mathematics

MDPI

Article

Microwave-Enabled Two-Step Scheme for Continuous Variable Quantum Communications in Integrated Superconducting

Yun Mao [1,2,†], Lei Mao [2,†], Wanyi Wang [2,†], Yijun Wang [2,*], Hang Zhang [2,*] and Ying Guo [2]

[1] College of Information Science and Engineering, Provincial Key Laboratory of Informational Service for Rural Area of Southwestern Hunan, Shaoyang University, Shaoyang 422000, China
[2] School of Automation, Central South University, Changsha 410083, China
* Correspondence: xxywyj@sina.com (Y.W.); zhang22@csu.edu.cn (H.Z.)
† These authors contributed equally to this work.

Abstract

Quantum secure direct communication (QSDC) is convenient for the direct transmission of secure messages without requiring a prior key exchange by two participants, offering an elegant advantage in transmission security. The traditional implementations usually focus on the discrete-variable (DV) system, whereas its continuous-variable (CV) counterpart has attracted much attention due to its compatibility with existing optical infrastructure. In order to address its practical deployment in harsh environments, we propose a microwave-based scheme for the CV-QSDC that leverages entangled microwave quantum states through free-space channels in cryogenic environments. The two-step scheme is designed for the secure direct communication, where the classical messages can be encoded by using Gaussian modulation and then transmitted via displacement operations on microwave quantum states. The data processing procedures involve microwave entangled state generation, channel detection, parameter estimation, and so on. Simulation results demonstrate the feasibility of the microwave-based CV-QSDC, highlighting its potential for secure communication in integrated superconducting and solid-state quantum technologies.

Keywords: quantum secure direct communication; quantum communications; quantum cryptography

MSC: 81P94; 81P45

check for updates

Academic Editors: Chia-Wei Tsai, Chun-Wei Yang and Narn Yih Lee

Received: 29 July 2025
Revised: 11 September 2025
Accepted: 8 October 2025
Published: 12 October 2025

Citation: Mao, Y.; Mao, L.; Wang, W.; Wang, Y.; Zhang, H.; Guo, Y. Microwave-Enabled Two-Step Scheme for Continuous Variable Quantum Communications in Integrated Superconducting. *Mathematics* **2025**, *13*, 3263. https://doi.org/10.3390/math13203263

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Quantum communication, which has the advantage of compatibility in signal preparations [1,2], has been proposed for secure communications with two participants. With the popularization of quantum communication, however, the demand for quantum secure direct communication (QSDC) has increased since it can directly transmit the deterministic messages, unlike quantum key distribution (QKD), which is usually used for key exchange between legal participants. This unique paradigm not only inherently mitigates the risk of information leakage during key management but also streamlines the overall communication architecture [3,4], presenting a novel pathway for highly secure information exchange.

The traditional QSDC was predominantly focused on discrete-variable (DV) systems, where theoretical frameworks and experimental validations advanced in parallel. The pioneering two-step scheme [5] and the one-time-pad scheme [6] established the fundamental QSDC. Subsequently, more sophisticated schemes emerged, such as high-dimensional

QSDC based on quantum dense coding [7]. These schemes ensure security by encoding secret information directly onto quantum states, thereby restricting an eavesdropper's ability to access multiple entangled states simultaneously. Furthermore, the measurement-device-independent (MDI) QSDC [8,9] suggested potential security vulnerabilities in physical devices. In addition, the device-independent (DI) QSDC offers a solution to photon loss and decoherence [10], providing a viable path toward secure communication over noisy and lossy quantum channels.

The traditional QSDC was the discrete variable (DV) QSDC [5,6] since it uses a single photon for the signal single-photon source and a single-photon detector for detection. In contrast to the DV systems, the continuous-variable (CV) counterparts exhibit an advantage for the practical deployment, primarily due to their high compatibility with existing optical communication infrastructure [11,12]. In 2008, Pirandola suggested the first CV-QSDC protocol using coherent states, pioneering the use of continuous variables for information encoding and performance analysis [13]. It employs continuous light for the signal source and uses either a homodyne detector or heterodyne detector for detection. It presents an advantage since it can be carried out by using the existing optical communication technology, resulting in good compatibility and usability. However, implementations of CV-QSDC have been concentrated almost exclusively within the optical frequency domain.

Fortunately, leveraging a natural synergy with superconducting quantum computing platforms, microwave quantum communication may hold immense potential, whereas research for QSDC within this domain has remained relatively unexplored. Motivated by structure characteristics of the CV-QSDC, we addresses this gap by proposing a microwave-based scheme designed for CV-QSDC with the microwave frequency band and operation in cryogenic environments. The feasibility of our approach is underscored by recent breakthroughs in CV-QKD [14] and quantum teleportation (QT) of microwave states [15]. These accomplishments provide the technological foundation for realizing the microwave-based CV-QSDC under the realized cryogenic conditions.

The CV-QSDC presented herein utilizes microwave quantum states as its resource and is tailored for cryogenic operation. We employ Gaussian mapping to represent secret information as a sequence of Gaussian random numbers, which are then encoded onto a microwave quantum state with a displacement operation. In order to establish an implementation of CV-QSDC with microwave states, we divide the initial messages into many pieces, which are then transmitted with the two-step scheme through free space in cryogenic environments, with the aim of performance demonstration with parameter estimation. The legal participants can recover the initial messages only if they cooperate together. The microwave-based CV-QSDC can provided compatibility with the traditional optical CV-QSDC infrastructure in terms of noise immunity and losses.

The remainder of this paper is organized as follows. Section 2 details our proposed CV-QSDC scheme, covering the generation of microwave entangled states and the protocol's implementation. Section 3 presents the process of parameter estimation and provides a security analysis of the scheme. Finally, Section 4 offers a summary and conclusion of our work.

2. The Microwave-Based CV-QSDC

2.1. Two-Step CV-QSDC Protocol

As shown in Figure 1, the details of the two-step CV- QSDC protocol are demonstrated. Without loss of generality, the first and second free space channels have the same channel parameters in the cryogenic condition (e.g., transmittance and thermal noise). The sender, Alice, generates and sends the microwave-based Einstein–Podolsky–Rosen (M-EPR) states

through the cryogenic free space, to the receiver, Bob. The microwave-based scheme for the CV-QSDC can be designed as follows.

Step 1 (S1): Preparation of M-EPR states. Alice prepares an ordered sequence of the M-EPR pairs, as shown in Figure 1, which includes two mode sequences as sources. One sequence is used for channel detection, called the mode D sequence. The other remaining sequence of the EPR partner modes is used for message transmission, called the mode M sequence.

Step 2 (S2): Transmission of the mode D sequence. The mode D sequence is sent from Alice to Bob through the first cryogenic channel that could be used for channel detection. Bob randomly selects modes and measures both quadratures with a heterodyne detector. After Bob informs Alice of the positions of the measured modes and his measurement results, Alice conducts the same measurement on the corresponding partner modes in the mode M sequence and estimates the channel parameters.

Step 3 (S3): Transmission of the mode M sequence. Alice encodes the mode M sequence corresponding to the divided messages, which are encoded and transmitted to Bob through the second cryogenic channel with the same channel parameters.

Step 4 (S4): Channel detection. After Bob receive the M sequence, he performs the Bell measurement while combining it with the corresponding mode D sequence. For the channel detection, Bob calculates the variances of the two related quadratures of the Bell measurement locally, and then determines the quantum correlations between the first and second channels in terms of the results of the first channel detection. Based on the results of both the first and second channel detections, they achieve the channel capacity of the QSDC.

Step 5 (S5): Message encoding with displacement. Assume Alice encodes two bits of message (m_k, m_l) into the message amplitude $\alpha_m = x_{m_k} + ip_{m_l}, \forall\{k,l\} \in Z_n$, where the variables x_{m_k} and p_{m_l} correspond to m_k and m_l, respectively. She picks a random signal amplitude $\alpha_M = x_{M_k} + ip_{M_l}$ in the mode M sequence and performs the encoding operation while performing the operation as $\bar{\alpha} = \alpha_m + \alpha_M$. Subsequently, the signal amplitude α_m is encoded as $\bar{\alpha}$ on the mode M sequence. After Bob classically communicates the encoded state $\bar{\alpha}$, Alice can decode the signal amplitude α_m from the resulting state $\bar{\alpha}$ with α_M, finally recovering the message amplitude, together with (m_k, m_l).

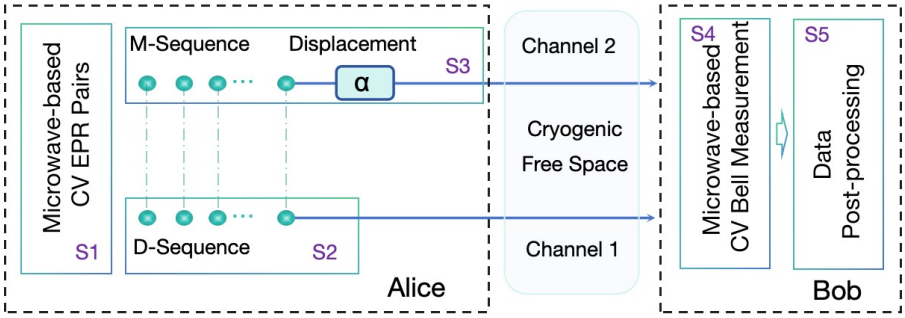


Figure 1. The microwave-based CV-QSDC with two-step protocol in two cryogenic channels.

Because of the displacement of each message (x_{m_k}, p_{m_l}), the resulting signal at the receiver can be expressed as (x_{d_k}, p_{d_l}) with

$$x_{d_k} = \sqrt{2T}x_{m_k}, \quad p_{d_l} = \sqrt{2T}p_{m_l}, \tag{1}$$

where T is the channel transmittance established between Alice and Bob. Bob can select a random subset of remaining raw data while Alice announces her raw data. Consequently, the measurement results can be updated as follows

$$x_{r_k} = x_{d_k} - \sqrt{2T}x_{m_k}, \quad p_{r_l} = p_{d_l} - \sqrt{2T}p_{m_l}. \tag{2}$$

When considering the noise characteristics of the CV-QSDC, as derived and shown in Appendix A, we consider the effect of the phase noise given by [13]

$$\xi_{\text{phase}} = 2V_A\left(1 - e^{-\frac{V_{\text{est}}}{2}}\right), \tag{3}$$

where V_A denotes the modulation variance and V_{est} is the variance of the phase noise given by $V_{\text{est}} = \text{var}\left(\theta_S - \hat{\theta}_S\right)$ with the real phase rotation value θ_S and the estimated value $\hat{\theta}_S$. Therefore, the relations of the phase noise, the total channel added noise, and the total detection added noise can be achieved.

2.2. Generation of Two-Mode Squeezed Microwave States

The implementation of the CV-QSDC in the microwave regime is based on the specialized cryogenic components, as schematically illustrated in Figure 1, which includes the generation and manipulation of quantum microwave states.

In the proposed scheme, an M-EPR state is firstly generated by Alice. One of the entangled modes (the signal mode M) can be retained for subsequent information encoding, while the other mode (the idler mode D) is transmitted to Bob. The generation of the M-EPR state begins with two orthogonal microwave vacuum states, which are sourced from the 50 Ω resistor in a 50 mK environment [16,17]. This temperature is crucial for mitigating thermal noise and enabling the superconducting properties of the core components. Each vacuum state is then injected into a separate Josephson parametric amplifier (JPA), which performs a squeezing operation based on the degenerate parametric amplification.

By setting the JPA's pump frequency to exactly twice that of the signal frequency, a phase-sensitive gain profile is created. This allows the JPA to amplify one quadrature of the input signal while de-amplifying, or squeezing, the orthogonal quadrature. The two resulting single-mode squeezed states are then interfered with using a microwave hybrid coupler, which functions as a 50:50 beam splitter, to produce the final entangled EPR state [18]. The resulting M-EPR state is described by the covariance matrix as follows:

$$\sum_{\text{EPR}} = \begin{bmatrix} V\mathbb{I} & \sqrt{V^2-1}\hat{\sigma}_z \\ \sqrt{V^2-1}\hat{\sigma}_z & V\mathbb{I} \end{bmatrix}, \tag{4}$$

where $\mathbb{I} = \text{diag}(1,1)$, $\hat{\sigma}_z = \text{diag}(1,-1)$, and $V = \cosh(2r)$ denotes the variance of the orthogonal components of each mode. Here, the parameter r denotes the squeezing perimeter for the state preparation.

2.3. Data Post-Processing for Messages Recovery

The successful completion of the displacement operation signifies that the secret information has been effectively encoded onto the M-EPR states. The signal mode M carrying this confidential information is then transmitted from Alice to Bob through a cryogenic channel. Bob combines the incoming signal mode from Alice with his locally retained idler mode at a microwave hybrid coupler, which functions as a balanced beam splitter. Subsequently, Bob performs heterodyne detection on both output modes of the coupler. Based on the measurement outcomes, Bob applies a Gaussian random sequence to estimate the transmission parameters of the quantum channel. Leveraging these estimated parameters, Bob then implements an appropriate information reconciliation protocol to decode the message sequence from the measurement data.

To extract the encoded message, Bob performs a joint measurement on the signal state in the mode M sequence received from Alice and the idler state he retains in the mode D sequence. Following this, a procedure for data post-processing is carried out, enabling

him to ultimately retrieve the message originally sent by Alice. Upon receiving the signal state encoded in the mode M sequence, Bob conducts heterodyne detection in conjunction with his local idler state in the mode D sequence. Finally, Bob engages in a post-processing protocol with Alice via a publicly authenticated classical channel to distill a secure key. During this stage, Alice and Bob collaboratively implement either a direct reconciliation (DR) or reverse reconciliation (RR) scheme, along with privacy amplification [11,12], to obtain the initially encoded messages. However, the transmission and measurement of quantum states are inevitably affected by the unknown characteristics of the quantum channel and the imperfections inherent in practical commercial devices, which can further degrade system performance. Therefore, data post-processing must be conducted before performing Gaussian inverse mapping to ensure the fidelity and security of the decoded messages, which includes three sequential steps, i.e., parameter estimation, reconciliation, and privacy amplification.

As for parameter estimation, Bob measures the quadrature components modulated on the mode M sequence and records the corresponding results. Alice then transmits the original mode D sequence to Bob through a publicly authenticated classical channel. By comparing his measurement outcomes with the known values received from Alice, Bob can construct a set of correlated data and perform accurate estimation of quantum channel parameters, such as transmittance and excess noise. Once parameter estimation is completed, Alice and Bob proceed with the reconciliation process, during which they aim to correct discrepancies between their respective data sequences caused by channel noise and device imperfections. This step is typically realized through a carefully designed reconciliation scheme. One approach is reverse reconciliation (RR), where measurement results at the receiver can be served as the reference for aligning Alice's data. Specifically, Alice holds the original mode M sequence, while Bob receives the degraded version of mode M sequence after quantum channel transmission. By applying an error-correcting code, Alice and Bob collaboratively refine their sequences into a shared reconciled message. The choice of reconciliation direction, whether direct or reverse has significant implications for both the efficiency and the security of the QSDC, with reverse reconciliation generally offering better tolerance to channel loss and noise. Finally, prior to restoring the secret information block, both Alice and Bob apply privacy amplification to eliminate any redundant information introduced during the Gaussian mapping process and to erase potential information leakage to an eavesdropper, Eve, throughout the transmission. Through hashing or other randomness extraction methods, privacy amplification effectively compresses the reconciled message into a shorter, fully secure message, free from partial knowledge that might have been acquired by an adversary.

3. Performance Analysis

3.1. Effect of Channel Loss and Noise

As for the practical implementation of the CV-QSDC system, channel loss has an effect on the performance of the communication system. In a microwave-based setup, the source of loss arises from the transmission of microwave signals through a superconducting coaxial cable. This loss can be modeled by using a beam splitter with transmittance τ_E as follows

$$\tau_E = 10^{\frac{-L}{10}}, \tag{5}$$

where $L = \gamma d$ represents the channel loss for a microwave signal propagating through the superconducting coaxial cable. Here, γ denotes the attenuation coefficient and d is the transmission distance.

In quantum channels, channel coupling noise is the other parameter that has an effect on the fidelity of the transmitted quantum states. It can be described with the input–output relation as follows:

$$\hat{a}_{out} = \sqrt{\tau_E}\hat{a}_{in} + \sqrt{1-\tau_E}\hat{n}, \tag{6}$$

where $\hat{n}$ denotes the ambient thermal photon noise caused by environmental thermal fluctuations. This noise is intrinsically related to both the signal frequency and the ambient temperature. The average thermal photon number can be calculated using the Planck distribution

$$\bar{n} = \frac{1}{e^{h\omega/2\pi k_B T} - 1}, \tag{7}$$

where $\omega/2\pi$ is the signal frequency, T denotes the ambient temperature, h denotes Planck constant, and k_B denotes Boltzmann's constant. Based on the above-mentioned average thermal photon number, the number of photons for the coupled noise can be derived as

$$\hat{n} = \frac{1}{2}(1-\tau_E)\bar{n}. \tag{8}$$

Since the generation of the M-EPR state is in a 50 mK environment that enables the superconducting of the core components, the thermal noise can be mitigated for the source preparation in the proposed CV-QSDC system.

While taking into account the lossy channel, we evaluate the effective information capacity of the communication process for microwave signals at different frequencies by employing either the DR or RR scheme, as shown in Figure 2a. We find that the DR scheme performs better under low channel loss. However, as the channel loss increases, the RR scheme exhibits better performance compared to the DR scheme. This is consistent with the underlying principles of the DR and RR schemes. When the channel loss increases, the signal received by Bob becomes weaker, leading to larger measurement errors in the DR scheme. In other words, as the channel loss grows, the amount of effective information in the DR scheme decays more rapidly than in the RR scheme.

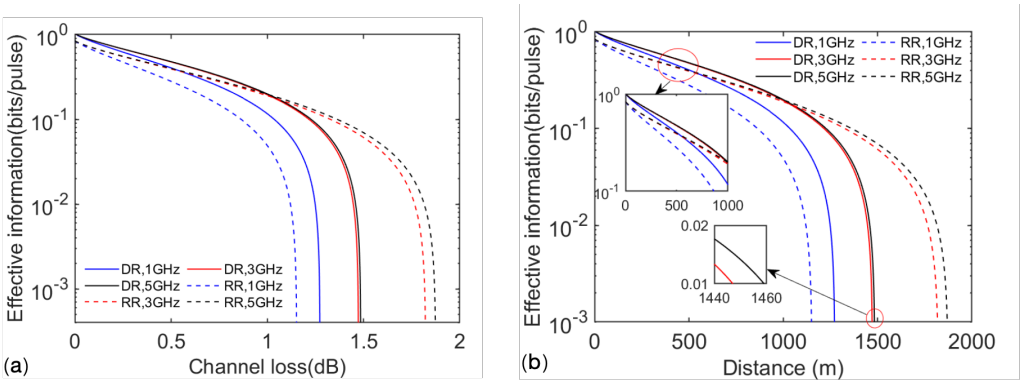


Figure 2. Performance of the CV-QSDC system using the DR and RR schemes, respectively. (**a**) Relationship between the amount of effective information and the channel transmission loss. (**b**) Relationship between the amount of effective information and the transmission distance. The solid and dashed lines indicate that the DR and RR protocols are used for data post-processing, respectively, and the blue, red, and black colors indicate that the signals are modulated for 1 GHz, 3 GHz, and 5 GHz, respectively.

Moreover, we illustrate the relationship between the average thermal noise photon number and microwave frequency and ambient temperature during propagation. In Figure 3a, it is revealed that for the given ambient temperature, higher microwave frequencies result in lower average thermal noise photon numbers during wave propagation. In Figure 3b, it is demonstrated that the limited variations in ambient temperature have a negligible impact on

the average thermal noise photon number generated during microwave propagation. However, microwave frequency exhibits a more pronounced influence on the generation of average thermal noise photon numbers, and thus it demonstrates an exponential decrease with increasing microwave frequency.

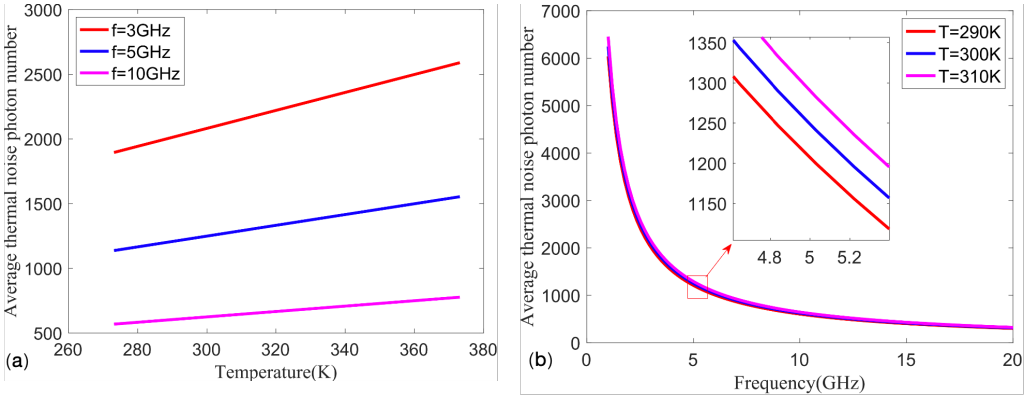


Figure 3. The variation curve of the average thermal noise photon number with (**a**) microwave frequency and (**b**) ambient temperature.

3.2. Derivation of Effective Information Transmission Rate

The eavesdropper, Eve, may perform three kinds of the attack strategies to obtain the useful information from a quantum Gaussian source, including the individual attack, the collective attack, and the coherence attack. It is known that the collective attack is a serious threat to the CV-QSDC system while being compared to those of the individual and coherent attacks [11]. Therefore, we focuses on the performance of the CV-QSDC system under collective attack, where the amount of security-effective information between Alice and Bob is described as [12]

$$\Delta I = \beta I_{AB} - \chi_{B(A)E}, \tag{9}$$

where I_{AB} denotes the mutual information between Alice and Bob, $\beta \in (0,1)$ denotes the efficiency of the reconciliation protocol, and $\chi_{B(A)E}$ denotes the maximum amount of information Eve can access from Bob/Alice under the constraints of the Holevo bound, the former corresponding to the DR scheme and the latter to the RR scheme.

The mutual information I_{AB} between Alice and Bob can be given by [19]

$$I_{AB} = \frac{1}{2}\log_2 \frac{V_B}{V_{B|A}} = \frac{1}{2}\log_2 \left[\frac{V_A + 1}{V_{A|B} + 1}\right] = \frac{1}{2}\log_2 \left[\frac{V + \chi}{\chi + 1}\right]. \tag{10}$$

In addition, the value of χ_{BE} depends heavily on the reconciliation algorithm [20]. When Eve is assumed to purify the entire system, the effective information derived from the respective DR and RR schemes is as follows [21]:

$$\chi_E^{DR} = S(\rho_{AB}) - S(\rho_{AB}|x_A^M), \tag{11}$$

and

$$\chi_E^{DR} = S(\rho_{AB}) - S(\rho_{AB}|x_B), \tag{12}$$

where $S(\rho_{AB})$ denotes the von Neumann entropy between Alice and Bob, and the von Neumann entropy of the Gaussian state can be obtained from

$$S(\rho_{AB}) = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right), \tag{13}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2(x)$. Here, the notations $\lambda_{1,2}$ are the symplectic eigenvalues corresponding to the covariance matrix between Alice and Bob, which can be described as

$$\sum_{AB} = \begin{bmatrix} a\mathbb{I} & b\hat{\sigma}_z \\ b\hat{\sigma}_z & c\mathbb{I} \end{bmatrix}, \tag{14}$$

where $a = V$, $b = \tau_E(V+\chi)$ and $c = \sqrt{\tau_E(V^2-1)}$. Here, $V = V_A + 1$ denotes the modulation variance, τ_E denotes the transmittance of the quantum channel, and $\chi = (1-\tau_E)/\tau_E + \varepsilon$ denotes the noise variance (ε being the excess noise). Moreover, the symplectic eigenvalues can be given by

$$\lambda_{1,2} = \sqrt{\frac{1}{2}\left[\Delta \pm \sqrt{\Delta^2 - 4D^2}\right]}, \tag{15}$$

where

$$\Delta = a^2 + b^2 - 2c^2, \tag{16}$$

and

$$D = ab - c^2. \tag{17}$$

For the DR scheme, the symplectic eigenvalues can be calculated as [22]

$$\lambda^2_{3,4} = \frac{1}{2}(A \pm \sqrt{A^2 - 4B^2}), \tag{18}$$

where

$$A = \frac{1}{a+1}(a + bD + \Delta), \tag{19}$$

$$B = \frac{D}{a+1}(b + D). \tag{20}$$

For the RR algorithm, the symplectic eigenvalues can be calculated as

$$\lambda^2_5 = a(a - c^2/b). \tag{21}$$

Consequently, the amount of effective information for security is derived as follows:

$$\chi_E^{DR} = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{4} G\left(\frac{\lambda_i - 1}{2}\right), \tag{22}$$

$$\chi_E^{RR} = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - G\left(\frac{\lambda_5 - 1}{2}\right). \tag{23}$$

3.3. Security Analysis for Collective Attacks

In order to demonstrate the performance of the microwave-based CV-QSDC, we take into account three frequencies of microwave signals as sources. In addition, the collective attack has been considered while performing the numerical simulations. In addition, the attenuation coefficient used in this work can be assumed as 6×10^{-3} dB/km and the temperature condition is 30 °C at room temperature, used for the numerical simulations. As shown in Figure 2b, we demonstrate the performance of the microwave-based CV-QSDC system while taking into account the selected quantum signals for the given frequencies at 1 GHz, 3 GHz, and 5 GHz. We find that the broader bandwidth results in the higher transmission rate of the system. Namely, when microwave signal for M-EPR generation is selected at 5 GHz, the effective information transmission rate performs better when

compared to those of the 1 GHz and 3 GHz signals. In the field of the traditional microwave communication, the most commonly used microwave frequency is 5GHz.

Furthermore, we have conducted numerical simulations to evaluate the effective transmission information for both the DR and RR schemes. As shown in Figure 4, the effective information depends on both the modulation variance V_A and the channel transmittance τ_E. When the channel transmittance is high, the DR scheme outperforms the RR scheme. However, as the channel loss increases, the RR scheme demonstrates superior performance. In addition, the modulation variance plays an important role, as higher values of V_A yield greater effective information.

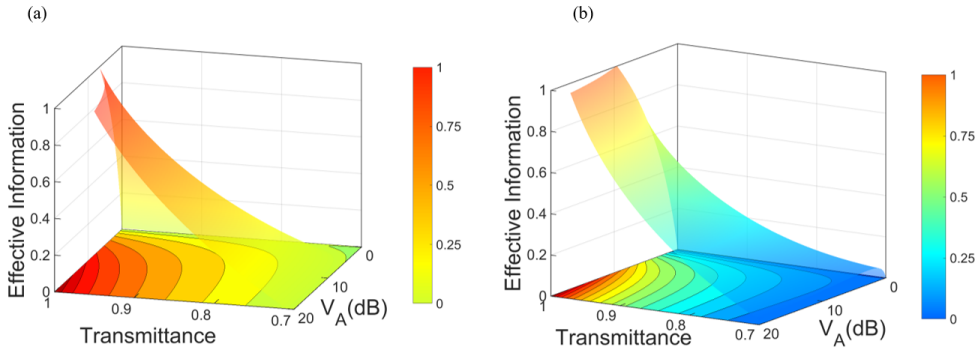


Figure 4. Performance of the effective information of the microwave-based CV-QSDC for the DR scheme (**a**) and the RR scheme (**b**). It also shows the relationship between the effective information of the system and the protocol modulation variance V_A and channel transmittance τ_E.

So far, we have considered the ideal security of the CV-QSDC under collective attacks using both DR and RR schemes. Namely, Alice and Bob would exchange an infinite number of signals to ensure the perfect security of the protocol. However, in practice, the number of exchanged signals is finite, making the asymptotic assumption unrealistic. In what follows, we demonstrate the practical security needed to address this limitation, when taking into account the finite-size security framework.

3.4. Security with Finite-Size Effects

Since the quantum channels are not known in advance, a subset of the exchanged signals should be selected for parameter estimation, whose complexity grows proportionally with the total number of exchanged signals. Within the finite-size regime [23], the mutual information (bit/pulse) can be described as follows:

$$\Delta I = \frac{n}{N}[\beta I_{AB} - \chi_{BE} - \Delta(n)], \tag{24}$$

where m denotes the number of signals used for information transmission, N denotes the total number of signals exchanged, and n is the number of signals used for parameter estimation. In addition, the parameter $\Delta(n)$ is related to privacy amplification security, which is given by

$$\Delta(n) = (2\dim\Lambda + 3)\sqrt{\frac{\log_2(2/\epsilon_S)}{n}} + \frac{2}{n}\log_2(1+\epsilon_{PA}), \tag{25}$$

where $\dim\Lambda$ denotes the dimension of the original key space Λ, ϵ_S denotes the smoothing coefficient, and ϵ_{PA} denotes the probability of privacy amplification failure. Since a binary encoding of the original version of the secret message is used for the CV-QSDC, we have the parameter $\dim\Lambda = 2$.

Alice and Bob share a portion of a secret message of length m over an open channel, which allows them to parameterize the loss and the number of coupled photons in the quantum channel during communication. This allows them to build a statistical estimator such that a lower bound on the quantum channel transmittance and an upper bound on the excess noise can be provided.

While considering the finite-size effects, we have to derive $S_{\epsilon_{PE}}$ using a covariance matrix $\Phi_{\epsilon_{PE}}$ that minimizes the key rate of the QSDC system with probability $1-\epsilon_{PE}$. We can achieve the covariance matrix $\Phi_{\epsilon_{PE}}$ by using m pairs of correlated variables, which can be analyzed with the normal linear model given by

$$y = tx + z, \tag{26}$$

where $t = \sqrt{\tau_E}$, and z obeys a normal distribution with zero mean and variance $\delta^2 = 1 + \tau_E\epsilon$. The parameter ϵ is the calculated accounts for various noise factors. Thus, the covariance matrix $\Phi_{\epsilon_{PE}}$ is expressed as [24]

$$\Phi_{\epsilon_{PE}} = \begin{bmatrix} (V_a+1)\mathbb{I} & t_{\min}Z\hat{\sigma}_z \\ t_{\min}Z\hat{\sigma}_z & (t_{\min}^2 V_a + \delta_{\max}^2)\mathbb{I} \end{bmatrix}, \tag{27}$$

where t_{min} and $\delta_{\max}$ denote the minimum value of t and the maximum value of δ that are compatible with the sampling pair, except with probability $\epsilon_{\mathrm{PE}}/2$ and $Z = \sqrt{V_a^2 + 2V_a}$.

The maximum likelihood estimation can be calculated as

$$\hat{t} = \frac{\sum_{k=1}^{m} x_k y_k}{\sum_{k=1}^{m} x_k^2}, \tag{28}$$

and

$$\hat{\delta}^2 = \frac{1}{s}\sum_{k=1}^{s}(y_k - \hat{t}x_k)^2. \tag{29}$$

Based on the above-derived results, we have

$$t_{\min} \approx \sqrt{T} - Z_{\epsilon_{PE}/2}\sqrt{\frac{1+T}{sV_A}}, \tag{30}$$

$$\delta_{\max}^2 \approx 1 + T + Z_{\epsilon_{PE}/2}\sqrt{\frac{2(1+T)}{\sqrt{s}}}. \tag{31}$$

In addition, the parameter $Z_{\epsilon_{PE}/2}$ satisfies the constraints

$$1 - \mathrm{erf}\left(\frac{Z_{\epsilon_{PE}/2}}{\sqrt{2}}\right)/2 = \epsilon_{\mathrm{PE}}/2, \tag{32}$$

with the notation $\mathrm{erf}(x)$ defined by

$$\mathrm{erf}(x) = \frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2}dt. \tag{33}$$

The theoretical values of the above error probabilities are realized when taking into account the given parameters $\epsilon_{\mathrm{PE}} = \epsilon_{\mathrm{PA}} = \epsilon_{\mathrm{S}} = 10^{-10}$ [24]. The covariance matrix of the quantum state shared by Alice and Bob can be rewritten as follows

$$\gamma_{AB} = \begin{bmatrix} V_a\mathbb{I} & (t_{\min}^2 V_a + \delta_{\max}^2)\hat{\sigma}_z \\ (t_{\min}^2 V_a + \delta_{\max}^2)\hat{\sigma}_z & \left(t_{\min}\sqrt{V_a^2 + 2V_a}\right)\mathbb{I} \end{bmatrix}. \tag{34}$$

Consequently, the effective information of the CV-QSDC can be achieved from this covariance matrix.

As shown in Figure 5, we have obtained the effective information capacity of this CVQSDC system for the given encoding lengths and signal frequencies (with modulation variance $V_A = 7$ for numerical simulations). In addition, the attenuation coefficient used in numerical simulation is still 6×10^{-3} dB/km for the simplified implementation. It demonstrates the impact of signal frequency on system performance. Compared with low-frequency signals, the 5 GHz signal demonstrates an advantage when considering both effective information capacity and maximum transmission distance. This improvement is attributed to the reduced channel background thermal noise for the high-rate signal frequencies.

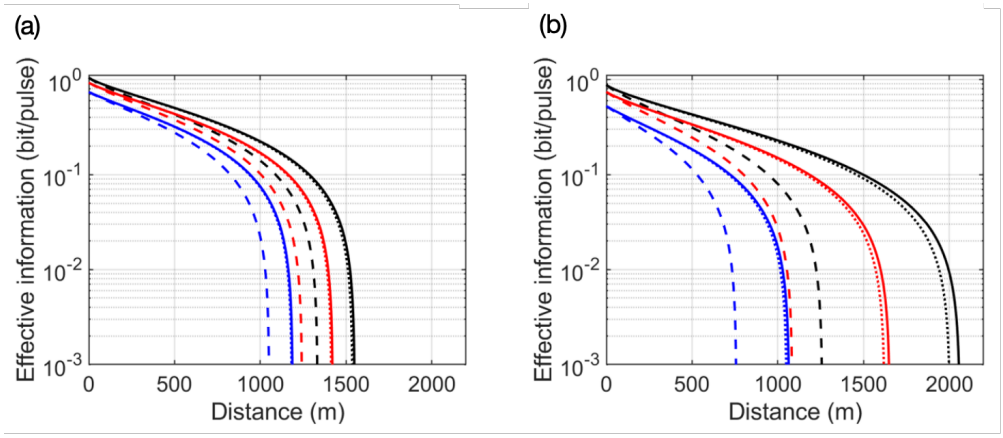


Figure 5. The effective information for the communication process is a function of the transmission distance using the DR and RR algorithm. (**a**,**b**) Relationship between effective information and transmission distance for ideal conditions, with multiple different frequency correspondences. From left to right, the dashed, dotted, and solid lines indicate signals with frequencies of 1 GHz, 3 GHz, and 5 GHz, respectively. While the type of line corresponds to the information code length used, blue, red, and black lines correspond to N = 10^5, 10^6 and system asymptotic effective information, respectively.

When we select a signal frequency of 5 GHz, the asymptotic key rates of the DR and RR schemes remain positive at transmission distances of 1500 m and 2000 m, respectively, indicating that the QSDC is theoretically feasible in implementation. However, when taking the finite-size effect of the available resources into account, the maximum transmission distance of the system is reduced. For example, when the key length is set $N = 10^5$, the transmission distances for both DR and RR schemes are both shortened to approximately 1000 m. Furthermore, when N increases to 10^6, the corresponding maximum transmission distance exceeds 1500 m, approaching the maximum transmission distance of the asymptotic capacity for effective information.

4. Conclusions

In this paper, we have proposed an approach to implementing the microwave-based CV-QSDC using entangled M-EPR states. We evaluate the performance of the communication process while considering effects of the external incorporating parameter estimation for both DR and RR strategies. Numerical simulations demonstrate that the high GHz microwave signals results in the long secure transmission distance of covert information achieved when different calibration strategies are taken into account in a cryogenic environment under various reconciliation strategies. In addition, we demonstrate the impact of message block length on the effective information rate and achievable transmission distance. The numerical simulations show that as the block length increases from 10^5 to 10^6, the maximum transmission distance of the system approaches to the asymptotic limit pre-

dicted by the effective information capacity. The influence of microwave signal frequency on communication performance has been shown. The 5 GHz microwave signal enable the longest effective transmission distance, which can be attributed to its relatively low background thermal noise. It means that the performance of the system can be improved by making full use of the partially trusted phase noise. It leaves an optimization space for CVQSDC in practical implementation.

These results are useful for the confirmation of microwave-provided entangled quantum states as a source for practical CV-QSDC. Compared to the optical implementations, the microwave-based CVQSDC has unique advantages, particularly in terms of integration with superconducting circuits and on-chip quantum technologies. This makes it a promising candidate for short-range secure quantum communication in cryogenic or solid-state platforms, offering both practicality and scalability for the scaled quantum network architectures provided with a large number of nodes, switching, routing, and synchronization.

Author Contributions: Conceptualization, Y.M.; writing—original draft preparation, L.M.; writing—simulation, W.W.; writing—review, Y.W.; writing—simulation, H.Z.; writing—editing, Y.G. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Natural Science Foundation of Hunan Province (No. 2023JJ50269) and Scientific research project of Hunan Provincial Department of Education (No. 22C0446).

Data Availability Statement: All data generated or analyzed during this study are included in this published article.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A. The Phase Noise

The parameter V_{error} denotes the variance generated by the error between the real phase rotation value θ_{R} and estimated value $\hat{\theta}_R$, given by [19,20]

$$V_{\text{error}} = \text{var}(\theta_R - \hat{\theta}_R) = \frac{\chi + 1}{E_R^2}, \tag{A1}$$

where χ is the total noise of phase reference, it can be calculated by

$$\chi = \frac{1}{T} - 1 + \varepsilon_0 + \frac{2 - \mu + 2v_{\text{el}}}{T\mu}. \tag{A2}$$

The first three items mentioned above are the components of channel-added noise in quantum communications, and the last item denotes the heterodyne detector noise. The parameter V_{drift} represents the variance of the relative phase drift between two lasers for ΔT, which can be described as

$$V_{\text{drift}} = 2\pi(\Delta v_A + \Delta v_B)\Delta T \tag{A3}$$

where Δv_A and Δv_B correspond to the line widths of the two free-running lasers. The parameter V_{channel} represents the variance of the noise resulting from the accumulated drift of phase of the signal pulse. Therefore, when V_{est} approaches 0, the phase noise can be approximated as

$$\xi_{\text{phase}} = V_A(V_{\text{drift}} + V_{\text{channel}} + V_{\text{error}}) = \xi_{\text{drift}} + \xi_{\text{channel}} + \xi_{\text{error}}. \tag{A4}$$

Furthermore, we consider the characteristics of the trusted noise after calibration [21,22]. The excess noise ξ is a component element of the channel added noise, which is part of the total added noise, and hence it can be described as

$$\xi = \xi_{\text{phase}} + \xi_{\text{rest}}. \tag{A5}$$

Then, the total channel added noise χ_{line} can be given by

$$\chi_{\text{line}} = 1/\text{T} - 1 + \xi. \tag{A6}$$

The total detection added noise χ_{het} can be calculated as

$$\chi_{\text{het}} = (2 - \mu + 2v_{el})/\mu. \tag{A7}$$

Combined with the noise calculation method, the total noise can be derived as

$$\chi_{\text{tot}} = \chi_{\text{line}} + \frac{\chi_{\text{het}}}{T}. \tag{A8}$$

In what follows, we try to distinguish the trusted and untrusted parts among them. We assume that χ_{het} is the trusted noise based on μ and v_{el} being well calibrated. Meanwhile, since the part of the phase noise ξ_{error} can be perfectly controlled and calibrated by Bob, it can be regarded as the trusted noise [24].

Based on (A8), we achieve the total phase noise of reference given by

$$\chi = \chi^{\text{u}} + \frac{\chi^T}{T}, \tag{A9}$$

where $\chi^u = 1/T - 1 + \varepsilon_0$ and $\chi^T = (2 - \mu + 2v_{\text{el}})/\mu$.

Combined with (A1), (A2), (A4), and (A9), the measurement noise of phase reference can calculated as

$$\xi_{\text{error}} = \xi^u_{\text{error}} + \frac{\xi^T_{\text{error}}}{T}, \tag{A10}$$

where

$$\xi^u_{\text{error}} = V_A\left(\frac{\chi^u + 1}{E_R^2}\right) = V_A\left(\frac{1 + T\varepsilon_0}{TE_R^2}\right), \tag{A11}$$

and

$$\xi^T_{\text{error}} = V_A\left(\frac{\chi^T}{E_R^2}\right) = V_A\left(\frac{2 - \mu + 2v_{\text{el}}}{\mu E_R^2}\right). \tag{A12}$$

References

1. Grosshans, F.; Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **2002**, *88*, 057902. [CrossRef]
2. Liao, Q.; Xiao, G.; Zhong, H.; Guo, Y. Multi-label learning for improving discretely-modulated continuous- variable quantum key distribution. *New J. Phys.* **2021**, *22*, 083086. [CrossRef]
3. Zhou, K.; Yi, C.; Yan, W.; Hou, Z.; Zhu, H.; Xiang, G.; Li, C.; Guo, G. Experimental Realization of Genuine Three-Copy Collective Measurements for Optimal Information Extraction. *Phys. Rev. Lett.* **2025**, *134*, 210201. [CrossRef] [PubMed]
4. Xie, M.; Niu, S.; Han, Z.; Li, Y.; Chen, R.; Wang, X.; Gao, M.; Chen, L.; Song, Y.; Zhou, Z.; et al. Quantum-enhanced imaging for characterizing anisotropic material. *npj Quantum Inf.* **2025**, *11*, 57. [CrossRef]
5. Deng, F.; Long, G.; Liu, X. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Phys. Rev. A* **2003**, *68*, 042317.
6. Deng, F.; Long, G. Secure direct communication with a quantum one-time pad. *Phys. Rev. A* **2004**, *69*, 052319. [CrossRef]
7. Wang, C.; Deng, F.; Li, Y.; Liu, X.; Long, G. Quantum secure direct communication with high-dimension quantum superdense coding. *Phys. Rev. A* **2005**, *71*, 044305. [CrossRef]

8. Niu, P.; Zhou, Z.; Lin Z.; Sheng, Y.; Yin, L.; Long, G. Measurement-device-independent quantum communication without encryption. *Sci. Bull.* **2018**, *63*, 1345–1350.
9. Zhou, Z.; Niu, P.; Sheng, Y., Yin, L.; Long, G. Measurement-device-independent quantum secure direct communication. *Sci. China Phys. Mech. Astron.* **2019**, *63*, 230362. [CrossRef]
10. Zhou, L.; Sheng, Y.; Long, G. Device-independent quantum secure direct communication against collective attacks. *Sci. Bull.* **2020**, *65*, 12–20. [CrossRef]
11. Zhong, H.; Ye, W.; Zuo, Z.; Huang, D.; Guo, Y. Kalman filter-enabled parameter estimation for simultaneous quantum key distribution and classical communication scheme over a satellite-mediated link. *Opt. Express* **2022**, *30*, 5981.
12. Liao, Q.; Xiao, G.; Xu, C.-G.; Xu, Y.; Guo, Y. Discretely modulated continuous-variable quantum key distribution with an untrusted entanglement source. *Phys. Rev. A* **2020**, *102*, 032604. [CrossRef]
13. Pirandola, S.; Braunstein, S. L.; Mancini, S.; Lloyd, S. Quantum direct communication with continuous variables. *Europhys. Lett.* **2018**, *84*, 20013.
14. Fesquet, F.; Kronowetter, F.; Renger, M.; Gross, R.; Fedorov, K.G. Demonstration of microwave single-shot quantum key distribution. *Nat. Commun.* **2024**, *15*, 2041–1723. [CrossRef] [PubMed]
15. Fedorov, K.; Renger, M.: Pogorzalek, S.; Di Candia, R.; Chen, Q.; Nojiri, Y.; Inomata, K.; Nakamura, Y.; Partanen, M.; Marx, A.; et al. Experimental quantum teleportation of propagating microwaves. *Sci. Adv.* **2021**, *7*, 0891.
16. Fedorov, K.G.; Pogorzalek, S.; Las Heras, U.; Sanz, M.; Yard, P.; Eder, P.; Fischer, M.; Goetz, J.; Xie, E.; Inomata, K.; et al. Finite-time quantum entanglement in propagating squeezed microwaves. *Sci. Rep.* **2018**, *8*, 6416. [CrossRef]
17. Pogorzalek, S.; Fedorov, K.G.; Xu, M.; Parra-Rodriguez, A.; Sanz, M.; Fischer, M.; Xie, E.; Inomata, K.; Nakamura, Y.; Solano, E.; et al. Secure quantum remote state preparation of squeezed microwave states. *Nat. Commun.* **2019**, *10*, 2604. [CrossRef]
18. Menzel, E.P.; Di Candia, R.; Deppe, F.; Eder, P.; Zhong, L.; Ihmig, M.; Haeberlein, M.; Baust, A.; Hoffmann, E.; Ballester, D.; et al. Path Entanglement of Continuous-Variable Quantum Microwaves. *Phys. Rev. Lett.* **2012**, *109*, 250502. [CrossRef]
19. Paul, J.; Kunz-Jacques S.; Leverrier, A. Long-distance continuous-variable quantum key distribution with a Gaussian modulation. *Phys. Rev. A* **2011**, *84*, 062317.
20. Lodewyck, J.; Bloch, M.; Fossier, S.; Karpo, E.; Diamanti, E.; Debuisschert, T.; Cerf N.J.; Tualle-Brouri, R.; McLaughlin, S.W.; Grangier, P. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A* **2007** , *76*, 042305. [CrossRef]
21. Usenko, V.C.; Laszlo, R.; Radim, F. Entanglement-based continuous-variable quantum key distribution with multimode states and detectors. *Phys. Rev. A* **2014**, *90*, 062326. [CrossRef]
22. Tene, A.G.; Anne, M.; Stephanie, K. Error correction based artificial neural network in multi-modes CV-QKD with simultaneous type-I and type-II parametric-down conversion entangled photon source. *Opt. Commun.* **2024**, *565*, 130681. [CrossRef]
23. Leverrier, A. Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States. *Phys. Rev. Lett.* **2015**, *114*, 042317. [CrossRef] [PubMed]
24. Leverrier, A.; Grosshans, F.; Grangier, P. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A* **2010**, *81*, 062343. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.