J. Renaudier, E. Diamanti, and P. Grangier, “254.6 Mbs secret key rate transmission over 13.5 km SMF using PCS-256QAM super-channel continuous variable quantum key distribution,” in Proc. Opt. Fiber Commun. Conf., 2022, paper Tu3U4-1.

[35] A. Milewski, “Periodic sequences with optimal properties for channel estimation and fast start-up equalization,” IBM J. Res. Dev., vol. 27, pp. 426–431, 1983.

[36] M. S. Faruk, Y. Mori, C. Zhang, K. Igarashi, and K. Kikuchi, “Multimaintenance monitoring from adaptive finite-impulse-response filters in a digital coherent receiver,” Opt. Exp., vol. 18, pp. 26929–26936, 2010.

[37] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, “Long-distance continuous-variable quantum key distribution with a Gaussian modulation,” Phys. Rev. A, vol. 84, 2011, Art. no. 062317.

[38] V. Scarani and R. Renner, “Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing,” Phys. Rev. Lett., vol. 100, 2008, Art. no. 200501.

[39] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, “Analysis of imperfections in practical continuous-variable quantum key distribution,” Phys. Rev. A, vol. 86, 2012, Art. no. 032309.

[40] K. Kikuchi, “Fundamentals of coherent optical fiber communications,” J. Lightw. Technol., vol. 34, no. 1, pp. 157–179, Jan. 2016.

[41] S. Wehner, D. Elkouss, and R. Hanson, “Quantum internet: A vision for the road ahead,” Science, vol. 362, 2018, Art. no. eaam9288.

[42] L. Gyongyosi and S. Imre, “Advances in the quantum internet,” Commun. ACM, vol. 65, no. 8, pp. 52–63, 2022.

[43] L. Mandel and E. Wolf, Optical Coherence and Quantum Optics. New York, NY, USA: Cambridge Univ. Press, 1995.

[44] F. Loidl et al., “Continuous-variable quantum key distribution with gaussian modulation — the theory of practical implementations,” Adv. Quantum Technol., vol. 1, 2018, Art. no. 1800011.

[45] A. Leverrier, “SU(p,q) coherent states and a Gaussian de Finetti theorem,” J. Math. Phys., vol. 59, 2018, Art. no. 042202.

[46] H. Mani, “Error reconciliation protocols for continuous-variable quantum key distribution,” Ph.D. dissertation, DTU, 2021.