ARTICLE OPEN

Check for updates

Continuous-mode quantum key distribution with digital signal processing

Ziyang Chen[1], Xiangyu Wang[2], Song Yu[2], Zhengyu Li[3]✉ and Hong Guo[1]✉

Continuous-variable quantum key distribution (CVQKD) offers the specific advantage of sharing keys remotely by the use of standard telecom components, thereby promoting cost-effective and high-performance metropolitan applications. Nevertheless, the introduction of high-rate spectrum broadening has pushed CVQKD from a single-mode to a continuous-mode region, resulting in the adoption of modern digital signal processing (DSP) technologies to recover quadrature information from continuous-mode quantum states. However, the security proof of DSP involving multi-point processing is a missing step. Here, we propose a generalized method of analyzing continuous-mode state processing by linear DSP via temporal modes theory. The construction of temporal modes is key in reducing the security proof to single-mode scenarios. The proposed practicality oriented security analysis method paves the way for building classical compatible digital CVQKD.

npj Quantum Information (2023)9:28 ; https://doi.org/10.1038/s41534-023-00695-8

INTRODUCTION

Quantum key distribution (QKD)[1–3] promises an information-theoretically secure symmetric key distribution for distant partners. The past three decades have witnessed rapid development of QKD technologies and the growth of QKD network deployment globally, which have been employed in various security applications[4–11]. Within the QKD family, continuous-variable (CV) QKD benefits from the use of off-the-shelf commercial telecom components[12,13] and provides a cost-effective alternative in metropolitan networks. Twenty years since the pioneering GG02 protocol[14] was proposed, the theory[15–20] and experimentation[21–23] of CVQKD have made remarkable progress.

Moreover, the tremendous breakthroughs of local oscillator (LO) schemes since 2015[24,25] have pushed CVQKD into a new stage, in which techniques from modern digital coherent communication have been brought in[26–29]. We call this stage *digital* CVQKD. Specifically, digital signal processing (DSP) significantly improves the signal-to-noise ratio (SNR) by compensating for channel drifting and device impairments, which greatly simplifies physical systems. This paves the way for an ultra-high secret key rate with tens of GHz of bandwidth in the CVQKD system. However, this phenomenon also complicates the security analysis.

Two barriers exist in the security analysis of a digital CVQKD system. One is the discrete modulation format, and the other is DSP. The former results from the destruction of estimating the covariance matrix directly from the measurement results and was recently solved with the semidefinite programming[30–32] or other novel methods[33,34]. The other barrier is the difficulty of constructing an appropriate measurement operator to describe the output of DSP.

Specifically, a single-point quadrature measurement of each state in one ensemble is sufficient for reliable tomography of single-mode states. However, for the tomography of continuous-mode states, the extraction of quadrature information involves multi-point sampling and processing. Therefore, a time-domain description of system's behavior should be introduced, which is beyond the traditional single-mode description.

Here, to narrow the gap between practical systems and theoretical models, we develop a generalized security proof framework for continuous-mode systems processed by linear DSP algorithms. The key step is the temporal-mode (TM) construction using DSP results, which is suitable for the analysis of high-speed, multi-point sampling systems. Specifically, in continuous-mode formalism, time-domain field operators can be introduced by Fourier transformation, based on which the generalized receiver can be well modeled. By properly calibrating the shot-noise unit (SNU), we model the linear processing of sampled data by recombination of time-domain field operators, which defines a specific TM field operator[35–37]. Consequently, the security of DSP is reduced to the security of a specific single TM measurement. Then, the rest of the analysis is compatible with traditional methods.

Moreover, the results show that the mismatch between the measured state's TM and the receiver's TM leads to inefficiency in detection. The mission of the DSP algorithm is to merge this mismatch, thus improving the detection efficiency, which coincides with improving SNR in its classical correspondence.

Our work provides a feasible way of analyzing the security and performance of a continuous-mode system processed by linear DSP algorithms, so it could provide important guidance for the DSP design of digital CVQKD. Linear DSP toolboxes are expected to be directly employed in CVQKD, reinforcing the importance of our work.

RESULTS

Temporal modes of continuous-mode states

We start by introducing the basics of continuous-mode formalism of quantum optics and then describing the state preparation phase. Recall that in traditional CVQKD analysis, the coherent state is represented by the creation and annihilation operators in terms

[1]State Key Laboratory of Advanced Optical Communication Systems and Networks, School of Electronics, and Center for Quantum Information Technology, Peking University, Beijing 100871, China. [2]State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China. [3]Huawei Technologies Co., Ltd., Shenzhen 518129, China. ✉email: lizhengyu2@huawei.com; hongguo@pku.edu.cn

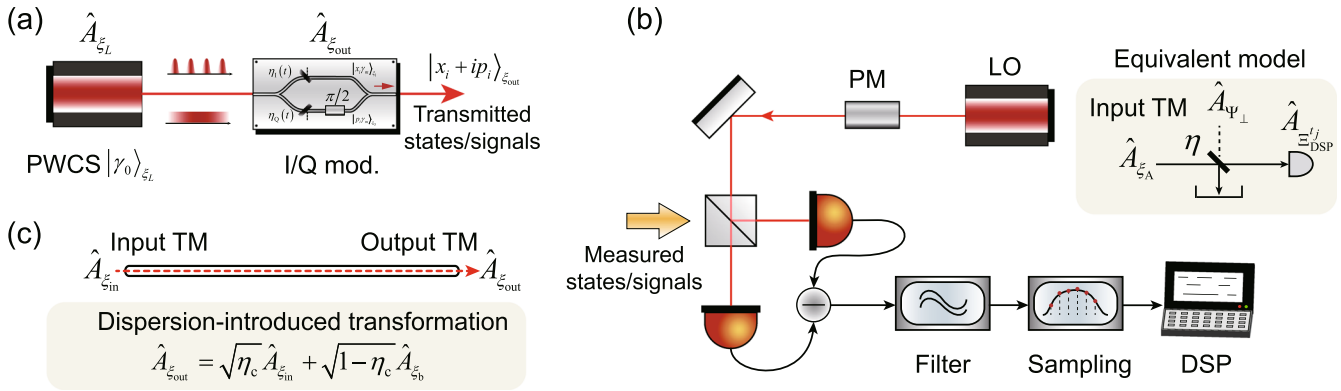

Fig. 1 Models of digital CVQKD. a The transmitter prepares a photon-wavepacket coherent state (PWCS) with an arbitrary form of envelope $\xi_L(t)$; via the I/Q modulation, the quadratures of the PWCS are modulated by Gaussian distributed random numbers. The carrier can be either a continuous wave or pulsed coherent state. **b** Measured states are fed to a practical receiver, interfering with the local oscillator (LO) at a balanced beam splitter (BS) and detected by a band-limited homodyne detector (HD) (modeled by an ideal HD and a filter), followed by the sampling and DSP devices. The mismatch between the measured state's temporal mode (TM) and the receiver's TM is equivalent to a BS with a transmitivity of η. **c** In the experiment, channel transmission causes a transformation of TM, which, if ignored, will cause a degradation in system performance. PM phase modulator.

of a single-mode field, given by $\hat{a}_i^\dagger, \hat{a}_i$. By contrast, in a practical system, high-speed modulation inevitably introduces a nonuniform temporal waveform, so continuous-mode formalism of field operators[35,37,38] should be introduced, which is widely used in studying continuous-mode quantum optics. By transforming the annihilation and creation operators from their discrete-mode counterparts, the continuous-mode field operators are defined as $\hat{a}_i \to (\Delta\omega)^{\frac{1}{2}}\hat{a}(\omega)$ and $\hat{a}_i^\dagger \to (\Delta\omega)^{\frac{1}{2}}\hat{a}^\dagger(\omega)$, where $\Delta\omega$ denotes the mode spacing, which satisfies the commutation relation $[\hat{a}(\omega), \hat{a}^\dagger(\omega')] = \delta(\omega - \omega')$. In the time domain, it is useful to define the Fourier transforms of $\hat{a}(\omega)$, namely $\hat{a}(t)$, given by $\hat{a}(t) = \frac{1}{\sqrt{2\pi}}\int d\omega \hat{a}(\omega)\exp(-i\omega t)$. The creation operator $\hat{a}^\dagger(t)$ follows a similar definition.

Based on this, the photon-wavepacket creation operator $\hat{A}_{\xi_i}^\dagger$ [35,39] can be defined as

$$\hat{A}_{\xi_i}^\dagger = \int dt \xi_i(t)\hat{a}^\dagger(t), \tag{1}$$

in which the wavepacket $\xi_i(t)$ usually reads $\xi_i^0(t)e^{-i\omega t}$, as an envelope $\xi_i^0(t)$ with a carrier $e^{-i\omega t}$. It is also known as the TM field operator[36,37] if $\xi_i(t)$ meets the orthonormalization that $\int dt \xi_i^*(t)\xi_j(t) = \delta_{ij}$, for different i, j. The TM operators also obey the commutation relation, which reads

$$\left[\hat{A}_{\xi_i}, \hat{A}_{\xi_j}^\dagger\right] = \delta_{ij}. \tag{2}$$

It is then important to define the photon-wavepacket coherent state $|\gamma_i\rangle_{\xi_i}$ on ξ_i-TM, as[35]

$$|\gamma_i\rangle_{\xi_i} = \hat{D}_{\xi_i}(\gamma_i)|0\rangle = \exp\left(\gamma_i\hat{A}_{\xi_i}^\dagger - \gamma_i^*\hat{A}_{\xi_i}\right)|0\rangle, \tag{3}$$

where γ_i denotes the displacement parameter, and $|\gamma_i|^2$ represents the average photon number. The photon-wavepacket coherent state obeys the eigenvalue equation $\hat{A}_{\xi_i}|\gamma_i\rangle_{\xi_i} = \gamma_i|\gamma_i\rangle_{\xi_i}$. Under this notation, the quadrature operator with the phase angle θ can be defined as

$$\hat{X}_{\xi_i}^\theta = \hat{A}_{\xi_i}^\dagger\exp(i\theta) + \hat{A}_{\xi_i}\exp(-i\theta). \tag{4}$$

In a digital CVQKD system, coherent states are generated by widely used in-phase/quadrature (I/Q) modulation. As shown in Fig. 1(a), assuming that $|\gamma_0\rangle_{\xi_L}$ is the photon-wavepacket coherent state fed to the I/Q modulator, $|\gamma_m\rangle_{\xi_L}$ are then the state of the I or Q arm after the balanced beam splitter (BS), where $\gamma_m = \gamma_0/\sqrt{2}$. Then, each arm performs the intensity modulation with a certain waveform, which is modeled by a time-dependent BS with transmitivity $\eta(t)$ related to modulation[40,41]. Assuming that the data encoded on the I and Q components in the i-th period are $\{x_i\}$ and $\{p_i\}$ and that their normalized waveform envelopes are $\xi_{\rm I}(t)$ and $\xi_{\rm Q}(t)$, we can rewrite $\sqrt{\eta_{\rm I}(t)}\xi_L^0(t) = x_i\xi_{\rm I}(t)$ on the I path and $\sqrt{\eta_{\rm Q}(t)}\xi_L^0(t) = p_i\xi_{\rm Q}(t)$ on the Q path. Then, the I and Q path's output states are transformed into $|x_i\gamma_m\rangle_{\xi_{\rm I}}$ and $|p_i\gamma_m\rangle_{\xi_{\rm Q}}$. Finally, after passing through another balanced BS and a proper attenuator, the output photon-wavepacket coherent state is $|x_i + ip_i\rangle_{\xi_{\rm out}}$ if $\xi_{\rm I}(t) = \xi_{\rm Q}(t) = \xi_{\rm out}(t)$ with properly calibrated modulation. This means that in the entanglement-based scheme, the output coherent states can be seen as two-mode squeezed states, with $\xi_{\rm out}$-TM being measured on one mode with a heterodyne measurement. As for $\xi_{\rm I}(t) \neq \xi_{\rm Q}(t)$, the output state can be decomposed into two orthogonal TMs with different but correlated displacement parameters, which we leave for further investigations.

Measurement, sampling, and data processing

On the receiver side, the input state is first measured by a practical homodyne detector with limited bandwidth and then sampled by an analog-to-digital converter (ADC). After this, the sampled data go through a series of DSP algorithms, and the final data output from DSP are assumed to represent the quadrature measurement result, which can be used to construct the covariance matrix and then calculate the secret key rate. We only consider linear DSP algorithms here because the transmitted quantum light is extremely weak, so no obvious optical nonlinear effects occur. Thus, linear compensation algorithms are sufficient to recover the signal. When we use the above continuous-mode formalism notation, mapping the outputs of linear DSP to quadrature measurements is surprisingly natural; the crucial step is normalization with properly calibrated SNU. To paint a clear picture of this, we first ignore the imperfections of the homodyne detector and finite-resolution issue of ADC, and we discuss the trusted detection model considering the detector's efficiency and noise in the Methods section.

The receiver can be modeled as an ideal homodyne detector, followed by a filter, as shown in Fig. 1b. Assuming the filter has an impulse response function (IRF), namely, $g(t)$, the photocurrent flux operator of a homodyne detector is given by[35,39]

$$\hat{f}(t) = \left[\hat{a}^\dagger(t)\hat{a}_{\rm LO}(t) + \hat{a}_{\rm LO}^\dagger(t)\hat{a}(t)\right] * g(t), \tag{5}$$

where * denotes the convolution. The photon wavepacket of the local oscillator (LO) is given by $a_{\mathrm{LO}}(t) = \mu_{\mathrm{LO}}^{1/2}\xi_{\mathrm{LO}}(t)\exp(-i\omega_{\mathrm{LO}}t + i\theta)$, where μ_{LO} denotes the average number of photons contained in an envelope $\xi_{\mathrm{LO}}(t)$ for a pulsed LO, or a time period as defined. Because LO is considered a classical field with enough photons, the fluctuation in the measurement output mainly comes from the signal quadrature measurement part. Therefore, the photocurrent flux after taking the average over LO is more useful, given by $\hat{f}_{\mathrm{LO}}(t) = \langle a_{\mathrm{LO}}(t)|\hat{f}(t)|a_{\mathrm{LO}}(t)\rangle$.

Considering ADC as the integral sampling process with integral time Δt_s, the sampled data at time t_0 are

$$\hat{D}_{t_0} = \frac{1}{\Delta t_s}\int_{t_0}^{t_0+\Delta t_s} dt\hat{f}_{\mathrm{LO}}(t), \tag{6}$$

in which the electronics amplification is ignored.

Multiple sampling points may exist within one period T_r. Generally, types of linear data processing exist: (i) directly choose one sampled data of each period as final data of this period, for instance, the sampling point near the peak of the envelope of measured state; (ii) using the sampled data within one period to define the final data of this period, for instance, calculating the weighted averaging of all sampled data within the same period; and (iii) generally, a DSP algorithm may use the sampled data from multiple periods, for instance, the root raised cosine (RRC) filter[42] introduces a convolution over multiple periods.

For a DSP algorithm involving N sampled data, the output data at the time corresponding to the t_j sampling time could be

$$\hat{D}_{t_j}^{N} = f_{\mathrm{dsp}}(\hat{D}_{t_{j-k+1}}, \ldots \hat{D}_{t_{j-k+N}}) = \sum_{i=1}^{N} f_{\mathrm{dsp}}^{i}\,\hat{D}_{t_{j-k+i}} \tag{7}$$

with linear expansion, where f_{dsp}^{i} and k are real numbers determined by DSP algorithms. After simplification, Eq. (7) is given by

$$\hat{D}_{t_j}^{N} = \frac{\mu_{\mathrm{LO}}^{1/2}}{\Delta t_s}\int G_{\mathrm{dsp}}^{t_j}(\tau)\hat{X}^{a_{\mathrm{LO}}}(\tau)d\tau, \tag{8}$$

where

$$G_{\mathrm{dsp}}^{t_j}(\tau) = \sum_{i=1}^{N} f_{\mathrm{dsp}}^{i}\int_{t_{j-k+i}}^{t_{j-k+i}+\Delta t_s} g(t-\tau)dt \tag{9}$$

is related to the detector's IRF, sampling points, and the DSP algorithm. In addition, $X^{a_{\mathrm{LO}}}(\tau)$ is the intermediate quadrature operator related to the LO's features, which is given by

$$X^{\hat{a}_{\mathrm{LO}}}(\tau) = \xi_{\mathrm{LO}}(\tau)e^{-i(\omega_{\mathrm{LO}}\tau-\theta)}\hat{a}^{\dagger}(\tau) + \mathrm{h.c.} \tag{10}$$

SNU calibration and normalization

To normalize the output data from DSP, one key step is to define and calibrate the SNU, which is the most distinguishable phase from classical optical communication. Considering $\hat{D}_{t_j}^{N}$ as the final data for the period in which t_j lies, we can easily verify that for the vacuum input, the mean is $\langle 0|\hat{D}_{t_j}^{N}|0\rangle = 0$, and the variance $\sigma_{\mathrm{SNU}}^2 = \langle 0|\hat{D}_{t_j}^{N}\hat{D}_{t_j}^{N}|0\rangle$ is

$$\sigma_{\mathrm{SNU}}^2 = \frac{\mu_{\mathrm{LO}}}{\Delta t_s{}^2}\int |\xi_{\mathrm{LO}}(\tau)|^2\left[G_{\mathrm{dsp}}^{t_j}(\tau)\right]^2 d\tau. \tag{11}$$

For normalization, the sampled data $\hat{D}_{t_j}^{\mathrm{SNU}}$ are divided by $\sigma_{\mathrm{SNU}} = \sqrt{\sigma_{\mathrm{SNU}}^2}$, which gives

$$\hat{D}_{t_j}^{\mathrm{SNU}} = e^{i\theta}\int d\tau\frac{G_{\mathrm{dsp}}^{t_j}(\tau)\xi_{\mathrm{LO}}(\tau)e^{-i\omega_{\mathrm{LO}}\tau}}{\sigma_{\mathrm{cal}}}\hat{a}^{\dagger}(\tau) + \mathrm{h.c.}, \tag{12}$$

where $\sigma_{\mathrm{cal}} = \sqrt{\int d\tau|\xi_{\mathrm{LO}}(\tau)|^2[G_{\mathrm{dsp}}^{t_j}(\tau)]^2}$ is the rescaled factor when calibrating output data by SNU. It can be verified that the coefficient function of $\hat{a}(\tau)$ is a normalized photon-wavepacket function, which is

$$\Xi_{\mathrm{DSP}}^{t_j}(\tau) = \frac{1}{\sigma_{\mathrm{cal}}}\xi_{\mathrm{LO}}(\tau)G_{\mathrm{dsp}}^{t_j}(\tau)\exp(-i\omega_{\mathrm{LO}}\tau), \tag{13}$$

with the normalization condition $\int d\tau|\Xi_{\mathrm{DSP}}^{t_j}(\tau)|^2 = 1$. This introduces $\Xi_{\mathrm{DSP}}^{t_j}$-TM, which is jointly defined by the LO, filter, sampling, and DSP algorithms. Then, we can further define its creation operator as

$$\hat{A}_{\Xi_{\mathrm{DSP}}^{t_j}}^{\dagger} = \int d\tau\Xi_{\mathrm{DSP}}^{t_j}(\tau)\hat{a}^{\dagger}(\tau). \tag{14}$$

Consequently, a simplified form of Eq. (12) in terms of the $\Xi_{\mathrm{DSP}}^{t_j}$-TM operators is rewritten as

$$\hat{D}_{t_j}^{\mathrm{SNU}} = \hat{A}_{\Xi_{\mathrm{DSP}}^{t_j}}^{\dagger}\exp(i\theta) + \hat{A}_{\Xi_{\mathrm{DSP}}^{t_j}}\exp(-i\theta) = \hat{X}_{\Xi_{\mathrm{DSP}}^{t_j}}^{\theta}, \tag{15}$$

which shares the same form as Eq. (4).

Therefore, the final data (output from DSP and being normalized) can be treated as a quadrature measurement of $\Xi_{\mathrm{DSP}}^{t_j}$-TM. As long as the data represent a quadrature measurement result, they can be used to construct the covariance matrix and are thus compatible with traditional security analysis methods. The above-mentioned analysis also highlights one key point of SNU calibration, which is that the sampled data of vacuum input should be processed by the same DSP as the usual signal input case before the data are used to calculate the variance of shot noise.

Another important issue is that for a DSP involving sampled data exceeding one period, the possible crosstalk should be avoided. In this case, the TMs related to different periods should be orthogonal, that is, $\int \Xi_{\mathrm{DSP}}^{t_i}\Xi_{\mathrm{DSP}}^{t_j*} = 0$, where t_i, t_j belong to two different periods. This also coincides with classical DSP's purpose, as crosstalk lowers the SNR. For instance, the RRC pulse shaping and filtering methods are commonly used to improve spectrum efficiency. Moreover, the RRC filter is designed with no intersymbol interference for different optimal sampling points, which is associated with the TMs related to different optimal sampling points being orthogonal.

This completes our security analysis framework for linear DSP, which can be summarized in two key points. One is properly calibrating SNU, which naturally leads the final data to be a quadrature measurement result with respect to the TM defined jointly defined by LO, detector, sampling, and DSP. The second is to avoid the complex measurement model introduced by intersymbol crosstalk, where TMs corresponding to different periods should be orthogonal. If these two conditions apply, the final data can be directly used to construct the covariance matrix, and then we can calculate the secret key rate through the current security analysis method.

Below, two examples are given to analyze the performance after considering the continuous-mode scenario, including the mode-matching issue and transmission-dispersion issue.

Projection on the measurement temporal mode

Besides security, our analysis also provides insights into imperfect detection efficiency, related to the mismatch between the measured state's TM and the receiver's TM. The whole measurement process under the TM representation is equivalent to the projection of the measured state's TM to the receiver's TM, and vice versa.

Now, consider a case where the measured state is a coherent state on ξ_A-TM, which is different from the receiver's $\Xi_{\mathrm{DSP}}^{t_j}$-TM.

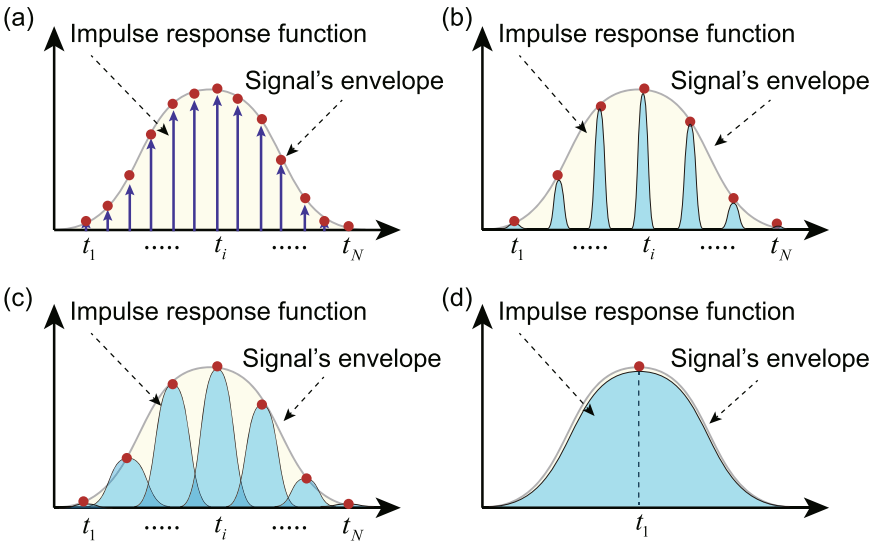

Fig. 2 Weighted averaging of sampled data. Assume the LO is a continuous-wave (CW) laser. **a** The bandwidth of the detector is large enough, and the impulse response function (IRF) is approximate to the δ-function. The final data are recovered by weighted averaging of all of the sampled data within one period, and the weight follows the shape of the measured state's envelope. **b**, **c** The bandwidth of the detector is limited, resulting in a widened IRF, which convolutes the signal around each sampling point. **d** If the detector's IRF is similar to the measured state's envelope, single-point sampling can represent the final data.

Using the Gram–Schmidt orthogonalization, we can define a third TM from $\Xi_{\mathrm{DSP}}^{t_j}$-TM and orthogonal to ξ_{A}-TM, denoted as $\Psi_{\perp}$-TM, which leads to the following decomposition of the creation operator:

$$\hat{A}^{\dagger}_{\Xi^{t_j}_{\mathrm{DSP}}} = \sqrt{\eta}\hat{A}^{\dagger}_{\xi_{\mathrm{A}}} + \sqrt{1-\eta}\hat{A}^{\dagger}_{\psi_{\perp}}, \tag{16}$$

where $\eta = \left[\int dt \Xi^{t_j,*}_{\mathrm{DSP}}(t)\xi_{\mathrm{A}}(t)\right]^2 \leq 1$ denotes the mode-matching coefficient. With further examination of the first-order and second-order moments, the abovementioned decomposition can be modeled by an extra BS at the receiver side, with transmitivity η, quantifying the matching degree between ξ_{A}-TM and $\Xi_{\mathrm{DSP}}^{t_j}$-TM. A detailed derivation can be found in the Methods section. Here, $\eta < 1$ means an extra loss induced by the mode mismatch, which decreases the performance of the system. This degradation is rather covert, different from the physical components introduced by loss, that is, fiber coupling loss and the non-unit quantum efficiency of photodiodes. The closer η is to 1, the better the performance of a DSP algorithm.

Here, we take the weighted averaging scenario to further illustrate the mode-matching issue in the time domain. In this case, the DSP function is given by $f^i_{\mathrm{dsp}} = w_i$, where w_i is the weight of the i-th sampling point within one period. The measurement results can be described by Fig. 2. A sampled data point measures not only the signal at one time point but also convoluted nearby signals around the sampling point. Therefore, an intuitive understanding of mode matching is that the sum of all sampled data covers a certain signal area. In Fig. 2a, the bandwidth of the detector is large enough that the IRF is approximate to the δ-function, and then ultra-dense sampling is needed. By contrast, if the bandwidth gradually decreases, the IRF becomes wider, and fewer sampling points are required to achieve a similar mode-matching degree, as shown in Fig. 2b, c. If the detector's IRF is similar to the measured state's envelope, a single-sampling point is enough, as in Fig. 2d.

We also note that, the discussion of system's side information is an interesting research topic. We discuss it in two scenarios: (1) Alice performs a good calibration of the modulation variance of the transmitted signal; (2) Alice performs a poor calibration of the modulation variance, for example, neglecting optical modes that may exist on Alice's side.

For the first scenario, all of the optical modes in the spectrum are taken into account, including the part outside the bandwidth of Bob's detector. Because the information of the whole transmitter is included in the variance of Alice's TM, any energy that Bob does not detect (either the energy beyond the detector's bandwidth or the energy loss caused by the mode mismatch) contributes to the channel loss estimated from covariance matrix, which will be considered as caused by the eavesdropper. Therefore, this is not a side channel, but rather a performance degradation.

For the second scenario, Alice fails to perform a proper calibration, which will open a source-flaw-related side channel. For example, part of the signal's energy of the sideband is not included when calibrating the modulation variance of Alice. This issue has been extensively studied in the single-mode case[43–47]. Note that this is not caused by the continuous-mode model proposed by our work, but by the improper calibration method of the modulation variance at the transmitter. To avoid this issue, three alternative methods are proposed: (1) Add a power meter at Alice's side to calibrate Alice's overall energy and determine the modulation variance of the whole TM; (2) avoid information leakage through single-sideband modulation[43]; (3) take the leakage information into account in the overall security analysis[44–47].

Therefore, in the practical security analysis of a CVQKD system, especially when the homodyne detector is used to calibrate Alice's modulation variance (such as using Bob's device to perform back-to-back test for engineering convenience), we should deal with this phenomenon more carefully. We will investigate this issue in detail in the future.

Continuous-mode transmission

The measured state's TM is determined by the modulation at the transmitter side, which is controlled, and also the channel transmission, which is not controlled. Therefore, the DSP needs to be designed or adjusted according to the channel condition. We take channel dispersion as an example to show how it influences the measurement, which is significant in a high-speed system. Considering a coherent state with a narrow Gaussian wavepacket $\xi_{\mathrm{in}}(t)$, after passing through the channel, its output

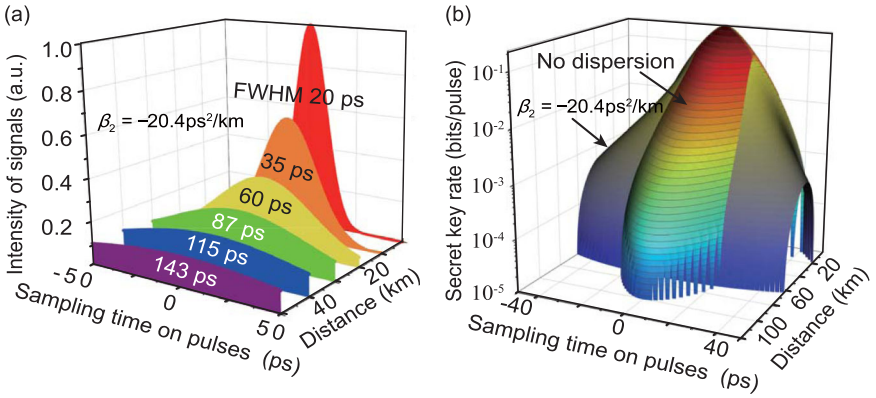

Fig. 3 Simulation results of the channel dispersion effect. a Evolution of the envelope of a Gaussian pulse with a full width at half-maximum (FWHM) of 20 ps in optical fibers, ignoring the fiber loss, where $\beta_2 = -20.4\,\mathrm{ps}^2/\mathrm{km}$ is considered, which is a typical value of standard G.652 telecom fiber at 1550 nm. **b** Secret key rates for narrow-pulse (Gaussian pulse) propagation considering fiber-dispersion-induced TM mismatch, where $\beta_2 = 0\,\mathrm{ps}^2/\mathrm{km}$ and $\beta_2 = -20.4\,\mathrm{ps}^2/\mathrm{km}$ are considered, which are typical values of no dispersion channel and the standard G.652 telecom fiber at 1550 nm. In the simulation, we use the single-sampling-point scheme, and the sampling time accuracy is considered. The sampling time $t = 0$ ps is assumed as the peak of Gaussian pulse. It is shown that the increasing mode mismatch reduces the secret key rate while also relaxing the accuracy requirement of the sampling time.

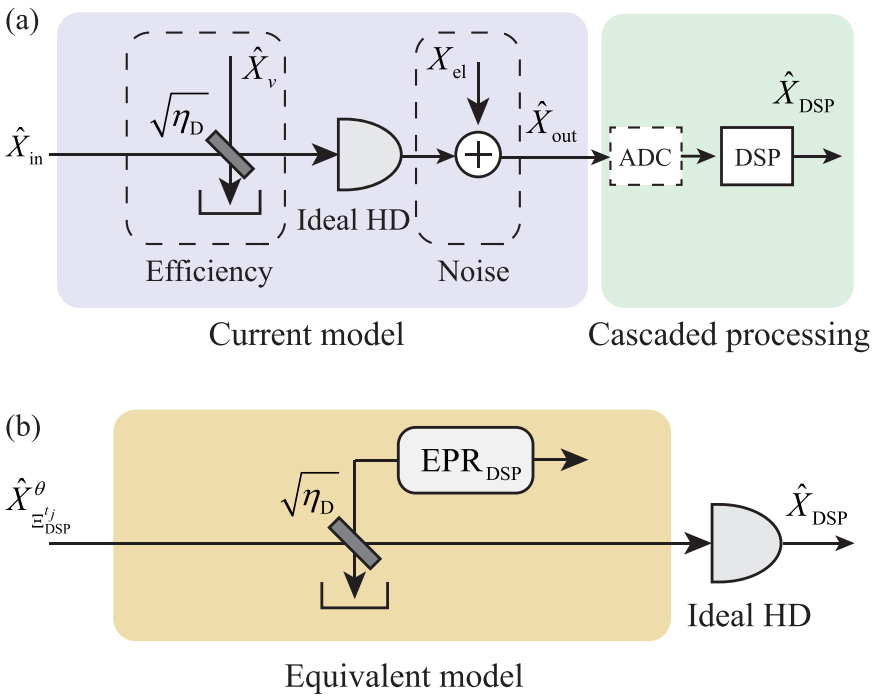

Fig. 4 The proposed detection model considering non-ideal efficiency and electronic noise. a The PM version of our detection model. **b** The equivalent EB version of our detection model.

envelope is transformed with a transfer function $h(t,z)$, given by $\xi_{\mathrm{out}}(t) = \xi_{\mathrm{in}}(t) * h(t,z)$, where $h(t,z)$ is the channel transfer function in the time domain, and its Fourier transform is given by $\mathscr{F}[h(t,z)] = \exp\left(-k_i z + ik_1\Omega z + i\frac{k_2}{2}\Omega^2 z\right)$, in which the second-order Taylor expansion of the real part of the wave vector is considered, z is the transmission distance, Ω is the Fourier frequency, and k_1 and k_2 denote the inverse group velocity and second-order dispersion coefficient, respectively. Only for the ultrashort period, the influence of third-order nonlinear dispersion needs to be considered. It can be seen that the output state's TM varies with increasing distance, as in Fig. 3a. Therefore, if the DSP does not consider this TM varying, there will be an increasing extra loss as the transmission distance increases, which will decrease the maximal transmission distance, as simulated in Fig. 3b. This is where self-adaptive algorithms apply.

DISCUSSION

In this study, we have developed a generalized practical system model with continuous-mode formalism of quantum optics, based on which the IQ modulation at the transmitter side and band-limited homodyne detection with the sampling process at the receiver side can be well described. Then, with proper calibration of SNU, the output data of a linear DSP can be modeled by the quadrature measurement result with respect to a specific TM, jointly defined by the LO, filter, sampling, and DSP algorithms. This immediately results in good compatibility with traditional security

analysis methods, which completes the security proof of linear DSP algorithms. Linear DSP toolboxes are expected to be directly employed in CVQKD, which highlights the importance of our work.

In addition to the security, our work also provides a method to analyze the performance of a DSP algorithm through a factor quantifying the matching degree between the measured state's TM and the receiver's TM. Moreover, interesting concepts like the DSP-induced fast fading-channel effect can be further analyzed to explore the practical limitations of a CVQKD system. By the guidance of our work, secure and better-performing DSP algorithms can be designed, which will exploit the significant potential of digital CVQKD to achieve ultra-high secret key-generation speed and cost-effective implementations.

METHODS

Trusted detection model considering DSP

Our model mainly deals with the DSP part, which is cascaded after the trusted physical detection process. The input of the DSP modular is actually the output of the practical trusted detector, namely, $\hat{X}_{\text{out}}$, as shown in Fig. 4 (a). From this point of view, our analysis is actually a complement to the existing trusted model after considering the time-related information and its processing.

Since we restrict the discussed DSP algorithms to linear algorithms, the processing of the output signal is equivalent to the independent processing of the incident signal and the electronic noise. Then the output of DSP shares the same form as the output of the current trusted model, given by

$$\begin{aligned}\hat{X}_{\text{DSP}} &= f_{\text{dsp}}(\hat{X}_{\text{out}}) \\ &= \sqrt{\eta_{\text{D}}} f_{\text{dsp}}(\hat{X}_{\text{in}}) + \sqrt{1-\eta_{\text{D}}} f_{\text{dsp}}(\hat{X}_{v}) + f_{\text{dsp}}(X_{\text{el}}) \\ &\overset{\text{PM}}{=} \sqrt{\eta_{\text{D}}}\hat{X}^{\theta}_{\Xi^{t_j}_{\text{DSP}}} + \sqrt{1-\eta_{\text{D}}}\hat{X}_{\Xi^{t_j}_{\text{DSP},v}} + X^{\text{DSP}}_{\text{el}}\end{aligned} \tag{17}$$

$$\overset{\text{EB}}{=} \sqrt{\eta_{\text{D}}}\hat{X}^{\theta}_{\Xi^{t_j}_{\text{DSP}}} + \sqrt{1-\eta_{\text{D}}}\hat{X}^{\text{DSP}}_{\text{EPR}}, \tag{18}$$

where $f_{\text{dsp}}(\cdot)$ denotes the linear DSP function, and $\hat{X}^{\theta}_{\Xi^{t_j}_{\text{DSP}}}$ is the incident TM defined by a specific DSP algorithm. The result of the prepare-and-measure (PM) scheme (Fig. 4a) is given in Eq. (17), where $\hat{X}_{\Xi^{t_j}_{\text{DSP},v}}$ refers to the TM of a vacuum input, and the equivalent electronic noise $X^{\text{DSP}}_{\text{el}}$ is the broadband electronic noise filtered by the same DSP algorithm. The result of the equivalent entanglement-based (EB) scheme (Fig. 4b) is given in Eq. (18), where $\hat{X}^{\text{DSP}}_{\text{EPR}}$ is the equivalent trusted mode introduced by our model.

Therefore, the trusted model of a practical detector with DSP can be simplified as Fig. 4b, as long as we re-calibrate the variance of the equivalent electronic noise $v^{\text{DSP}}_{\text{el}}$.

In experiments, the practical calibrating steps are actually very similar to the current method, given by the following two steps:

(1) Turn off the quantum input signal, turn off the LO, and directly sample the output of the detector, which corresponds to the measurement data of the electronic noise;
(2) Process the collected data by the same DSP function as measured signal and then use the processing result to calculate the variance of the electronic noise.

After the calibrated electronic noise variance is obtained, the variance of the trusted EPR mode introduced in the EB scheme can be obtained, given by $V^{\text{DSP}}_{\text{EPR}} = 1 + v^{\text{DSP}}_{\text{el}}/(1-\eta_{\text{D}})$, referred to as Bob's input.

Derivation of the mode-matching coefficient

Assume that the measured state at Bob's input is an unknown wavepacket coherent state $|\gamma\rangle_{\xi_{\text{A}}}$ related to the wavepacket $\xi_{\text{A}}(t)$. To obtain the equivalent performance of mode matching, we first decompose the receiver's basis function $\Xi^{t_j}_{\text{DSP}}(t)$ into the input basis $\xi_{\text{A}}(t)$ and its orthogonal basis $\Psi_{\perp}(t)$. Then we show the mode-matching coefficient.

Using the Gram–Schmidt process, we can map the receiver's operator from the basis $\Xi^{t_j}_{\text{DSP}}(t)$ to the set of bases $\{\xi_{\text{A}}(t), \Psi_{\perp}(t)\}$. In this transformation, the basis $\Xi^{t_j}_{\text{DSP}}(t)$ represents the measurement mode-matched basis function. The Gram–Schmidt process is given as follows:

- Step 1: The overlapping of two bases (also called the mode-matching coefficient) is defined as

$$\sqrt{\eta} = \int dt \Xi^{t_j,*}_{\text{DSP}}(t)\xi_{\text{A}}(t). \tag{19}$$

- Step 2: The mode-matched basis is written as $\zeta_1(t) = \xi_{\text{A}}(t)$ directly.
- Step 3: The second orthonormal basis is calculated by

$$\begin{aligned}\zeta_2(t) &= \Xi^{t_j}_{\text{DSP}}(t) - \frac{\int dt \Xi^{t_j,*}_{\text{DSP}}(t)\zeta_1(t)}{\int dt \zeta^*_1(t)\zeta_1(t)}\zeta_1(t) \\ &= \Xi^{t_j}_{\text{DSP}}(t) - \sqrt{\eta}\xi_{\text{A}}(t).\end{aligned} \tag{20}$$

It is easy to verify that

$$\begin{aligned}&\int dt \zeta^*_2(t)\zeta_2(t) \\ &= \int dt \left[\Xi^{t_j,*}_{\text{DSP}}(t) - \sqrt{\eta}\xi^*_{\text{A}}(t)\right]\left[\Xi^{t_j}_{\text{DSP}}(t) - \sqrt{\eta}\xi_{\text{A}}(t)\right] \\ &= 1 + \eta - 2\sqrt{\eta}\int dt \xi_{\text{A}}(t)\Xi^{t_j}_{\text{DSP}}(t) \\ &= 1 - \eta.\end{aligned} \tag{21}$$

After normalizing the basis function, we can obtain

$$\begin{aligned}\Psi_{\perp}(t) &= \frac{\zeta_2(t)}{\sqrt{\int dt \zeta^*_2(t)\zeta_2(t)}} \\ &= \frac{1}{\sqrt{1-\eta}}\left(\Xi^{t_j}_{\text{DSP}}(t) - \sqrt{\eta}\xi_{\text{A}}(t)\right).\end{aligned} \tag{22}$$

The receiver's basis function is then decomposed as

$$\Xi^{t_j}_{\text{DSP}}(t) = \sqrt{\eta}\xi_{\text{A}}(t) + \sqrt{1-\eta}\Psi_{\perp}(t), \tag{23}$$

and based on this, we can define two temporal modes (TMs) given by

$$\hat{A}^{\dagger}_{\xi_{\text{A}}} = \int dt \xi_{\text{A}}(t)\hat{a}^{\dagger}(t), \tag{24}$$

$$\hat{A}^{\dagger}_{\Psi_{\perp}} = \int dt \Psi_{\perp}(t)\hat{a}^{\dagger}(t). \tag{25}$$

Now, the measurement results can be rewritten as

$$\hat{D}^{\text{SNU}}_{t_j} = \hat{X}^{\theta}_{\Xi^{t_j}_{\text{DSP}}} = \sqrt{\eta}\hat{X}_{\xi_{\text{A}}} + \sqrt{1-\eta}\hat{X}_{\Psi_{\perp}}, \tag{26}$$

where $\hat{X}_{\xi} = \hat{A}_{\xi} + \hat{A}^{\dagger}_{\xi}$ denotes the quadrature operator of ξ-TM.

Moments of measured data

Now, let us investigate the first-order and second-order moments of the final data. The mean value (first-order moment) is given by

$$\begin{aligned}d_{\text{out}} &= \langle\gamma|\hat{D}^{\text{SNU}}_{t_j}|\gamma\rangle_{\xi_{\text{A}}} = \langle\gamma|\left(\sqrt{\eta}\hat{X}_{\xi_{\text{A}}} + \sqrt{1-\eta}\hat{X}_{\Psi_{\perp}}\right)|\gamma\rangle_{\xi_{\text{A}}} \\ &= \sqrt{\eta}\langle\gamma|\hat{X}_{\xi_{\text{A}}}|\gamma\rangle_{\xi_{\text{A}}} + \sqrt{1-\eta}\langle\gamma|\hat{X}_{\Psi_{\perp}}|\gamma\rangle_{\xi_{\text{A}}} \\ &= \sqrt{\eta}d_{\text{in}},\end{aligned} \tag{27}$$

where $\langle\varphi|\hat{A}|\varphi\rangle$ is the expectation value of $\hat{A}$ in the state φ, and d_{in} denotes the mean value of the input mode.

The variance of the final data can be obtained and is

$$\begin{aligned}\sigma^2 &= \langle\gamma|\hat{D}_{t_j}^{\text{SNU}}\hat{D}_{t_j}^{\text{SNU}}|\gamma\rangle_{\xi_A} - \langle\gamma|\hat{D}_{t_j}^{\text{SNU}}|\gamma\rangle_{\xi_A}^2 \\ &= \eta\langle\gamma|\hat{X}_{\xi_A}\hat{X}_{\xi_A}|\gamma\rangle_{\xi_A} + 2\sqrt{\eta(1-\eta)}\langle\gamma|\hat{X}_{\xi_A}\hat{X}_{\psi_\perp}|\gamma\rangle_{\xi_A} \\ &\quad +(1-\eta)\langle\gamma|\hat{X}_{\psi_\perp}\hat{X}_{\psi_\perp}|\gamma\rangle_{\xi_A} \\ &= \eta V_{\text{in}} + (1-\eta)\cdot 1,\end{aligned} \tag{28}$$

where V_{in} is the variance of the input mode.

From Eq. (26), we can see that the measurement results are equivalent to a mode-matching loss added before the receiver side, which is modeled by a beam splitter (BS). After the first-order and second-order moments of measured data are given, it is more intuitive to see that the transmittance of equivalent BS is η. In the above discussion, we assume that $|\gamma\rangle$ is a TM coherent state to simplify the calculation of Eqs. (27) and (28). While one can further exam that, for an arbitrary input state, Eqs. (27) and (28) still hold. The above derivations also hold considering heterodyne detection.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request.

CODE AVAILABILITY

The code used in this study is available from the corresponding author upon reasonable request.

Received: 13 September 2022; Accepted: 8 March 2023;
Published online: 24 March 2023

REFERENCES

1. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145 (2002).
2. Pirandola, S. et al. Advances in quantum cryptography. *Adv. Opt. Photon.* **12**, 1012 (2020).
3. Xu, F., Ma, X., Zhang, Q., Lo, H.-K. & Pan, J.-W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **92**, 025002 (2020).
4. Peev, M. et al. The SECOQC quantum key distribution network in vienna. *New J. Phys.* **11**, 075001 (2009).
5. Sasaki, M. et al. Tokyo QKD network and the evolution to secure photonic network. In *CLEO: 2011 - Laser Science to Photonic Applications,* 1–3 (Optica Publishing Group, 2011).
6. Zhang, Q., Xu, F., Chen, Y.-A., Peng, C.-Z. & Pan, J.-W. Large scale quantum key distribution: challenges and solutions. *Opt. Express* **26**, 24260 (2018).
7. Hosseinidehaj, N. et al. Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook. *IEEE Commun. Surv. Tutor.* **21**, 881 (2019).
8. Dynes, J. F. et al. Cambridge quantum network. *npj Quantum Inf.* **5**, 101 (2019).
9. Joshi, S. K. et al. A trusted node-free eight-user metropolitan quantum communication network. *Sci. Adv.* **6**, eaba0959 (2020).
10. Paraïso, T. K. et al. A photonic integrated quantum secure communication system. *Nat. Photon.* **15**, 850 (2021).
11. Chen, Y.-A. et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature* **589**, 214 (2021).
12. Diamanti, E. & Leverrier, A. Distributing secret keys with quantum continuous variables: principle security and implementations. *Entropy* **17**, 6072 (2015).
13. Laudenbach, F. et al. Continuous-variable quantum key distribution with gaussian modulation-the theory of practical implementations. *Adv. Quantum Technol.* **1**, 1800011 (2018).
14. Grosshans, F. & Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **88**, 057902 (2002).
15. García-Patrón, R. & Cerf, N. J. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.* **97**, 190503 (2006).
16. Furrer, F. et al. Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks. *Phys. Rev. Lett.* **109**, 100502 (2012).
17. Leverrier, A. Composable security proof for continuous variable quantum key distribution with coherent states. *Phys. Rev. Lett.* **114**, 070501 (2015).
18. Leverrier, A. Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction. *Phys. Rev. Lett.* **118**, 200501 (2017).
19. Pirandola, S. Limits and security of free-space quantum communications. *Phys. Rev. Res.* **3**, 013279 (2021).
20. Pirandola, S. Composable security for continuous variable quantum key distribution: trust levels and practical key rates in wired and wireless networks. *Phys. Rev. Res.* **3**, 043014 (2021).
21. Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P. & Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat. Photon.* **7**, 378 (2013).
22. Huang, D., Huang, P., Lin, D. & Zeng, G. Long-distance continuous-variable quantum key distribution by controlling excess noise. *Sci. Rep.* **6**, 19201 (2016).
23. Zhang, Y. et al. Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. *Phys. Rev. Lett.* **125**, 010502 (2020).
24. 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).
25. Soh, D. B. S. et al. Self-referenced continuous-variable quantum key distribution protocol. *Phys. Rev. X* **5**, 041010 (2015).
26. Karinou, F. et al. Toward the integration of CV quantum key distribution in deployed optical networks. *IEEE Photon.Technol. Lett.* **30**, 650 (2018).
27. Eriksson, T. A. et al. Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels. *Commun. Phys.* **2**, 9 (2019).
28. Eriksson, T. A. et al. Wavelength division multiplexing of 194 continuous variable quantum key distribution channels. *J. Lightwave Technol.* **38**, 2214 (2020).
29. Wang, H. et al. Sub-Gbps key rate four-state continuous-variable quantum key distribution within metropolitan area. *Commun. Phys.* **5**, 162 (2022).
30. Ghorai, S., Grangier, P., Diamanti, E. & Leverrier, A. Asymptotic security of continuous-variable quantum key distribution with a discrete modulation. *Phys. Rev. X* **9**, 021059 (2019).
31. Lin, J., Upadhyaya, T. & Lütkenhaus, N. Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution. *Phys. Rev. X* **9**, 041064 (2019).
32. Denys, A., Brown, P. & Leverrier, A. Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. *Quantum* **5**, 540 (2021).
33. Li, Z., Zhang, Y.-C., Guo, H. User-defined quantum key distribution. Preprint at https://arxiv.org/abs/1805.04249 (2018).
34. Matsuura, T., Maeda, K., Sasaki, T. & Koashi, M. Finite-size security of continuous-variable quantum key distribution with digital signal processing. *Nat. Commun.* **12**, 252 (2021).
35. Blow, K. J., Loudon, R., Phoenix, S. J. D. & Shepherd, T. J. Continuum fields in quantum optics. *Phys. Rev. A* **42**, 4102 (1990).
36. Fabre, C. & Treps, N. Modes and states in quantum optics. *Rev. Mod. Phys.* **92**, 40 (2020).
37. Raymer, M. G. & Walmsley, I. A. Temporal modes in quantum optics: then and now. *Phys. Scr.* **95**, 064002 (2020).
38. Raymer, M. G., Li, Z. W. & Walmsley, I. A. Temporal quantum fluctuations in stimulated Raman scattering: coherent-modes description. *Phys. Rev. Lett.* **63**, 1586 (1989).
39. Loudon, R. *The Quantum Theory of Light: 3rd edn.* (Oxford University Press, New York, 2000).
40. Bachor, H.-A. & Ralph, T. C. *A Guide to Experiments in Quantum Optics: 3rd edn.* (Wiley-VCH, Berlin, 2019).
41. Collett, M. J., Loudon, R. & Gardiner, C. W. Quantum theory of optical homodyne and heterodyne detection. *J. Mod. Opt.* **34**, 881 (1987).
42. S.Alagha, N. & Kabal, P. Generalized raised-cosine filters. *IEEE Trans. Commun.* **47**, 989 (1999).
43. Hajomer, A. A. E. et al. Modulation leakage-free continuous-variable quantum key distribution. *npj Quantum Inf.* **8**, 136 (2022).
44. Derkach, I., Usenko, V. C. & Filip, R. Preventing side-channel effects in continuous-variable quantum key distribution. *Phys. Rev. A* **93**, 032309 (2016).
45. Derkach, I., Usenko, V. C. & Filip, R. Continuous-variable quantum key distribution with a leakage from state preparation. *Phys. Rev. A* **96**, 062309 (2017).

46. Pereira, J. & Pirandola, S. Hacking Alice's box in continuous-variable quantum key distribution. *Phys. Rev. A* **98**, 062319 (2018).
47. Jain, N. et al. Modulation leakage vulnerability in continuous-variable quantum key distribution. *Quantum Sci. Technol.* **6**, 045001 (2021).

ACKNOWLEDGEMENTS

This work was supported by the National Natural Science Foundation of China (Grants Nos. 62201012, 62001041, and 61531003), the China Postdoctoral Science Foundation (Grant No. 2020TQ0016), the Fundamental Research Funds of BUPT (Grant No. 2022RC08), and the Fund of State Key Laboratory of Information Photonics and Optical Communications (Grant No. IPOC2022ZT09).

AUTHOR CONTRIBUTIONS

All authors contributed to the scientific discussions and the theoretical developments of the study. Z.C. and Z.L. carried out the theoretical calculations, X.W. performed the simulation, Z.C. wrote the manuscript, and X.W., S.Y., Z.L., and H.G. provided revisions.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Correspondence and requests for materials should be addressed to Zhengyu Li or Hong Guo.