


FPGA-based microsystematic design of Gaussian modulation for continuous-variable quantum communication

Geng Chai^{1,2}, Yang Yuan,¹ Zhengwen Cao,^{1,2,*} Hao Yu,¹ Xinlei Chen,¹ and Jinye Peng¹

¹*Institute for Quantum Information and Technology, School of Information Science and Technology, Northwest University, Xi'an, 710127, China*

²*State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, 710071, China*

 (Received 8 November 2022; revised 26 April 2023; accepted 30 October 2023; published 17 November 2023)

Continuous-variable (CV) quantum communication is an important branch of quantum information technology and promises information-theoretical secure communication. High-performance and lightweight CV quantum devices are one of the keys to realizing quantum networks. Among them, the Gaussian-modulation module still has problems such as cumbersome photoelectric calibration and inconvenient use in the experimental stage, which introduces modulation noise and brings additional excess noise to the system, reducing the signal-to-noise ratio of the system and thus reducing system performance. To this end, by designing a field-programmable gate array and integrating all optical components (except the laser source), we achieved a miniaturized and low-cost Gaussian-modulation unit compatible with the existing fiber-optic communication infrastructure, realizing quantum signal modulation under adaptive photoelectric calibration. Taking CV quantum key distribution as the verification object, we analyzed the signal characteristics and the stability of the unit experimentally. The experimental results show that the proposed scheme exhibits quality Gaussian properties and correlations. Moreover, the temporal stability of the device is relatively high (the mean fluctuation is on the order of 10^{-31} and the variance fluctuation is 0.0363), which provides more possibilities for the subsequent popularization of quantum communication and the development of quantum information networks.

DOI: [10.1103/PhysRevApplied.20.054037](https://doi.org/10.1103/PhysRevApplied.20.054037)

I. INTRODUCTION

Quantum communication is an important branch of quantum information science and aims to use quantum states as information carriers for information interaction technology. Compared with traditional communication, it has incomparable advantages, and its security is guaranteed by quantum mechanics. The Heisenberg uncertainty theorem [1], the noncloning theorem [2], and the theorem of nonseparability of nonorthogonal quantum states in quantum mechanics can theoretically ensure the unconditional security of quantum communication [3,4]. Typical application forms of quantum communication include quantum key distribution (QKD) [5] and quantum secure direct communication (QSDC) [6,7].

QKD enables both parties to share a secret key through a quantum channel, which is the product of the combination of cryptography and quantum mechanics [5]. QSDC means that both parties use a quantum state as the information carrier and use a quantum channel to directly transmit a secret message safely [8]. In associated research, the early stage is based on discrete-variable

quantum signals. Much progress has also been made in related theories and experiments [9–14]. Because of the difficulty and high cost of preparing and detecting single photons in discrete-variable quantum communication systems, research on quantum communication based on continuous-variable (CV) quantum signals has begun to emerge.

Continuous-variable quantum communication systems are mainly embodied in CVQKD and CVQSDC. In 1999, the idea of CVQKD was proposed by Ralph [15], and it has attracted attention since then [15]. In 2002, Grosshans and Grangier [16] proposed the CVQKD protocol (GG02) based on a Gaussian-modulated coherent state and balanced homodyne detection, which was the first feasible CVQKD protocol under existing technical conditions and is currently the mainstream protocol. Subsequently, reverse reconciliation and entanglement equivalent models were successively proposed, which provided a more-comprehensive theoretical basis for experimental realization [17]. Thereafter, experiments with the GG02 protocol under the fiber channel and free space were realized. Among them, a scheme based on a fiber channel has made a bold attempt to realize an optical fiber network with CVQKD technology [18–20].

*caozhw@nwu.edu.cn

The preparation of CVQKD quantum states mainly includes the preparation of squeezed states, entangled states, and coherent states [16,21,22]. At present, the preparation and realization of the first two are more difficult, and so experimental research into systems based on coherent states is more extensive. In the field of QSDC, Quantum states can be prepared by semiconductor lasers in classical optical communication, followed by Gaussian modulation through optical modulators, and can then be detected by balanced homodyne detectors when received [23–26]. Meanwhile, CVQSDC can be well compatible with fully developed optical communication technology, which is also a big advantage of continuous-variable quantum communication [27,28]. In 2008, a coherent-state-based secure quantum direct communication scheme was proposed and its security was briefly discussed [29]. QSDC schemes based on a compressed state, a dual-mode compressed state, etc., have also been developed [30–32]. For QSDC, the introduction of continuous-variable forms makes research in this field more meaningful.

Gaussian modulation of a quantum signal is particularly important, so it is necessary to realize microsystematization, low cost, and high precision of the Gaussian-modulation unit. The modulation scheme uses cascaded amplitude modulators (AMs) and a phase modulator (PM) to load the control signal [24,33]. To stabilize the modulation, a feedback module needs to be added, so the structure is difficult to simplify. Inspired by the inherently bias-free drift of an AM, an amplitude and phase modulator was proposed that can achieve bias-free amplitude and phase modulation [34]. Later, a scheme using a ring structure to complete Gaussian modulation was proposed; it used two PMs, but the cost was still not controlled [35]. Furthermore, a scheme to realize Gaussian modulation based on a Sagnac loop and a PM was proposed; this increased the stability of Gaussian-modulated-coherent-state generation and reduced the implementation cost since only one PM is used [36].

However, it is worth noting that in existing research, the modulation module still needs to be tediously aligned with the optical and electrical signals, and the chopping is still highly dependent on the characteristics of the AM used to achieve pulse modulation before Gaussian modulation, and a microsystematic design has not yet been realized, which results in complex operation, high cost, limited accuracy, inconvenience, etc. Therefore, it is very necessary to realize the microsystematic design of a low-cost continuous-variable quantum signal modulation unit, aiming to complete the hardware platform with regard to high precision, low cost, microsystematization, and suitability for research and application of a CV quantum communication system.

In this work, a corresponding miniaturized experimental platform is designed that is based on a field-programmable gate array (FPGA), which needs only to connect the input

light source and the host computer to realize the transmission of optical signals, which achieves miniaturization and low cost of the device. The platform is mainly composed of a Universal Serial Bus (USB) communication block, an FPGA, a data-processing module, and an optical device. The unit is tested and verified mainly for the CVQKD system, mainly including functional verification and performance verification. Firstly, the module can achieve photoelectric adaptive calibration within 18.4 m. Secondly, the control signal can be processed with the 10% duty cycle, and then the detected output extinction ratio can reach 31.54 dB. Subsequently, the characteristics of the two control signals obey a uniform distribution and a Rayleigh distribution, respectively. Meanwhile, the transmitted and received signals both have Gaussian characteristics and have a high correlation of 0.97. Finally, temporal stability is verified; that is, the time average of the device fluctuates by an order of up to of 10^{-31} and the variance fluctuates by up to 0.0363, confirming that the device is stable over time. The unit is suitable for different continuous-variable quantum communication systems and can be adjusted according to needs. It provides more possibilities for low-cost, scalable, and lightweight quantum networks.

II. MICROSYSTEMATIC DESIGN OF GAUSSIAN MODULATION

A. System architecture

In CVQKD and CVQSDC systems, there are still problems such as separation of electro-optical design, cumbersome electro-optical synchronization, and a non-lightweight Gaussian-modulation unit. To solve the problem of cumbersome debugging in electro-optical intermodulation, we designed and built a microsystematized Gaussian-modulation unit (MGMU) based on an FPGA to realize the Gaussian-modulation function of continuous-variable quantum signals by systematizing the electro-optical part for electro-optical synchronization. The structure of the MGMU is shown in Fig. 1, and consists mainly of a USB communication block, an FPGA, and optical devices. The Gaussian-modulated optical signal can be output directly by feeding the MGMU with the host-computer sequence as input 1 and the laser-source signal as input 2.

The random sequence as input 1 from the host computer enters the USB communication module, which then generates packets that can communicate with the FPGA. Then, the FPGA can be used to parse the data to generate control signals for the optical modulator, as well as for electrical signal processing, data caching, and timing control. Input 2 represents the input continuous light source and relies on optical devices to generate the Gaussian-light-source signal. Finally, output 1 and output 2 can be subsequently transmitted to the quantum channel through multiplexing

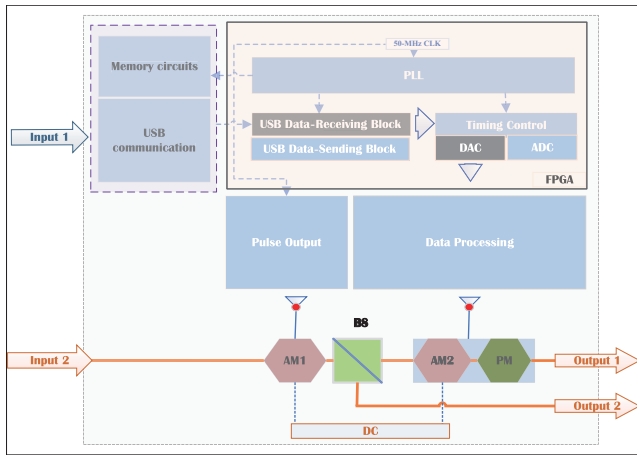


FIG. 1. Microsystematized Gaussian-modulation unit. Input 1 and input 2, respectively, represent the random sequence input by the host computer and the input light source with a wavelength of 1550 nm. Output 1 and output 2 refer to Gaussian signal light and local-oscillator light, respectively. BS, beam splitter; CLK, clock cycle; DC, direct-current power supply; PLL, phase-locked loop.

technology (time-division multiplexing and polarization multiplexing) for information transmission, or output 1 can also be directly sent to the channel for transmission.

Inside the FPGA, the USB data-receiving module is responsible for receiving, parsing, and sending the input random sequence to the timing-control module. Specifically, the timing-control module provides clock signals for data processing and sends data to the data-processing module. The pulse-signal output module provides pulse signals to the outside. The phase-locked loop converts the input 50-MHz clock into clock signals of different frequencies required by each module to drive each internal module. The 120-MHz clock is provided to the USB communication module, and the data-processing module is driven by an 80-MHz clock signal, which is maintained at a sampling rate of 2×10^6 samples per second.

The continuous pulse signal generated by the FPGA has the same frequency and synchronization as the control signal generated by the data-processing module. The pulse signal is then added to AM1 with a high extinction ratio. AM1 makes the power of the optical signal maximum at a high level and lowest at a low level, thereby generating an optical pulse signal where the high and low levels are a representation of voltage in digital circuits. High level indicates a state of high voltage, generally specified as 3.5–5 V; Low level indicates a state of low voltage, generally defined as 0~0.25 V. The optical pulse signal is split by a beam splitter (90:10), 10% of which is used for the generation of signal light and 90% of which is used as output 2. The control signal loaded onto AM2 can be circuit-modified internally by the FPGA to achieve the same duty cycle as the pulse signal to enhance extinction

and reduce light leakage. After loading, Gaussian modulation is completed together with the optical pulse generated by AM1 after 10% beam splitting to obtain output 1. Output 2, which can be used as local-oscillator (LO) light, is sent to the receiving end together with the quantum signal (i.e., the transmitted local oscillator scheme), which can be directly transmitted to the channel after multiplexing. Output 2 can also not pass through the channel. We directly generate LO light from the receiver Bob, which avoids all attacks on the LO light of the system (that is, the local local oscillator scheme).

The control part of acquisition of the data on Bob's side is also involved internally in the microsystemized design. The timing-control module within the FPGA ensures synchronization of sampling between the analog-to-digital conversion (ADC) and the digital-to-analogue conversion (DAC) when information is collected on Bob's side. At the same time, the ADC timing module implements two successive averaging filters on the ADC sampling results, which increases the immunity of the system, while maintaining synchronous sampling. In addition, a transmitter module within the USB communication module is designed to package the data received by the ADC module and send it to the host computer at Bob's end when the system is receiving.

B. Photoelectric adaptive calibration

In an actual platform, there is an optical path difference ΔL from the chopped optical pulse to AM2, which varies according to different-optical-path platforms.

There is a time delay Δt between the optical signal and the electrical signal when the modulation is realized,

$$\Delta t = \Delta L \frac{n}{c}, \quad (1)$$

where n is the refractive index in the fiber and c is the speed of light. In view of the different photoelectric delays corresponding to different platforms, and the inconvenience of adaptive and flexible calibration in the currently packaged Gaussian-modulation control unit, a photoelectric-adaptive-calibration scheme is proposed. After AM2 modulation, the output light field E_{out} is given by

$$E_{\text{out}} = E_{\text{in}} e^{i\Delta\phi} \cos\left(\frac{\alpha_1 + \alpha_2}{2} V\right), \quad (2)$$

where $\Delta\phi = [(\alpha_1 - \alpha_2)/2]V$ and $\alpha_1 + \alpha_2 = \pi/V_\pi$, where α_1 and α_2 are the phase coefficients of the two waveguides inside AM2, V_π is the half-wave voltage, and V is the voltage loaded on AM2—that is, $V = V(t) + V_b$, where $V(t)$ is the control signal loaded on AM2 and V_b is the bias voltage. It can be seen from the above that the corresponding

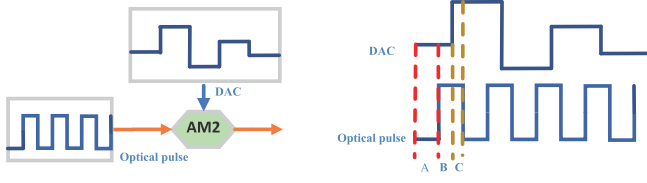


FIG. 2. The case where the optical and electrical signals are not calibrated. For state A, the control signal is loaded on a low-pass-rate optical pulse. For states B and C, different amplitudes of the control signal are loaded on the same high-pass-rate optical pulse. Here the amplitude of the control signal corresponding to state A is the same as that of state B but is not the same as that of state C. The horizontal coordinate refers to the time (nanoseconds). The vertical coordinate represents the voltage amplitude (millivolts).

output light intensity can be expressed as

$$I_{\text{out}} = \gamma \frac{I_{\text{in}}}{2} (\cos(\alpha_1 + \alpha_2) V + 1), \quad (3)$$

where γ is the correlation loss factor of AM2. If there is a delay, the uncalibrated light intensity corresponds to three types, as shown in Fig. 2.

Here we give three states of photoelectricity mismatch: A, B, and C. States A and B, respectively, represent the misalignment and the alignment of the control-signal amplitude and the high level of an optical pulse. State C refers to the amplitude of the next control signal loaded by the optical pulse due to misalignment. According to Fig. 2, the corresponding light-intensity formulas for states A, B, and C are obtained as follows:.

$$I_{\text{out}}^A = 0, \quad (4a)$$

$$I_{\text{out}}^B = \gamma \frac{I_{\text{in}}}{2} \left(\cos\left(\frac{\pi}{V_{\pi}} (V(t) + V_b)\right) + 1 \right), \quad (4b)$$

$$I_{\text{out}}^C = \gamma \frac{I_{\text{in}}}{2} \left(\cos\left(\frac{\pi}{V_{\pi}} (V(t + \Delta t) + V_b)\right) + 1 \right). \quad (4c)$$

The light field in the Δt segment of the optical-path delay is denoted by $E_{\text{out}}^C = E_{\text{in}} e^{i\Delta\phi} \cos((\pi/2)V_{\pi}(V(t + \Delta t) + V_b))$, and the corresponding light intensity is not equal to 0, $I_{\text{out}}^C \neq 0$, which will disturb the modulation result of the overall AM2. In response to this situation, the optical-path difference needs to be fed back to the inside of the FPGA, and then the electrical signal output is adjusted through the DAC timing-control module to achieve synchronization between the optical signal and the electrical signal and achieve $I_{\text{out}}^C = 0$. Then, we extract the desired I_{out}^B and complete the calibration verification with the chopped optical pulse. According to different adaptive schemes of photoelectric calibration, the function of the adjustable delay under different-optical-path platforms is realized. When implemented, different ΔL is reflected

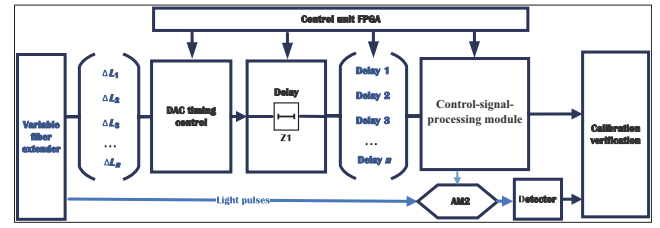


FIG. 3. Photoelectric self-adaptive calibration. Z1, resistance-capacitance time delay.

by addition of a variable optical fiber delay, and the self-adaptive calibration as shown in Fig. 3 can be completed on the basis of the FPGA.

The increased different ΔL values are fed back into the FPGA. Through its internal DAC timing-control module, the corresponding different delays are precisely controlled, which requires resistance-capacitance time delay Z1 to complete different delays. The data after timing control are sent to the control-signal processing module to realize the final processing of the data, which is specifically completed by the internal DAC module and the corresponding driving module. The RC time delay is used in the time-delay calibration, which can be precisely adjusted according to different optical-path differences. Subsequently, the control signal is loaded into AM2. Then the results of adaptive calibration are compared and verified. For ideal optical pulse modulation, if the pulse carrier is an impulse pulse sequence, the sampling theorem is the principle of pulse-amplitude modulation. Since the real impulse pulse train cannot be realized, the real impulse pulse can be realized only by a narrow pulse train. To be as close as possible to the ideal impulse pulse signal, the pulse signal and the control signal can be made at the same frequency on the basis of photoelectric calibration, so that the duty cycle can theoretically be infinitely reduced. The problem of the existing transmitting device is solved due to the mismatch between the code rate of the control signal and the frequency of the optical pulse, which is also convenient for subsequent ideal collection of data.

C. Data-processing module based on an FPGA

Inside the FPGA, the data are parsed and the timing is controlled. Then the data and the clock information parsed in the FPGA are sent to the data-processing block to complete the processing and then drive the optical device, as shown in Fig. 4.

The processing part consists of a DAC chip and a processing block to realize data conversion (digital-to-analog conversion). The converter is a dual-channel precision current-type multiplier digital-to-analog converter with an inverted-T-shaped R-2R resistor network as the core, a 16-bit DAC bit width, 0.5- μ s setup time, a reference voltage range up to ± 12 V, and a rated operating frequency of

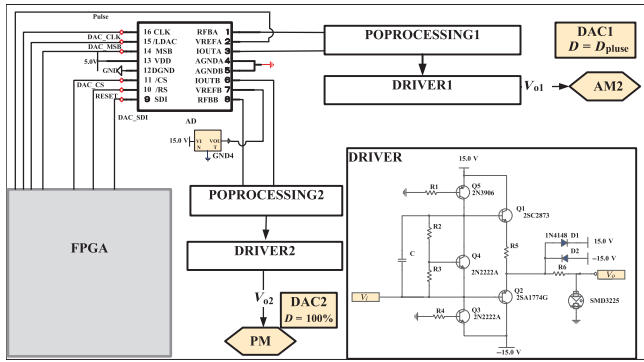


FIG. 4. Simplified design of the data-processing module based on an FPGA. POPPROCESSING converts the DAC output current signal into a voltage signal (0 to $\pm V_{ref}$), and through an inverse-proportional-amplifier circuit for driving the subsequent driver module. DRIVER processes the voltage signal to a voltage range that can drive the light modulator. Within DRIVER, V_i is the input voltage signal and V_o is the output drive voltage signal. C, capacitor; Q1–Q5, triodes; R1–R4, resistors; AD, digital to analog conversion chip; D1–D2, diode; D, duty cycle; SMD3225, gas discharge tube; GND, reference ground.

50 MHz. To meet the requirement that the control voltage in quantum communication is not less than the minimum driving voltage of the optical modulator, the drive-module DRIVER linear amplifier is designed to increase the driving power of the output signal. Therefore, a precision operational amplifier is used together with a push-free-type power-amplifier circuit, which has higher accuracy and smaller ripple voltage than a class-D amplifier. The whole system is then optimized by our controlling the duty cycle of the control signal loaded on AM2, which is named “DAC1.” When the optical path is implemented, the optical pulse signal may not be extinguished enough, resulting in a power residual at the position where the tuned signal should have been zero. Therefore, when the data-control block is being designed, the output control signal is pre-processed, as in Fig. 4, to synchronize the duty cycle of the optical pulse by introducing the pulse signal as V_{ref} into the DAC module so that the control signal DAC1 has the same duty cycle as the pulse signal to achieve Gaussian modulation while finishing the extinction at the Gaussian-modulator end.

III. RESULTS

A. Calibration verification

The optical-path difference can be changed by extending the optical fibers to different lengths. At the same time, the specific situation before and after calibration is detected and recorded to complete the inspection of adaptive calibration. Since the optical pulse is set to synchronize with the control signal at the same frequency, the duty cycle of the two can be compressed indefinitely.

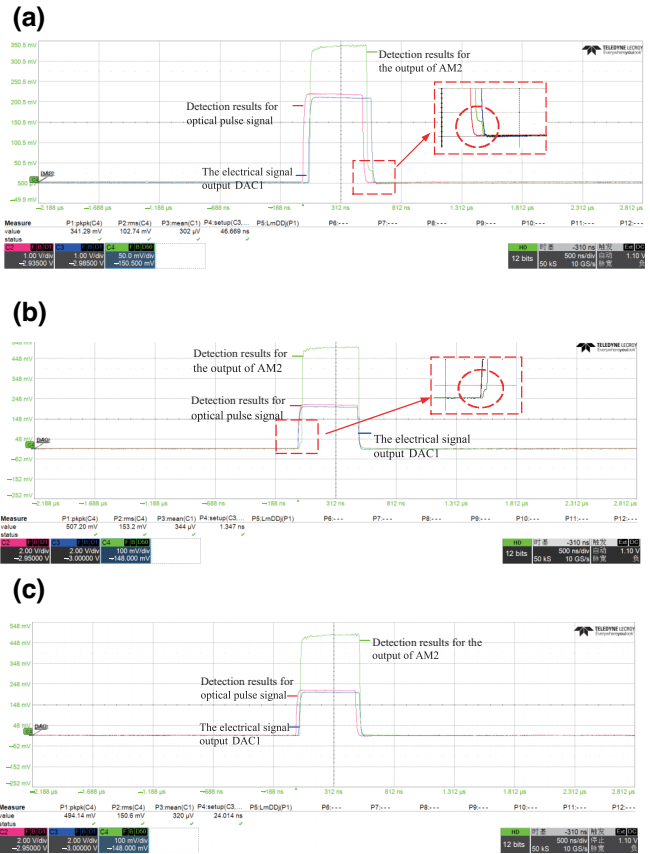


FIG. 5. Comparison of waveforms before and after adaptive calibration. (a),(b) Signals before calibration. (c) Result after calibration. The red line corresponds to the optical pulse signal and the blue line corresponds to the output DAC1. The green line corresponds to output optical signal of AM2, which fluctuates in a staircase manner. Theoretically, the larger the optical-path difference, the stronger the fluctuation.

For easy observation, the duty cycle is adjusted to 10%, and the signal detection results before and after calibration can be obtained from Fig. 5. It can be seen from the

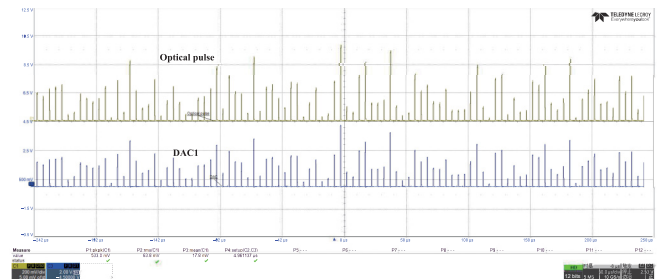


FIG. 6. Real-time waveform of optoelectronic signal after adaptive calibration. The lower trace corresponds to the control signal DAC1 and the upper trace corresponds to the modulated output optical signal. The change trend of the two is the same, and the AM2 output optical signal is stable, indicating complete calibration.

detection results for the front and rear optical signals that the optical signal before calibration will fluctuate. After calibration, the optical signal and the electrical signal are completely aligned, and the output waveform is stable. After adaptive calibration, the AM2 output results can be seen in Fig. 6.

To measure the calibrated boundary in the scheme, calibration verification is performed by our taking multiple sets of different sets of optical-path differences, starting from 0 m and then increasing the optical-path difference in 1-m intervals. At 19 m, the specific calibration result is no longer perfect (i.e., deviation begins), so the detection is performed with use of the idea of dichotomy and continuous recursion, and the boundary value of adaptive calibration is finally obtained to be about 18.4 m. When less than or equal to the boundary value, the actual calibration is consistent with the ideal calibration result, otherwise the calibrated delay reaches the upper limit and does not change, as shown in Fig. 7, where y_1 and y_2 refer to the ideal state and the actual situation, respectively, where the turning point in y_2 is at about 18.4 m.

B. Output verification

During data processing, the FPGA completes the data-parsing process of the original random sequence, timing control, analog-to-digital conversion, and driving the amplification process to output the pulse signal and the control signals DAC1 and DAC2 required by AM2 and the PM, respectively. Internally, to reasonably and sufficiently improve the extinction effect, a preprocessing process is introduced; that is, the pulse signal is introduced as the reference voltage signal V_{ref} of the converter

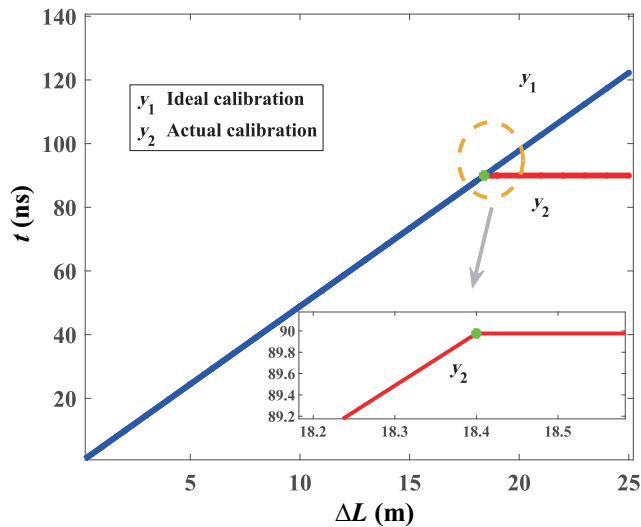


FIG. 7. Adaptive calibration results. y_1 , y_2 , and the green circle, respectively, refer to the agent’s desired calibration result, the actual calibration result, and the actual calibration limit.

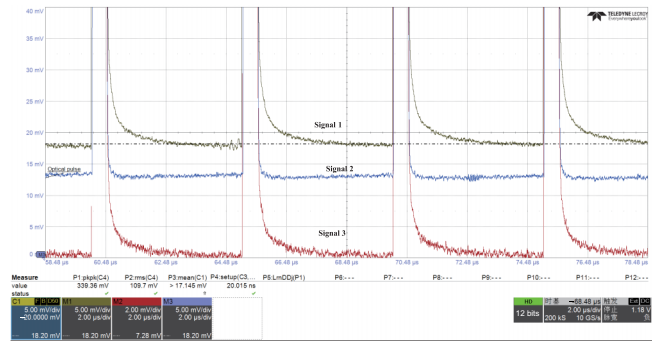


FIG. 8. Output optical pulse (signal 1) of AM1 and signals (signals 2 and 3) output by AM2, for which the duty ratios are uncompressed and 10%, respectively.

to synchronize the duty cycle of the optical pulse, so that the cascaded Gaussian modulator can not only complete Gaussian modulation but can also achieve extinction. After addition of the pulse and control signals to AM1 and AM2, respectively, the output is detected and verified. Before this, the control signals before and after optimization were loaded on AM2 to photomeasure its output, while we kept AM1 loading the pulse signal unchanged and measured the output; the specific results are shown in Fig. 8.

The AM1 chopper output is detected to get signal 1, which should have had a millivolt signal at zero pass rate, and the actual extinction ratio is about 18.20 dB. Signal 2 is the result of AM2 output detection in traditional cascade modulation, and its extinction effect after cascade is slightly improved, but there is still residual optical signal, which will pose a threat to signal light. Signal 3 is then obtained by our loading the optimized control signal DAC1 and probing the output of AM2, which has an amplitude of nearly 0 at low levels compared with signals 1 and 2. The extinction ratio can reach 31.54 dB at this time, indicating that the extinction effect has been improved, which provides a certain guarantee for the safe and accurate transmission of the subsequent overall system signal. In summary, the optimization of the scheme allows AM2 in Gaussian modulation to complete further chopping while achieving modulation.

When the output of the modulation unit is being validated, it is also necessary to analyze and verify the overall characteristics as well as the partial output data characteristics. Firstly, we verify DAC1 and DAC2 added to the upper ends of AM2 and the PM by sending 3000 groups of corresponding random numbers from the host computer. The waveforms and characteristics are shown in Fig. 9.

When the output of the modulation unit is being verified, a frame of data needs to be sent, and then the detection light signal is detected by the detector. The frame head and frame tail are positioned, and a frame is collected every 20 min. The sample is X_p^i and its size is 1000; that

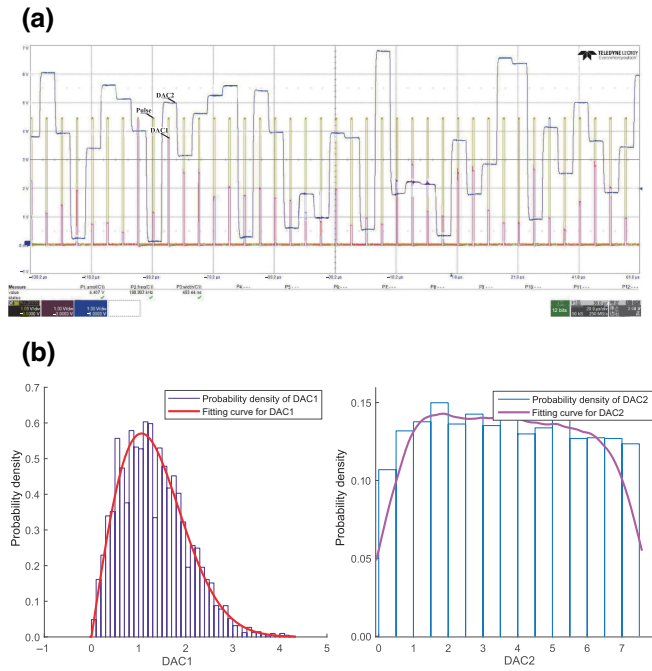


FIG. 9. Output results for the control signal. DAC1 and DAC2 in (a) refer to control signals loaded on AM2 and the PM, respectively, and their characteristic distributions are a Rayleigh distribution and a uniform distribution, respectively, as shown in (b). The unit of abscissa in (b) is millivolts.

is, X_p^i ($p = 1-1000$). The collected dataset is $X = \{X_i\} = \{X_1, X_2, \dots, X_n\}$, where $n = t/20$ min, where t is the total measurement time and n groups are collected here. Characteristic analysis and verification of the data collected every 60 min are performed by means of the Kolmogorov-Smirnov (K-S) test [37], the Shapiro-Wilk (S-W) test [38], the Jarque-Bera (J-B) test [39], and the quantile-quantile (Q-Q) plot [40].

The detection results of the K-S test, the S-W test, the J-B test, and the Q-Q plot are given in Table I. Firstly, we make the assumption M: the sample data conform to a Gaussian distribution. Then, we calculate the significance p for the K-S test, and accept the hypothesis M if $p > 0.05$. To meet the data-length requirements of the S-W test, the samples need to be tested in groups; that is, $m = X/n$ (m is the total number of subsamples after division and n is the size that should be controlled between 3 and 50). Here the significance p for the S-W test is calculated, and if $p > 0.05$, the test is passed, and finally the success rate of m groups of subsamples is counted. For the J-B test, if the variable follows a Gaussian distribution, the skewness is 0, the kurtosis is 3, and the value of the J-B statistic h is 0, otherwise h is a gradually increasing value. A dummy variable r is used to indicate whether the Q-Q plot satisfies the linear characteristics. If it does, $r = 1$, otherwise it is 0.

After output of the modulation unit has been ensured that the module conforms to Gaussian characteristics, it

TABLE I. Feature verification at different times. r is used to indicate whether the fitted result is linear or not linear. If it is linear, it is represented by 1, otherwise it is represented by 0. $p = 0.200^*$ means the lower bound of true significance, $p > 0.05$.

i ($i = \frac{t}{60}$)	K-S test (p)	S-W test (success rate)	J-B test (h)	Q-Q plot (r)
1	0.200*	0.94	0	1
2	0.200*	0.92	0	1
3	0.200*	0.96	0	1
4	0.200*	0.92	0	1

is sent to the receiver through the channel. The signal is collected from the receiving end, and then the data relationship between Alice and Bob is drawn as shown in Fig. 10.

Alice’s data and Bob’s data directly obey a linear model, such as in the inset in the plot on the left in Fig. 10. We randomly select any piece of Alice’s data, corresponding to all possible data of Bob under the same length, and then calculate the correlation coefficient and draw the correlation diagram. When the positions correspond, the correlation is the largest, and the correlation coefficient is about 0.97. The correlation coefficients of other positions are close to 0, indicating that Alice’s data and Bob’s data have high correspondence.

Finally, the stability of the entire device must also be considered. The characteristics of the transmitted signal

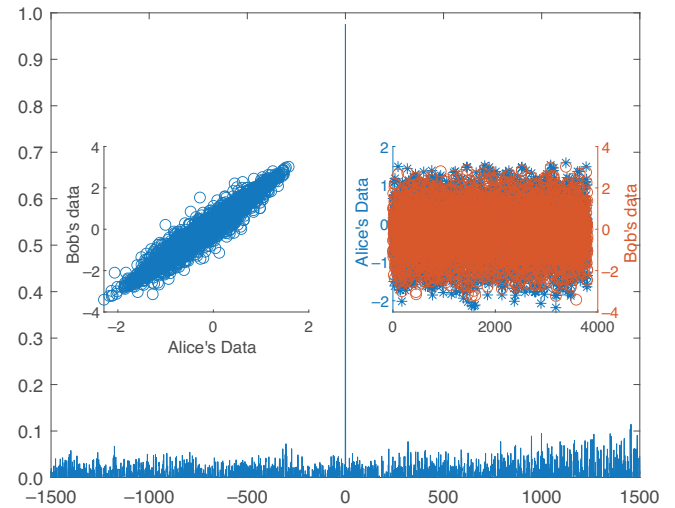


FIG. 10. Correlation between Alice’s data and Bob’s data where the horizontal axis represents the delay between Alice and Bob data points, the vertical axis represents the correlation between data points. The inset on the left represents the data relationship between Alice and Bob. The inset on the right is a real-time display of the sender’s data and the receiver’s data where the horizontal axis represents the data point.

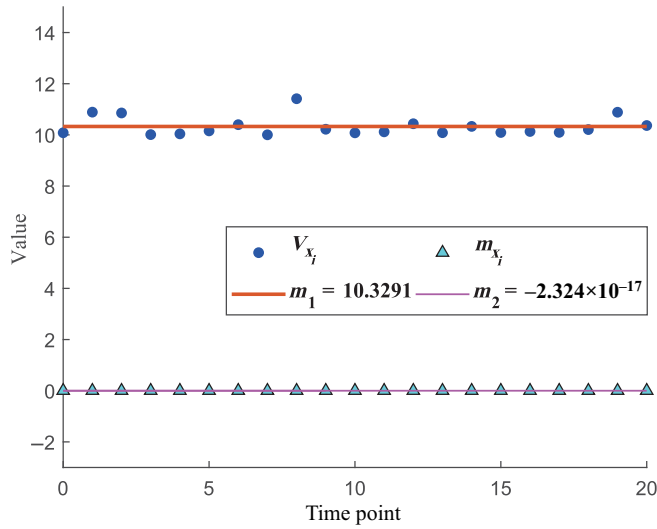


FIG. 11. Time stability of the system performance where the unit of ordinate is shot noise unit. The time interval is 20 min. The triangular distribution represents the change in the mean of the samples collected at different times, and the lower line represents the mean of this change. The dot distribution represents the change in sample variance over time, and the upper line represents the central tendency of this change.

over time still need to be analyzed. The X_i all obey the Gaussian distribution, and the changes of the mean and variance over time can reflect the time-stable characteristics according to the equations

$$m_{X_i} = \frac{1}{p} \left(\sum_1^p X_{i_p} \right), \quad (5a)$$

$$V_{X_i} = \frac{1}{p} \left(\sum_1^p (X_{i_p} - m_{X_i})^2 \right). \quad (5b)$$

The mean and variance of each $\{m_{x_1}, m_{x_2}, \dots, m_{x_n}\}$ and $\{V_{x_1}, V_{x_2}, \dots, V_{x_n}\}$ are obtained, and Fig. 11 is drawn. As the system running time increases, we get

$$m_1 = \frac{1}{n} \sum_1^n V_{X_i} = 10.329, \quad (6a)$$

$$\sigma_1 = \left(\frac{1}{n} \sum_1^n (V_{X_i} - m_1)^2 \right)^{\frac{1}{2}} = 0.3751, \quad (6b)$$

$$C_v = \frac{\sigma_1}{m_1} = 0.0363, \quad (6c)$$

where m_1 represents the central tendency of all variances, and the volatility of the data variance is 0.0363. In data statistics and analysis, the larger the coefficient of variation, the stronger the discreteness of the data, and the more

unstable the data will be. This means that the data difference is small if coefficient of variation is less than 5%. Similarly, the variation characteristics of the mean value of the data can be calculated, $m_2 = -2.324 \times 10^{-17}$. Since this is close to 0, the volatility can be directly represented by the mean square error, which is about 2.116×10^{-31} . The magnitude of the data mean fluctuation over time is 10^{-31} , and it can be approximately considered that the volatility of the data mean is 0 (i.e., the data mean is stable over time). Therefore, the data characteristics of the output of the MGMU at different times are stable and in line with expectations.

C. System-performance analysis

The method of chopping extinction is improved in the scheme, which increases the extinction ratio of the signal, improves the anti-interference of the signal, and strengthens the robustness of the transmission system. In addition, because of the support of adaptive photoelectric calibration, Alice and Bob can send and receive signals synchronously at the same frequency, which makes the system duty cycle controllable and has good synchronization characteristics when receiving. The following analysis is performed in accordance with the above description.

Firstly, if there is calibration inaccuracy, the code rate R used by Bob in the reconciliation and error correction phase will be reduced, making the reconciliation efficiency β decrease under decrease under certain C_{channel} according to $\beta = R/C_{\text{channel}}$, and thus the key rate will eventually decrease. Additionally, the improvement of the extinction effect through circuit modification will reduce the leakage of residual photons between the LO and the signal light, which affects the signal light by an order of magnitude, resulting in excess noise ε that cannot be ignored. The effect is reduced to a certain extent by the improved solution, making the overall system excess noise ε smaller. According to Eq. (7), the improved solution reduces ε , so the signal-to-noise ratio (SNR) is increased:

$$\text{SNR} = \frac{T\eta V_A N_0}{N_0 + T\eta\varepsilon + v_{\text{el}}} = \frac{T\eta V_A}{1 + \frac{T\eta\varepsilon + v_{\text{el}}}{N_0}}, \quad (7)$$

where V_A is the modulation variance, N_0 is the shot noise, and v_{el} is the electrical noise.

Furthermore, if sufficient extinction is not achieved during the experiment, the average intensity of the LO light will be too high, which will lead to the measured shot noise N_0 being too large, thus reducing the SNR. In summary, the overall CVQKD system with the proposed scheme increases the SNR to a certain extent. For CVQKD, which usually measures system performance in terms of K , if there is an erroneous frame, the entire frame will be discarded in the postprocessing stage, so the actual key rate

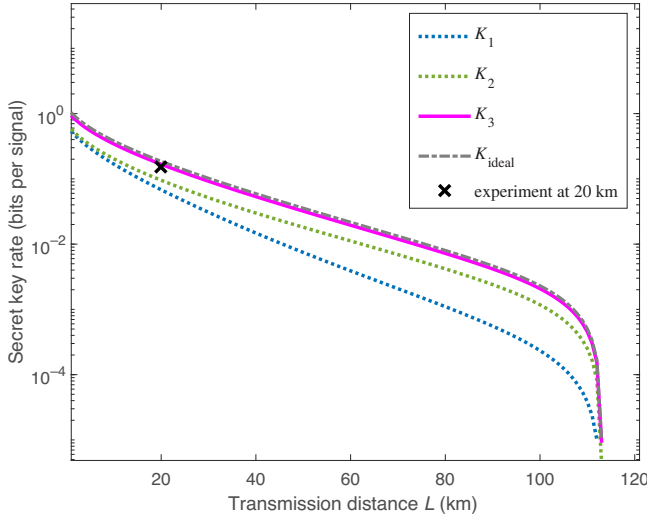


FIG. 12. Key-rate curve of the CVQKD system under the improved scheme. K_1 is the key rate without photoelectric calibration, K_2 is the key rate without improved extinction ratio, and K_3 is the key rate of the proposed scheme.

can be expressed as

$$K_{\text{actual}} = (1 - P_e(R, \text{SNR}))(\beta I_{AB} - \chi_{BE}), \quad (8)$$

where I_{AB} is the Shannon mutual information of Alice and Bob, χ_{BE} is the maximum of the Holevo information that Eve can obtain from information from Bob $P_e(\cdot)$ is the frame error rate at R and the error function concerning the SNR as seen in the following equation:

$$P_e(\cdot) = \frac{1}{2}[1 - \text{erf}(k \times \sqrt{\text{SNR}})], \quad (9)$$

where $\text{erf}(\cdot)$ is the error function and $k > 0$, where k is determined by different coding in postprocessing. $P_e(\cdot)$ decreases with increasing SNR in this scheme, which further increases communication quality.

To sum up, the key-rate curves under different conditions are analyzed and plotted in Fig. 12, which shows that the key rate K_1 without the microsystemization is the lowest overall and differs considerably from the ideal case, K_{ideal} . With the completion of the adaptive calibration, the efficiency of the negotiations undertaken by the system increases and the accuracy of the data becomes higher, resulting in improved performance of the overall solution as shown in K_2 , but also showing that the key rate of the system is easily overestimated when it is not calibrated. Moreover, the circuit modification in the proposed scheme not only increases the SNR by increasing the extinction ratio but also increases the identification accuracy at the receiver side, thus allowing the overall improved scheme to be optimized again after calibration has been achieved, as can be seen in the K_3 curve. The specific parameters

involved in the realization of Fig. 12 are $V_A = 10$, $\eta = 0.6$, $v_{\text{el}} = 0.01$, $R = 0.5$, and $k = 1/\sqrt{2}$, and the data block is 10^{11} .

Compared with traditional cascade modulation, this scheme can reduce the number of AMs and reduce the control cost to a certain extent.

IV. CONCLUSION

A Gaussian-modulation module is the core component in a continuous-variable quantum communication system, and its performance is closely related to the characteristics of the system. However, in the current Gaussian-modulation module for continuous-variable quantum communication, there are still problems such as cumbersome photoelectric calibration, unstable performance, and a nonlightweight device. In this regard, a microsystematic design scheme for a Gaussian-modulation module for continuous-variable quantum communication based on an FPGA is proposed, aiming to realize a microsystematic and high-performance Gaussian-modulation module. On the one hand, the module involved has adaptive optoelectronic calibration, which is achieved by feedback for different distance differences. Subsequently, on the basis of the calibration results, the duty cycle of the optical pulse signal is theoretically compressed infinitely, paving the way for subsequent ideal sampling. On the other hand, the processing and output of the core-control-module data play a driving role to increase the system extinction ratio and reduce the dependence on the chopping-phase AM in the local LO scheme by adjusting the control-signal DAC1 duty cycle.

In the experimental validation, we firstly find that the limit of adaptive calibration of the MGMU is 18.4 m, within which adaptive calibration can be fully realized. Secondly, a 10% duty cycle is used for the DAC, and then the output extinction ratio after detection is changed from 18.2 to 31.54 dB, with a significant extinction effect. Subsequently, the data characteristics are analyzed, in which the characteristics of the two control signals obey a uniform distribution and a Rayleigh distribution, respectively. At the same time, the Gaussian characteristics of the data collected at 20-min intervals are verified by the K-S test, the S-W test, the J-B test, and the Q-Q plot. Also, it is verified that the received signals have Gaussian characteristics and the correlation between the transmitted and received signals is high at 0.97. Finally, temporal stability is verified, with time mean of the device fluctuating by order of up to an of 10^{-31} and with the variance fluctuating by 0.0363, confirming that the device is stable over time. The designed microsystematic Gaussian-modulation module is stable and compatible with the existing fiber-optic-communication infrastructure, providing more possibilities for the development of high-performance and microsystematic CV quantum communication systems,

and further facilitating the construction of communication networks.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China (Grants No. 62071381 and No 62301430), the Shaanxi Provincial Key R&D Program General Project (Grant No. 2022GY-023), the Scientific Research Plan Project of Shaanxi Education Department (Natural Science Special Project, Grant No. 23JK0680), the Young Talent Fund of Xi'an Association for Science and Technology (Grant No. 959202313011), and the 23rd Open Project of the State Key Laboratory of Integrated Services Networks (Xidian University) (Grant No. ISN23-06).

-
- [1] Jang Young Bang and Micheal S. Berger, Quantum mechanics and the generalized uncertainty principle, *Phys. Rev. D* **74**, 125012 (2006).
- [2] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, *Nature* **299**, 802 (1982).
- [3] Ao Shen, Bo Du, Ze Hao Wang, Yang Dong, Xiang Dong Chen, Guang Can Guo, and Fang Wen Sun, Indistinguishability-induced classical-to-nonclassical transition of photon statistics, *Phys. Rev. A* **95**, 053851 (2017).
- [4] Stefano Pirandola, Ulrik L. Andersen, Leonardo Banchi, Mario Berta, Darius Bunandar, Roger Colbeck, Dirk Englund, Tobias Gehring, Cosmo Lupo, Carlo Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in quantum cryptography, *Adv. Opt. Photonics* **12**, 1012 (2020).
- [5] Charles H. Bennett and Gilles Brassard, Quantum cryptography: Public key distribution and coin tossing, *Theor. Comput. Sci.* **560**, 7 (2014).
- [6] Gui-Lu Long and Xiao-Shu Liu, Theoretically efficient high-capacity quantum-key-distribution scheme, *Phys. Rev. A* **65**, 032302 (2002).
- [7] Fu-Guo Deng, Gui Lu Long, and Xiao-Shu Liu, Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block, *Phys. Rev. A* **68**, 042317 (2003).
- [8] Yu-Bo Sheng, Lan Zhou, and Gui-Lu Long, One-step quantum secure direct communication, *Sci. Bull.* **67**, 367 (2022).
- [9] Wei Zhang, Dong-Sheng Ding, Yu-Bo Sheng, Lan Zhou, Bao-Sen Shi, and Guang-Can Guo, Quantum secure direct communication with quantum memory, *Phys. Rev. Lett.* **118**, 220501 (2017).
- [10] Feng Zhu, Wei Zhang, Yubo Sheng, and Yidong Huang, Experimental long-distance quantum secure direct communication, *Sci. Bull.* **62**, 1519 (2017).
- [11] Haoran Zhang, Zhen Sun, Ruoyang Qi, Liuguo Yin, Gui-Lu Long, and Jianhua Lu, Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states, *Light: Sci. Appl.* **11**, 83 (2022).
- [12] Jia-Wei Ying, Lan Zhou, Wei Zhong, and Yu-Bo Sheng, Measurement-device-independent one-step quantum secure direct communication, *Chin. Phys. B* **31**, 120303 (2022).
- [13] Lan Zhou, Bao-Wen Xu, Wei Zhong, and Yu-Bo Sheng, Device-independent quantum secure direct communication with single-photon sources, *Phys. Rev. Appl.* **19**, 014036 (2023).
- [14] Lan Zhou and Yu-Bo Sheng, One-step device-independent quantum secure direct communication, *Sci. China Phys. Mech. Astron.* **65**, 250311 (2022).
- [15] T. C. Ralph, Continuous variable quantum cryptography, *Phys. Rev. A* **61**, 010303 (1999).
- [16] Mark Hillery, Quantum cryptography with squeezed states, *Phys. Rev. A* **61**, 022309 (2000).
- [17] Stefano Pirandola, Raul García-Patrón, Samuel L. Braunstein, and Seth Lloyd, Direct and reverse secret-key capacities of a quantum channel, *Phys. Rev. Lett.* **102**, 050503 (2009).
- [18] Frédéric Grosshans, Gilles Van Assche, Jérôme Wenger, Rosa Brouri, Nicolas J. Cerf, and Philippe Grangier, Quantum key distribution using Gaussian-modulated coherent states, *Nature* **421**, 238 (2003).
- [19] Jérôme Lodewyck, Thierry Debuisschert, Rosa Tualle-Brouri, and Philippe Grangier, Controlling excess noise in fiber-optics continuous-variable quantum key distribution, *Phys. Rev. A* **72**, 050303 (2005).
- [20] Tobias A. Eriksson, Benjamin J. Puttnam, Georg Rademacher, Ruben S. Luis, Masahiro Takeoka, Yoshinari Awaji, Masahide Sasaki, and Naoya Wada, in *2019 Optical Fiber Communications Conference and Exhibition (OFC)* (IEEE, 2019), p. 1.
- [21] Margaret D. Reid, Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations, *Phys. Rev. A* **62**, 062308 (2000).
- [22] Frédéric Grosshans and Philippe Grangier, Continuous variable quantum cryptography using coherent states, *Phys. Rev. Lett.* **88**, 057902 (2002).
- [23] Duan Huang, Jian Fang, Chao Wang, Peng Huang, and Gui-Hua Zeng, A 300-MHz bandwidth balanced homodyne detector for continuous variable quantum key distribution, *Chin. Phys. Lett.* **30**, 114209 (2013).
- [24] Paul Jouguet, Sébastien Kunz-Jacques, Anthony Leverrier, Philippe Grangier, and Eleni Diamanti, Experimental demonstration of long-distance continuous-variable quantum key distribution, *Nat. Photonics* **7**, 378 (2013).
- [25] Yichen Zhang, Zhengyu Li, Ziyang Chen, Christian Weedbrook, Yijia Zhao, Xiangyu Wang, Yundi Huang, Chunchao Xu, Xiaoxiong Zhang, and Zhenya Wang, Continuous-variable QKD over 50 km commercial fiber, *Quantum Sci. Technol.* **4**, 035006 (2019).
- [26] Yichen Zhang, Ziyang Chen, Stefano Pirandola, Xiangyu Wang, Chao Zhou, Binjie Chu, Yijia Zhao, Bingjie Xu, Song Yu, and Hong Guo, Long-distance continuous-variable quantum key distribution over 202.81 km of fiber, *Phys. Rev. Lett.* **125**, 010502 (2020).
- [27] Zhenju Feng, Jinxiaand Wan, Yuanji Li, and Kuanshou Zhang, Generation of 8.3 dB continuous variable quantum entanglement at a telecommunication wavelength of 1550 nm, *Laser Phys. Lett.* **15**, 015209 (2017).
- [28] Zhengwen Cao, Lei Wang, Kexin Liang, Geng Chai, and Jinye Peng, Continuous-variable quantum secure direct

- communication based on Gaussian mapping, *Phys. Rev. Appl.* **16**, 024012 (2021).
- [29] S. Pirandola, S. L. Braunstein, S. Mancini, and S. Lloyd, Quantum direct communication with continuous variables, *Europhys. Lett.* **84**, 20013 (2008).
- [30] Guan Yu Wang, Tao Li, Qing Ai, Ahmed Alsaedi, Tasawar Hayat, and Fu Guo Deng, Faithful entanglement purification for high-capacity quantum communication with two-photon four-qubit systems, *Phys. Rev. Appl.* **10**, 054058 (2018).
- [31] Peng Liang Guo, Tao Li, Qing Ai, and Fu Guo Deng, Self-error-rejecting quantum state transmission of entangled photons for faithful quantum communication without calibrated reference frames, *Europhys. Lett.* **127**, 60001 (2019).
- [32] S. Srikara, Kishore Thapliyal, and Anirban Pathak, Continuous variable direct secure quantum communication using Gaussian states, *Quantum Inf. Process.* **19**, 132 (2020).
- [33] Duan Huang, Peng Huang, Dakai Lin, and Guihua Zeng, Long-distance continuous-variable quantum key distribution by controlling excess noise, *Sci. Rep.* **6**, 19201 (2016).
- [34] Bing Qi and CharlesCiWen Lim, Noise analysis of simultaneous quantum key distribution and classical communication scheme using a true local oscillator, *Phys. Rev. Appl.* **9**, 054008 (2018).
- [35] Xiunan Sun and Hao Liang, Design of Gaussian modulator for continuous-variable quantum key distribution, *Opt. Eng.* **61**, 014101 (2021).
- [36] Huanxi Zhao, Huasheng Li, Yuehan Xu, Peng Huang, Tao Wang, and Guihua Zeng, Simple continuous-variable quantum key distribution scheme using a Sagnac-based Gaussian modulator, *Opt. Lett.* **47**, 2939 (2022).
- [37] Frank J. Massey, Jr., The Kolmogorov-Smirnov test for goodness of fit, *J. Am. Stat. Assoc.* **46**, 68 (1951).
- [38] Samuel Sanford Shapiro and Martin B. Wilk, An analysis of variance test for normality (complete samples), *Biometrika* **52**, 591 (1965).
- [39] Carlos M. Jarque and Anil K. Bera, Efficient tests for normality, homoscedasticity and serial independence of regression residuals, *Economics Lett.* **6**, 255 (1980).
- [40] Du-Ming Tsai and Cheng-Hsiang Yang, A quantile–quantile plot based pattern matching for defect detection, *Pattern Recognit. Lett.* **26**, 1948 (2005).