ARTICLE OPEN

Modulation leakage-free continuous-variable quantum key distribution

Adnan A. E. Hajomer [1 ✉], Nitin Jain[1], Hossein Mani [1], Hou-Man Chin [1,2], Ulrik L. Andersen [1] and Tobias Gehring [1 ✉]

Distributing cryptographic keys over public channels in a way that can provide information-theoretic security is the holy grail for secure communication. This can be achieved by exploiting quantum mechanical principles in so-called quantum key distribution (QKD). Continuous-variable (CV) QKD based on coherent states, in particular, is an attractive scheme for secure communication since it requires only standard telecommunication technology that can operate at room temperature. However, a recently discovered side-channel created in the process of state preparation leads to a leakage of information about the transmitted quantum state, opening a security loophole for eavesdroppers to compromise the security of the CVQKD system. Here, we present a CVQKD system without this modulation leakage vulnerability. Our implementation is based on a baseband modulation approach and uses an in-phase and quadrature (IQ) modulator for state preparation and radio frequency heterodyne detection together with carefully designed digital signal processing for state measurement. We consider practical aspects in the implementation and demonstrate the generation of a composable secret key secure against collective attacks. This work is a step towards protecting CVQKD systems against practical imperfections of physical devices and operational limitations without performance degradation.

INTRODUCTION

Quantum key distribution (QKD) allows communicating parties to securely distribute cryptographic keys by harnessing the fundamental properties of quantum mechanics. Theoretically, using QKD together with one-time pad encryption provides information-theoretic secure data transmission that cannot be broken either by current or by future technology[1,2]. However, any practical realization of QKD is vulnerable to side-channels, resulting mainly from imperfections of physical devices and operational limitations, which may not be taken into account in an idealized security proof. For instance, in discrete variable QKD, typical attacks exploiting side-channels are Trojan horse attacks[3,4] and detector control attacks[5–7].

In continuous variable (CV) QKD, quantum states are encoded into the two orthogonal—phase and amplitude—quadratures of the electromagnetic light field. Prepare-and-measure protocols, where the sender (Alice) prepares coherent quantum states using quadrature modulation, are particularly common as the CVQKD system can be built from telecommunication components[2,8–14]. The prepared quantum states are transmitted through an insecure quantum channel, assumed to be fully controlled by an eavesdropper (Eve). At the receiver (Bob), the quantum states are measured in a coherent manner, e.g., using homodyne or heterodyne detection[15,16]. Finally, the QKD protocol ends with classical data processing and security analysis, characterizing the information advantage of Alice and Bob over Eve. Similar to its discrete variable counterpart, CVQKD is prone to implementational loopholes. For example, attacks on the local oscillator's intensity and the shot noise calibration have been demonstrated[17–20].

Recently, the impact of side-channel leakage during coherent state preparation in a CVQKD protocol has been theoretically analyzed and experimentally demonstrated in a setup that established the coherent state's mode in an optical single sideband (OSSB) using in-phase and quadrature (IQ) modulation[21,22]. In the proof-of-concept experiment, the authors showed that a side-channel is created due to the finite suppression of the quantum-information-carrying image sideband during OSSB modulation. This side-channel can significantly reduce the secret key rate and can even break the security of the system if neglected in the security proof. Therefore, exploring a modulation scheme for quantum state preparation that is information-leakage-free, is of great importance to CVQKD implementations.

Here we report a CVQKD implementation that is capable of removing the modulation leakage vulnerability without considering the practical imperfections of the modulation process in the security proof. We achieve this by implementing an optical baseband modulation scheme using an IQ modulator for quantum state preparation, and radio frequency (RF) heterodyne detection. In contrast to previous implementations[22–26], the proposed modulation scheme does not frequency shift the coherent states at a radio frequency but keeps the quantum signal band centered at the optical carrier frequency. Thereby, it removes the side-channel leakage from the suppressed (image) sideband of quantum signals. Simultaneously, our scheme still employs a continuous-wave laser and digital mode shaping and does not require an additional amplitude modulator for pulse carving. We experimentally evaluate the performance of our implementation in terms of the so-called excess noise[2,11,27]: with the help of digital signal processing (DSP) that includes an optimized high pass filter (HPF) and a machine learning framework for phase carrier recovery[25], our implementation achieved one of the lowest-ever reported excess noise of 0.72×10^{-3} photon number units (PNU). In addition, we also achieved a composable secure key

[1]Center for Macroscopic Quantum States (bigQ), Department of Physics, Technical University of Denmark, 2800 Kongens Lyngby, Denmark. [2]Department of Electrical and Photonics Engineering, Technical University of Denmark, 2800 Kongens Lyngby, Denmark. ✉email: aaeha@dtu.dk; tobias.gehring@fysik.dtu.dk

fraction[28,29] of 0.007 bits/symbol, calculated under the assumption of collective attacks.
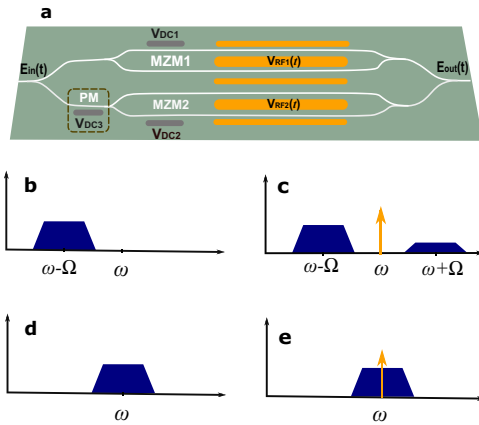
RESULTS

Coherent state preparation

To prepare coherent states, quadrature modulation is used in CVQKD systems[9]. In practice, quadrature modulation can be implemented either by using discrete amplitude and phase modulators or an IQ modulator[8,23,24,30]. The latter option offers more compact design, cost-effectiveness and potential robustness against Trojan-horse attacks[4,22]. Since in the IQ modulator the electro-optical modulators are fabricated on a single substrate, they have similar electrical-to-optical transfer functions which is an important property for generating coherent states in OSSBs.

The IQ modulator is, in principle, a Mach-Zehnder interferometer with dual nested Mach-Zehnder modulators (MZMs) and a phase modulator (PM), as shown in Fig. 1(a). Given an electric field $E_{in}(t)$ at the input of an ideal IQ modulator, the electric field at the output can be expressed as[31,32],

$$E_{out}(t) = \frac{E_{in}(t)}{2}\left[\cos\left(\pi\frac{V_{RF1}(t)+V_{DC1}}{2V_\pi}\right)+\cos\left(\pi\frac{V_{RF2}(t)+V_{DC2}}{2V_\pi}\right)e^{-j\pi\left(\frac{V_{DC3}}{2V_{\pi/2}}\right)}\right],$$

(1)

where $V_{RF1}(t)$ and $V_{RF2}(t)$ are RF waveforms and $V_{DC1,2,3}$ are direct current (DC) bias voltages applied on the modulators. The latter are usually controlled by an automatic bias controller (ABC). Here, V_π is the half-wave voltage, i.e., the voltage at which the optical phase changes by π. In CVQKD, the modulator is usually operated in the linear regime. Hence, $V_{RF1}(t)$ and $V_{RF2}(t)$ are typically (at least) an order of magnitude smaller than V_π and only the first order sidebands of the electric field get significantly excited.

For CVQKD purposes, OSSB modulation for the generation of coherent states provides practical advantages as it avoids low-frequency noise by shifting the quantum states with coherent excitation $a(t) = I(t) + jQ(t)$ away from the optical carrier[23,25]. As illustrated in Fig. 1(b), in an ideal scenario, the optical carrier at ω as well as the (upper) sidebands around $\omega + \Omega$ are completely

suppressed, leading to true OSSB modulation with carrier suppression (OSSB-CS). However, in practice, the IQ modulator is capable of providing only a finite level of OSSB-CS as depicted in Fig. 1(c). In this practical scenario, the output electric field of equation (1) can be expressed as,

$$E_{out}(t) \approx \frac{\mu}{2}a(t)e^{j(\omega-\Omega)t} + \frac{\delta}{2}a^*(t)e^{j(\omega+\Omega)t} + \Delta e^{j\omega t},$$

(2)

Here, μ is the modulation index, $\delta < \mu$ is an effective modulation index including the sideband suppression ratio, and Δ describes the residual electric-field amplitude of the carrier after suppression. A detailed derivation can be found in the Methods section.

The modulation leakage vulnerability gets manifested when Alice and Bob do not account for the finite suppression, i.e., $\delta > 0$, while Eve extracts the not-completely-suppressed sideband (centered at $\omega + \Omega$ in Fig. 1(d)), using, for instance, an optical filter[22]. Basically, this allows Eve to gain more information about the secret key without alerting Alice and Bob.
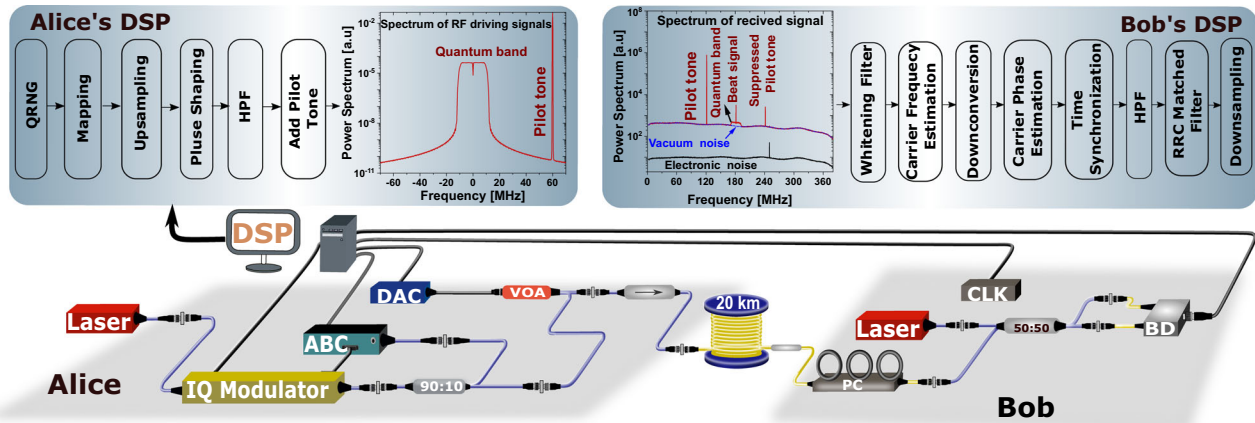
One way to deal with this side-channel while keeping the advantages of OSSB modulation is to consider the information leakage from the suppressed sideband in the security proof. Nevertheless, this approach reduces the range over which a secret key can be obtained, requires additional measurements when characterizing the system and guarantees on the long-term stability of the achieved suppression[22]. Alternatively, one can completely remove the issue of finite sideband suppression and therefore the modulation leakage vulnerability by considering a modulation scheme in which no suppressed image sideband is generated.

One possible candidate for such a modulation scheme is optical baseband modulation[33], a technique in which the driving RF waveforms of the IQ modulator are baseband signals, i.e., the signals have not been up-converted to a higher radio frequency. This results in the quantum signal band centered at the optical carrier frequency as shown in Fig. 1(d). In fact, by driving the IQ modulator such that $V_{RF1}(t) \propto \text{Real}(a(t)) = I(t)$ and $V_{RF2}(t) \propto \text{Imag}(a(t)) = Q(t)$ and considering the imperfect bias settings of the MZMs, the electric field at the output of the IQ modulator can be expressed as,

$$E_{out}(t) = [\sin(\mu_1 I(t)+\phi_1) + j\sin(\mu_2 Q(t)+\phi_2)]\frac{e^{j\omega t}}{2} \approx [\mu_1 I(t)$$

$$+j\mu_2 Q(t)+\phi_1+j\phi_2]\frac{e^{j\omega t}}{2} \approx \left(\frac{\mu}{2}a(t)+\Delta\right)e^{j\omega t},$$

(3)

assuming $\mu_1 \approx \mu_2 = \mu$ and $\phi_1 + j\phi_2 = 2\Delta$. Here, ϕ_1 and ϕ_2 are phase errors due to bias deviation from V_π of the MZMs. Note that to simplify, we have neglected the deviation of phase modulation bias in the above. From equation (3), where the approximation $\sin(\theta) \approx \theta$ is justified due to the low RF modulation depth and minor deviations from the expected DC bias values, it is clear that the output of the IQ modulator is side-channel free and the modulated signal is mixed with the optical carrier component $\Delta \exp(j\omega t)$ due to the finite carrier suppression, as presented in Fig. 1(e). This carrier component can be easily removed using a digital filter, as we will explain later. Therefore, the use of baseband modulation for quantum state preparation can remove the sideband leakage vulnerability while keeping the advantages of OSSB in high spectral efficiency and better noise performance by avoiding the low-frequency noise using RF heterodyne detection.

The schematic of our CVQKD system is shown in Fig. 2. It consists of an optical module and a DSP module. The sender (Alice) prepared a 20 MBaud baseband quantum signal and frequency multiplexed pilot tone, both encoded into the phase and amplitude quadratures of the electromagnetic light field by an IQ modulator. After suitable attenuation, the optical signal was then sent over a 20 km fiber channel to the receiver (Bob), where RF heterodyne detection was performed. Finally, after data

Fig. 1 IQ modulator internal structure and its operation modes. **a** An IQ modulator consists of two MZMs driven by RF signals $V_{RF1}(t)$ and $V_{RF2}(t)$ with 90° phase difference. For OSSB-CS, the two MZMs operate at a dark fringe, e.g., through $V_{DC1} = V_{DC2} = V_\pi$, while the PM maintains the relative phase of 90° using V_{DC3}. **b-e** Output spectra of OSSB and baseband operation modes. **b** Infinite carrier and sideband suppression, and therefore ideal OSSB-CS. **c** OSSB-CS with finite carrier and sideband suppression due to sub-optimal settings of the DC bias and manufacturing imperfections. **d** Ideal baseband modulation with carrier suppression. **e** Practical baseband modulation with finite carrier suppression.

Fig. 2 Optical layout and DSP routine of our modulation-leakage-free CVQKD system. Alice digitally prepared an ensemble of Gaussian-modulated coherent states with a frequency multiplexed pilot tone using her DSP module. The spectrum of the complex digital signal is shown in the inset. The corresponding RF signals were generated using an arbitrary waveform generator (AWG; not shown in the figure) with a 1 GSample/s sampling rate. These signals were then used to drive an IQ modulator modulating light from a 1550 nm continuous-wave laser. For optical carrier suppression, an automatic bias controller (ABC) was used with the IQ modulator. The quantum signal was obtained after the output of the IQ modulator was suitably attenuated using a variable optical attenuator (VOA; input and output pigtails on the same side) driven by a digital-to-analog converter (DAC). At Bob's station, the polarization of the signal transmitted through a 20 km SMF-28 fiber was corrected with a manual polarization controller (PC) to match the polarization of an independent local oscillator for RF heterodyne detection. The digitized output of the balanced detector (BD) was fed through Bob's DSP module. The ADC output spectra from 3 different measurements are shown as the input to Bob's DSP routine. An external 10 MHz clock reference (CLK) was used to synchronize the AWG and ADC.

Table 1. Parameters of the designed MET-LDPC code.

R	Degree distribution	σ^*_{DE}	SNR [dB]	σ^*_{Sh}	β^*_{Code}
0.02	$v(r,x) = 0.0225\,r_1 x_1^2 x_2^{52} + 0.0175\,r_1 x_1^3 x_2^{57} + 0.96\,r_1 x_3^1$, $\varrho(x) = 0.0165\,x_1^4 + 0.0035\,x_1^9 + 0.2475\,x_2^3 x_3^1 + 0.7125\,x_2^2 x_3^1$	5.93	-15.46	5.96	98.8%

σ^*_{Sh} denotes the threshold at Shannon capacity at which the SNR is specified. β^*_{Code} is the asymptotic code efficiency.

acquisition and by performing several DSP steps, one of which is the proposed digital filtering applied at Alice's and Bob's sides to remove low-frequency noise and carrier components, Bob recovered a noisy version of Alice's quantum symbols. These quantum data symbols were stored as frames by both parties. Further details of the system implementation can be found in the Methods section.

Classical data processing

After the quantum stage of the protocol, Alice and Bob performed information reconciliation (IR) based on a multi-dimensional (MD) scheme using a multi-edge-type low-density-parity-check (MET-LDPC) error correcting code[34], assuming they were connected through an authenticated classical channel. Table 1 summarizes the related parameters of the constructed MET-LDPC code, optimized for a binary input additive white Gaussian noise (BI-AWGN) channel. The convergence threshold of the degree distribution of the designed MET-LDPC code (asymptotic threshold σ^*_{DE}) of 5.93 was estimated by running the density evolution until the error probability was $< 10^{-10}$. This threshold indicates how close to the Shannon limit the code can operate: the larger the threshold, the closer to the theoretical limit the MET-LDPC code can operate. The code rate R of the designed MET-LDPC code was 0.02. As the convergence threshold was specified at signal-to-noise ratio (SNR) of -15.46 dB, the asymptotic code efficiency, $\beta^*_{Code} = R/C(\sigma^*_{DE})$, where $C(\sigma^*_{DE})$, denotes the Shannon capacity at σ^*_{DE}, was 98.8%.

To achieve a high IR efficiency with this code rate at a non-optimal SNR of 0.0443, we adopted the rate-adaptive

Table 2. The reconciliation efficiency and FER for different puncturing lengths.

β(%)	FER	p	R_{punc}
92.77	0.075	318000	0.0290
93.04	0.215	320000	0.0291
93.70	0.378	325000	0.0293
94.37	0.480	330000	0.0295
95.06	0.716	335000	0.0297
95.75	0.850	340000	0.0299
96.46	0.962	345000	0.0302

The original code has a rate $R = 0.02$, with codeword length $n = 1.024 \times 10^6$ and information length $k = 20480$.

reconciliation protocol, using the so-called puncturing technique to change the code rate of the designed MET-LDPC code[34]. We should mention that the optimal SNR for MET-LDPC code with a rate of 0.02 is 0.0281. By adding punctured symbols whose values between Alice and Bob are uncorrelated, the mutual information between Alice and Bob data decreases, allowing us to use an error correction code of rate 0.02. The overall MD reconciliation efficiency with puncturing for a dimension dim = 8 was computed as $\beta = R_{punc}/C_{AWGN}(s)$, where R_{punc} is the code rate after puncturing. For a codeword of length n and k information bits the original code rate is $R = k/n$, while after puncturing the
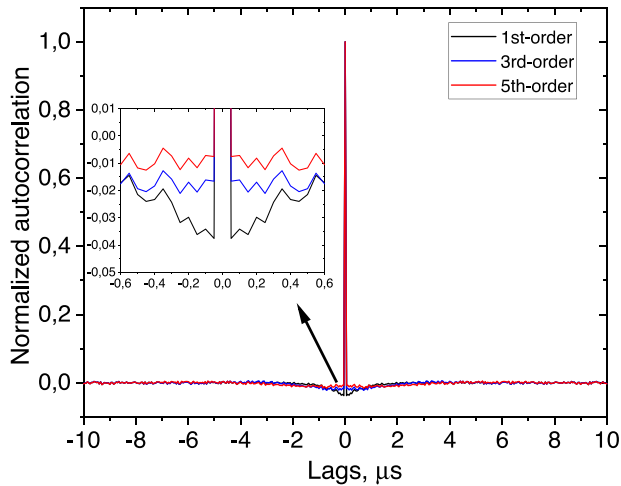
Fig. 3 The effect of HPFs. Plot of normalized autocorrelation functions of demodulated quantum symbols using HPFs of the same bandwidth and different orders.
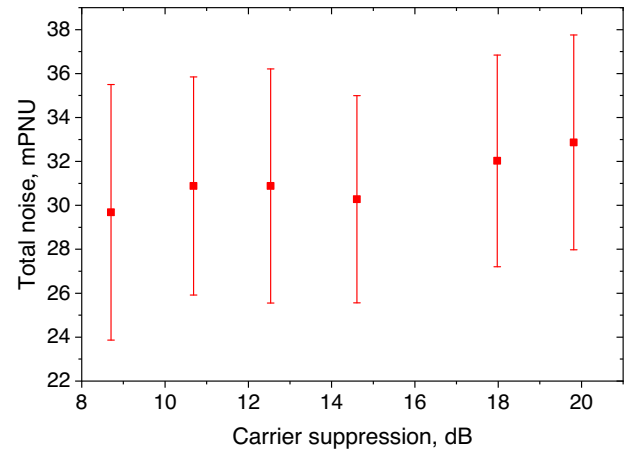

Fig. 4 Total noise versus carrier suppression. Error bars represent one standard deviation, while squares depict the average value.

final code rate becomes $R_{\text{punc}} = k/(n - p)$, where p denotes the puncturing length. Table 2 shows simulated IR efficiencies and frame error rates (FERs) for different puncturing lengths. High IR efficiencies up to 96.46 % can be achieved at the cost of high FER, which will significantly reduce the final secret key length. Therefore, as a trade-off between the FER and efficiency, we set the puncturing length to 320,000, which corresponds to an efficiency of 93.04% and FER = 0.215.

Next, Alice performed parameter estimation to obtain a bound on Eve's Holevo information, calculating the number of bits expected in the output secret key in the worst-case scenario. This length was communicated together with a seed to Bob. For privacy amplification (PA), the shared seed from the previous step was used to select a random Toeplitz hash function by Alice and Bob, who then employed the high-speed and large-scale PA scheme[35] to generate the final secret key.

Experimental investigation

The use of HPFs in Alice's and Bob's DSP modules is the key ingredient of our CVQKD implementation. To understand the effect of these HPFs on the security and system performance, we first investigated the normalized auto-correlation functions of received quantum symbols from one frame, demodulated using three different HPFs with the same bandwidth of 190 kHz but different orders, as depicted in Fig. 3. In general, applying these HPFs can introduce correlations between consecutive symbols as indicated by the dip around the correlation peak, clearly seen in the figure in the case of the 1st-order filter. With reference to the spectrum of the RF driving signal in Fig. 2, this correlation could be attributed to the fact that the HPF gives rise to frequency-selective fading, indicated by the notch in the spectrum, and causes inter-symbol interference in the time domain[36]. Moreover, the inset in Fig. 3 shows that the strength of correlation depends on the filter order: as the order reduces the dip in correlation increases. Therefore, one could also anticipate the same dependence for the filter bandwidth since the delay spread is proportional to the notch bandwidth in the spectrum introduced by the HPF[36].

From a security point of view, such correlations can destroy the independent and identically distributed property of the quantum symbols, which would violate an assumption commonly made in the security proofs. Therefore, optimizing filter parameters is extremely important to keep the effect on the

Table 3. Overview of experimental parameters for composable security.

Alice	Bob	channel	IR
$B = 20$ MBaud	$\tau = 0.68$	$\eta = 0.24$	FER $= 0.215$
$V_a = 0.27$ PNU	$t = 31.40$ mPNU	$u = 0.73$ mPNU	$\beta = 93.04\%$

τ Trusted efficiency, η Untrusted efficiency, t trusted detection noise, u untrusted channel noise, FER frame error rate, β IR efficiency.

independence as small as possible. However, we note, that even without HPF perfect independence cannot be achieved in practice due to the physical properties of the modulator. One way the results suggest for filter optimization is to minimize the correlation coefficient in the vicinity of the correlation peak, as in the case of the 5th-order filter.

As a next step, we explored the tolerance of the optimized HPFs to finite carrier suppression provided by the ABC. To do this, we performed regular heterodyne measurements while varying the amount of carrier suppression by tuning the dither amplitude applied by the ABC on MZM1 and MZM2. As a figure of merit for the HPF's performance, Fig. 4 shows the total noise, i.e., the sum of the trusted electronic noise (t) and the untrusted noise (u) contributed by Eve, as a function of the carrier suppression. Each data point in the plot is represented by the mean and standard deviation over 200 frames. It is clear that the HPF has no significant performance degradation over 10 dB carrier suppression, implied by the highly overlapping error bars. This result confirms the effectiveness of the optimized HPF over a relatively wide range of carrier suppression. We note that as the ABC cannot provide lower than 9 dB carrier suppression, we were not able to reach the performance breaking point.

Finally, to demonstrate the practical feasibility of modulation-leakage-free CVQKD, we generated a secret key over the 20 km fiber considering composable security and collective attacks[29]. Table 3 summarizes the main experimental parameters used for secret key generation. Alice sent 10^9 coherent states with a modulation strength of 0.27 mPNU to Bob. After channel parameter estimation, a total noise $u + t = 0.73 + 31.40 = 32.13$ mPNU and a total average transmittance $\eta \cdot \tau = 0.24 \cdot 0.68 = 0.16$ were measured. Here, η is the untrusted channel transmission and τ is the trusted detection efficiency. As our CVQKD system uses a local local oscillator[37], the main contributor to untrusted channel noise u is the excess noise due to the residual phase noise,
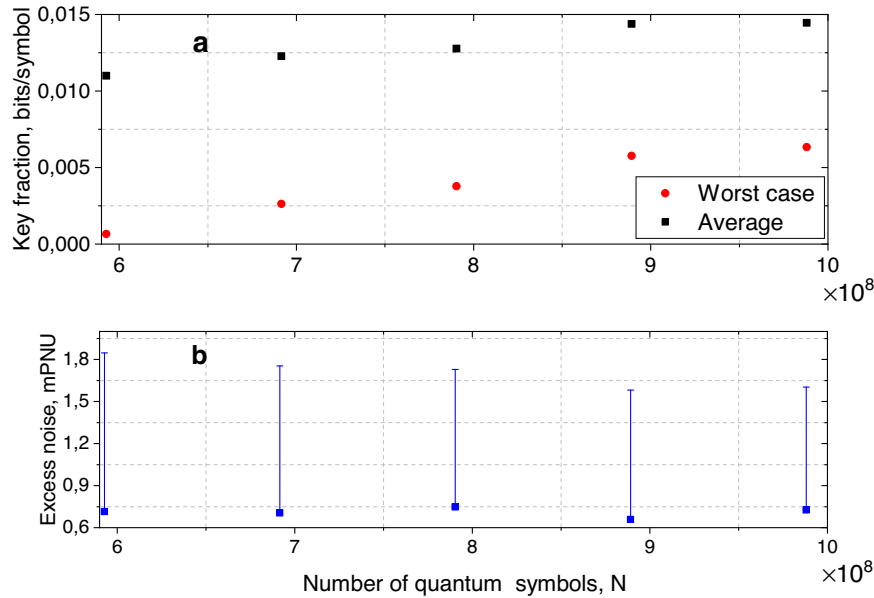
Fig. 5 **Experimental results demonstrating the CVQKD system performance. a** Composable secret key fraction versus number of quantum symbols. **b** Measured excess noise and its worst-case estimator.

$\xi_{\text{phase}} = 2V_a\left(1 - e^{-\frac{V_{\text{est}}}{2}}\right)$, where V_{est} is the variance of the residual phase after phase noise compensation[38,39]. In comparison to[29], the untrusted noise u achieved here is lower because our system operated at a lower modulation strength, resulting in a lower ξ_{phase}. Also, careful optimization of our DSP chain played a significant role to obtain such noise performance. We note that η is relatively small for a 20 km fiber channel with a physical transmission of ≈ 0.38, which could be attributed to the polarization optimization after the fiber channel.

As for IR, Alice and Bob used 9.8×10^8 complex symbols to perform reverse reconciliation with an efficiency $\beta = 93.04\%$ with the IR code described above in frames of 1024×10^3 bits. The total number of corrected symbols after IR was reduced to 7.7×10^8 due to FER $= 0.215$. The maximum iteration number of the MET-LDPC decoder was set to 500. Joining data from both I and Q quadratures, we obtained a total of $2 \times 7.7 \times 10^8$ symbols. Finally, we calculated the composable secret key length $l = 1 \times 10^8$ bits, which translates into a secret key fraction of 0.007 bits/symbol. The security parameters of calibration (ϵ_{cal}) and parameter estimation (ϵ_{PE}) were both set to 10^{-10} while ϵ_{IR} was set to 10^{-12}.

Figure 5 (a) shows the composable secret key fraction as a function of the number N of available quantum symbols (before IR) both for the average (black squares) and worst-case (red dots) scenarios – the latter given by the considered confidence intervals[29]. Likewise, the measured untrusted noise with a worst-case estimator is shown in Fig. 5 (b). A positive key fraction was obtained for $N \gtrsim 6 \times 10^8$, corresponding to a null key fraction threshold of ≈ 1.8 mPNU. From an experimental point of view, the reason for being able to achieve a positive key fraction with a relatively small number of symbols could be attributed to our system noise performance, implying the practical feasibility of our implementation. Also considering an estimated η of 0.24, a composable secret key for a long distance can be achieved by optimizing the polarization control circuit.

DISCUSSION

In this work, we demonstrated a practical CVQKD system that is free of the modulation leakage vulnerability. This was enabled by means of optical baseband modulation for coherent states preparation and

RF heterodyne reception together with carefully designed DSP. Our system showed low noise performance with high tolerance to finite carrier suppression of the IQ modulator due to the use of digital HPFs. This allowed us to generate a composable secret key secure against collective attacks over 20 km fiber channel. However, careful optimization of the HPFs is necessary to avoid intersymbol interference, which may leak more information to Eve.

Compared with phase-diverse intradyne or homodyne CVQKD systems, where the security is not affected by the sideband modulation leakage as Bob measures both sidebands, our system provides a cost-effective solution since it does not require a 90-degree optical hybrid nor an amplitude modulator in the transmitter to generate pulses. Besides, like OSSB CVQKD systems, our implementation facilitates spectral efficiency and better noise performance by avoiding the low-frequency noise at the detection side. The proposed baseband modulation together with the DSP chain is also suitable for other CVQKD systems based on modulated coherent states, including measurement-device-independent CVQKD[40]. We anticipate that our implementation can be a potential solution to protect future CVQKD systems against side-channels from modulation leakage with better system performance, and remove the need for a complex characterization of the leakage and the risk of a failure in system security due to long-term stability issues which may increase the leakage over time.

METHODS

Derivation of Eq. (2). In the practical OSSB modulation, where the bias voltages of IQ modulator deviate from the optimal condition, e.g., $V_{DC_1} = V_{DC_2} = -V_\pi + dV_{\text{MZM}}$, and $V_{DC_3} = -V_{\frac{\pi}{2}} + dV_{\text{PM}}$, the output electric field of equation (1) can be expressed as,

$$
\begin{aligned}
E_{\text{out}}(t) &= \frac{E_{\text{in}}(t)}{2}\left[\sin(\theta_1(t) + \phi) + j\sin(\theta_2(t) + \phi)e^{j\Phi}\right] \\
&= \frac{E_{\text{in}}(t)}{2}\left[\sin(\theta_1(t))\cos(\phi) + \cos(\theta_1(t))\sin(\phi)\right. \\
&\quad \left. + je^{j\Phi}(\sin(\theta_2(t))\cos(\phi) + \cos(\theta_2(t))\sin(\phi))\right].
\end{aligned}
\tag{4}
$$

Here, $\phi = \frac{\pi}{2V_\pi}dV_{\text{MZM}}$ and $\Phi = \frac{\pi}{2V_{\frac{\pi}{2}}}dV_{\text{PM}}$ captures the phase error due to non-optimal bias voltages setting and $\theta_i(t) = \frac{\pi}{2V_\pi}V_{\text{RF}i}(t)$ for $i = 1$ or 2. For very small $\theta_i(t)$, we can take the second-order Taylor series expansion of (4) as,

$$E_{\text{out}}(t) \approx \frac{E_{\text{in}}(t)}{2}\left[\theta_1(t)\cos(\phi) + \left(1 - \frac{1}{2}\theta_1^2(t)\right)\sin(\phi) + je^{j\Phi}\left(\theta_2(t)\cos(\phi) + \left(1 - \frac{1}{2}\theta_2^2(t)\right)\sin(\phi)\right)\right]$$

$$\approx \frac{E_{\text{in}}(t)}{2}\left[(\theta_1(t) + je^{j\Phi}\theta_2(t))\cos(\phi) + (1 + je^{j\Phi})\sin(\phi) - \frac{1}{2}(\theta_1^2(t) + je^{j\Phi}\theta_2^2(t))\sin(\phi)\right]$$

$$\approx \frac{E_{\text{in}}(t)}{2}\left[(\theta_1(t) + je^{j\Phi}\theta_2(t))\cos(\phi) + (1 + je^{j\Phi})\sin(\phi)\right]$$

$$\approx \frac{E_{\text{in}}(t)}{2}\left[e^{j\frac{\Phi}{2}}\cos(\phi)\left(\theta_1(t)e^{-j\frac{\Phi}{2}} + je^{j\frac{\Phi}{2}}\theta_2(t)\right) + (1 + je^{j\Phi})\sin(\phi(t))\right]$$

$$\approx \frac{E_{\text{in}}(t)}{2}\left[e^{j\frac{\Phi(t)}{2}}\cos(\phi)\left(\theta_1(t)(\cos\left(\frac{\Phi}{2}\right) - j\sin\left(\frac{\Phi}{2}\right)) + j(\cos\left(\frac{\Phi}{2}\right) + j\sin\left(\frac{\Phi}{2}\right))\theta_2(t)\right) + (1 + je^{j\Phi})\sin(\phi)\right]$$

$$\approx \frac{E_{\text{in}}(t)}{2}\left[e^{j\frac{\Phi}{2}}\cos(\phi)\left((\theta_1(t) + j\theta_2(t))\cos\left(\frac{\Phi}{2}\right) - j(\theta_1(t) - j\theta_2(t))\sin\left(\frac{\Phi}{2}\right)\right) + (1 + je^{j\Phi})\sin(\phi)\right]$$

$$\approx \frac{E_{\text{in}}(t)}{2}\left[\frac{\pi e^{j\frac{\Phi}{2}}\cos(\phi)}{2V_\pi}\left((V_{\text{RF1}}(t) + jV_{\text{RF2}}(t))\cos\left(\frac{\Phi}{2}\right) - j(V_{\text{RF1}}(t) - jV_{\text{RF2}}(t))\sin\left(\frac{\Phi}{2}\right)\right) + (1 + je^{j\Phi})\sin(\phi)\right], \tag{5}$$

therefore, for OSSB, where the driving signal of IQ modulator can be expressed as $V_{\text{RF1}}(t) + jV_{\text{RF2}}(t) = a(t)e^{-j\Omega t}$, the output of the IQ modulator can be written as,

$$E_{\text{out}}(t) \approx \frac{\mu}{2}a(t)e^{j(\omega-\Omega)t} + \frac{\delta}{2}a^*(t)e^{j(\omega+\Omega)t} + \Delta e^{j\omega t}. \tag{6}$$

Details of the experimental setup

Sender (Alice). We digitally generated baseband RF driving signals using Alice's DSP module as shown in Fig. 2. As a first step, a quantum random number generator (QRNG) with a security parameter $\epsilon_{\text{qrng}} = 2 \times 10^{-6}$ was employed to generate uniformly distributed random bit sequences[41]. Then, the inversion sampling method based on the cumulative distribution function was used to map the uniformly distributed sequences to Gaussian distributed integers with 6 bits resolution covering 7 standard deviations[29]. Afterwards, the quantum symbols $A_i = I_i + jQ_i$ were drawn from these Gaussian distributed integers at rate B = 20 MBaud. These symbols were upsampled to 1 GSample/s and pulse-shaped by a root raised cosine (RRC) filter with a roll-off factor of 0.2 to obtain the baseband quantum signal $q(t) = h(t) * \Sigma_i A_i \delta(t - iT)$. Here, $h(t)$ is the impulse response of the RRC filter. A 5th-order Butterworth high pass filter (HPF) with a cut-off frequency of 190 kHz was applied to the quantum signal for the purpose of temporal mode shaping. A reference pilot tone at a frequency of 60 MHz was multiplexed with the quantum signal for frequency offset estimation and phase noise compensation. Figure 2 (left inset) shows the complex spectrum of $V(t)$, the output of Alice's DSP module. Finally, the RF driving waveforms, $V_{\text{RF1}}(t) = \text{Real}(V(t))$ and $V_{\text{RF2}}(t) = \text{Imag}(V(t))$ were uploaded to a dual-channel arbitrary waveform generator (AWG) with 16 bit resolution and sampling frequency of 1 GSample/s.

In the optical module, a continuous wave (CW) laser at 1550 nm with a line-width of $\approx$100 Hz was used as the optical carrier. Random coherent states were prepared using a commercial off-the-shelf IQ modulator driven by the AWG. The DC bias voltages of the IQ modulator were controlled using a commercial ABC to achieve optical baseband modulation with finite carrier suppression. For such an ABC the amount of carrier suppression can be controlled by tuning parameters such as the dither signal amplitude and the feedback photodiode gain of the bias circuit. To reduce the effect of the laser intensity noise, after the IQ modulator the optical signal was suitably attenuated using an electro-optic variable optical attenuator (VOA) driven by a digital-to-analog converter so that the modulated laser beam was shot-noise limited. To avoid back reflections and thus Trojan-horse attacks[4], a Faraday isolator was added before the input of the quantum channel, which was a 20 km standard single mode fiber.

Receiver (Bob). After the quantum channel, a manual polarization controller was used to optimize the polarization of the optical signal for RF heterodyne detection with a free-running local oscillator (LO), generated by a CW laser with a frequency offset of $\approx$ 200 MHz with respect to Alice's laser. A home-made broadband balanced detector with a bandwidth of $\approx$ 365 MHz detected the interference between the LO and the transmitted optical signal. The output of the balanced detector was then digitized at a sampling rate of 1 GSample/s using an analog-to-digital converter (ADC), which was clock synchronized to Alice's AWG using a 10 MHz external reference.

The measurement time was divided into frames, each containing 10^7 samples. Three individual measurements were performed. In order, these were: modulated signal measurement, vacuum noise measurement where Alice's laser was switched off while Bob's laser was on, and finally an electronic noise measurement in which both Alice's and Bob's lasers were switched off. To avoid the effect of the LO power fluctuation on the measurement, particularly on vacuum measurement, an autonomous system based on python code has been developed to perform the modulation process and data acquisition. Figure 2 (right inset) shows the labeled spectral traces from these measurements, evaluated for one frame each, as input to Bob's DSP module. The clearance of the vacuum noise with respect to the electronic noise was $\approx$ 15 dB. It should also be mentioned that for the modulation strength (V_a) calibration, we performed a back-to-back measurement, i.e., the transmitter and the receiver were directly connected without the quantum channel. The modulation strength, described as the mean photon number of a thermal state, was $\approx$ 0.27 PNU, where PNU stands for photon number units[15,29].

To recover Alice's modulated quantum symbols, Bob's DSP module, shown in Fig. 2, was applied offline. Whitening filter coefficients were first created by taking the inverse Fourier transform of the averaged frequency response of the vacuum noise. The whitening filter was then applied to electronic, vacuum and quantum signal traces to obtain a flat response across the entire spectrum. The frequency offset was estimated by means of a Hilbert transform of the pilot tone and a linear fit of the extracted phase profile. Using the estimated frequency offset, the pilot tone and the quantum signal were downconverted to baseband. The baseband pilot signal was used as input to an unscented Kalman filter (UKF) for carrier phase estimation[25]. Afterward, the quantum signal was corrected by the obtained phase estimate from the UKF. Temporal synchronization was achieved through the cross-correlation between transmitted and received reference symbols. As a result of baseband modulation,

the baseband quantum signal contained undesirable low-frequency components, namely, the optical carrier (beat signal) after down-mixing and the ABC dither signals. To remove these components and measure the same temporal mode as the transmitted coherent states, a HPF with the same type, order and bandwidth as Alice's HPF was applied to the quantum signal as well as the vacuum and electronic noise measurements. We should mention that the bandwidth of the HPFs mainly relies on the spectral width of the beat signal, and the dither frequencies of the ABC. Finally, the received quantum symbols were obtained after RRC matched filtering and downsampling.

DATA AVAILABILITY

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

REFERENCES

1. Scarani, V. et al. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301–1350 (2009).
2. Pirandola, S. et al. Advances in quantum cryptography. *Adv. Opt. Photonics* **12**, 1012–1236 (2020).
3. Gisin, N., Fasel, S., Kraus, B., Zbinden, H. & Ribordy, G. Trojan-horse attacks on quantum-key-distribution systems. *Phys. Rev. A* **73**, 022320 (2006).
4. Jain, N. et al. Risk analysis of Trojan-horse attacks on practical quantum key distribution systems. *IEEE J. Sel. Top. Quantum Electron.* **21**, 168–177 (2014).
5. Lydersen, L. et al. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photonics* **4**, 686–689 (2010).
6. Gerhardt, I. et al. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nat. Commun.* **2**, 1–6 (2011).
7. Jain, N. et al. Device calibration impacts security of quantum key distribution. *Phys. Rev. Lett.* **107**, 110501 (2011).
8. Zhang, Y. et al. Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. *Phys. Rev. Lett.* **125**, 010502 (2020).
9. Grosshans, F. & Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **88**, 057902 (2002).
10. Weedbrook, C. et al. Quantum cryptography without switching. *Phys. Rev. Lett.* **93**, 170504 (2004).
11. Laudenbach, F. et al. Continuous-variable quantum key distribution with gaussian modulation–the theory of practical implementations. *Adv. Quant. Technol.* **1**, 1800011 (2018).
12. Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P. & Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat. Photonics* **7**, 378–381 (2013).
13. Lodewyck, J. et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A* **76**, 042305 (2007).
14. Xuan, Q. D., Zhang, Z. & Voss, P. L. A 24 km fiber-based discretely signaled continuous variable quantum key distribution system. *Opt. Express* **17**, 24244–24249 (2009).
15. Weedbrook, C. et al. Gaussian quantum information. *Rev. Mod. Phys.* **84**, 621 (2012).
16. Kikuchi, K. Fundamentals of coherent optical fiber communications. *J. Lightwave Technol.* **34**, 157–179 (2015).
17. Ma, X.-C., Sun, S.-H., Jiang, M.-S. & Liang, L.-M. Local oscillator fluctuation opens a loophole for eve in practical continuous-variable quantum-key-distribution systems. *Phys. Rev. A* **88**, 022339 (2013).
18. Jouguet, P., Kunz-Jacques, S. & Diamanti, E. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. *Phys. Rev. A* **87**, 062313 (2013).
19. Qin, H., Kumar, R. & Alléaume, R. Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution. *Phys. Rev. A* **94**, 012325 (2016).
20. Huang, J.-Z. et al. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. *Phys. Rev. A* **87**, 062329 (2013).
21. Derkach, I., Usenko, V. C. & Filip, R. Continuous-variable quantum key distribution with a leakage from state preparation. *Phys. Rev. A* **96**, 062309 (2017).
22. Jain, N. et al. Modulation leakage vulnerability in continuous-variable quantum key distribution. *Quant. Sci. Technol.* **6**, 045001 (2021).
23. Kleis, S., Rueckmann, M. & Schaeffer, C. G. Continuous variable quantum key distribution with a real local oscillator using simultaneous pilot signals. *Opt. Lett.* **42**, 1588–1591 (2017).
24. Qu, Z., Djordjevic, I. B. & Neifeld, M. A. RF-subcarrier-assisted four-state continuous-variable qkd based on coherent detection. *Opt. Lett.* **41**, 5507–5510 (2016).
25. Chin, H.-M., Jain, N., Zibar, D., Andersen, U. L. & Gehring, T. Machine learning aided carrier recovery in continuous-variable quantum key distribution. *npj Quant. Inf.* **7**, 20 (2021).
26. Brunner, H. H. et al. A low-complexity heterodyne CV-QKD architecture. In *19th International Conference on Transparent Optical Networks (ICTON)*, 1–4 (2017).
27. Symul, T. et al. Experimental demonstration of post-selection-based continuous-variable quantum key distribution in the presence of gaussian noise. *Phys. Rev. A* **76**, 030303 (2007).
28. Gehring, T. et al. Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks. *Nat. Commun.* **6**, 1–7 (2015).
29. Jain, N. et al. Practical continuous-variable quantum key distribution with composable security. *Nat. Commun.* **13**, 4740 (2022).
30. Lance, A. M. et al. No-switching quantum key distribution using broadband modulated coherent light. *Phys. Rev. Lett.* **95**, 180503 (2005).
31. Izutsu, M., Shikama, S. & Sueta, T. Integrated optical ssb modulator/frequency shifter. *IEEE J. Quant. Electron.* **17**, 2225–2227 (1981).
32. Li, X. et al. Modulation-format-free and automatic bias control for optical IQ modulators based on dither-correlation detection. *Opt. Express* **25**, 9333–9345 (2017).
33. Agrawal, G. P. Fiber-optic communication systems (John Wiley & Sons, 2012).
34. Mani, H. et al. Multiedge-type low-density parity-check codes for continuous-variable quantum key distribution. *Phys. Rev. A* **103**, 062419 (2021).
35. Tang, B.-Y., Liu, B., Zhai, Y.-P., Wu, C.-Q. & Yu, W.-R. High-speed and large-scale privacy amplification scheme for quantum key distribution. *Sci. Rep.* **9**, 15733 (2019).
36. Armstrong, J. OFDM for optical communications. *J. Lightwave Technol.* **27**, 189–204 (2009).
37. Qi, B., Lougovski, P., Pooser, R., Grice, W. & Bobrek, M. Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection. *Phys. Rev. X* **5**, 041009 (2015).
38. Marie, A. & Alleaume, R. Self-coherent phase reference sharing for continuous-variable quantum key distribution. *Phys. Rev. A* **95**, 012316 (2017).
39. Soh, D. B. et al. Self-referenced continuous-variable quantum key distribution protocol. *Phys. Rev. X* **5**, 041010 (2015).
40. Li, Z., Zhang, Y.-C., Xu, F., Peng, X. & Guo, H. Continuous-variable measurement-device-independent quantum key distribution. *Phys. Rev. A* **89**, 052301 (2014).
41. Gehring, T. et al. Homodyne-based quantum random number generator at 2.9 Gbps secure against quantum side-information. *Nat. Commun.* **12**, 1–11 (2021).

AUTHOR CONTRIBUTIONS

A.A.E.H. performed the experiment and the data analysis as well as implemented the DSP with help from H.M.C. and N.J. H.M. performed error correction. T.G. contributed to all parts of the work. A.A.E.H. and T.G. wrote the manuscript. A.A.E.H. and T.G. conceived of the experiment, and U.L.A and T.G. supervised the project. All authors were involved in discussions and interpretations of the results.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Correspondence and requests for materials should be addressed to Adnan A. E. Hajomer or Tobias Gehring.

Reprints and permission information is available at http://www.nature.com/reprints