entropy

MDPI

Article

Continuous-Variable Quantum Secret Sharing Based on Thermal Terahertz Sources in Inter-Satellite Wireless Links

Chengji Liu [1], Changhua Zhu [1,2,3,*], Zhihui Li [4], Min Nie [3,5], Hong Yang [1,6] and Changxing Pei [1]

1 State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China; liuchengjixidian@163.com (C.L.); 13381105509@189.cn (H.Y.); chxpei@xidian.edu.cn (C.P.)
2 Collaborative Innovation Center of Quantum Information of Shaanxi Province, Xidian University, Xi'an 710071, China
3 Shaanxi Key Laboratory of Information Communication Network and Security, Xi'an University of Posts & Telecommunications, Xi'an 710121, China; niemin@xupt.edu.cn
4 School of Mathematics and Statistics, Shannxi Normal University, Xi'an 710119, China; lizhihui@snnu.edu.cn
5 School of Communications and Information Engineering, Xi'an University of Posts & Telecommunications, Xi'an 710121, China
6 Institute of Spacecraft System Engineering, China Academy of Space Technology (CAST), Beijing 100094, China
* Correspondence: chhzhu@xidian.edu.cn

Abstract: We propose a continuous-variable quantum secret sharing (CVQSS) scheme based on thermal terahertz (THz) sources in inter-satellite wireless links (THz-CVQSS). In this scheme, firstly, each player locally preforms Gaussian modulation to prepare a thermal THz state, and then couples it into a circulating spatiotemporal mode using a highly asymmetric beam splitter. At the end, the dealer measures the quadrature components of the received spatiotemporal mode through performing the heterodyne detection to share secure keys with all the players of a group. This design enables that the key can be recovered only by the whole group players' knowledge in cooperation and neither a single player nor any subset of the players in the group can recover the key correctly. We analyze both the security and the performance of THz-CVQSS in inter-satellite links. Results show that a long-distance inter-satellite THz-CVQSS scheme with multiple players is feasible. This work will provide an effective way for building an inter-satellite quantum communication network.

Keywords: continuous-variable; quantum secret sharing; terahertz band; thermal state; inter-satellite communication

check for updates

Citation: Liu, C.; Zhu, C.; Li, Z.; Nie, M.; Yang, H.; Pei, C. Continuous-Variable Quantum Secret Sharing Based on Thermal Terahertz Sources in Inter-Satellite Wireless Links. *Entropy* **2021**, *23*, 1223. https://doi.org/10.3390/e23091223

Academic Editor: Rosario Lo Franco

Received: 28 July 2021
Accepted: 15 September 2021
Published: 17 September 2021

1. Introduction

Standard point-to-point quantum key distribution (QKD) based on the fundamental laws of quantum mechanism can achieve unconditionally secure key establishment on unsafe channels [1–4]. Generally speaking, QKD can be further divided into two types according to different modulation methods, i.e., discrete-variable (DV) QKD [5–9] and continuous-variable (CV) QKD [10–13]. Compared with DVQKD systems, CVQKD systems can be easily integrated with traditional optical communication systems and do not necessitate single photon detectors [14,15]. At present, most QKD schemes use photons to carry encoded information through free space or telecom fiber channels for transmission. Nevertheless, as wireless communications rapidly develop, the leakage of information and the scarcity spectrum resources have become increasingly serious. Nowadays, terahertz (THz) communication is envisaged to be a key technology to meet the needs of high-speed data transmission due to the large availability of its bandwidth, especially for short-distance high-speed wireless communication [16,17] and satellite communication [18,19].

THz communication which is also conceived as one of the key technologies of 6G communication can be quantum secure by using QKD at THz bands. Compared with free-space optical communication, THz communication has the advantage of better penetrating

power in the presence of fog, dust, and atmospheric turbulence, etc.; and compared with the microwave communication, it has larger capacity and better directionality. However, THz communication has a fatal weakness in the atmosphere, that is, it is easily absorbed by the pervasive atmospheric water molecules, which severely limits its communication distance [20,21]. Fortunately, THz communication is feasible in inter-satellite links since the concentration of water molecules there can be negligible and a previous work has studied the feasibility [18]. Thus, THz communication can provide an efficient path to build inter-satellite quantum communication networks.

With development of communication networks, the point-to-point QKD system may be difficult to meet the requirements of multi-party secret key sharing (at least 3 players). In this paper, we extend the standard point-to-point CVQKD to a (n, n) threshold quantum secret sharing (QSS) protocol that allows multiple players to share keys securely. The (n, n) threshold QSS which has been proven high security and efficiency with important practical applications based quantum technology [22–25], means that the dealer securely distributes the secret to n remote players; the secret can be recovered only by the whole group players' knowledge in cooperation; a single player or any subset of the players in the group cannot recover the secret correctly. As a rule, QSS schemes involve more players than point-to-point QKD schemes and some players may be dishonest. Thus, QSS schemes will suffer additional attacks to make its security analysis more demanding than QKD schemes. In 2013, Lau et al. [26] utilized CVQKD technology for the first time to analyze the security of CVQSS. In 2017, Kogias et al. [27] proposed the security proof of entanglement-based CVQSS against both dishonest players and eavesdroppers appeared in the channels. Nevertheless, this protocol may hard to be implemented with the current technology when the number of players is large. Moreover, the tolerable losses of the channel in the protocol are very small.

To alleviate the implementation difficulties of entanglement-based QSS, some previous works [28,29] have proposed single qubit sequential QSS schemes. However, the general security of these schemes is still contentious [30,31]. In particular, these schemes are vulnerable to Trojan horse attacks owing to that such a design allows a spiteful eavesdropper Eve to accurately determine the corresponding polarization rotation by measuring the output of multi-photon signals she sends to the polarization rotation device of the targeted player in the link. Recently, Grice et al. [32] proposed a sequential CVQSS protocol by employing double homodyne detectors and traditional laser sources. The main idea of the protocol is that each player locally preform Gaussian modulation to prepare a standard coherent state and merges it into a circulating spatiotemporal mode by using a beam splitter. This design can prevent the eavesdropper from accessing the preparation process of quantum states, so that the protocol is immune to Trojan horse attacks. More recently, some further works [33–35] have been proposed to improve the performance of the sequential CVQSS protocol. Wu et al. [33] proposed a more convenient implementation of sequential CVQSS by using a thermal source and further improved the tolerance of the number of players. Liao et al. [34] further improved the maximal transmission distance of sequential CVQSS by using discrete modulated coherent states. Wang et al. [35] proposed an improved (t, n) threshold sequential CVQSS scheme based on the Lagrange interpolation formula and Gaussian modulated coherent states.

In this paper, inspired by Grice et al.'s work [32], we propose a CVQSS scheme based on thermal THz sources in inter-satellite wireless links (THz-CVQSS). In this scheme, instead of using optical photons to carry information and transmitting them by wired telecom fiber channels, we use THz photons to carry information and transmit them through wireless inter-satellite links. Similar to the original sequential CVQSS, the main idea of THz-CVQSS is that each player locally preforms Gaussian modulation to prepare a standard Gaussian-modulated thermal state (GMTS) and couples it into a circulating spatiotemporal mode using a highly asymmetric beam splitter (HABS), which can be efficiently immune to Trojan horse attacks. We apply an inter-satellite channel model to the THz-CVQSS and analyze both the security and the performance of the protocol. Simulation

results strongly support the feasibility of the long-distance THz-CVQSS in inter-satellite links.

This paper is organized as follows. In Section 2, we show details of THz-CVQSS and analyze its security. In Section 3, we evaluate the secret key rate in inter-satellite links. Finally, in Section 4, we draw the conclusions.

2. The Proposed Quantum Secret Sharing Protocol and Its Security

The schematic diagram of the proposed QSS protocol is shown in Figure 1. n players (Bob_1, Bob_2, ..., Bob_n) are linked with the dealer by a single quantum channel such as a inter-satellite channel (see Section 3.1 for details). For each round of quantum transmission, the first player (Bob_1) at one far end of the link generates a pair of independent Gaussian random numbers $\{x_1, p_1\}$ (zero mean) and uses them to modulate the output of the local THz source through amplitude and phase modulators to prepare a GMTS $|x_1 + jp_1\rangle$, where j denotes the imaginary unit. The state prepared by Bob_1 is then sent to the adjacent player Bob_2. For now, Bob_2 also prepares a GMTS $|x_2 + jp_2\rangle$ and couples it with the transmitted state from Bob_1 into the same spatiotemporal mode through a HABS (the transmittance $T_B \cong 1$). All the other players in the link perform similar operations. At final, the state that the dealer receives can be expressed as $\left|\sum_{i=1}^{n}\sqrt{T_i}x_i + j\sum_{i=1}^{n}\sqrt{T_i}p_i\right\rangle$, where T_i is the channel transmittance experienced by the quantum signal between the dealer and the i-th player. The dealer uses the heterodyne detector to measure quadrature components of the received states. In the case of heterodyne detection, the quantum signal is split using a balanced beam splitter. One arm is used to measure the quadrature component X and the other one is used to measure the quadrature component P after $\pi/2$ phase shift of local oscillator. This operation can allow the dealer to share a secure key which can only be recovered by all n players in cooperation but not by any subset of less than n players. The details of the protocol are as follows.

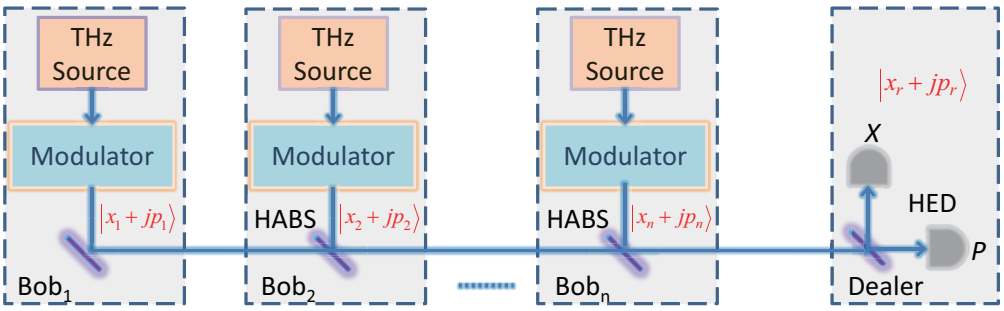

Figure 1. Structure diagram of THz-CVQSS system. HABS, highly asymmetric beam splitter; HED, heterodyne detector.

Step 1 (Preparation). For each round of quantum transmission, n players (Bob_1, Bob_2, ..., Bob_n) each locally prepare a thermal Gaussian state $|x_i + jp_i\rangle (i = 1, 2, \ldots, n)$ based on THz sources, Gaussian random numbers $\{x_i, p_i\}_{i=1}^{n}$ and modulators at their stations.

Step 2 (Transmission). First of all, the first player Bob_1 sends the prepared state $|x_1 + jp_1\rangle$ to the nearest player Bob_2. After receiving Bob_1's quantum state, Bob_2 couples his state and the received state to the same spatiotemporal mode by using the HABS. The merged quantum state is then sent to the next player.

The remaining players in the link perform similar operations, so that they can inject the locally prepared state into the same spatiotemporal mode as Bob_1. Finally, the state arriving at the dealer's station can be expressed as $\left|\sum_{i=1}^{n}\sqrt{T_i}x_i + j\sum_{i=1}^{n}\sqrt{T_i}p_i\right\rangle$.

Step 3 (Detection). After receiving the quantum signal state, the dealer performs heterodyne detection to measure its quadrature components and then obtain the measurement results (x_r, p_r) which are kept as raw data. Repeat the above procedure many rounds until the dealer obtains sufficient raw data.

Step 4 (Post-processing). The remaining steps use classical post-processing technologies to process these raw data.

Step 4.1. The dealer and all the players randomly choose and disclose a group of the raw data to deduce the channel transmittances $\{T_i\}_{i=1}^n$[32]. Then all the players discard their disclosed Gaussian random numbers to prevent the eavesdropper from obtaining information about the key.

Step 4.2. The dealer assume that all the players except Bob_1 are dishonest (if all the players are dishonest, then the QSS protocol is meaningless).

Step 4.3. The dealer randomly choose another group of raw data and requests all dishonest players to disclose their corresponding Gaussian random numbers.

Step 4.4. The dealer can displace measurement results of the group in step 4.3 utilizing $x_M = x_r - \sum_{i=2}^n \sqrt{T_i} x_i$ and $p_M = p_r - \sum_{i=2}^n \sqrt{T_i} p_i$. Therefore, a two-party CVQKD between the dealer and Bob_1 is established. Then they can estimate a lower bound of secret key rate (SKR) R_1 with the standard post-processing procedures in the GMTS QKD [12,36]. After that, all the players abandon the disclosed data.

Step 4.5. Repeat steps 4.2–4.4 n times. In each round, the dealer chooses a different player as the honest player and at final obtains n secret key rates $\{R_i\}_{i=1}^n$.

Step 4.6. Finally, the dealer employs the minimum of $\{R_i\}_{i=1}^n$ as the SKR of the THz-CVQSS protocol and obtains the final SKR from undisclosed data by taking advantage of the reverse reconciliation method. The dealer can use the final shared key to implement a QSS protocol. Through cooperation, n players can recover the shared key. However, any group of fewer n players cannot recover the shared key correctly, since only an exponentially small amount of information about the shared key can be obtained by them.

Next, we will analyze the security of the protocol. In a word, the proposed QSS protocol actually establishes n independent point-to-point CVQKD links in each round of quantum transmission. As assumed in steps 4.2–4.5, there is a honest player (Bob_i) and the remaining $n-1$ dishonest players in each CVQKD. Note that this assumption is the worst case, since if all the players are dishonest, then the QSS is meaningless. In this most pessimistic case, the QSS is actually reduced to a standard CVQKD model, that is, there are two legitimate players, i.e., the sender, Bob_i and the receiver, Alice (the dealer). Now we need to analyze whether the remaining $n-1$ players (and potential eavesdroppers in the channel) can cooperate to recover the key shared by Bob_i and Alice. As mentioned in step 4.3, the dealer requests all the players except Bob_i to publish their corresponding Gaussian random numbers, which makes Bob_i own the complete information of all the players, while the remaining $n-1$ players cannot infer the information about the shared key between Bob_i and Alice in this CVQKD link. As a result, whether there are $n-1$ dishonest players or not, Alice and Bob_i can share a secure key. As for the eavesdroppers in the channel, we can consider their quantum attack in each individual CVQKD link. This allows us to apply the standard security proof of GMTS QKD. Some previous work [11,12] has proved the security of GMTS QKD. Thus, we can use the existing security proof for GMTS QKD to evaluate the SKR of THz-CVQSS. In addition, since the players inject the locally prepared thermal Gaussian states into the circulating spatiotemporal mode, the detection signals of the eavesdropper cannot reach the modulators within the secure stations of the honest players. In other words, the honest players can prevent the eavesdropper from accessing the preparation process of the signal states, so that the protocol is immune to Trojan horse attacks.

3. Secret Key Rate in Inter-Satellite Links

3.1. Channel Model

In recent years, THz communication is considered to be one of the key technologies to prop up the growing demand of high-speed wireless communication networks. When THz waves propagate through a free space channel, it can be impaired by turbulence, scattering, and absorption, etc. As we mentioned in the introduction, these atmosphere effects limit the transmission performance of THz waves. Nevertheless, in inter-satellite links, the beam

drift effect can be neglected and the absorption of atmospheric water molecules is nearly insignificant, which can allow us to approximatively present a diffraction-only channel model as a immovable attenuation. The loss caused by the diffraction effect is only derived from the size of the diffracted beam at the receiving aperture. Thus, the transmittance T can be expressed as [18]

$$T = 1 - \exp[-2(r_a/l)^2], \tag{1}$$

where, r_a stands for the receiving aperture radius, and l stands for the beam radius of THz waves at transmission distance d. Taking advantage of the Gaussian approximation, l can be expressed as

$$l = r_b\sqrt{1 + (\lambda d/\pi r_b^2)^2}, \tag{2}$$

where r_b is the beam-waist radius, and λ is the wavelength of THz waves.

In this channel model, we assume that both the receiving aperture radius r_a and the beam-waist radius r_b to 0.6 m [13] and the environment temperature is 30 K [37].

3.2. Secret Key Rate

Now, we will apply inter-satellite links to estimate the SKR of the QSS protocol. According to step 4.6, the final SKR is the minimum of $\{R_i\}_{i=1}^n$. We assume that the transmission distance between the dealer (Alice) and the farthest player (Bob) is d and the other $n-1$ players are located between them at same intervals. Each player introduces the same amount of noise ξ_0. Theoretically, the smallest SKR comes from the farthest player. However, the smallest SKR in a realistic QSS system must be estimated according to the practical data, so it does not necessarily come from the farthest player. Thus, when Alice implement the proposed QSS protocol in practice, she should employ the experimental data to evaluate SKR of each player, and select the smallest one as the SKR of QSS. The asymptotic SKR of the protocol by using reverse reconciliation can be calculated by [38,39]

$$R = \beta I_{AB} - \chi_{AE}, \tag{3}$$

where I_{AB} is the mutual information between Alice and Bob, β is the reconciliation efficiency, and χ_{AE} is the Holevo bound information available to the eavesdropper Eve and the other dishonest players on Alice's measurement. Note that in this protocol, classical information is passed from Alice to the players for reverse reconciliation.

The transmittance of the i-th player in the inter-satellite channel can be calculated by

$$T_i = 1 - \exp(-2{r_a}^2/l_i^2), \tag{4}$$

where,

$$l_i = r_b\sqrt{1 + (\lambda d_i/\pi r_b^2)^2}, \tag{5}$$

and $d_i = \frac{n-i+1}{n}d$ is the transmission distance between the dealer and the i-th player. Thus, when referred to the channel input, the excess noise contributed by the i-th player, expressed in shot noise units, can be given by [32]

$$\xi_i = \xi_0\frac{T_i}{T_1}. \tag{6}$$

The excess noise is an additional noise except vacuum noise which is mainly caused by the imperfection of system, e.g., modulation noise, Raman noise, background light, etc. Therefore, the total channel-added noise referred to the channel input can be defined as

$$\chi_{\text{line}} = \frac{1 - T_1}{T_1} + \sum_{i=1}^{n}\xi_i, \tag{7}$$

where, $(1 - T_1)/T_1$ represents the channel loss. The heterodyne detection added noise referred to Alice's input is given by

$$\chi_{\text{het}} = \frac{(2-\eta+2v_{el})}{\eta}, \tag{8}$$

where, η denotes the detection efficiency and v_{el} denotes electronics noise of Alice's detector.

The overall noise referred to the channel input can then be expressed as

$$\chi_{\text{tot}} = \chi_{\text{line}} + \frac{\chi_{\text{het}}}{T_1}. \tag{9}$$

The mutual information between Alice and Bob can be calculated by [12]

$$I_{AB} = \log_2 \frac{V+\chi_{\text{tot}}}{1+\chi_{\text{tot}}}, \tag{10}$$

where, $V = V_M + V_0$, V_M is the modulation variance of Bob and V_0 is the shot noise given by [12]

$$V_0 = 2\bar{n} + 1, \tag{11}$$

where,

$$\bar{n} = \frac{1}{\exp(f\hbar/k_T\tau_B) - 1}, \tag{12}$$

f is the frequency of quantum signals, $\hbar$ is Planck's constant, k_T is Boltzmann's constant, and τ_B is the absolute temperature.

For reverse reconciliation, Eve's information is bounded by the Holevo bound χ_{AE} which can be calculated by [39]

$$\chi_{AE} = S(\rho_E) - \int P(x_A, p_A) S\left(\rho_E^{x_A,p_A}\right) dx_A, p_A \tag{13}$$

where $S(\cdot)$ is the von Neumann entropy. $\rho_E^{x_A,p_A}$ is Eve's conditional density operator for the states on Alice's measurement result. $P(x_A, p_A)$ is the measured probability density. x_A and p_A are Alice's measurement results. We assume that the noise and loss of Alice's detector are trusted and cannot be accessed by Eve, then χ_{AE} can be further calculated by [39]

$$\chi_{AE} = \sum_{i=1}^{2} h(v_i) - \sum_{i=3}^{5} h(v_i), \tag{14}$$

where $h(x) = (\frac{x+1}{2})\log_2(\frac{x+1}{2}) - (\frac{x-1}{2})\log_2(\frac{x-1}{2})$, and

$$v_{1,2}^2 = \frac{1}{2}\left[\Delta_1 \pm \sqrt{\Delta_1^2 - 4\Delta_2}\right], \tag{15}$$

where,

$$\Delta_1 = 2T_1 + T_1^2(V+\chi_{\text{line}})^2 + V^2(1-2T_1), \tag{16}$$

$$\Delta_2 = (V\chi_{\text{line}} + 1)^2 T_1^2, \tag{17}$$

$$v_{3,4}^2 = \frac{1}{2}\left[\Delta_3 \pm \sqrt{\Delta_3^2 - 4\Delta_4}\right], \tag{18}$$

where,

$$\begin{aligned}\Delta_3 = &\frac{1}{[T_1(V+\chi_{\text{tot}})]^2}\Big\{\Delta_1\chi_{\text{het}}^2 + 1 + \Delta_2 + 2\chi_{\text{het}} \\ &\times[T_1(V+\chi_{\text{line}}) + V\sqrt{\Delta_2}] + 2\left(V^2-1\right)T_1\Big\},\end{aligned} \tag{19}$$

$$\Delta_4 = \left(\frac{V+\sqrt{\Delta_2}\chi_{\text{het}}}{T_1(V+\chi_{\text{tot}})}\right)^2, \tag{20}$$

and

$$v_5 = 1. \tag{21}$$

3.3. Simulation and Discussion

In this section, we will show the performance of THz-CVQSS. We assume that the transmission distance between the dealer and the farthest player is at least 1500 km. As shown in Figure 2, we plot the relationship between the SKR and the frequency (0.1 THz–50 THz) with $n = 2, 5, 8, 10, 12, 15$, respectively in a 1500 km inter-satellite link. We observe that as the number of players increases, the required frequency increases. In the case of the same number of players, SKR increases with higher frequency. The required frequency for a 10^{-3} bits/pulse SKR with $n = 2$ is about 18 THz and a 10^{-4} bits/pulse SKR with $n = 8$ is about 22 THz. When $n \geq 5$, the required frequency is at least 1 THz. When $n = 15$, the required frequency needs to reach 49 THz. Thus, it is necessary to extend traditional THz frequency (0.1 THz–10 THz) to the mid infrared (MIR) and the far infrared (FIR) bands to study the THz-CVQSS system with high SKR and multiple players. However, in a practical communication system, the higher the frequency, the smaller the beam radius. That is to say, high-frequency communication system requires a high-precision acquisition, pointing, and tracking (APT) subsystem to communicate with the secure receiver. Here, we consider extending the frequency to a relatively suitable range (up to 50 THz) to estimate the performance of THz-CVQSS in inter-satellite links.

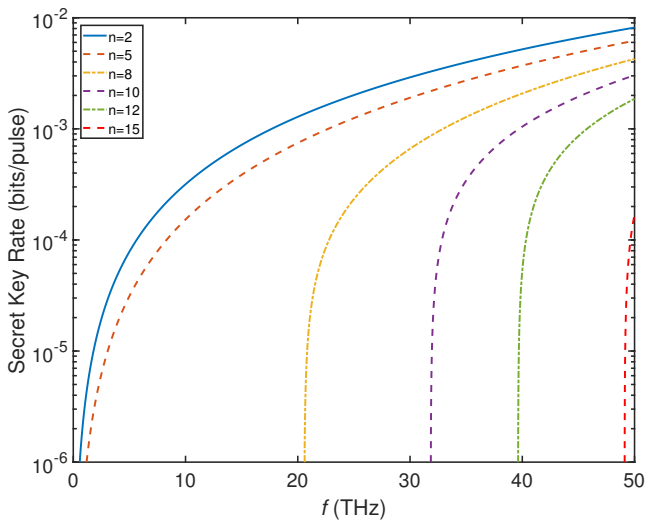

Figure 2. The relationship between the SKR and the frequency (0.1 THz–50 THz) with $n = 2, 5, 8, 10, 12, 15$, respectively. The simulation parameters are $\xi_0 = 0.001, \eta = 0.6, v_{el} = 0.1, \beta = 0.98$, $V_M = 7$ and $d = 1500$ km.

Figure 3 shows the SKR of inter-satellite THz-CVQSS versus transmission distance at different THz frequencies. We obtain that as the frequency increases, the performance of the THz-CVQSS system also improves. In Figure 3a, for $n = 8, f = 1$ THz, the maximal transmission distance can only attain 70 km. This is far from enough for long-distance communication between satellites. In Figure 3b, when the frequency is increased to 10 THz, for $n = 8$, the maximal transmission distance can attain 715 km. This still cannot reach the assumed communication distance (1500 km). In Figure 3c, the maximal transmission distance can reach 1440 km for $n = 8, f = 20$ THz. As the number of players increases to 10 ($n = 10$), the maximal transmission distance decreases rapidly, which can reach 940 km. In Figure 3d,e, the transmission distance can reach 1980 km and 2640 km with a 10^{-4} bits/pulse SKR for $n = 8$. The results indicate that a long-distance THz-CVQSS can be achieved in the inter-satellite channel. However, when the frequency is increased to 50 THz as shown in Figure 3f, the transmission distance for $n = 8, 10, 12, 15$ can reach almost 3290 km, 2280 km, 1860 km and 1510 km, respectively with a 10^{-4} bits/pulse SKR. In particular, for $n = 8$ and a 10^{-3} bits/pulse SKR, the transmission distance can exceed

1900 km. The results shown here again strongly support the feasibility of inter-satellite THz-CVQSS.

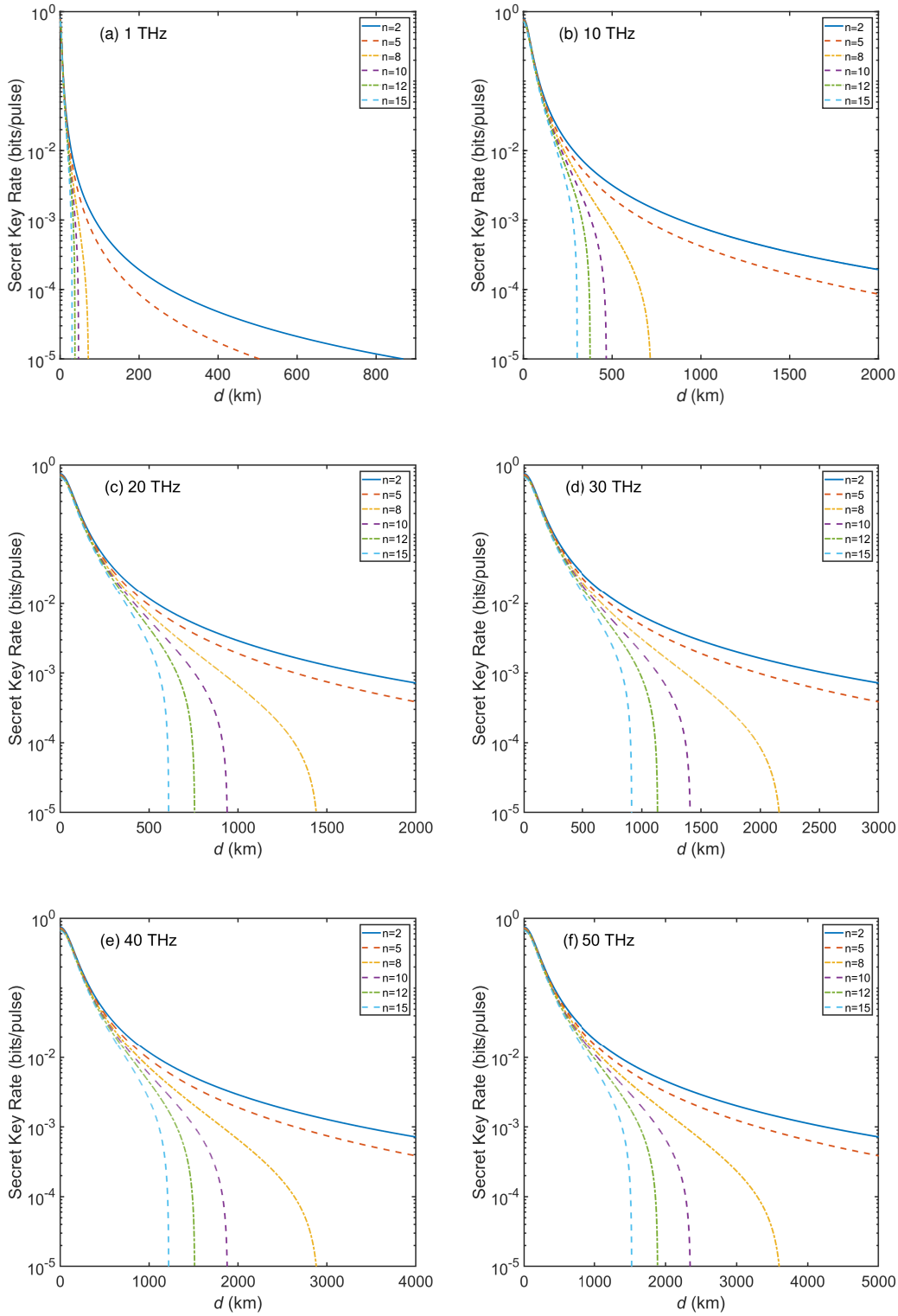

Figure 3. The SKR of inter-satellite THz-CVQSS versus transmission distance (km) for (**a**) $f = 1$ THz, (**b**) $f = 10$ THz, (**c**) $f = 20$ THz, (**d**) $f = 30$ THz, (**e**) $f = 40$ THz, and (**f**) $f = 50$ THz. The simulation parameters are $\xi_0 = 0.001, \eta = 0.6, v_{el} = 0.1, \beta = 0.98, V_M = 7$.

According to the analysis results in Figure 3, we obtain that 50 THz is an optimal frequency for our system. In order to achieve the maximal value of SKR in different scenarios, we analyze the optimal domain and optimal value of the modulation variance V_M at 50 THz as illustrated in Figure 4. It can be clearly observed that the optimal domains of V_M are constricted with the increase of transmission distance. In Figure 4a, as the number of players increases, the optimal domains of V_M are also constricted. However, there is a common domain in these different optimal domains. Here, we can select the common symmetric point $V_M = 7$ as the common optimal value. For $d = 3000$ km, $V_M = 7$ and $n = 5$, the SKR can exceed 10^{-3} bits/pulse. We also plot the relationship between the SKR and V_M with different excess noise ξ_0 as shown in Figure 4b. We can see that as the excess noise ξ_0 increases, the optimal domains of V_M are constricted. Similarly, there is also a symmetric point located at $V_M = 7$. Thus, we can obtain a common optimal V_M as 7. In particular, we find that the SKR can achieve 2×10^{-3} bits/pulse for $d = 1500$ km, $V_M = 7$, and $\xi_0 = 0.003$.

In view of Figure 5a, we analyze the influence of different reconciliation efficiency and numbers of players on the SKR with $f = 50$ THz and $V_M = 7$. We can observe that β is very sensitive to the influence of the maximal transmission distance. For $n = 8$, the maximal transmission distance can reach 3600 km with $\beta = 0.98$ and 2165 km with $\beta = 0.95$. The difference between them is 1435 km. Nevertheless, for $n = 15$, the difference between them is 377 km (the maximal transmission distance is 1525 km for $\beta = 0.98$ and 1148 km for $\beta = 0.95$). Figure 5b demonstrates the influence of different excess noise and numbers of players on the SKR. It is clear that in the case of the same number of players, ξ_0 is also very sensitive to the influence of the maximal transmission distance. For $n = 8$, the maximal transmission distance can achieve 3600 km with $\xi_0 = 0.001$, 1615 km with $\xi_0 = 0.002$ and 1146 km with $\xi_0 = 0.003$. Interestingly, we can see that a 10^{-5} bits/pulse SKR at almost 2300 km can be achieved with $n = 10$, $\xi = 0.001$ and $\beta = 0.98$ from Figure 5. This result shows the powerful performance of our THz-CVQSS system.

In short, from the aforementioned analysis, THz-CVQSS can achieve the optimal SKR with higher frequency, the optimal V_M value, higher reconciliation efficiency and lower excess noise in inter-satellite links.

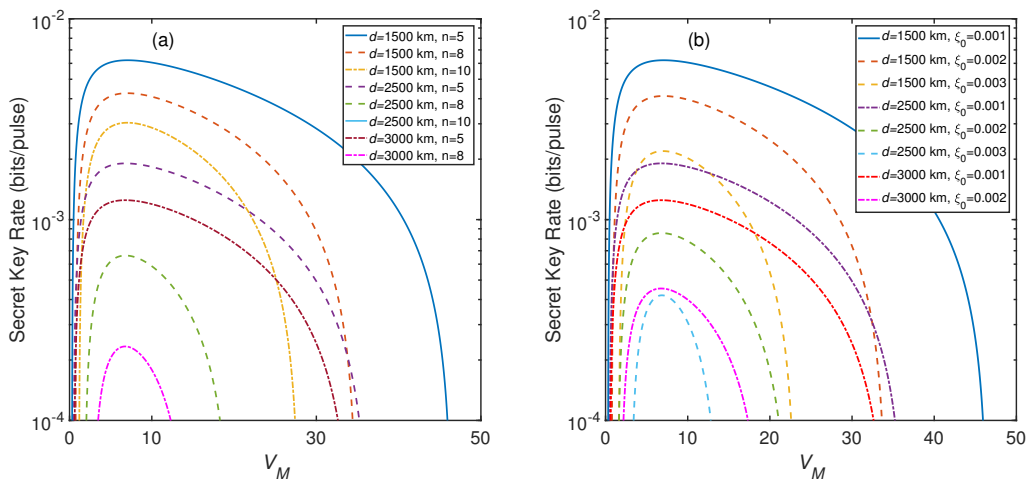

Figure 4. (**a**) The relationship between the SKR and the modulation variance V_M with different transmission distance and numbers of players. $\xi_0 = 0.001, \eta = 0.6, v_{el} = 0.1, \beta = 0.98$, and $f = 50$ THz. (**b**) The relationship between the SKR and the modulation variance V_M with different transmission distance and excess noise. $n = 5, \eta = 0.6, v_{el} = 0.1, \beta = 0.98$, and $f = 50$ THz.

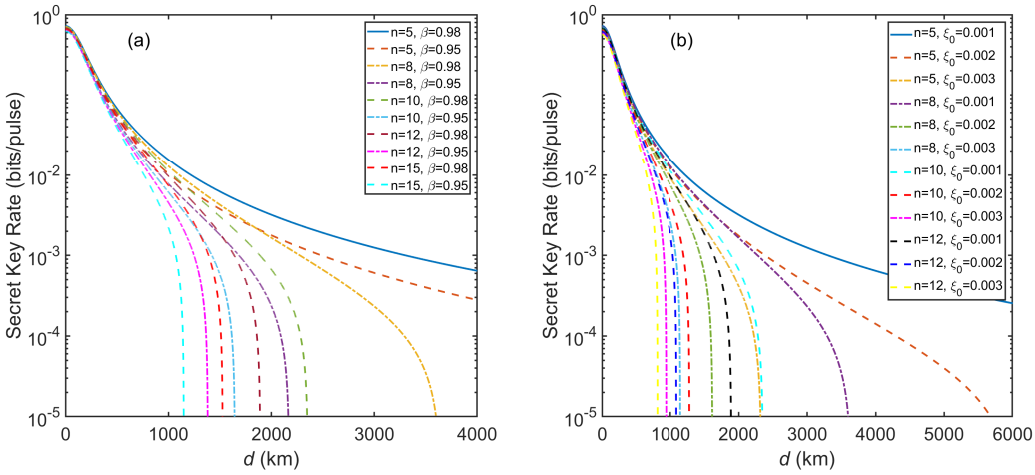

Figure 5. (**a**) The SKR of inter-satellite THz-CVQSS versus transmission distance (km) with different reconciliation efficiency and numbers of players. $\xi_0 = 0.001, \eta = 0.6, v_{el} = 0.1, V_M = 7$, and $f = 50$ THz. (**b**) The SKR of inter-satellite THz-CVQSS versus transmission distance (km) with different excess noise and numbers of players. $\beta = 0.98, \eta = 0.6, v_{el} = 0.1, V_M = 7$, and $f = 50$ THz.

Due to the length of the SKR is limited at finite-size of data in the actual CVQSS system, we further consider the finite-size SKR of THz-CVQSS as shown in Figure 6. The detailed analysis of finite-size SKR is provided in Appendix A. We can observe that the maximal transmission distance increases with the increase of M and gradually approaches the case of SKR-unlimited. For $M = 10^{14}$ and $n = 5$, the maximal transmission distance can attain about 2300 km with $\xi = 0.003$. Results indicate that inter-satellite THz-CVQSS can still maintain the reasonable performance in the finite-size scenario although the excess noise is comparatively high.

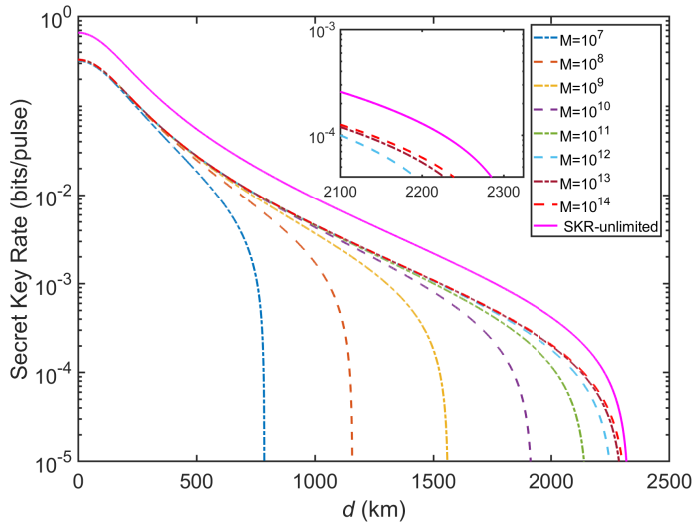

Figure 6. The finite-size SKR of inter-satellite THz-CVQSS versus transmission distance (km). $n = 5, \xi_0 = 0.003, \eta = 0.6, v_{el} = 0.1, V_M = 7$, and $f = 50$ THz.

We also plot the finite-size SKR of inter-satellite THz-CVQSS versus the reconciliation efficiency with different numbers of players in view of Figure 7. In the finite-size scenario, we set the block size $M = 10^{10}$ to demonstrate the available range of reconciliation efficiency. We find that as the number of players increases, the required reconciliation efficiency increases. For $n = 5$ and $d = 2000$ km, a 10^{-4} bits/pulse finite-size SKR can be achieved with the reconciliation efficiency of at least 0.93. However, when $n = 10$, the required

reconciliation efficiency exceeds 0.98. Thus, for the actual inter-satellite THz-CVQSS system, it is essential to employ an efficient reconciliation efficiency.

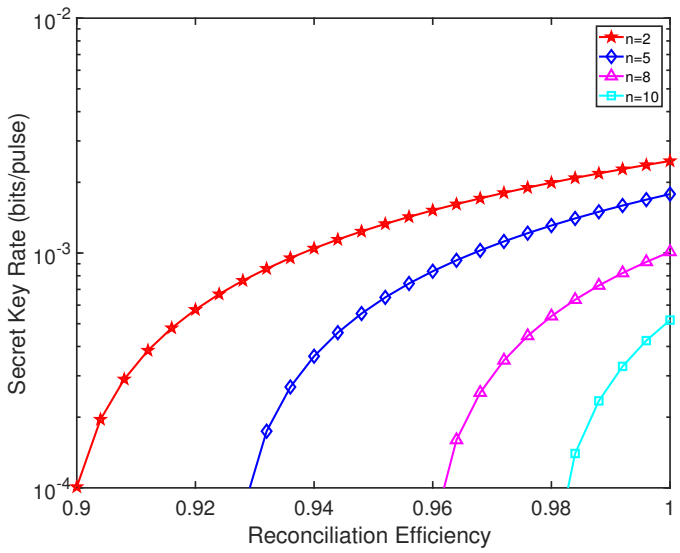

Figure 7. The finite-size SKR of inter-satellite THz-CVQSS versus the reconciliation efficiency with different numbers of players. $\xi_0 = 0.001, \eta = 0.6, v_{el} = 0.1, V_M = 7, d = 2000$ km, $f = 50$ THz and $M = 10^{10}$.

4. Conclusions

We have presented a THz-CVQSS scheme based on thermal THz sources and heterodyne detectors, which can be efficiently immune to Trojan horse attacks. On the whole, THz-CVQSS protocol actually establishes n independent point-to-point CVQKD links based on GMTS in each round of quantum transmission. By connecting THz-CVQSS to CVQKD based on GMTS, the security of the proposed protocol can be proved. We analyze the performance of THz-CVQSS in inter-satellite links. Results show that THz-CVQSS can achieve the optimal SKR with higher frequency, the optimal V_M value, higher reconciliation efficiency and lower excess noise in inter-satellite links. We also verify the feasibility of inter-satellite long-distance THz-CVQSS. In particular, when the frequency is increased to 50 THz, the maximal transmission distance can reach 2300 km with the comparatively high excess noise ($\xi_0 = 0.003$) and $n = 5$ players in the finite-size scenario. This work can provide an effective way to build an inter-satellite quantum communication network. We expect that in future work, some non-Gaussian operations, e.g., quantum catalysis and photon subtraction, can be used to further improve the performance of THz-CVQSS.

Author Contributions: Conceptualization, C.L. and C.Z.; methodology, C.L. and C.P.; formal analysis, Z.L.; validation, M.N.; writing—original draft preparation, C.L.; writing—review and editing, C.Z. and H.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Natural Science Foundation of China (Grant Nos. 61372076, 61971348, and 62001351), Foundation of Shaanxi Key Laboratory of Information Communication Network and Security (Grant No. ICNS201802), Natural Science Basic Research Program of Shaanxi, China (Grant No. 2021JM-142), and Key Research and Development Program of Shaanxi Province, China (Grant No. 2019ZDLGY09-02).

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

Appendix A. Secret Key Rate Analysis of THz-CVQSS in the Finite-Size Scenario

In the actual CVQSS system, the number of quantum signals transmitted between the dealer and the players is limited at finite-size of data, which has a profound impact on

the transmission distance and SKR. Thus, in this section, we analyze the finite-size SKR of THz-CVQSS with reverse reconciliation which can be expressed by [40]

$$R_f = \frac{m}{M}\left(\beta I_{AB} - S_{\Theta_{PE}}(AE) - \Delta(m)\right), \tag{A1}$$

where, m denotes the number of quantum signals utilized to share the secure keys. M denotes the total number of quantum signals exchanged. $h = M - m$ denotes the remaining number of quantum signals utilized to parameter estimation. β and I_{AB} are defined in Equation (3). $S_{\Theta_{PE}}(AE)$ denotes the maximal Holevo information compatible with the statistics except with probability Θ_{PE} and can be calculated by the covariance matrix $\Omega_{\Theta_{PE}}$. $\Delta(m)$ denotes a security parameter which is related to the privacy amplification and can be expressed by [40]

$$\Delta(m) = \frac{2}{m}\log_2\left(\frac{1}{\Theta_{PA}}\right) + 7\sqrt{\frac{\log_2\left(\frac{2}{\bar{\Theta}}\right)}{m}}, \tag{A2}$$

where, Θ_{PA} denotes the probability of lack of success in privacy amplification. $\bar{\Theta}$ denotes the smoothing parameter.

Next, we will calculate the covariance matrix $\Omega_{\Theta_{PE}}$. The finite-size SKR R_f is minimized by $\Omega_{\Theta_{PE}}$ with a probability of at least $1 - \Theta_{PE}$. The covariance matrix $\Omega_{\Theta_{PE}}$ can be obtained by using h couples of correlated variables $(x_i, y_i)_{i=1\ldots h}$. We consider a normal model for the correlated variables given by

$$y = qx + p, \tag{A3}$$

where, $q = \sqrt{T_1}$ and p denotes a centered normal variable with the variance $\omega^2 = T_1\xi_{tot} + 1$, $\xi_{tot} = \sum_{i=1}^{n}\xi_i$. The covariance matrix $\Omega_{\Theta_{PE}}$ can be calculated by

$$\Omega_{\Theta_{PE}} = \begin{bmatrix} V\mathrm{I}_2 & q_{\min}\sqrt{V^2-1}\sigma_z \\ q_{\min}\sqrt{V^2-1}\sigma_z & (q_{\min}^2(V-1) + \omega_{\max}^2)\mathrm{I}_2 \end{bmatrix}, \tag{A4}$$

where, $q_{\min}$ is the minimal value of $\hat{q}$ and $\omega_{\max}^2$ is the maximal value of $\hat{\omega}^2$. The estimated value of $\hat{q}$ and $\hat{\omega}^2$ can be obtained by the maximum likelihood estimation

$$\begin{aligned} \hat{q} &= \frac{\sum_{i=1}^{h} x_i y_i}{\sum_{i=1}^{h} x_i^2}, \\ \hat{\omega}^2 &= \frac{1}{h}\sum_{i=1}^{h}(y_i - \hat{q}x_i)^2. \end{aligned} \tag{A5}$$

Through the large number theorem, $\hat{q}$ and $\hat{\omega}^2$ satisfy the following distributions

$$\hat{q} \sim N\left(q, \frac{\omega^2}{\sum_{i=1}^{h} x_i^2}\right), \quad \frac{h\hat{\omega}^2}{\omega^2} \sim \chi^2(h-1). \tag{A6}$$

Owing to the estimated values of $\hat{q}$ and $\hat{\omega}^2$ are true values, i.e., $E[\hat{q}] = \sqrt{T_1}$ and $E\left[\hat{\omega}^2\right] = T_1\xi_{tot} + 1$, we then can obtain the expressions

$$\begin{aligned} q_{\min} &\approx \sqrt{T_1} - z_\delta\sqrt{\frac{T_1\xi_{tot}+1}{hV_M}}, \\ \omega_{\max}^2 &\approx z_\delta\frac{\sqrt{2}(T_1\xi_{tot}+1)}{\sqrt{h}} + 1 + T_1\xi_{tot}, \end{aligned} \tag{A7}$$

where, z_δ satisfies $1 - \mathrm{erf}\left(z_{\delta/\sqrt{2}}\right)/2 = \Theta_{PE}/2$, here, $\mathrm{erf}(x)$ denotes the error function given by

$$\mathrm{erf}(x) = \int_0^x \frac{2}{\sqrt{\pi}} e^{-u^2}\, \mathrm{d}u. \tag{A8}$$

Note that, we set the parameter values as

$$\bar{\Theta} = \Theta_{PE} = \Theta_{PB} = 10^{-10}, \quad m = h = M/2. \tag{A9}$$

References

1. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computer, System and Signal Processing, Bangalore, India, 9–12 December 1984; IEEE: New York, NY, USA, 1984; pp. 175–179.
2. Gisin, N.; Thew, R. Quantum communication. *Nat. Photon.* **2015**, *55*, 298–303.
3. Scarani, V.; Bechmannpasquinucci, H.; Cerf, N.J.; Dusek, M.; Lutkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301–1350. [CrossRef]
4. Lucamarini, M.; Patel, K.A.; Dynes, J.F.; FröHlich, B.; Sharpe, A.W.; Dixon, A.R.; Yuan, Z.L.; Penty, R.V.; Shields, A.J. Efficient decoy-state quantum key distribution with quantified security. *Opt. Express* **2013**, *21*, 24550–24565. [CrossRef]
5. Lucamarini, M.; Yuan, Z.L.; Dynes, J.F.; Shields, A.J. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. *Nature* **2018**, *557*, 400–403. [CrossRef]
6. Wang, X.B.; Yu, Z.W.; Hu, X.L. Twin-field quantum key distribution with large misalignment error. *Phys. Rev. A* **2018**, *98*, 062323. [CrossRef]
7. Zhou, Y.H.; Yu, Z.W.; Wang, X.B. Making the decoy-state measurement-device-independent quantum key distribution practically useful. *Phys. Rev. A* **2015**, *93*, 042324. [CrossRef]
8. Wei, K.J.; Li, W.; Tan, H.; Li, Y.; Min, H.; Zhang, W.J.; Li, H.; You, L.X.; Wang, Z.; Jiang, X.; et al. High-speed measurement-device-independent quantum key distribution with integrated silicon photonics. *Phys. Rev. X* **2020**, *10*, 031030.
9. Liu, C.J.; Zhu, C.H.; Nie, M.; Yang, H.; Pei, C.X. An improved quantum key distribution based on lucas-valued oribital angular momentum states. *J. Opt. Soc. Am. B* **2020**, *37*, 876–887. [CrossRef]
10. Grosshans, F.; Van, A.G.; Wenger, J.; Brouri, R.; Cerf, N.J.; Grangier, P. Quantum key distribution using Gaussian-modulated coherent states. *Nature* **2003**, *421*, 238–241. [CrossRef] [PubMed]
11. Weedbrook, C.; Pirandola, S.; García-Patrón, R.; Cerf, N.; Ralph, T.; Shapiro, J.; Lloyd, S. Gaussian quantum information. *Rev. Mod. Phys.* **2011**, *84*, 621–669. [CrossRef]
12. Weedbrook, C.; Pirandola, S.; Ralph, T.C. Continuous-variable quantum key distribution using thermal states. *Phys. Rev. A* **2012**, *86*, 022318. [CrossRef]
13. Derkach, I.; Usenko, V.C. Applicability of squeezed- and coherent-state continuous-variable quantum key distribution over satellite links. *Entropy* **2021**, *23*, 55. [CrossRef]
14. Laudenbach, F.; Pacher, C.; Fung, C.F.; Poppe, A.; Peev, M.; Schrenk, B.; Hentschel, M.; Walther, P.; Hübel, H. Continuous-variable quantum key distribution with Gaussian Modulation-The theory of practical implementations. *Adv. Quantum Technol.* **2018**, *1*, 1800011. [CrossRef]
15. Xu, F.H.; Ma, X.F.; Zhang, Q.; Lo, H.K.; Pan, J.W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **2020**, *92*, 025002. [CrossRef]
16. Ottaviani, C.; Woolley, M.J.; Erementchouk, M.; Federici, J.F.; Mazumder, P.; Pirandola, S.; Weedbrook, C. Terahertz quantum cryptography. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 483–495. [CrossRef]
17. Liu, X.; Zhu, C.; Chen, N.; Pei, C. Practical aspects of terahertz wireless quantum key distribution in indoor environments. *Quantum Inf. Process.* **2018**, *17*, 304. [CrossRef]
18. Wang, Z.; Malaney, R.; Green, J. Inter-Satellite Quantum Key Distribution at Terahertz Frequencies. In Proceedings of the ICC 2019—2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–7.
19. Walker, C.K.; Kulesa, C.A. Terahertz astronomy from the coldest place on Earth. In Proceedings of the 2005 Joint 30th International Conference on Infrared and Millimeter Waves & 13th International Conference on Terahertz Electronics, Williamsburg, VA, USA, 19–23 September 2005; pp. 3–4.
20. Seeds, A.J.; Shams, H.; Fice, M.J.; Renaud, C.C. TeraHertz photonics for wireless communications. *J. Light. Technol.* **2015**, *33*, 579–587. [CrossRef]
21. He, Y.; Mao, Y.; Huang, D.; Liao, Q.; Guo, Y. Indoor channel modeling for continuous variable quantum key distribution in the terahertz band. *Opt. Express* **2020**, *28*, 32386–32402. [CrossRef]
22. Karlsson, A.; Koashi, M.; Imoto, N. Quantum entanglement for secret sharing and secret splitting. *Phys. Rev. A* **1999**, *59*, 162–168. [CrossRef]
23. Hillery, M.; Bužek, V.; Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **1999**, *59*, 1829–1834. [CrossRef]

24. Chen, Y.A.; Zhang, A.N.; Zhao, Z.; Zhou, X.Q.; Lu, C.Y.; Peng, C.Z.; Yang, T.; Pan, J.W. Experimental quantum secret sharing and third-man quantum cryptography. *Phys. Rev. Lett.* **2005**, *95*, 200502. [CrossRef]
25. Xiao, L.; Long, G.L.; Deng, F.G.; Pan, J.W. Efficient multi-party quantum secret sharing schemes. *Phys. Rev. A* **2004**, *69*, 521–524. [CrossRef]
26. Lau, H.K.; Weedbrook, C. Quantum secret sharing with continuous-variable cluster states. *Phys. Rev. A* **2013**, *88*, 1985–1988. [CrossRef]
27. Kogias, I.; Xiang, Y.; He, Q.; Adesso, G. Unconditional security of entanglement-based continuous-variable quantum secret sharing. *Phys. Rev. A* **2017**, *95*, 012315. [CrossRef]
28. Grice, W.P.; Evans, P.G.; Lawrie, B.; Legré, M.; Lougovski, P.; Ray, W.; Williams, B.P.; Qi, B.; Smith, A.M. Two-Party secret key distribution via a modified quantum secret sharing protocol. *Opt. Express* **2015**, *23*, 7300. [CrossRef] [PubMed]
29. Phoenix, S.; Barnett, S.; Townsend, P.D.; Blow, K. Multi-user quantum cryptography on optical networks. *J. Mod. Opt.* **2015**, *42*, 1155. [CrossRef]
30. He, G.P. Comment on "Experimental single qubit quantum secret sharing". *Phys. Rev. Lett.* **2007**, *98*, 028901. [CrossRef]
31. Schmid, C.; Trojek, P.; Bourennane, M.; Kurtsiefer, C.; Zukowski, M.; Weinfurter, H. Reply to Comment on "Experimental single qubit quantum secret sharing". *Phys. Rev. Lett.* **2007**, *98*, 028902. [CrossRef]
32. Grice, W.P.; Qi, B. Quantum secret sharing using weak coherent states. *Phys. Rev. A* **2019**, *100*, 022339. [CrossRef]
33. Wu, X.; Wang, Y.; Huang, D. Passive continuous-variable quantum secret sharing using a thermal source. *Phys. Rev. A* **2020**, *101*, 022301. [CrossRef]
34. Liao, Q.; Liu, H.; Zhu, L.; Guo, Y. Quantum secret sharing using discretely modulated coherent states. *Phys. Rev. A* **2021**, *103*, 032410. [CrossRef]
35. Wang, Y.; Jia, B.; Mao, Y.; Wu, X.; Guo, Y. Improving continuous variable quantum secret sharing with weak coherent states. *Appl. Sci.* **2020**, *10*, 2411. [CrossRef]
36. Diamanti, E.; Leverrier, A. Distributing secret keys with quantum continuous variables: Principle, security and implementations. *Entropy* **2015**, *17*, 6072. [CrossRef]
37. Hechenblaikner, G.; Hufgard, F.; Burkhardt, J.; Kiesel, N.; Johann, U.; Aspelmeyer, M.; Kaltenbaek, R. How cold can you get in space? Quantum Physics at cryogenic temperatures in space. *New J. Phys.* **2014**, *16*, 013058. [CrossRef]
38. Leverrier, A.; Grangier, P. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Phys. Rev. Lett.* **2009**, *102*, 180504. [CrossRef] [PubMed]
39. Lodewyck, J.; Bloch, M.; García-Patrón, R.; Fossier, S.; Karpov, E.; Diamanti, E.; Debuisschert, T.; Cerf, N.J.; Tuallebrouri, R.; Mclaughlin, S.W.; et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A* **2007**, *76*, 042305. [CrossRef]
40. Leverrier, A.; Grosshans, F.; Grangier, P. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A* **2010**, *81*, 062343. [CrossRef]