Research Article Vol. 11, No. 9 / September 2024 / Optica 1197


# Continuous-variable quantum key distribution at 10 GBaud using an integrated photonic-electronic receiver

Adnan A. E. Hajomer,[1,†,*] Cédric Bruynsteen,[2,†] Ivan Derkach,[1,3] Nitin Jain,[1] Axl Bomhals,[2] Sarah Bastiaens,[2] Ulrik L. Andersen,[1] Xin Yin,[2] and Tobias Gehring[1,4]

[1]Center for Macroscopic Quantum States (bigQ), Department of Physics, Technical University of Denmark, 2800 Kongens Lyngby, Denmark
[2]Ghent University-IMEC, IDLab, Dep. INTEC, 9052 Ghent, Belgium
[3]Department of Optics, Faculty of Science, Palacky University, 17. listopadu 12, 771 46 Olomouc, Czech Republic
[4]tobias.gehring@fysik.dtu.dk
[†]These authors contributed equally to this work.
[*]aaeha@dtu.dk

Received 13 May 2024; revised 7 July 2024; accepted 29 July 2024; published 21 August 2024

**Quantum key distribution (QKD) is a widely recognized application of quantum information theory, guaranteeing information-theoretically secure key exchange. However, commercial viability of QKD systems is currently impeded by issues such as scalability, network integration, and high manufacturing costs. Low-cost, high-volume production of photonic and electronic integrated circuits could be the breakthrough needed for broad-scale deployment of cutting-edge QKD systems. Here, we present a continuous-variable (CV) QKD system that is based on an integrated photonic-electronic receiver. It combines a silicon photonic integrated circuit, featuring a phase-diverse receiver, with custom-designed GaAs pHEMT transimpedance amplifiers. Operating at a classical telecom symbol rate of 10 GBaud, our QKD system generates high secret key rates - exceeding 0.7 Gb/s over a 5 km distance and 0.3 Gb/s over a 10 km. The secret keys are secure against collective attacks, even when accounting for finite-size effects in the parameter estimation, thanks to well-designed digital signal processing that enables broadband system operation. Our experiment sets a record for secure key exchange and paves the way for the implementation of real-time broadband CV-QKD systems.** 

https://doi.org/10.1364/OPTICA.530080

## 1. INTRODUCTION

Quantum key distribution (QKD) is a method for sharing cryptographic keys between remote users, leveraging the principles of quantum mechanics [1,2]. When combined with one-time pad encryption, QKD offers information-theoretic secure data transmission, invulnerable to breach by current or future technologies. However, this requires a shared secret key that can only be used once, with a length of at least as long as the message [3]. Therefore, increasing the secret key rate (SKR) of QKD is of paramount importance to facilitate secure communication in networks with a large number of users or high-data-rate applications, such as distributed storage encryption and high-speed access networks [4,5].

In the continuous variable (CV) flavor of QKD, quantum information is encoded in the continuous degrees of freedom of quantum systems, such as the amplitude and phase quadrature of the electromagnetic field of light [6]. This modality has gained significant attention in the scientific community due to its ability to provide high rates, approaching the ultimate limit of secure communication known as the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) [7] bound. In the prepare-and-measure version of the CV-QKD protocol, the sender, Alice, prepares coherent quantum states using a quadrature modulator and sends them to the receiver, Bob. The quantum states propagate through an insecure channel controlled by a potential eavesdropper, Eve. Bob measures the quantum state using coherent detection, e.g., heterodyne or homodyne detection, supported by a local oscillator (LO) [8,9]. Importantly, these detection techniques need to be quantum-noise-limited across the entire quantum signal bandwidth.

Recently, a number of high-rate CV-QKD systems have been engineered, using both Gaussian [10–17] and discrete modulation [18–22] of coherent states. While protocols based on Gaussian modulation have the most advanced security proof [10], they also require a high-resolution digital-to-analog converter (DAC) to approximate the analog constellation space adequately. This requirement presents an issue when increasing the symbol rate of the QKD system since the signal-to-noise performance of DACs diminishes at elevated sampling rates [23]. In contrast, discrete modulation uses a discrete constellation space, making it much more compatible with high-speed wireline components. However, despite this potential advantage, there are very few

discrete-modulated (DM) CV-QKD systems operating in the multi-GBaud regime [17,19], which is attributed to the difficulty in ensuring consistent and quantum-noise-limited behavior over such extensive bandwidths.

Although CV-QKD is well-suited for photonic integration thanks to its compatibility with standard telecom components [24], recent efforts have focused primarily on integrating discrete variable (DV) QKD [25,26]. While Zhang *et al*. [27] have successfully demonstrated the feasibility of using integrated circuits for CV-QKD, their achieved SKR of 0.25 Mb/s is relatively low, especially compared to bulk fiber-based CV-QKD implementations [17–22]. In this work, we show that integrating CV-QKD not only offers the potential for miniaturization and cost-effectiveness but also provides higher key rates, facilitated by high-bandwidth components [28] and low-noise design techniques. Therefore, integrating CV-QKD has the potential to significantly enhance the cost-effectiveness, performance, and practicality of QKD systems.

In this article, we report our efforts to overcome the bandwidth limitations in CV-QKD transmitters and receivers. Specifically, we focus on improving the receiver's performance by introducing a co-integrated phase diverse receiver consisting of a silicon photonics optical front-end and custom-integrated transimpedance amplifiers (TIAs) designed in a 100 nm GaAs pHEMT technology. Although high-bandwidth TIAs for telecom applications are commercially available, they are generally not suited for balanced detection schemes or cannot achieve quantum-noise-limited performance [29]. Leveraging high-speed integrated components and adopting a low-noise design, our receiver can access a shot-noise-limited bandwidth exceeding 20 GHz. Silicon photonics makes use of existing CMOS infrastructure for mass production [30], while GaAs pHEMTs offer high performance with mature manufacturing processes. For these reasons, we believe our receiver offers a path toward a cost-effective, large-scale adoption of CV-QKD technology.

On the transmitter's side, we design a digital signal processing (DSP) pipeline, including a pre-emphasis filter, for quantum state preparation. This advancement allows our transmitter to operate at a symbol rate of 10 GBaud. By combining the improvements of both receiver and transmitter, we demonstrate the highest secret key rate (SKR) for any DM coherent state CV-QKD system to date. Specifically, we achieve SKRs of 0.92 Gb/s and 0.48 Gb/s in the asymptotic regime and 0.737 Gb/s and 0.315 Gb/s when accounting for finite-size effects over distances of 5 km and 10 km, respectively. These advances represent a significant step towards realizing practical, high-performance CV-QKD systems.

## 2. INTEGRATED RECEIVER

Our phase-diverse optical front-end, designed utilizing imec's iSiPP50G silicon photonics platform [31], is shown schematically in Fig. 1. We coupled the light into the chip using two grating couplers, with one input receiving the LO and the other receiving the incoming quantum signal. The quantum signal and the LO were then divided into two arms via a $1 \times 2$ multimode interferometer (MMI) to measure the conjugate quadratures. To ensure a 90° phase shift between the measured quadratures, we incorporated two waveguide heaters and controlled them actively. This setup was followed by two balanced homodyne detectors, which were composed of a Mach-Zehnder interferometer (MZI) and two photodetectors with a responsivity of 1.1 A/W [31]. The MZI was implemented using two $2 \times 2$ MMIs and two heaters, which

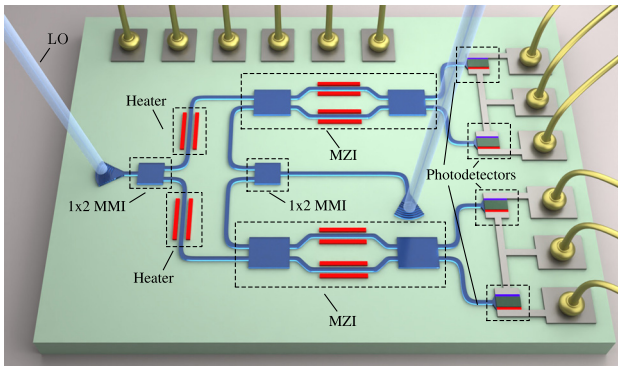


**Fig. 1.** Diagram of the photonic integrated circuit. MZI: Mach-Zehnder interferometer; MMI: multimode interferometer; LO: local oscillator.

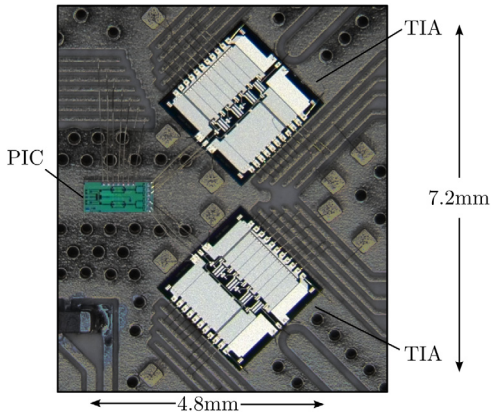


**Fig. 2.** Micrograph of the integrated receiver assembly. PIC: photonic integrated circuit; TIA: transimpedance amplifier.

were adjusted based on the feedback from the TIA to minimize the amount of direct current (DC) flowing into the TIA, thus augmenting the common-mode rejection ratio. The overall efficiency of the phase-diverse homodyne receiver was measured to $\eta = 44\%$, with the majority of the loss attributed to the grating coupler insertion loss (IL) = 2.5 dB [31]. However, this may be improved in future designs by employing edge couplers (IL = 1.1 dB [32]), potentially raising the theoretical efficiency to $\eta \approx 61\%$. This improvement could lead to an increase of more than 60% in the secure key rate.

Each pair of balanced photodetectors was connected to a separate TIA, devised in a 100 nm GaAs pHEMT process. The TIA architecture implements a three-stage core amplifier, enabling higher transimpedance values while lowering the electronic noise [29]. Using two separate dies minimizes the risk of interchannel crosstalk through parasitic paths, such as the substrate. Additionally, we took care to reduce the risk of electromagnetic interference by rigorously decoupling the power supplies and employing coplanar waveguides for the output transmission lines. A micrograph of the PIC accompanied by the two TIA dies is shown in Fig. 2. The overall dimensions of the three chips spanned 4.8 mm by 7.2 mm. The chips were mounted on an interposer printed circuit board (PCB) that was temperature stabilized by a thermo-electric cooler and a surface-mounted thermistor. The output of each TIA was connected to a 50 Ω transmission line, which was terminated in a coaxial connector. For more detailed

information on the receiver characterization and the impact of its performance on security analysis, please refer to Supplement 1.

## 3. HIGH-RATE CV-QKD SYSTEM

Figure 3 shows the schematic design of our high-speed CV-QKD system, comprising two stations: the transmitter (Alice) and the receiver (Bob), connected through a quantum channel utilizing standard single-mode fiber (SSMF). The system is designed to perform state preparation and measurement without requiring manual intervention. This was achieved by a single system on a module that monitored and controlled the different optical and electronic sub-components. In the following subsection, we will provide a detailed description of each station.

### A. Transmitter (Alice)

Alice's station is built around a high-speed, 8-bit arbitrary waveform generator (AWG, Keysight M8195A) with two channels operating at a sampling rate of 32 GSample/s. This drives our developed transmitter unit, known as qTReX [33], housing all necessary optical and electronic components. The internal schematic of qTReX is illustrated in the inset of Fig. 3. A 1550 nm continuous wave (CW) laser with a linewidth of 100 Hz was used as an optical source. To avoid analog pulse carving [34], the coherent states were generated at sideband frequencies by modulating the CW laser using an in-phase and quadrature (IQ) modulator driven by the AWG. An automatic bias controller regulated the DC voltages to maintain the IQ modulator at its minimum transmission point [35]. The modulation variance of the generated thermal state was controlled by a variable optical attenuator (VOA). To avoid Trojan-horse attacks enabled by back reflection, a Faraday isolator (FI) and wavelength filter were connected to the output of the VOA [36].

Producing coherent states at GBaud symbol rates requires a transmitter with a large bandwidth. In practice, however, any transmitter exhibits a high-frequency roll-off, introducing correlations intersymbol interference (ISI) between the transmitted symbols. This phenomenon can compromise the independent and identically distributed nature of the quantum symbols, potentially violating a common assumption made in security proofs [37].

To address the ISI challenge, we carefully designed a digital signal processing (DSP) pipeline, incorporating a pre-emphasis filter [38,39] for coherent state preparation, as depicted in Fig. 4. The complex amplitude of the coherent state, $|\alpha\rangle = |x + jp\rangle$, was randomly drawn from a probabilistically shaped discrete constellation with a defined modulation order (M) and a Gaussian-like probability distribution. This process is also referred to as probabilistic constellation shaping (PCS) in classical telecommunication [39]. The coherent states were initially drawn at symbol rates of 8 GBaud or 10 GBaud and then up-sampled to 32 GSample/s, after which they were pulse-shaped using a root-raised cosine filter with a roll-off of 0.2, defining the temporal mode of the generated quantum state. As a result, this leads to the creation of a continuous-mode quantum state, living in a frequency band of 9.6 GHz and 12 GHz for a symbol rate of 8 GBaud and 10 GBaud, respectively. However, the continuous mode state can effectively be simplified to a specific single mode [40], facilitating the application of a traditional security proof that assumes a single temporal mode [41,42]. To compensate for the high-frequency slope of the transmitter, the baseband signal was digitally pre-emphasized using the inverse frequency response of the transmitter. The pre-emphasis filter coefficients were measured using a 16 GBaud reference signal, and therefore, it supports a wide range of symbol rates without recalculating the filter coefficients. The inset of Fig. 4 shows the frequency response of the transmitter, including the IQ modulator, AWG, and the RF cables, as well as the spectrum of the 10 GBaud quantum signal before and after the pre-emphasis filter. To establish a shared reference phase between the transmitter and the receiver, pilot tones set at 8 GHz or 7 GHz were frequency multiplexed with the 10 GBaud or 8 GBaud pre-emphasized quantum signals,

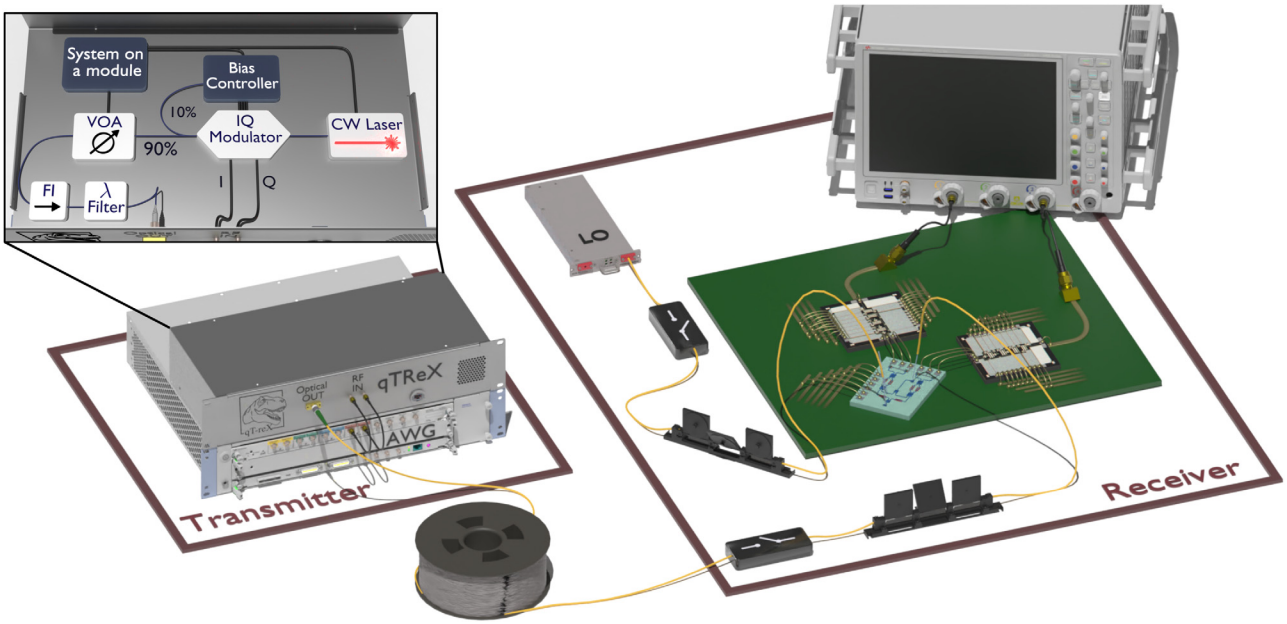


**Fig. 3.** High-rate CV-QKD setup. Diagram of the QKD system with all key components. At the transmitter side: CW laser (continuous wave laser), IQ modulator (in-phase and quadrature modulator), VOA (variable optical attenuator), FI (Faraday isolator), wavelength filter, and AWG (arbitrary waveform generator). At the receiver side: CW laser used as a local oscillator (LO), two optical switches, two polarization controllers, the photonic and electronic integrated circuits on an interposer PCB (dark green box), and RTO (real-time oscilloscope).

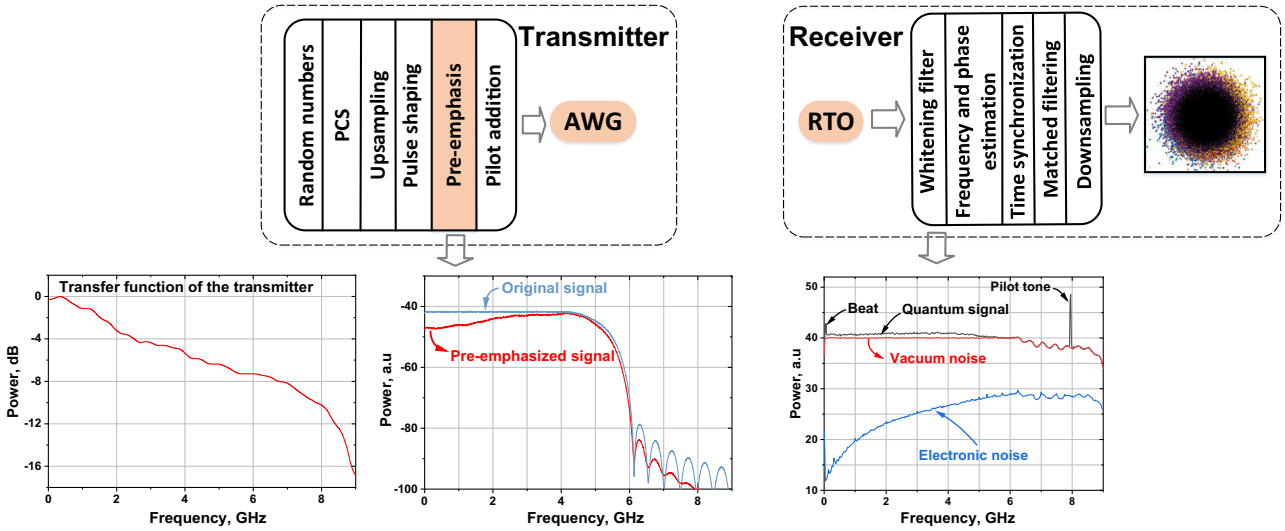


**Fig. 4.** The DSP routine of GBaud CV-QKD system. AWG: arbitrary waveform generator; PCS: probabilistic constellation shaping; RTO: real-time oscilloscope. See the main text for the details.

respectively. Finally, the modulation variance of the generated state ensemble was characterized through a back-to-back measurement, where the transmitter and the receiver were connected through a fiber patch cord.

### B. Receiver (Bob)

To accurately measure the coherent quantum states, we employed intradyne detection [9], leveraging our integrated phase-diverse receiver and a free-running CW laser with respect to the transmitter's laser. In comparison to phase-diversity homodyne receivers, intradyne detection offers a more simplified optical subsystem, as it does not require an optical phase-lock loop. For optimal intradyne detection, the frequency difference between these lasers was set to be less than half of the bandwidth of the quantum signal. The one-sided spectrum of the received signal, as illustrated in Fig. 4, shows a beat signal at ≈56 MHz, which is less than the bandwidth of the quantum signal. It also indicates that the generated baseband quantum signal was frequency-shifted by the same laser frequency difference of ≈56 MHz. Maintaining this frequency difference is crucial to avoid the penalties associated with the vacuum mode in the image sideband.

To maximize the coupling into the chip, we used two polarization controllers (PCs) to adjust the polarization of the LO and the quantum signal. We further enhanced the system by incorporating electronically controlled optical switches into both the LO and signal paths. These switches enable autonomous system calibration, allowing for consecutive measurements of vacuum noise (signal off and LO on) and electronic noise (signal off and LO off) following each quantum signal measurement. The two outputs of the phase-diverse receiver were digitized using an 8-bit real-time oscilloscope (RTO, Keysight DSA Z634A) operating at a sampling rate of 80 GSamples/s, which was clock synchronized with the AWG using a 100 MHz reference clock. Finally, the digitized signals were recorded for offline DSP.

Figure 4 illustrates the DSP routine used for quantum symbols recovery. First, a digital post-equalizer (whitening filter) was applied to the quantum signal, the vacuum noise, and the electronic noise traces to compensate for the high-frequency roll-off of the receiver. The filter coefficients were determined by fitting the inverse frequency response of the receiver, computed from the vacuum noise measurement. The equalized spectra are shown through the black, red, and blue traces on the right side of Fig. 4. Next, the pilot tone frequency was estimated by applying a Hilbert transform on the filtered pilot tone and the linear fit of its phase profile. To derive the relative phase between the transmitter and the receiver, the pilot tone was baseband transformed using the pilot frequency estimate. Subsequently, the quantum signal was baseband transformed by the frequency difference between the known pilot frequency at the transmitter and the pilot frequency estimate at the receiver. The phase of the quantum signal was then corrected using the extracted phase of the pilot tone. Next, the temporal shift caused by the propagation delay of the quantum channel and different electronic components was calculated by cross-correlating the reference transmitted samples with the received samples. After applying root-raised-cosine matched filtering and downsampling, the corresponding quantum symbols were obtained. Finally, to account for a residual phase shift due to the frequency difference between the quantum signal and the pilot tone, the quantum symbols were rotated.

## 4. SECURITY ANALYSIS

Contrary to Gaussian CV-QKD protocols where coherent states follow a two-dimensional zero-centered continuous Gaussian distribution $\mathcal{N}(0, \Sigma)$, in discrete-modulated (DM) CV-QKD protocols, coherent states are drawn from a discretized set $\{\alpha_k\}_{k=1,\ldots M}$, with respective probabilities $\mathcal{P}(\alpha_k)$, where $\alpha$ represents the amplitude of the coherent state, and $\ldots$ $M$ is the cardinality of the discrete constellation. On the receiver side the measurement of incoming quantum states yields a complex number $\zeta_k$. After transmitting and receiving a block of $N$ symbols, the trusted parties hold two correlated strings (one for each quadrature) of equal length, which they then correct for errors and use to distill secret keys, i.e., identical random sequences that are completely uncorrelated with any unauthorized party.

The security analysis of QKD protocols is based on the equivalent entanglement-based representation of state preparation. In

this representation, Alice generates an entangled state $|\Psi\rangle_{AB}$ and measures one of the modes to conditionally prepare the other. Attribution of the channel to Eve, without loss of generality, implies that after transmission Eve uses her share of the joint pure state $|\Psi\rangle_{ABE}$ to infer Bob's measurement outcomes.

The security against collective attacks is defined as the positivity of accessible information difference [43]:

$$R_\infty = \beta I_{AB} - \chi_E, \tag{1}$$

where $\beta$ is the reconciliation efficiency that indicates the inability to recover full mutual information $I_{AB}$ between Alice's and Bob's data sets, while $\chi_E$ is the Holevo bound that bounds the information an adversary may hold on the generated data sequence at the reference side (Bob). Both $I_{AB}$ and $\chi_E$ can be evaluated based on the covariance matrix $\Gamma_{AB}$ of the state shared after channel $\rho_{AB}$. While Alice and Bob can directly obtain variances of local quadrature operators, the term corresponding to the correlations between modes $A$ and $B$ is not trivially assessed when a general non-Gaussian measurement of the former prepares the state in the latter. We employ a theory developed in Ref. [42] that allows to analytically bound the correlation term in $\Gamma_{AB}$ and consequently the secure key rate (SKR) in Eq. (1) in the asymptotic regime of infinitely many exchanged quantum states.

We use three constellations for quadrature amplitude modulation (QAM) given by discretized Gaussian distributions: $M = 16, 32, 64$ (see top Fig. 5). Each constellation is characterized by the variance of the distribution $V_M$ and assigned probabilities within the constellation $\mathcal{P}(\alpha_k)$, determined by the cardinality $M$ and the parameter $\nu$ related to the variability or statistical dispersion of the probability distribution. The optimal value of modulation variance $V_M = 2\alpha^2$ that maximizes the SKR strongly depends on the reconciliation efficiency $\beta$. We choose a variance $V_M \approx 1$ shot-noise unit (SNU) as it allows us to operate at low excess noise and it ensures that the mutual information $I_{AB}$ of the continuous-Gaussian protocol is a good approximation for the DM protocol [44]. The choice of parameter $\nu$ is crucial for the protocol's performance and thus is optimized based on the cardinality $M$ and modulation variance $V_M$.

In the analysis, we presume that the receiver station is fully trusted. Hence, the heterodyne detector efficiency $\eta = 44\%$ and electronic noise with variance $V_{el}$ were modeled as linear coupling of the signal to a thermal noise source purified by trusted parties. This partially decouples Eve from Bob's accumulated key and decreases the Holevo bound $\chi_E$ [45].

## 5. RESULTS

The results of the security analysis in the asymptotic regime are shown in Fig. 5 (bottom). The triangles represent experimental results for several measurements conducted over distances of 5 km and 10 km at symbol rates of 8 GBaud and 10 GBaud for the three modulation formats. With an information reconciliation efficiency of 95%, the 64 QAM modulation format led to the highest secret key rate of 0.92 Gb/s over a 5 km fiber channel. This superior performance is primarily attributed to its high cardinality and the comparatively lower excess noise relative to 16 QAM and 32 QAM. Conversely, measurements with $M = 32$ displayed greater excess noise, resulting in a reduced SKR of 0.33 Gb/s. This rate is comparable to that achieved with the lower cardinality $M = 16$ set operating over the same fiber, but with reduced excess noise.

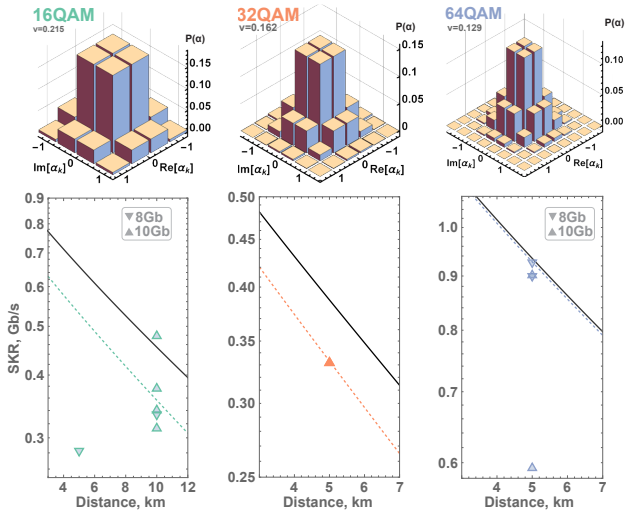


**Fig. 5.** (Top) The constellation probability distributions used in the experiment: 16, 32 (four corner points have a probability of 0), and 64 QAM. $\alpha$'s are in $\sqrt{\text{SNU}}$. (Bottom) Asymptotic secure key rate against fiber length (0.2 dB/km). Lines show the theoretical curves for GG02 and respective constellation with a repetition rate of 10 Gbaud, $\beta = 95\%$; modulation variance $V_M$, excess noise $\epsilon$, and coupling efficiency are mean of observed experimental values for respective constellation. Points show the experimental results for each constellation and distance used, with repetition rate of 8 GBaud (down triangle) and 10 GBaud (up triangle).

Table 1 provides a summary of the best experimental results for each constellation and distance.

Furthermore, the lines in Fig. 5 (bottom) show the theoretical predictions for protocols at $V_M = 1$ SNU with $M = 16$, 32, and 64 (with optimized $\nu$), along with the GG02 protocol with Gaussian modulation [6]. Theoretical predictions assume (from left to right) mean modulation variance $V_M = 0.87, 0.93, 1.02$ SNU, fiber loss of 0.2 dB/km and mean coupling efficiency of $\eta_D = 84.5, 88.4, 92.3\%$, the mean excess noise observed in our experiment $\epsilon = 0.035, 0.071, 0.032$ SNU (at channel input), and the mean electronic noise $V_{el} = 0.061, 0.067, 0.054$ SNU. Additionally, we assumed the highest repetition rate $s$ of 10 GBaud, with the secure key given as $s \times R_\infty$. It is noteworthy that using the 64-point constellation essentially recovers the performance of the protocol with "continuous" Gaussian modulation.

Figure 6 illustrates the impact of channel parameter fluctuations on system performance. Slight variations in channel excess noise and untrusted loss result in noticeable differences in the asymptotic key rate (represented as points). These variations can arise from a variety of sources, such as polarization drifts, temperature variances, or mechanical drift that can occur during the optical probing of the photonic IC. Even with a small cardinality, the performance of GG02 (depicted by contour lines) can be regained when operating under conditions of low noise. This suggests that while reducing the channel excess noise and approaching the performance of GG02 protocol through low modulation variance, the system becomes increasingly susceptible to unavoidable channel parameter fluctuations in practical applications.

In the absence of rigorous finite-size key evaluation techniques, we examine the significant impact of parameter estimation on the key length in this regime. Channel parameters are chosen with worst-case assumptions, ensuring that the information accessible to Eve is not underestimated. We estimate the conservative key rate

**Table 1. Summary of Experimental Parameters and Secure Key Rates for Best Results at Each Distance[a]**

| M | $\nu$, a.u. | Rep. Rates, GBaud | Distance, km | $V_M$, SNU | $T$, a.u. | $V_{el}$, % SNU | $\epsilon$, % SNU | $R_\infty$, Bits/Symbol | $R_{finite}$, Bits/Symbol | $SKR_{finite}$, Gb/s |
|---|---|---|---|---|---|---|---|---|---|---|
| 16 | 0.215 | 10 | 10 | 0.87 | 0.569 | 6.50 | 2.622 | 0.048 | 0.035 | 0.351 |
| 16 | 0.215 | 8 | 5 | 1.01 | 0.618 | 4.95 | 5.187 | 0.035 | 0.021 | 0.171 |
| 32 | 0.162 | 10 | 5 | 0.93 | 0.702 | 6.76 | 7.183 | 0.033 | 0.019 | 0.194 |
| 64 | 0.129 | 8 | 5 | 1.03 | 0.733 | 5.03 | 1.590 | 0.115 | 0.093 | 0.746 |

[a]Reconciliation efficiency $\beta = 0.95$, detector efficiency $\eta = 0.44$, block size $N = 1.6 \times 10^7$.

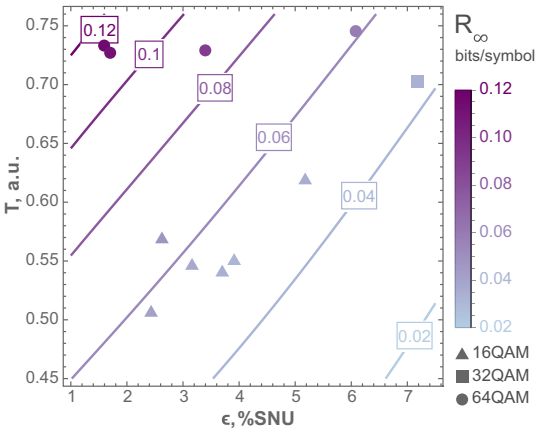


**Fig. 6.** Dependence of the key rate on the channel loss and excess noise. Lines indicate key rate levels of GG02, and points are for experimental results.

$R_{\text{finite}}(T^{\text{low}}, \epsilon^{\text{up}})$ (see Table 1) within the well-established confidence intervals of the Gaussian channel parameters, corresponding to a parameter estimation failure probability of $\varepsilon_{\text{fail}}^{\text{PE}} = 10^{-10}$ at 6.5 standard deviations [46]. Additionally, since error correction precedes the parameter estimation stage, the entire raw key sequence can concurrently be used for parameter estimation and key extraction [41]. This approach can substantially improve the actual key length and secret key rate in the finite regime.

## 6. DISCUSSION

DM CV-QKD is a technique that employs a discrete constellation of coherent states with finite cardinality. It is compatible with high-speed telecom components, making it a promising candidate for achieving ultra-high secret key rates. In this work, we have reported the fastest DM CV-QKD system to date, operating at a symbol rate of 10 GBaud.

Compared to recent progress in high-rate DM CV-QKD [17,19,20], which is limited to a symbol rate of 5 GBaud, our demonstration successfully doubles the symbol rate by enhancing the overall system bandwidth. In particular, we developed an integrated photonic-electronic phase-diverse receiver that maintains a wide shot-noise-limited bandwidth. Moreover, the transmitter bandwidth was improved through meticulously designed DSP, incorporating a pre-emphasis filter for quantum state preparation. These improvements have enabled our system to generate secret keys at rates exceeding 0.7 Gb/s both in the asymptotic regime and after accounting for the dominant effects of the finite-size regime. With the current system performance, based on the averaged measured values of modulation variance, electronic noise, and excess noise (assumed constant at the channel input) for a given constellation, the secure distance could be extended to ≈85 km for the smallest constellation and over ≈150 km for 64QAM.

Furthermore, our system operates at room temperature, unlike high-speed discrete-variable (DV) QKD systems that use superconducting nanowire single-photon detectors [47,48]. Nevertheless, there are several opportunities for further improvement. Foremost enhancement is an extension of composable security proofs against general attacks accommodating arbitrary modulation patterns. Application of currently available security proofs for four-state phase-shift keying protocol [49–51] to large modulation constellations remains computationally intensive. However, techniques such as entropy accumulation theorem [52] combined with parameter estimation data discretization [51], or generalized entropy accumulation theorem [53], are promising candidates for strengthening the security. Next, system stability can be improved through fiber attachment to the photonic chip in the next receiver version. Moreover, the symbol rate can be further increased by fully utilizing our receiver's bandwidth. To achieve this, the issue of interleaving spurs in the analog-to-digital converters (ADCs) has to be addressed, which can be accomplished in two ways: i) by employing an advanced ADC designed for more precise calibration among the sub-ADCs being interleaved, and ii) by implementing analog equalization, such as using a continuous time linear equalizer (CTLE). The CTLE method is effective in smoothing the spectral response prior to the digitization step, thereby boosting the high-frequency contents of the signal above the interference caused by interleaving spurs. Extending the distance of the current system is achievable by reducing the excess noise associated with laser phase noise. This can be done by optimizing the modulation variance and employing machine learning for precise carrier phase recovery [54].

Although this demonstration used bulk components on the transmitter's end, the integration level could also be improved here. Implementing a high-speed integrated transmitter would further improve the technology readiness level of CV-QKD, and opens up the possibility of creating a complete transceiver for bi-directional communication. Silicon photonics could once again be a possible candidate due to the availability of high bandwidth Mach-Zehnder modulators [55], wavelength filters [56], and variable optical attenuators. Furthermore, lasers can be co-integrated via flip-chipping, microtransfer printing, wafer-bonding or nanoridge engineering [57].

Another area for improvement is to make the system real-time by incorporating a real-time ultrafast quantum random number generator on the order of 100 Gb/s [58] and utilizing a high-speed real-time DSP module, along with multi-GPUs-based implementation for information reconciliation [59] and privacy amplification. To this end, our results pave the way for

real-time ultra-high-rate QKD systems, enabling secret-key-demanding applications such as real-time one-time-pad secured video encryption [60].

**Funding.** Innovation Fund Denmark (Innovationsfonden) (CryptQ, 017500018A); Danish National Research Foundation (Danmarks Grundforskningsfond) (bigQ, DNRF142); QuantERA (01017733); Czech Science Foundation (Grantová Agentura České Republiky) (22-28254O); Digital Europe Project BE-QCI (01091625); Research Foundation–Flanders (FWO) (SQOPE (G092922)); Quantum Secure Networks Partnership (QSNP) (10108011); CSA–Coordination and Support Action, H2020-WIDESPREAD-2020-5 (NONGAUSS, 951737) .

**Acknowledgment.** AAEH, NJ, ULA and TG acknowledge support from Innovation Fund Denmark and from the Danish National Research Foundation, Center for Macroscopic Quantum States. This project was funded within the QuantERA II Programme (project CVSTAR) that has received funding from the European Union's Horizon 2020 research and innovation programme. ID acknowledges support from the Czech Science Foundation. CB, AB, SB and XY acknowledge support from the Digital Europe project BE-QCI, Research Foundation Flanders through the Research Foundation–Flanders (FWO) Weave project Squeezed Quantum processing with Photonics and Electronics (SQOPE). We acknowledge support from the Horizon Europe framework programme Quantum Secure Networks Partnership and the CSA-Coordination and support action, H2020-WIDESPREAD-2020-5.

**Author contributions.** A.A.E.H. designed the experiment, implemented the DSP routine, and performed the overall data processing and analysis under supervision of T.G. C.B. designed the integrated Photonic-Electronic Chip under the supervision of X.Y. A.A.E.H., C.B. and N.J. implemented the experimental setup, and A.A.E.H. and C.B. performed the experimental measurements. I.D. performed the security analysis. A.B. and S.B. performed chip characterization. A.A.E.H. and T.G. wrote the manuscript with input from I.D. and C.B. A.A.E.H. and T.G. conceived the experiment. U.L.A., X.Y. and T.G. supervised the project. All authors were involved in discussions and interpretations of the results.

**Disclosures.** The authors declare no conflicts of interest.

**Data availability.** Data underlying the results presented in this paper are available from the authors upon reasonable request.

**Supplemental document.** See Supplement 1 for supporting content.

## REFERENCES

1. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (1984), pp. 175.
2. A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. **67**, 661 (1991).
3. C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J. **28**, 656–715 (1949).
4. E. Diamanti, H.-K. Lo, B. Qi, *et al.*, "Practical challenges in quantum key distribution," npj Quantum Inf. **2**, 16025 (2016).
5. M. Sasaki, "Quantum networks: where should we be heading?" Quantum Sci. Technol. **2**, 020501 (2017).
6. F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," Phys. Rev. Lett. **88**, 057902 (2002).
7. S. Pirandola, R. Laurenza, C. Ottaviani, *et al.*, "Fundamental limits of repeaterless quantum communications," Nat. Commun. **8**, 15043 (2017).
8. C. Weedbrook, S. Pirandola, R. García-Patrón, *et al.*, "Gaussian quantum information," Rev. Mod. Phys. **84**, 621 (2012).
9. K. Kikuchi, "Fundamentals of coherent optical fiber communications," J. Lightwave Technol. **34**, 157–179 (2015).
10. N. Jain, H.-M. Chin, H. Mani, *et al.*, "Practical continuous-variable quantum key distribution with composable security," Nat. Commun. **13**, 4740 (2022).
11. S. Sarmiento, S. Etcheverry, J. Aldama, *et al.*, "Continuous-variable quantum key distribution over a 15 km multi-core fiber," New J. Phys. **24**, 063011 (2022).
12. S. Ren, S. Yang, A. Wonfor, *et al.*, "Demonstration of high-speed and low-complexity continuous variable quantum key distribution system with local local oscillator," Sci. Rep. **11**, 9454 (2021).
13. T. Wang, P. Huang, Y. Zhou, *et al.*, "High key rate continuous-variable quantum key distribution with a real local oscillator," Opt. Express **26**, 2794–2806 (2018).
14. D. Huang, D. Lin, C. Wang, *et al.*, "Continuous-variable quantum key distribution with 1 mbps secure key rate," Opt. Express **23**, 17511–17519 (2015).
15. C. Wang, D. Huang, P. Huang, *et al.*, "25 MHz clock continuous-variable quantum key distribution system over 50 km fiber channel," Sci. Rep. **5**, 14607 (2015).
16. H. Wang, Y. Pi, W. Huang, *et al.*, "High-speed Gaussian-modulated continuous-variable quantum key distribution with a local local oscillator based on pilot-tone-assisted phase compensation," Opt. Express **28**, 32882–32893 (2020).
17. Y. Tian, Y. Zhang, S. Liu, *et al.*, "High-performance long-distance discrete-modulation continuous-variable quantum key distribution," Opt. Lett. **48**, 2953–2956 (2023).
18. F. Roumestan, A. Ghazisaeidi, J. Renaudier, *et al.*, "Experimental demonstration of discrete modulation formats for continuous variable quantum key distribution," arXiv (2022).
19. H. Wang, Y. Li, Y. Pi, *et al.*, "Sub-Gbps key rate four-state continuous-variable quantum key distribution within metropolitan area," Commun. Phys. **5**, 162 (2022).
20. Y. Pan, H. Wang, Y. Shao, *et al.*, "Experimental demonstration of high-rate discrete-modulated continuous-variable quantum key distribution system," Opt. Lett. **47**, 3307–3310 (2022).
21. D. Milovančev, N. Vokić, F. Laudenbach, *et al.*, "Spectrally-shaped continuous-variable QKD operating at 500 mhz over an optical pipe lit by 11 DWDM channels," in *Optical Fiber Communication Conference* (Optica Publishing Group, 2020), paper T3D–4.
22. T. A. Eriksson, R. S. Luís, B. J. Puttnam, *et al.*, "Wavelength division multiplexing of 194 continuous variable quantum key distribution channels," J. Lightwave Technol. **38**, 2214–2218 (2020).
23. B. Murmann, "ADC performance survey 1997-2022," https://github.com/bmurmann/ADC-survey.
24. J. Aldama, S. Sarmiento, I. H. López Grande, *et al.*, "Integrated QKD and QRNG photonic technologies," J. Lightwave Technol. **40**, 7498–7517 (2022).
25. X. Zheng, P. Zhang, R. Ge, *et al.*, "Heterogeneously integrated, superconducting silicon-photonic platform for measurement-device-independent quantum key distribution," Adv. Photon. **3**, 055002 (2021).
26. F. Beutel, H. Gehring, M. A. Wolff, *et al.*, "Detector-integrated on-chip QKD receiver for GHz clock rates," npj Quantum Inf. **7**, 40 (2021).
27. G. Zhang, J. Y. Haw, H. Cai, *et al.*, "An integrated silicon photonic chip platform for continuous-variable quantum key distribution," Nat. Photonics **13**, 839–842 (2019).
28. J. F. Tasker, J. Frazer, G. Ferranti, *et al.*, "A bi-CMOS electronic photonic integrated circuit quantum light detector," Sci. Adv. **10**, eadk6890 (2024).
29. C. Bruynsteen, M. Vanhoecke, J. Bauwelinck, *et al.*, "Integrated balanced homodyne photonic–electronic detector for beyond 20 GHz shot-noise-limited measurements," Optica **8**, 1146–1152 (2021).
30. D. Thomson, A. Zilkie, J. E. Bowers, *et al.*, "Roadmap on silicon photonics," J. Opt. **18**, 073003 (2016).
31. P. Absil, K. Croes, A. Lesniewska, *et al.*, "Reliable 50 gb/s silicon photonics platform for next-generation data center optical interconnects," in *IEEE International Electron Devices Meeting (IEDM)* (2017), pp. 34.2.1–34.2.4.
32. J. He, B. Snyder, G. Lepage, *et al.*, "V-Groove assisted passive assembly of single-mode fibers to ultra-broadband polarization-insensitive edge couplers for silicon photonics," in *45th European Conference on Optical Communication (ECOC)* (2019).
33. N. Jain, H.-M. Chin, H. Mani, *et al.*, "qTReX: a semi-autonomous continuous-variable quantum key distribution system," in *Optical Fiber Communications Conference and Exhibition (OFC)* (2022).
34. P. Jouguet, S. Kunz-Jacques, A. Leverrier, *et al.*, "Experimental demonstration of long-distance continuous-variable quantum key distribution," Nat. Photonics **7**, 378–381 (2013).
35. A. A. Hajomer, N. Jain, H. Mani, *et al.*, "Modulation leakage-free continuous-variable quantum key distribution," npj Quantum Inf. **8**, 136 (2022).

36. N. Jain, E. Anisimova, I. Khan, *et al.*, "Trojan-horse attacks threaten the security of practical quantum cryptography," New J. Phys. **16**, 123030 (2014).
37. F. Laudenbach, C. Pacher, C.-H. F. Fung, *et al.*, "Continuous-variable quantum key distribution with Gaussian modulation-the theory of practical implementations," Adv. Quantum Technol. **1**, 1800011 (2018).
38. D. Rafique, A. Napoli, S. Calabro, *et al.*, "Digital preemphasis in optical communication systems: on the DAC requirements for terabit transmission applications," J. Lightwave Technol. **32**, 3247–3256 (2014).
39. J. G. Proakis and M. Salehi, *Digital Communications*, 5th ed. (McGraw Hill, 2007).
40. Z. Chen, X. Wang, S. Yu, *et al.*, "Continuous-mode quantum key distribution with digital signal processing," npj Quantum Inf. **9**, 28 (2023).
41. A. Leverrier, "Composable security proof for continuous-variable quantum key distribution with coherent states," Phys. Rev. Lett. **114**, 070501 (2015).
42. A. Denys, P. Brown, and A. Leverrier, "Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation," Quantum **5**, 540 (2021).
43. I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," Proc. R. Soc. A **461**, 207–235 (2005).
44. Y. Wu and S. Verdú, "The impact of constellation cardinality on Gaussian channel capacity," in *48th Annual Allerton Conference on Communication, Control, and Computing (Allerton)* (IEEE, 2010), pp. 620–628.
45. V. C. Usenko and R. Filip, "Trusted noise in continuous-variable quantum key distribution: a threat and a defense," Entropy **18**, 20 (2016).
46. L. Ruppert, V. C. Usenko, and R. Filip, "Long-distance continuous-variable quantum key distribution with efficient channel estimation," Phys. Rev. A **90**, 062310 (2014).
47. W. Li, L. Zhang, H. Tan, *et al.*, "High-rate quantum key distribution exceeding 110 mb/s," Nat. Photonics **17**, 416–421 (2023).
48. F. Grünenfelder, A. Boaron, G. V. Resta, *et al.*, "Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems," Nat. Photonics **17**, 422–426 (2023).
49. C. Lupo and Y. Ouyang, "Quantum key distribution with nonideal heterodyne detection: composable security of discrete-modulation continuous-variable protocols," PRX Quantum **3**, 010341 (2022).
50. F. Kanitschar, I. George, J. Lin, *et al.*, "Finite-size security for discrete-modulated continuous-variable quantum key distribution protocols," arXiv (2023).
51. S. Bäuml, C. P. Garca, V. Wright, *et al.*, "Security of discrete-modulated continuous-variable quantum key distribution," arXiv (2023).
52. F. Dupuis, O. Fawzi, and R. Renner, "Entropy accumulation," Commun. Math. Phys. **379**, 867–913 (2020).
53. T. Metger and R. Renner, "Security of quantum key distribution from generalised entropy accumulation," Nat. Commun. **14**, 5272 (2023).
54. A. A. Hajomer, I. Derkach, N. Jain, *et al.*, "Long-distance continuous-variable quantum key distribution over 100-km fiber with local local oscillator," Sci. Adv. **10**, eadi9474 (2024).
55. E. Berikaa, M. S. Alam, A. Samani, *et al.*, "Silicon photonic single-segment IQ modulator for net 1tbps/$\lambda$ transmission using all-electronic equalization," J. Lightwave Technol. **41**, 1192–1199 (2023).
56. Q. Deng, A. H. El-Saeed, A. Elshazly, *et al.*, "32 $\times$ 00 GHzWDM filter based on ultra-compact silicon rings with a high thermal tuning efficiency of 5.85 mW/$\pi$," in *2024 Optical Fiber Communications Conference and Exhibition (OFC)* (2024), paper W1A.3.
57. R. Baets, J. Van Campenhout, B. Kunert, *et al.*, "4 Ways to Put Lasers on Silicon," in *IEEE Spectrum* (IEEE, 2023), https://spectrum.ieee.org/lasers-on-silicon.
58. C. Bruynsteen, T. Gehring, C. Lupo, *et al.*, "100-gbit/s integrated quantum random number generator based on vacuum fluctuations," PRX Quantum **4**, 010330 (2023).
59. Y. Li, X. Zhang, Y. Li, *et al.*, "High-throughput GPU layered decoder of quasi-cyclic multi-edge type low density parity check codes in continuous-variable quantum key distribution systems," Sci. Rep. **10**, 14561 (2020).
60. S.-K. Liao, W.-Q. Cai, J. Handsteiner, *et al.*, "Satellite-relayed intercontinental quantum network," Phys. Rev. Lett. **120**, 030501 (2018).