mathematics

IMPACT FACTOR 2.2

CITESCORE 4.6

Article

Optical Frequency Comb-Based Continuous-Variable Quantum Secret Sharing Scheme

Runsheng Peng, Yijun Wang, Hang Zhang, Yun Mao and Ying Guo

MDPI

https://doi.org/10.3390/math13152455

mathematics

MDPI

Article

Optical Frequency Comb-Based Continuous-Variable Quantum Secret Sharing Scheme

Runsheng Peng [1], Yijun Wang [1,*], Hang Zhang [1], Yun Mao [2] and Ying Guo [3]

[1] School of Automation, Central South University, Changsha 410083, China; 214601026@csu.edu.cn (R.P.)
[2] Provincial Key Laboratory of Informational Service for Rural Area of Southwestern Hunan, College of Information Science and Engineering, Shaoyang University, Shaoyang 422000, China
[3] School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China
* Correspondence: xxywyj@sina.com

Abstract

Quantum secret sharing (QSS) faces inherent limitations in scaling to multi-user networks due to excess noise introduced by highly asymmetric beam splitters (HABSs) in chain-structured topologies. To overcome this challenge, we propose an optical frequency comb-based continuous-variable QSS (OFC CV-QSS) scheme that establishes parallel frequency channels between users and the dealer via OFC-generated multi-wavelength carriers. By replacing the chain-structured links with dedicated frequency channels and integrating the Chinese remainder theorem (CRT) with a decentralized architecture, our design eliminates excess noise from all users using HABS while providing mathematical- and physical-layer security. Simulation results demonstrate that the scheme achieves a more than 50% improvement in maximum transmission distance compared to chain-based QSS, with significantly slower performance degradation as users scale to 20. Numerical simulations confirm the feasibility of this theoretical framework for multi-user quantum networks, offering dual-layer confidentiality without compromising key rates.

Keywords: optical frequency comb; quantum secret sharing; continuous-variable; quantum communications

MSC: 81P94; 81P45

Academic Editor: Jonathan Blackledge

Received: 30 June 2025
Revised: 27 July 2025
Accepted: 28 July 2025
Published: 30 July 2025

Citation: Peng, R.; Wang, Y.; Zhang, H.; Mao, Y.; Guo, Y. Optical Frequency Comb-Based Continuous-Variable Quantum Secret Sharing Scheme. *Mathematics* **2025**, *13*, 2455. https://doi.org/10.3390/math13152455

1. Introduction

Quantum secret sharing (QSS) [1–8], as a multi-party secure quantum communication protocol, achieves dual-layer (quantum and physical) confidentiality by partitioning secrets among participants so that only authorized user groups can reconstruct the full information. In such a system, a designated dealer receives quantum states from multiple users through quantum channels and then distributes secrets and keys to ensure that no subset below the threshold can access the complete key information. Since the initial QSS proposal [1], numerous schemes have emerged [2–4]. In 2005, Christian Schmid et al. [5] introduced a single-qubit QSS with chain-structured transmission. Subsequently, Warren P. Grice and Bing Qi [6] developed continuous-variable QSS (CV-QSS) using similar architectures, followed by user-side and structural refinements [7,8]. Nevertheless, these works remain constrained by chain topologies, inevitably introducing excess noise through highly asymmetric couplers in multi-user quantum channels.

Meanwhile, optical frequency combs (OFCs) have gained attention as efficient WDM sources [9]. An OFC spectrum comprises equally spaced narrowband lines, $f_n = f_0 + n \cdot f_r$

where f_0 is the carrier-envelope offset frequency, f_r is the repetition rate, and n is the mode index. Their advantages in spectral efficiency [10], receiver design [11–14], and signal processing [15–17] for WDM have motivated Lars Lundberg et al. [18] to implement OFC-based WDM transmission. Yijun Wang et al. [19] further leveraged OFCs for parallel transmission and coherent reception to boost CV-QKD key rates. While microresonator-based OFCs enable chip-scale integration [20,21], their phase noise (>100 rad/$Hz^{1/2}$ [22]) and line-spacing instability limit multi-user synchronization. We employ standard fiber-based OFCs due to their superior phase coherence (<10 rad/$Hz^{1/2}$ [19]) and precise frequency control, which are critical for parallel quantum channels requiring sub-Hz stability. Despite QSS's greater need for parallel multi-user quantum channels, no theoretical or experimental OFC-based QSS studies exist. While recent experimental advances have demonstrated chip-based generation of photonic graph states for measurement-driven quantum processing [23], hyperentanglement-enhanced high-capacity quantum secure direct communication [24], and robust coherent-state QSS implementations tolerant of channel imperfections [25], these approaches fundamentally constrain scalability in multi-user secret sharing. Chip-integrated architectures lack wavelength-agile parallelism for dynamic user access; hyperentanglement systems incur prohibitive hardware complexity beyond a few-user scenarios; and existing CV-QSS experiments remain bound to chain-structured topologies that suffer from cumulative noise. Although microresonator soliton microcombs offer chip-scale advantages [26], this work employs fiber-based OFCs due to compatibility constraints with existing CV-QSS implementations and laboratory capabilities.

This work proposes an OFC-based CV-QSS scheme. Building on decentralized QSS architectures, we establish dedicated frequency channels between the dealer and individual users via OFCs, eliminating excess noise from chain couplers and removing idealistic assumptions (e.g., equidistant users). Consequently, we resolve the severe degradation of key rates and transmission distance that occurs with user scaling. Simultaneously, the Chinese remainder theorem (CRT) and decentralized structures ensure mathematical and architectural security, providing non-quantum layer protection.

This paper is organized as follows. In Section 2, we detail the mathematical foundations of the OFC-based CV-QSS scheme and describe the process of generating multi-frequency quantum states via OFCS for quantum transmission of our proposed OFC-based CV-QSS scheme. Additionally, we present the protocol design and implementation workflow. In Section 3, we firstly establish the classical (non-quantum) security through mathematical formalism and architectural analysis, then analyze the system security in terms of quantum aspects. Through numerical simulations, we evaluate the system performance, confirming the feasibility and superiority of the proposed scheme. The performance of the scheme is analyzed and verified via numerical simulations in Section 4. And we present our conclusions in Section 5.

2. Optical Frequency Comb-Based Continuous-Variable Quantum Secret Sharing Scheme

2.1. Preliminaries of the Chinese Remainder Theorem

The Chinese remainder theorem states: Let $m_1, m_2, \cdots, m_k$ be k pairwise relatively prime positive integers. Then, for any integers $c_1, c_2, \cdots, c_k$, there exists an integer x such that

$$\begin{cases} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \\ \cdots \\ x \equiv c_k \pmod{m_k} \end{cases}$$

all of which hold. Moreover, in the sense of modulo $m_1 m_2 \cdots m_k$, the solution of the above system of congruence equations is unique and can be expressed as

$$x \equiv x_0 \pmod{m_1 m_2 \cdots m_k}$$

Here, x_0 can be determined as follows: Let $M_i = \frac{1}{m_i}(\prod_{j=1}^{k} m_j)$, $1 \leqslant i \leqslant k$, and assume that M_i^{-1} is the multiplicative inverse of M_i modulo m_i. Then we can take

$$x_0 = \sum_{j=1}^{k} M_j M_j^{-1} c_j$$

The proof of this theorem is straightforward. The integer x that satisfies the system of congruence equations can also be obtained in the following way: Let $x_1 = c_1$, then x_1 satisfies the first equation. Consider the numbers $x_1 + m_1, x_1 + 2m_1, \cdots, x_1 + m_2 m_1$. Since $(m_1, m_2) = 1$, they form a complete residue system modulo m_2. Therefore, there is an x_2 among them such that $x_2 \equiv c_2 \pmod{m_2}$, and this x_2 satisfies the first two equations simultaneously. Then consider $x_2 + m_2 m_1, x_2 + 2m_2 m_1, \cdots, x_2 + m_3 m_2 m_1$ and so on. By successive iteration, the integer x_k that satisfies all the equations can be found.

If we do not know all the remainders of the congruence equations, taking the number of users as three as an example, given moduli $n_1 = 3$ and $n_2 = 5$ (pairwise coprime) with known remainders $x \equiv 2 \pmod 3$ and $x \equiv 3 \pmod 5$, the equations can be merged into $x \equiv 8 \pmod{15}$. However, if the remainder constraint for the third modulus $n_3 = 7$ is missing, the solution is not unique; substituting $x = 15m + 8$ and iterating m from 0 to 6 yields seven candidate solutions modulo 105 (i.e., $x = 8, 23, 38, 53, 68, 83, 98$). All candidates satisfy the known equations, but the absence of the mod 7 constraint prevents the unique determination of x.

2.2. Optical Frequency Comb-Based Continuous-Variable Quantum Secret Sharing Scheme

This work presents a CV-QSS architecture that integrates phase-randomized optical frequency combs with displacement-driven quantum state modulation, enabling high-dimensional secure communication. The system leverages a multi-wavelength quantum source generated by the dealer, characterized by a central frequency f_0^s and repetition rate f_r^s. The quantum field optical comb is mathematically expressed as follows:

$$\hat{s}(t) = \sum_{n=n_{\min}}^{n_{\max}} \left(X_n^A + i P_n^A \right) \exp\{ j[-\varphi(t) + 2\pi(f_0^s + n f_r^s)t] \}, \tag{1}$$

where X_n^A and P_n^A denote quadrature components following zero-mean Gaussian distributions with variance σ^2 (in shot-noise units), and $\varphi(t)$ represents phase noise from laser fluctuations. Critically, each sub-comb branch is modulated with Rayleigh-distributed amplitudes $V_n \sim Ra(\sigma)$ and uniformly randomized phases $\Phi_n \in [0, 2\pi]$, which collectively act as displacement operators $D(\alpha_n)$ to coherently modulate the two-mode squeezed vacuum (TMSV) states transmitted by $User_j$, where $D(\alpha_k) = \exp(\alpha_k \hat{a}^\dagger - \alpha_k^* \hat{a})$ with $\alpha_k = V_k e^{j\Phi_k}$ encodes classical randomness into TMSV states.

The dealer demultiplexes the optical comb into $N = n_{\max} - n_{\min} + 1$ parallel sub-channels. For central sub-channels ($k = n_{\min} + 1, \ldots, n_{\max} - 1$), the displacement parameter $\alpha_k = V_k e^{j\Phi_k}$ is generated through Rayleigh-amplitude and random-phase modulation. This displacement operation directly impresses classical randomness onto the quantum noise of $User_j$'s TMSV states, achieving quadrature-dependent encoding while preserving their inherent squeezing correlations. The exponential decay of the Rayleigh distribution inherently suppresses large-amplitude modulation events, confining excess noise near the

shot-noise limit. Edge sub-channels ($r = n_{\min}, n_{\max}$) encode fixed quadratures X_r^A, P_r^A to facilitate phase drift compensation during detection.

At the receiver, $User_j$ employs a local optical frequency comb ($f_0^L = f_0^s, f_r^L = f_r^s$) to demultiplex the incoming signal into N frequency bins. Pilot tones are isolated for phase noise estimation via a phase-locked loop (PLL), while data-carrying sub-channels undergo adaptive homodyne detection. The pre-applied displacement modulation $D(\alpha_k)$ reshapes the quadrature noise of the TMSV states, enabling direct measurement of their variances through X/P-basis homodyne detectors. Real-time phase modulation aligns measurement bases with the dealer's encoding parameters, ensuring that the bases match for sifting.

Post-processing involves four key steps, as follows: (1) Basis sifting, where $User_j$ announces measurement bases and the dealer retains data from matched sub-channels; (2) parameter estimation, leveraging public disclosure of partial keys to evaluate channel transmittance T_k and excess noise ϵ_k, with Rayleigh statistics enabling precise noise-floor calibration; (3) multi-mode reconciliation using rate-adaptive LDPC codes optimized by displacement correlation matrices; and (4) privacy amplification via universal hashing, where security proofs exploit the phase-space symmetry induced by displacement operations.

By unifying classical phase randomization with quantum displacement operations as in Figure 1, this architecture establishes a resource-efficient framework for large-scale quantum-secured networks. Figures 1 and 2 depict the operational workflow of the proposed OFC CV-QSS scheme: (a) The dealer first determines the number of optical frequency comb (OFC) carrier pairs based on the user count. (b) Point-to-point quantum communication channels are established individually between the dealer and each user through dedicated OFC carriers. This process follows CV-QSS fairness protocols. (c) After all quantum links are established, the minimum key rate among the point-to-point connections defines the system key rate lower bound $R = \min\{R_1, R_2, \ldots, R_n\}$. The final shared secret key is then derived through classical post-processing of quantum-measurement outcomes. The dealer's optical comb not only serves as a multi-wavelength carrier but also physically enhances security through displacement-driven modulation of $User_j$'s TMSV states, ensuring compatibility with existing fiber-optic infrastructure and enabling high-rate, long-distance CV-QKD deployment.

Then, we present a secure CV-QSS scheme based on optical frequency combs, enabling the dealer to distribute a classical secret S to n participants via the CRT. The protocol consists of three phases [4].

2.2.1. Initialization

The dealer selects n primes $m^{U_1} = 2$, $m^{U_2} = 3$, ..., m^{U_n} (e.g., the first n primes), which are inherently coprime (i.e., $\gcd(m^{U_i}, m^{U_j}) = 1$ for all $1 \le i \ne j \le n$). The secret $S \in \{0, 1, ..., M\}^L$, a checksum sequence $R \in \{0, 1, ..., M\}^{L_1}$, and a unique pointer $P^* \in \{0, 1, ..., M\}^{L_2}$ are generated, where $M = \prod_{k=1}^{n} m^{U_k} - 1$. The dealer put P^* behind S and embeds them into R to form a sequence X as Figure 3, ensuring the uniqueness of P^* (i.e., if a substring $T_j = P^*$, all other $T_k \ne P^*$). Shadows $X^{U_i} = X \mod m^{U_i}$ are computed for each participant U_i, and the parameters $\{m^{U_1}, ..., m^{U_n}\}$, L, L_1, L_2, P^*, verification data V, and hash function $H()$ are published.

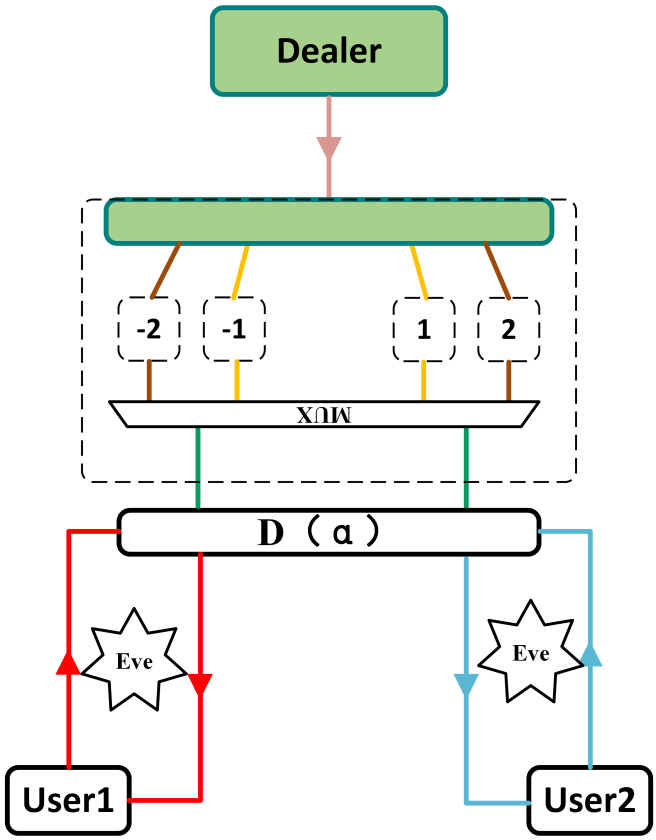


Figure 1. Proposed optical frequency comb–based continuous–variable quantum secret sharing scheme.

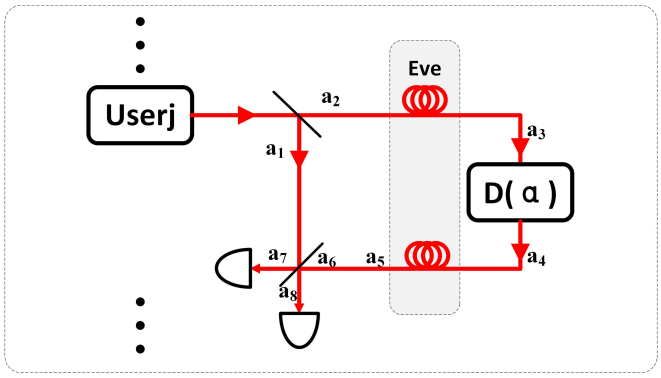


Figure 2. The quantum communication between a random user and the dealer. The a_i represent squeezed vacuum states at different transmission stage.

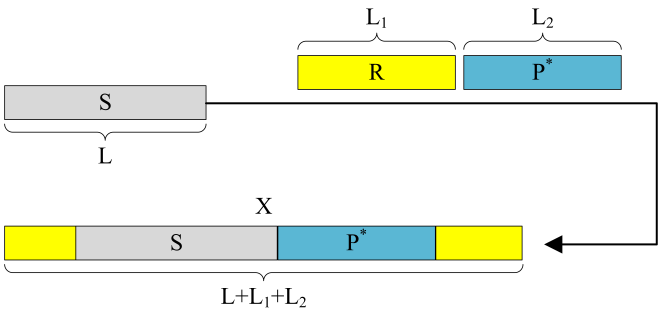


Figure 3. How to determine Message X through the ciphertext S, checking sequence R, and determine pointer P^*.

2.2.2. Distribution

The dealer distributes X^{U_i} to each user U_i via optical frequency comb-based quantum channels: 1. State Preparation: Each U_i prepares $L + L_1 + L_2$ two-mode squeezed vacuum states, with quadratures derived from vacuum states $\hat{x}_1^{(0)}, \hat{p}_1^{(0)}$ and $\hat{x}_2^{(0)}, \hat{p}_2^{(0)} \sim N(0,1)$ with squeezing parameter r, satisfying:

$$\lim_{r\to+\infty} x_1 = x_2, \quad \lim_{r\to+\infty} p_1 = -p_2.$$

2. Eavesdropping Detection: Users send the squeezed state a_2 and coherent states c to the dealer for error rate analysis. If anomalies are detected (e.g., excess error rate), communication is restarted. 3. Message Modulation: The dealer modulates received states with $\alpha_j \sim N(X^{U_i}, \sigma^2)$ and returns the modulated state a_4 for decryption. 4. Joint Measurement: Users perform two-mode Bell measurements (using balanced beam splitters and homodyne detectors) on local state a_1 and received state a_6 to decrypt X^{U_i}.

2.2.3. Reconstruction

To securely recover S, all n users collaborate as shown in Figure 3: 1. Encryption & Exchange: Each U_i generates a random sequence $U_i \in \{0, ..., M\}^{L+L_1+L_2}$, encrypts their shadow as $(X_j^{U_i} + U_{i,j}) \mod (M+1)$, and exchanges encrypted messages. 2. Iterative Verification: Starting from $j = 0$, users increment j, broadcast the j-th round keys $U_{1,j}, U_{2,j}, ..., U_{n,j}$, and decrypt $X_j^{U_i} = (M_{e_j}^{U_i} - U_{i,j}) \mod (M+1)$. Using CRT, they recover X_j, compute $V_j' = H(X_j + j(L+M))$, and abort if $V_j' \neq V_j$. 3. Secret Extraction: When $j = L + L_2$, users check if the substring $T_j = X_{j-L_2+1}, ..., X_j$ matches P^*. If matched, the secret $S = X_{j-L-L_2+1}, ..., X_{j-L_2}$ is extracted; otherwise, the loop continues.

3. Security Analysis

In this section, we first conduct a security analysis of the proposed OFCQSS scheme. Additionally, since the quantum key distribution protocol serves as a security technique in this paper, we evaluate the performance of the scheme based on the security analysis of quantum key distribution. This evaluation primarily focuses on the performance metrics of the scheme, such as the secure key rate and noise.

3.1. Mathematical and Structural Security Analysis

3.1.1. Mathematical Security Proof Based on the Chinese Remainder Theorem

In the application of the Chinese remainder theorem, the secret S is decomposed into multiple remainders (shares), with each user holding only the remainder under a specific modulus. For example, in a two-user scheme, the secret S is decomposed into $X^{U_1} \equiv X \mod m^{U_1}$ and $X^{U_2} \equiv X \mod m^{U_2}$, where the moduli m^{U_1} and m^{U_2} are coprime. Only by possessing both X^{U_1} and X^{U_2} can the original message X be recovered through CRT, and the secret S be extracted accordingly.

The security guarantee mechanism of CRT is as follows [4]:

(1) Mathematical irreversibility: Knowing a single remainder (e.g., X^{U_1} or X^{U_2}) cannot uniquely determine the original value X. For instance, if $m^{U_1} = 2$ and $X^{U_1} = 0$, X could be 0, 2, 4, etc.; if $m^{U_2} = 3$ and $X^{U_2} = 0$, X could be 0, 3, 6, etc. Thus, the information entropy of a single remainder is much lower than that of the complete secret, making it impossible to effectively recover the secret through exhaustive enumeration or reverse calculation.

(2) Information entropy separation: As analyzed in the paper, the information entropy of each share (e.g., X^{U_1} or X^{U_2}) is 1 bit and $\log_2 3$ bits, respectively, while the entropy of the complete message X is $\log_2 6$ bits. The information contained in a single share is

insufficient to cover the entropy of the complete secret, preventing participants from inferring the global secret through local information

(3) Time complexity: If an attacker attempts to guess other participants' shares through a single remainder, they need to enumerate all possible combinations. Since the product of the moduli grows exponentially with the number of participants, the complexity of exhaustive search is too high to be feasible.

The CRT—through its mathematical irreversibility and information entropy separation mechanism—ensures that the secret must be jointly recovered from multiple remainders. A single remainder provides only partial information and cannot be used to reverse-engineer the complete content. This characteristic completes the mathematical security proof of the system and eliminates the possibility that an attacker could guess other users' information from partial shares.

3.1.2. Structural Security Proof Based on Decentralization

Fairness structure: The fairness mechanism of our proposed protocol, as illustrated in Figure 3, ensures that all participants either successfully reconstruct the secret simultaneously or fail together by progressively verifying messages in each recovery round, utilizing a hidden determination pointer to mark the end of the secret, and incorporating a sufficiently long random check sequence. Specifically, if cheating occurs before the secret's position or after the pointer is fully revealed, it will either be detected immediately or render both parties unable to confirm the secret; if cheating occurs after the secret's position but before the pointer is fully revealed, both parties still have a high probability of recovering the secret; the only scenario where a cheater could exclusively obtain the secret (cheating at the secret's exact position) has an extremely low probability (inversely proportional to the check sequence length), and when the check sequence is sufficiently long, this unfairness becomes negligible [4].

Decentralized structure: Our system architecture employs a decentralized structure [7], where the traditional QSS scheme's receiving parties (dealer and user) are granted equal status—each node can function either as a user for key distribution or as a dealer serving as the system receiver. This decentralized architecture eliminates the security risks and vulnerabilities inherent in centralized systems, while providing more flexible path selection options. The approach establishes a theoretical foundation for constructing and implementing multi-user network configurations.

3.2. Quantum Security

3.2.1. Quantum Security Analysis

As for the no-attack situation in Figure 2, we consider a three-user CV-QSS protocol where an honest dealer is selected among the participants, while users U_1 and U_2 prepare squeezed vacuum states (a_1, a_2). Mode a_2 is transmitted to the dealer through a noisy quantum channel, resulting in mode a_3 characterized by the following [4]:

$$\begin{aligned} x_3 &= \sqrt{\eta_1}x_2 + \sqrt{1-\eta_1}x_{N1}, \\ p_3 &= \sqrt{\eta_1}p_2 + \sqrt{1-\eta_1}p_{N1}, \end{aligned} \tag{2}$$

where η_1 denotes channel transmissivity, and $x_{N1}, p_{N1} \sim \mathcal{N}(0, \Sigma_1^2)$ denotes model additive Gaussian noise. The dealer then performs displacement modulation on a_3 using the message $X^{A/B}$, generating mode a_4:

$$\begin{aligned} x_4 &= x_3 + X_k^A, \\ p_4 &= p_3 + P_k^A, \end{aligned} \tag{3}$$

With $X_k^A, P_k^A \sim \mathcal{N}(X^{(A/B)}, \sigma^2)$ [19], the modulated state is sent back to U_1, undergoing channel noise to become a_5:

$$\begin{aligned} x_5 &= \sqrt{\eta_2}x_4 + \sqrt{1-\eta_2}x_{N2}, \\ p_5 &= \sqrt{\eta_2}p_4 + \sqrt{1-\eta_2}p_{N2}, \end{aligned} \tag{4}$$

where $x_{N2}, p_{N2} \sim \mathcal{N}(0, \Sigma_2^2)$ and η_2 is the reverse channel parameter. To compensate for channel loss, a_5 is amplified with gain $g = \sqrt{1/(\eta_1\eta_2)}$:

$$x_6 = gx_5. \tag{5}$$

A Bell measurement on a_1 and a_6 produces the following outcomes:

$$\begin{aligned} x_7 &= \tfrac{1}{\sqrt{2}}(x_6 + x_1), \quad p_7 = \tfrac{1}{\sqrt{2}}(p_6 + p_1), \\ x_8 &= \tfrac{1}{\sqrt{2}}(x_6 - x_1), \quad p_8 = \tfrac{1}{\sqrt{2}}(p_6 - p_1). \end{aligned} \tag{6}$$

For a squeezing parameter $r > 0$, the x_8 quadrature follows a Gaussian distribution:

$$x_8 = \frac{X_k^A}{\sqrt{2\eta_1}} + \frac{\sqrt{1-\eta_1}\,x_{N1}}{\sqrt{2\eta_1}} + \frac{\sqrt{1-\eta_2}\,x_{N2}}{\sqrt{2\eta_1\eta_2}} - e^{-r}\hat{x}_2^0. \tag{7}$$

The corresponding signal and noise variances are as follows:

$$V_s = \frac{\sigma^2}{2\eta_1}, \tag{8}$$

$$N_s = \frac{1-\eta_1}{2\eta_1}\Sigma_1^2 + \frac{1-\eta_2}{2\eta_1\eta_2}\Sigma_2^2 - e^{-2r}, \tag{9}$$

Yielding the signal-to-noise ratio $\gamma = V_s/N_s$, the mutual information is then:

$$I(S,R) = \frac{1}{2}\log_2(1+\gamma). \tag{10}$$

Therefore, we can ensure that communication is reliable under certain conditions [4]. Similarly, we can also ensure that communication is reliable under internal attacks because the channel transmission efficiency η is large enough [4,6,7]. This relies on the fact that each sub-channel between individual users and the dealer is generated through the frequency entanglement properties of an optical frequency comb. These sub-channels remain spectrally independent while maintaining phase locking via a common pump laser source. Consequently, multiplexed QSS signals can be simultaneously transmitted through a single optical fiber, thereby enhancing the system's multi-user scalability.

3.2.2. Numerical Simulation

The parameters in our experiment are as follows: The attenuation coefficient of a standard fiber link is δ = 0.2 dB/km; the detection efficiency and electronic noise of the imperfect heterodyne detector are μ = 0.6 and v_{el} = 0.05; the reconciliation efficiency is β = 0.98; and the system excess noise is ξ_0 = 0.001. The nonlinear coefficient is γ = 1.3 $\mathrm{W^{-1}km^{-1}}$; the dispersion parameter is $D = 16 \times 10^{-6}\ \mathrm{s/(m \cdot km)} = 16\ \mathrm{ps/(nm \cdot km)}$; the system repetition rate is $f_{\mathrm{rep}} = 5 \times 10^7$ Hz, and the crosstalk coefficient is $\xi = 10^{-R_e/10}$, where the extinction ratio is $R_e = 40$ dB.

For the system's maximum transmission distance and key rate [7], we first consider the point-to-point QKD key rate R_i and transmission distance between each user U_i and the designated dealer. The system key rate is given by $R = \min\{R_1, R_2, \ldots, R_{d-1}, R_{d+1}, \ldots, R_n\}$,

which reaches its minimum at the maximum transmission distance [6,7]. The asymptotic secret key rate lower bound for the QSS scheme is given by [27,28]:

$$R = \beta I_{\mathrm{UD}} - \chi_{\mathrm{DE}}, \tag{11}$$

where β is the reconciliation efficiency, I_{UD} is the mutual information between the user and dealer, and χ_{DE} is the Holevo bound between Eve and the dealer.

However, because our system multiplexes multi-channel QSS signals in a single fiber via optical frequency comb technology, we must account for noise induced by frequency differences rather than noise from users U_j coupled through highly asymmetric beam splitters (HABSs). On the one hand, when multiplexing multiple quantum signals through a single optical fiber, the generation of optical frequency combs (OFCs) in practical systems is fundamentally constrained by a finite extinction ratio R_e [19], while inter-channel guard bands are intentionally incorporated during system design [18,29]. Consequently, we must account for *inter-channel crosstalk noise* ($\varepsilon_{\mathrm{cro}}$). On the other hand, since chromatic dispersion causes unavoidable phase deviations [18,19], it is necessary to consider the nonlinear noise ($\varepsilon_{\mathrm{non}}$) [30,31]. Therefore, the total excess noise can be expressed as follows:

$$\varepsilon_{\mathrm{total}} = \varepsilon_{\mathrm{cro}} + \varepsilon_{\mathrm{non}} + \varepsilon_0 \tag{12}$$

where

$$\begin{aligned} \varepsilon_{\mathrm{cro}} &= 2(N-1)\cdot\xi\cdot V_a, \\ \varepsilon_{\mathrm{non}} &\propto \gamma^2 P_{\mathrm{avg}}^2 L_{\mathrm{eff}}^2 e^{-\alpha L}\frac{D\lambda^2}{c}\Delta f^2 \end{aligned} \tag{13}$$

where

- N is the total number of channels;
- L_{eff} is the effective length;
- Δf is the channel spacing.

Then, the channel-added noise can be expressed as follows:

$$\chi_{\mathrm{line}} = \frac{1}{T} - 1 + \varepsilon_{total} \tag{14}$$

and the noise between the dealer and user is given by the following:

$$\chi_{\mathrm{het}} = \frac{2-\mu+2v_{\mathrm{el}}}{\mu}, \tag{15}$$

Then, the overall noise can be expressed as follows:

$$\chi_{\mathrm{tot}} = \chi_{\mathrm{line}} + \frac{\chi_{\mathrm{het}}}{T}. \tag{16}$$

The Shannon mutual information between the user and dealer is as follows:

$$I_{\mathrm{UD}} = \log_2\left(\frac{V+\chi_{\mathrm{tot}}}{1+\chi_{\mathrm{tot}}}\right), \tag{17}$$

where $V = 1 + V_U$, and V_U is the modulation variance at the user.

Assuming the loss and noise in Bob's detector are trusted (inaccessible to eavesdroppers), the Holevo bound between Eve and the dealer is as follows:

$$\chi_{\mathrm{DE}} = \sum_{j=1}^{2} G\left(\frac{\lambda_j - 1}{2}\right) - \sum_{j=3}^{5} G\left(\frac{\lambda_j - 1}{2}\right), \tag{18}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$, and λ_j are the symplectic eigenvalues derived from the covariance matrix:

$$\lambda_{1,2}^2 = \frac{1}{2}\left[A \pm \sqrt{A^2 - 4B}\right], \tag{19}$$

where

$$A = V^2(1-2T) + 2T + T^2(V + \chi_{\text{line}})^2 \tag{20}$$

$$B = T^2(V\chi_{\text{line}} + 1)^2, \tag{21}$$

and

$$\lambda_{3,4}^2 = \frac{1}{2}\left[C \pm \sqrt{C^2 - 4D}\right], \tag{22}$$

where

$$\begin{aligned} C = &\frac{1}{T^2(V+\chi_{\text{tot}})^2}\Big\{A(\chi_{\text{het}})^2 + B + 1 \\ &+2\chi_{\text{het}}\left[V\sqrt{B} + T(V+\chi_{\text{line}}) + 2T(V^2-1)\right]\Big\}, \end{aligned} \tag{23}$$

$$D = \left(\frac{V + \sqrt{B}\chi_{\text{het}}}{T(V+\chi_{\text{tot}})}\right)^2, \tag{24}$$

$$\lambda_5 = 1 \tag{25}$$

Subsequently, we use the maximum likelihood estimation (MLE) mentioned in Appendix A to determine the channel parameters, thereby achieving a more precise estimation of the upper bound for the asymptotic key rate.

4. Performance Analysis and Discussion

In Figure 4, we compare the key rate and distance relationships between the traditional chain-structured DQSS scheme and the OFC-based CV-QSS scheme under different user scenarios. As shown in the results, under identical parameter conditions, the OFC-based CV-QSS scheme achieves a 50% improvement in maximum transmission distance compared with the traditional chain-structured DQSS scheme. Moreover, this performance gap widens as the number of users increases.

In other words, similar to other chain-structured CV-QSS schemes [6,7], the maximum transmission distance of chain-structured DQSS schemes decreases significantly with increasing user count. By contrast, the OFC-based QSS scheme exhibits a substantially smaller reduction in maximum transmission distance as the number of users grows.

This outcome aligns with our theoretical expectations. In traditional chain-structured QSS schemes, the channel-added noise is given by the following:

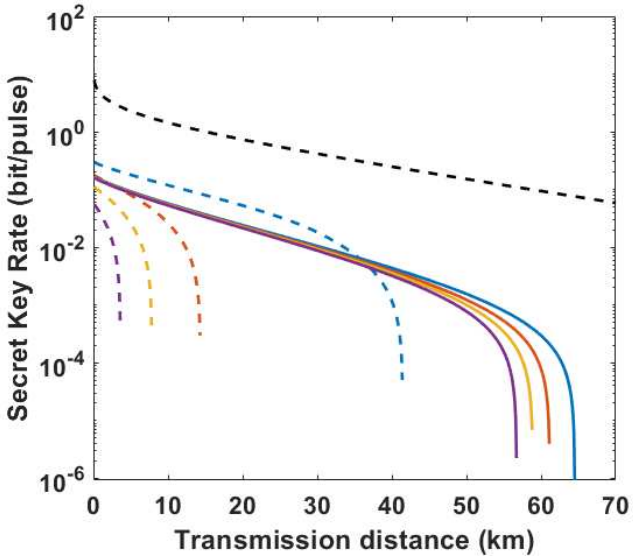
$$\chi_{\text{line}} = \frac{1}{T} - 1 + \sum_{j=1}^{n} \xi_j, \tag{26}$$

where each ξ_j increases with transmission distance, resulting in n-fold amplification. Conversely, in our proposed OFC-based CV-QSS scheme, an increase in distance or in the number of users causes only a single change in the variables ε_{cro} and ε_{non} in

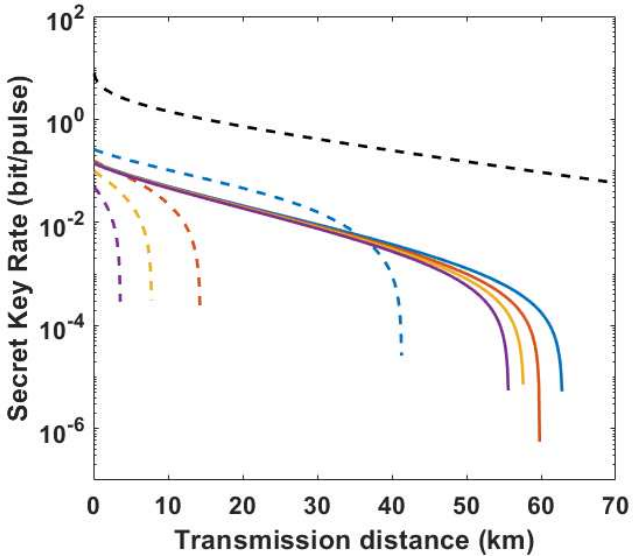
$$\chi_{\text{line}} = \frac{1}{T} - 1 + \varepsilon_{total} = \text{line} = \frac{1}{T} - 1 + \varepsilon_{\text{cro}} + \varepsilon_{\text{non}} + \varepsilon_0 \tag{27}$$

At the system level, an inverse correlation constraint exists among key rate, transmission distance, and user capacity; enhancing any one of these parameters inevitably

compromises the other two. This aligns with fundamental physical limits and constitutes an intrinsic characteristic of QSS schemes.



(**a**)



(**b**)

Figure 4. (**a**) Secretkey rate versus transmission distance for the proposed OFC-based quantum secret sharing scheme (solid line) and the decentralized quantum secret sharing scheme (dotted line). (**b**) Secret key rate under finite-size composable security analysis versus transmission distance for the proposed OFC-based quantum secret sharing scheme (solid line) and the decentralized quantum secret sharing scheme (dotted line). The blue, orange, yellow, and purple lines correspond to user quantities of $n = 3, 10, 15$, and 20, respectively. The black dotted line denotes the Piradola–Laurenza–Ottaviani–Banchi (PLOB) bound.

5. Conclusions

In this paper, we proposed an optical frequency comb-based continuous-variable quantum secret sharing (OFC CV-QSS) scheme that overcomes multi-user scalability limitations by replacing chain topologies with highly asymmetric beam splitters (HABSs) with OFC-generated parallel quantum channels. This eliminates the need to aggregate cumulative noise from sequential user couplings in system key rate calculations. Beyond inherent quantum-layer security, our solution establishes dual protection—the Chinese

remainder theorem (CRT) ensures mathematical security for classical shadows through information-theoretic irreversibility, while decentralized architectures enforce structural security via distributed control and collaborative reconstruction. Numerical simulations confirm that the scheme achieves a substantially extended maximum transmission distance compared with chain-QSS, with significantly slower performance degradation as users scale, while maintaining full compatibility with existing fiber infrastructure. Future work will focus on experimental validation and OFC spectral optimization.

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

Funding: This research was funded 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.

Abbreviations

The following abbreviations are used in this manuscript:

QSS	Quantum secret sharing
CV-QSS	Continuous-Variable Quantum Secret Sharing
OFC	Optical Frequency Comb
CRT	Chinese Remainder Theorem
WDM	Wavelength Division Multiplexing
TMSV	Two-Mode Squeezed Vacuum
PLL	Phase-Locked Loop
CV-QKD	Continuous-Variable Quantum Key Distribution
LDPC	Low-Density Parity-Check
HABS	Highly Asymmetric Beam Splitters
DQSS	Decentralized Quantum Secret Sharing
MLE	Maximum Likelihood Estimation
EC	Error Correction
AEP	Asymptotic Equipartition Property
SNR	Signal-to-Noise Ratio

Appendix A

The maximum likelihood estimators are employed to characterize channel parameters, thereby enabling tighter bounds on the achievable key rate. Based on finite-size regime assumptions and composable security analysis [28,32,33], the secret key rate is proven to satisfy the inequality:

$$R_{M,r} \geq (1-r)p\left[R_{\epsilon_{\mathrm{PE}}} - \frac{1}{\sqrt{(1-r)M}}\Delta_{\mathrm{AEP}}\left(p\epsilon_{\mathrm{s}}^2/3, N\right) + \frac{\log_2\left[p\left(1-\epsilon_{\mathrm{s}}^2/3\right)\right] + 2\log_2\sqrt{2}\epsilon_{\mathrm{h}}}{(1-r)M}\right], \tag{A1}$$

- M: Total signal states transmitted by Alice.

- m: Number of signal states (from a block M) for which Alice discloses the encoding k, with $r = \frac{m}{M}$.
- p: Error correction (EC) success probability.
- $R_{\epsilon_{\mathrm{PE}}}$: Finite-size key rate.
- $\epsilon_{\mathrm{tot}} = \epsilon_{\mathrm{cor}} + \epsilon_{\mathrm{s}} + \epsilon_{\mathrm{h}} + p\epsilon_{\mathrm{PE}}$: Total security error.
- Δ_{AEP}: Asymptotic equipartition property term, defined as follows:

$$\Delta_{\mathrm{AEP}}(\epsilon_{\mathrm{s}}, |\mathcal{L}|) := 4\log_2\left(2\sqrt{|\mathcal{L}|}+1\right)\sqrt{\log(2/\epsilon_{\mathrm{s}}^2)}, \tag{A2}$$

where $|\mathcal{L}|$ denotes the cardinality of the dealer's outcome, which equals N in our scheme.

References

1. Hillery, M.; Bužek, V.; Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **1999**, *59*, 1829. [CrossRef]
2. Karlsson, A.; Koashi, M.; Imoto, N. Quantum entanglement for secret sharing and secret splitting. *Phys. Rev. A* **1999**, *59*, 162–168. [CrossRef]
3. Zhang, Z.j.; Man, Z.x. Multiparty quantum secret sharing of classical messages based on entanglement swapping. *Phys. Rev. A* **2005**, *72*, 022303. [CrossRef]
4. Kang, Y.; Guo, Y.; Zhong, H.; Chen, G.; Jing, X. Continuous Variable Quantum Secret Sharing with Fairness. *Appl. Sci.* **2019**, *10*, 189. [CrossRef]
5. Schmid, C.; Trojek, P.; Bourennane, M.; Kurtsiefer, C.; Zukowski, M.; Weinfurter, H. Experimental Single Qubit Quantum Secret Sharing. *Phys. Rev. Lett.* **2005**, *95*, 230505. [CrossRef] [PubMed]
6. Grice, W.P.; Qi, B. Quantum secret sharing using weak coherent states. *Phys. Rev. A* **2019**, *100*, 022339. [CrossRef]
7. Peng, R.; Guo, Y.; Wang, Y.; Liao, Q. Decentralized continuous-variable quantum secret sharing. *Quantum Inf. Process.* **2023**, *22*, 368. [CrossRef]
8. Liao, Q.; Liu, X.; Ou, B.; Fu, X. Continuous-Variable Quantum Secret Sharing Based on Multi-Ring Discrete Modulation. *IEEE Trans. Commun.* **2023**, *71*, 6051–6060. [CrossRef]
9. Veselka, J.; Korotky, S. A multiwavelength source having precise channel spacing for WDM systems. *IEEE Photonics Technol. Lett.* **1998**, *10*, 958–960. [CrossRef]
10. Millar, D.S.; Maher, R.; Lavery, D.; Koike-Akino, T.; Pajovic, M.; Alvarado, A.; Paskov, M.; Kojima, K.; Parsons, K.; Thomsen, B.C.; et al. Design of a 1 Tb/s Superchannel Coherent Receiver. *J. Light. Technol.* **2016**, *34*, 1453–1463. [CrossRef]
11. Lorences-Riesgo, A.; Eriksson, T.A.; Fülöp, A.; Andrekson, P.A.; Karlsson, M. Frequency-Comb Regeneration for Self-Homodyne Superchannels. *J. Light. Technol.* **2016**, *34*, 1800–1806. [CrossRef]
12. Lorences-Riesgo, A.; Mazur, M.; Eriksson, T.A.; Andrekson, P.A.; Karlsson, M. Self-homodyne 24 × 32-QAM superchannel receiver enabled by all-optical comb regeneration using brillouin amplification. *Opt. Express* **2016**, *24*, 29714–29723. [CrossRef] [PubMed]
13. Mazur, M.; Lorences-Riesgo, A.; Schröder, J.; Andrekson, P.A.; Karlsson, M. High Spectral Efficiency PM-128QAM Comb-Based Superchannel Transmission Enabled by a Single Shared Optical Pilot Tone. *J. Light. Technol.* **2018**, *36*, 1318–1325. [CrossRef]
14. Mazur, M.; Schröder, J.; Lorences-Riesgo, A.; Yoshida, T.; Andrekson, P.A. 11.5 bits/s/Hz PM-256QAM Comb-Based Superchannel Transmission by Combining Optical and Digital Pilots. 2018. Available online: https://api.semanticscholar.org/CorpusID:49190505 (accessed on 29 June 2025).
15. Lundberg, L.; Mazur, M.; Lorences-Riesgo, A.; Karlsson, M.; Andrekson, P.A. Joint Carrier Recovery for DSP Complexity Reduction in Frequency Comb-Based Superchannel Transceivers. In Proceedings of the 2017 European Conference on Optical Communication (ECOC), Gothenburg, Sweden, 17–21 September 2017.
16. Liu, C.; Pan, J.; Detwiler, T.; Stark, A.; Hsueh, Y.T.; Chang, G.K.; Ralph, S.E. Joint digital signal processing for superchannel coherent optical communication systems. *Opt. Express* **2013**, *21*, 8342–8356. [CrossRef]
17. Souto, D.V.; Olsson, B.E.; Larsson, C.; Mello, D.A.A. Joint-Polarization and Joint-Subchannel Carrier Phase Estimation for 16-QAM Optical Systems. *J. Light. Technol.* **2012**, *30*, 3185–3191. [CrossRef]
18. Lundberg, L.; Karlsson, M.; Lorences-Riesgo, A.; Mazur, M.; Torres-Company, V.; Schröder, J.; Andrekson, P.A. Frequency Comb-Based WDM Transmission Systems Enabling Joint Signal Processing. *Appl. Sci.* **2018**, *8*, 718. [CrossRef]
19. Wang, Y.; Mao, Y.; Huang, W.; Huang, D.; Guo, Y. Optical frequency comb-based multichannel parallel continuous-variable quantum key distribution. *Opt. Express* **2019**, *27*, 25314–25329. [CrossRef]
20. Kippenberg, T.J.; Holzwarth, R.; Diddams, S.A. Microresonator-Based Optical Frequency Combs. *Science* **2011**, *332*, 555–559. [CrossRef] [PubMed]

21. Rueda, A.; Sedlmeir, F.; Kumari, M.; Leuchs, G.; Schwefel, H.G.L. Resonant electro-optic frequency comb. *Nature* **2019**, *569*, E11. [CrossRef]
22. Spencer, D.T.; Drake, T.; Briles, T.C.; Stone, J.; Sinclair, L.C.; Fredrick, C.; Li, Q.; Westly, D.; Ilic, B.R.; Bluestone, A.; et al. An optical-frequency synthesizer using integrated photonics. *Nature* **2018**, *557*, 81–85. [CrossRef]
23. Huang, J.; Chen, X.; Li, X.; Wang, J. Chip-based photonic graph states. *AAPPS Bull.* **2023**, *33*, 14. [CrossRef]
24. Zeng, H.; Du, M.M.; Zhong, W.; Zhou, L.; Sheng, Y.B. High-capacity device-independent quantum secure direct communication based on hyper-encoding. *Fundam. Res.* **2024**, *4*, 851–857. [CrossRef]
25. Shen, A.; Cao, X.Y.; Wang, Y.; Fu, Y.; Gu, J.; Liu, W.B.; Weng, C.X.; Yin, H.L.; Chen, Z.B. Experimental quantum secret sharing based on phase encoding of coherent states. *Sci. China-Phys. Mech. Astron.* **2023**, *66*, 260311. [CrossRef]
26. Corcoran, B.; Mitchell, A.; Morandotti, R.; Oxenlowe, L.K.; Moss, D.J. Optical microcombs for ultrahigh-bandwidth communications. *Nat. Photonics* **2025**, *19*, 451–462. [CrossRef]
27. Grosshans, F.; Grangier, P. Continuous Variable Quantum Cryptography Using Coherent States. *Phys. Rev. Lett.* **2002**, *88*, 057902. [CrossRef] [PubMed]
28. Fossier, S.; Diamanti, E.; Debuisschert, T.; Tualle-Brouri, R.; Grangier, P. Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers. *J. Phys. B At. Mol. Opt. Phys.* **2009**, *42*, 114014. [CrossRef]
29. Liu, X.; Chandrasekhar, S.; Winzer, P.J. Digital Signal Processing Techniques Enabling Multi-Tbs Superchannel Transmission: An overview of recent advances in DSP-enabled superchannels. *IEEE Signal Process. Mag.* **2014**, *31*, 16–24. [CrossRef]
30. Temprana, E.; Myslivets, E.; Kuo, B.P.; Liu, L.; Ataie, V.; Alic, N.; Radic, S. Overcoming Kerr-induced capacity limit in optical fiber transmission. *Science* **2015**, *348*, 1445–1448. [CrossRef] [PubMed]
31. Agrawal, G.P. *Fiber-Optic Communication Systems*, 4th ed.; John Wiley Sons: Hoboken, NJ, USA, 2010; ISBN 978-0-470-50511-3. Available online: https://www.wiley.com/en-us/Fiber+Optic+Communication+Systems%2C+4th+Edition-p-9780470505113 (accessed on 29 June 2025).
32. Papanastasiou, P.; Pirandola, S. Continuous-variable quantum cryptography with discrete alphabets: Composable security under collective Gaussian attacks. *Phys. Rev. Res.* **2021**, *3*, 013047. [CrossRef]
33. Ghorai, S.; Grangier, P.; Diamanti, E.; Leverrier, A. Asymptotic Security of Continuous-Variable Quantum Key Distribution with a Discrete Modulation. *Phys. Rev. X* **2019**, *9*, 021059. [CrossRef]