applied sciences

MDPI

Article

Continuous Variable Quantum Secret Sharing with Fairness

Ye Kang [1,2], Ying Guo [2,3], Hai Zhong [1,*], Guojun Chen [3] and Xiaojun Jing [4,*]

1 School of Computer Science and Engineering, Central South University, Changsha 410083, China; kangye@csu.edu.cn
2 School of Automation, Central South University, Changsha 410083, China; sdguoying@gmail.com
3 Jiangsu Key Construction Laboratory of IoT Application Technology, Wuxi Taihu University, Wuxi 214064, China; chengj@wxu.edu.cn
4 Key Laboratory of Trustworthy Distributed Computing and Service, Beijing University of Posts and Telecommunications, Beijing 100876, China
* Correspondence: zhonghai@csu.edu.cn (H.Z.); jxiaojun@bupt.edu.cn (X.J.)

Received: 29 October 2019; Accepted: 19 December 2019; Published: 25 December 2019

Abstract: The dishonest participants have many advantages to gain others' shares by cheating in quantum secret sharing (QSS) protocols. However, the traditional methods such as identity authentication and message authentication can not resolve this problem due to the reason that the share has already been released to dishonest participants before realizing the deception. In this paper, a continuous variable QSS (CVQSS) scheme is proposed with fairness which ensures all participants can acquire or can not acquire the secret simultaneously. The quantum channel based on two-mode squeezing states provides secure communications through which it can send shares successfully, as long as setting the squeezing and modulation parameters according to the quantum channel transmission efficiency and the Shannon information of shares. In addition, the Chinese Remainder Theorem (CRT) can provides tunable threshold structures according to demands of the complex quantum network and the strategy for fairness can be incorporated with other sharing schemes, resulting in perfect compatibility for practical implementations.

Keywords: quantum secret sharing; fairness; two-mode squeezed vacuum state

1. Introduction

The secret sharing (SS) plays a significant role in cryptography. Since 1999, Hillery et al. [1] firstly invited SS to the quantum domain by applying three-particle and four-particle GHZ states, more and more QSS scheme have been proposed [2–4]. Based on the quantum mechanics, the secret distribution can be ensured unconditional safety.

Conventionally, a (t, n)-threshold secret sharing scheme is built to prohibit $(t-1)$ or fewer dishonest participants conspiring for secret. At the same time, the participant has more advantages to steal the secret than outside eavesdroppers. Hence, compared with other protocols, such as quantum key distribution [5–7], quantum signature [8], Quantum anonymous voting [9] and so on, the QSS protocols need to analysis the attack from both inside and outside. But in the previous literatures, it is rarely discussed how the secret is revealed securely against inner attack [10–13]. Until now, many SS protocols have been improved to verify participants and check the validity of shares in the recovery phase [14–16], but the participant who is the last one to release share, would desire to obtain the secret alone by sending fake share or keeping silence. So, in order to solve this problem without the simultaneously releasing

constraint, Lin et al. [17] proposed a fair reconstruction, in which Dealer, in addition to the secret shadow, distributes a check vector, which is used to verify the validity of other participants' shadows in the reconstructing process and a certificate vector, which is used to prove the validity of his own shadow to each participant in classical scenario. Then, in quantum domain, Liu et al. [18] designed a QSS protocol based on partially and maximally entangled states, in which a secure and fair reconstruction mechanism is firstly organized to realize each participant can learn or cannot learn the secret simultaneously. Later, Maitra et al. [19] proposed a rational secret sharing scheme for the first time, in which the rational participant tries to maximize his or her utility by obtaining the secret alone, but it is impossible to occur, because the protocol is usually fair (everyone gets the secret).

The above-mentioned schemes are primarily based on discrete variable quantum entanglement states, which emerge some choke points as the extreme fragility, the low channel capacity and the difficulty of the preparation in experiment. So, in this paper, the continuous variable quantum information theory is invited to distribute shares [20,21]. The two-mode squeezed vacuum state is well done at preparation, operation and detection [22,23]. What's more, the modulation performed on the two-mode squeezed vacuum state is not only binary modulation, but also multiple modulation, which can improve the the channel capacity. Furthermore, the quantum channel based on two-mode squeezing states provides secure communication, which is proved that it can send shares successfully, as long as setting proper the squeezing and modulation parameters according to the quantum channel transmission efficiency and the Shannon information of shares. In order to ensure every participant learn or do not learn the secret simultaneously without the simultaneous channel, a fair construction is designed, in which a check sequence is used to hide real secret sequence, a determine pointer is used to find the hidden secret and a verify sequence is used to verify the recovered message. Furthermore, this fair protocol can be incorporated with other sharing schemes.

The organization of this paper is as follows. In Section 2, we design the $(2,2)$-threshold CVQSS scheme with fairness. Section 3 explicates the security analysis of the scheme. At last, in Section 4, the conclusion is given.

2. CVQSS Scheme with Fairness

In this section, the CRT is introduced and a verifying function is defined, which are play an important role in CVQSS scheme proposed below.

2.1. Chinese Remainder Theorem

Let $n \geq 2$, $m_1, ..., m_n \geq 2$ and $s_1, ..., s_n \in \mathbb{Z}$. The system of congruence equations

$$\begin{cases} S \equiv s_1 \bmod m_1, \\ \quad \vdots \\ S \equiv s_n \bmod m_n, \end{cases} \tag{1}$$

has solutions in $\mathbb{Z}$, when $gcd(m_i, m_j) = 1$, for all $i, j \in [1, n]$. It has been proved that this solution can be calculated as

$$S = \sum_{i=1}^{n} s_i T_i M_i \bmod M, \tag{2}$$

where $M = \prod_{i=1}^{n} m_i$, $M_i = M/m_i$ and $T_i \times M_i \bmod m_i = 1$.

According to the CRT equations described above, secret S can be divided to n shares named s_i for n participants and also can be recovered, when shares are all collected, which means the (n, n)-threshold secret sharing scheme can be achieved. Of course, the (t, n)-threshold scheme also can be similarly

designed, where $n \geq 2, t \leq n$ as long as the moduli m_i are prime numbers and secret $S \in [h, H]$, where $h = \prod_{i=n-(t-1)+1}^{n} m_i, H = \prod_{i=1}^{n} m_i$ [11]. Thus, whichever threshold scheme is demanded in practice, it can be designed by the CRT. What's more, compared with other traditional methods, such as the polynomial interpolation method of Shamir, whose key recovery interpolation formula requires $O(t \log^2 t)$ operations, the CRT-based scheme requires only $O(t)$ operations [24].

2.2. Verifying Function for CVQSS

In order to verify the message, usually the Hash function is utilized to obtain the signature or digest of the whole message, which almost contains huge information. But, in this thesis, the message X is verified one number by one number. Therefore, it is obvious that the number is much smaller than the whole message and the same number recurs many times in the whole message. If the Hash function play on the numbers directly, the hash values used for verifiction would repeat, which will come up with one serious problem, that is the number can be derived from its hash value, after several times verifiction. However, the important character of Hash function is irreversibility. In order to avoid the problem of repetition, the message X is preprocessed to X' with $X'_i \neq X'_j \mid i \neq j$ as follow

$$X'_i = X_i + i \times (L + M). \tag{3}$$

Here L is the length of the message, $i \in [1, L]$, $X_i \in \mathbb{N}$ and $M = max(X_i)$. It is easily to prove that $X'_i \neq X'_j \mid i \neq j, i, j \in [1, L]$. Setting $i > j$, $X'_i - X'_j = X_i - X_j + (i - j)(L + M)$, where $-M \leq X_i - X_j \leq M$ and $(i - j)(L + M) \geq L + M$. So, $X'_i - X'_j \geq L > 0$, which proves $X'_i \neq X'_j$ is true. Then, Hash function $H()$, such as SHA1, is invited to obtain verification information V for verifying. Above all, a modified Hash function for verifying a sequence X can be concluded as

$$V_i = H(X_i + i \times (L + M)). \tag{4}$$

2.3. (2, 2)-CVQSS Scheme with Fairness

In what follows, suppose Dealer has a classical secret S to be shared among participants. Dealer exploits CRT to decompose S and participants can reconstruct S. For simplicity, we consider the design of (2,2)-CVQSS scheme with fairness.

2.3.1. Initialization

I1 Dealer selects any two integers $m^a, m^b \geq 2$, satisfying $gcd(m^a, m^b) = 1$, as moduli for CRT, for example, $m^a = 2, m^b = 3$. Then, generates the secret $S \in \{0, 1, ..., M\}^L$, a checking sequence $R \in \{0, 1, ..., M\}^{L_1}$ and a determine pointer $P^* \in \{0, 1, ..., M\}^{L_2}$, where $M = m^a \times m^b - 1$ and L, L_1, L_2 are the lengths of S, R, P^* respectively.

I2 For security, S is hidden in sequence R to form a new sequence named X, which is shown in Figure 1 and described as following steps. (1) Add P^* to the end of S. (2) Insert S and P^* into R at one random place. The sequence P^* has to satisfy its uniqueness in message X, which means P^* meets the constraint i.e., define $T_i = X_i, X_{i+1}, \ldots, X_{i+L_2-1}$, if $T_j = P^*$, $T_k \neq P^*$, for all $k \neq j$, where $i, j, k \in [1, L + L_1]$.

I3 Dealer calculates the shadows $X^A = X \bmod m^a$ and $X^B = X \bmod m^b$, generates the verification information V of X according to Equation (4) and publishes the parameters i.e., $m^a, m^b, L, L_1, L_2, P^*, V$ and the selected Hash function $H()$.

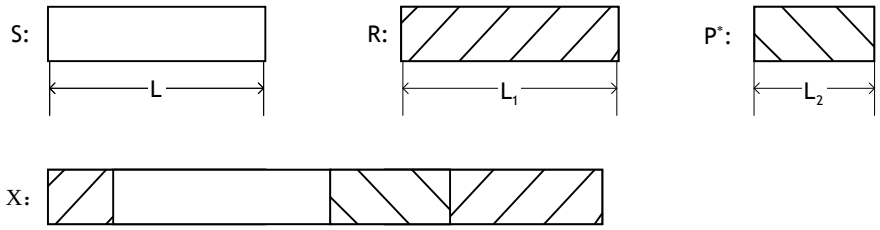

Figure 1. The generating of message X using secret S, checking sequence R and determine pointer $P*$.

2.3.2. Distribution

Dealer distributes X^A, X^B to the participants Alice, Bob respectively, via continuous variable quantum deterministic key distribution based on two-mode squeezed states protocol [21]. In another words, each communication is from one Sender (Dealer) to one Receiver (Alice or Bob). The communication is briefly described as follow.

D1 Every Receiver prepares $L + L_1 + L_2$ two-mode squeezed vacuum states $a_1 = x_1 + ip_1$ and $a_2 = x_2 + ip_2$ as Figure 2. Here

$$\begin{aligned} x_1 &= [e^r \hat{x}_1^{(0)} + e^{-r} \hat{x}_2^{(0)}]/\sqrt{2}, \\ p_1 &= [e^{-r} \hat{p}_1^{(0)} + e^r \hat{p}_2^{(0)}]/\sqrt{2}, \\ x_2 &= [e^r \hat{x}_1^{(0)} - e^{-r} \hat{x}_2^{(0)}]/\sqrt{2}, \\ p_2 &= [e^{-r} \hat{p}_1^{(0)} - e^r \hat{p}_2^{(0)}]/\sqrt{2}, \end{aligned} \tag{5}$$

where $a_{in1} = \hat{x}_1^{(0)} + i\hat{p}_1^{(0)}$ and $a_{in2} = \hat{x}_2^{(0)} + i\hat{p}_2^{(0)}$ are two vacuum states and $\hat{x}_{1,2}^{(0)}, \hat{p}_{1,2}^{(0)} \sim N(0,1)$ follow Gaussian distribution and $[\hat{x}_{1,2}^{(0)}, \hat{p}_{1,2}^{(0)}] = 2i$. As the squeezed parameter $|r|$ increases, the correlation between a_1 and a_2 becomes increasingly perfect, i.e.,

$$\lim_{r \to +\infty} x_1 = x_2, \quad \lim_{r \to +\infty} p_1 = -p_2. \tag{6}$$

D2 Receiver keeps a_1 at home and sends Sender a_2 with some coherent states $c = |x^c + ip^c\rangle$ for checking eavesdropping. After receiving the whole state a_3, Sender sends back an acknowledge. Following Receiver's instructions, Sender accurately selects out and measures the coherent states, so as to check eavesdropping. If the error rate exceeds certain threshold, receiver goes back to **D1**. In this paper, the strategy for checking eavesdropping is the same as above, so, it will be written as eavesdropper detection for short.

D3 According to the message $X^{A/B}$, Sender modulates a_3 by $D(\alpha_j)$ to obtain a_4. Here $\alpha = y + iy$, $y \sim N(X^{A/B}, \sigma^2)$ follows the Gaussian distribution and σ^2 is the variance of message.

D4 Sender sends back a_4 to Receiver with some coherent states. After receiving a_5, Receiver does eavesdropper detection under Sender's help. If the channel is insecure, they give up this communication and go back to **D1**.

D5 Receiver plays a gain on a_6 before joint Bell Measurement on a_1 and a_6 to obtain the message $X^{A/B}$. From Figure 2, it is shown that the joint Bell measurement consists one balanced beamsplitter (BS) and two detectors using homodyne measurement.

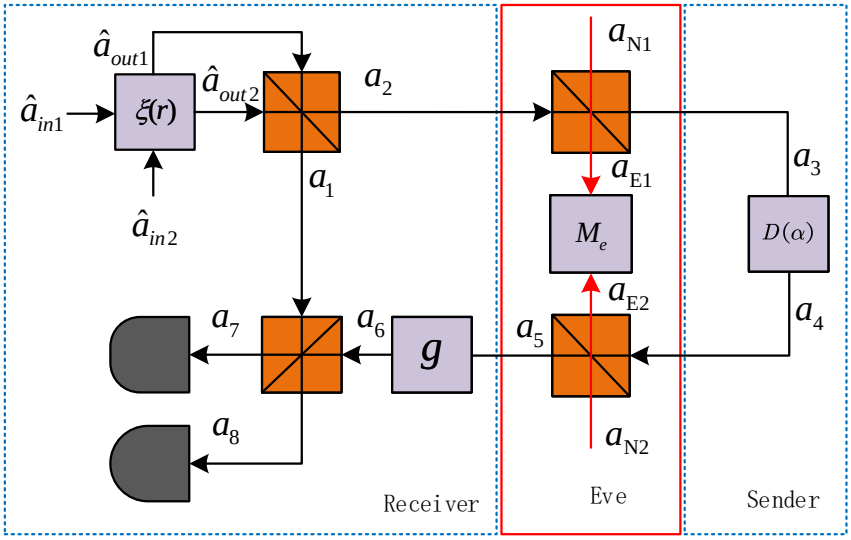

Figure 2. Schematic of distribution based on two-mode squeezed vacuum state.

2.3.3. Recovery

When Alice and Bob wants to rebuild secret S, they exchange their own shares. Dishonest one may refuse to send her or his correct share, after receiving the other one's. In order to avoid this situation, this protocol applies some strategies to achieve fairness, in another words, all participants can or cannot acquire the secret simultaneously.

In this part, firstly, Alice and Bob generate random number sequences $A, B \in \{0, 1, ..., M\}^{(L+L_1+L_2)}$ to encrypt their shares as $(X_j^{A/B} + A_j/B_j) \bmod (M+1), j \in [1, L+L_1+L_2]$, respectively. Then Alice and Bob exchange their encrypted messages as steps (D1) to (D5) and obtain the measurement results M_e^A and M_e^B. At last, they decrypt M_e^A and M_e^B to reconstruct X and verify them one by one number, which is described below in detail.

V1 Define j is the round of secret reconstruction and the initial value j = 0.

V2 j = j + 1.

V3 Alice and Bob exchange or broadcast the j^{th} key A_j and B_j in classical channel, decrypt $M_{e_j}^A$ and $M_{e_j}^B$ to obtain $X_j^B = (M_{e_j}^A - B_j) \bmod (M+1)$ and $X_j^A = (M_{e_j}^B - A_j) \bmod (M+1)$, recovery X_j according to Table 1 and calculate its verification information $V_j' = H(X_j + j(L+M))$.

Table 1. An example of splitting based on the CRT.

X_i	0	1	2	3	4	5
$X_i^A(m^a = 2)$	0	1	0	1	0	1
$X_i^B(m^b = 3)$	0	1	2	0	1	2

V4 If $V_j' \neq V_j$, return: "Error" and end, otherwise, continues.

V5 If $j < (L + L_2)$, go to (v2). Otherwise $T_j = X_{j-L_2+1}, X_{j-L_2}, \ldots, X_j$. If $T_j = P^*$, $S = X_{j-L-L_2+1}, X_{j-L-L_2}, \ldots, X_{j-L_2}$, end and return: S, otherwise, go to (v2).

3. Security Analysis

Figure 2 draws the schematic of CV quantum secure communication used in the progresses of distribution and recovery. During distribution, Alice and Bob are receivers and Dealer is a sender. In the stage of recovery, Alice sends her share to Bob and also Bob sends his share to Bob. Therefore, the security of this protocol is primarily based on security of this communication, which is detailedly analyzed below.

3.1. No Attack

At first, receiver prepares the initial two-mode squeezed states (a_1, a_2), then, send mode a_2 to sender through the quantum channel with the additive white Gaussian noise (AWGN), so, a_3 can be described as

$$x_3 = \sqrt{\eta_1}x_2 + \sqrt{1-\eta_1}x_{N1}, \;\; p_3 = \sqrt{\eta_1}p_2 + \sqrt{1-\eta_1}p_{N1}. \tag{7}$$

Here, η_1 is the channel transmission efficiency and $x_{N1}, p_{N1} \sim N(0, \Sigma_1^2)$ presents the channel noise from receiver to sender. Next, a_3 is modulated by displacement operation according to message $X^{A/B}$ and turns to a_4 expressed as

$$x_4 = x_3 + y, \;\; p_4 = p_3 + y. \tag{8}$$

Then, a_4 is sent back to receiver and becomes a_5,

$$x_5 = \sqrt{\eta_2}x_4 + \sqrt{1-\eta_2}x_{N2}, \;\; p_5 = \sqrt{\eta_2}p_4 + \sqrt{1-\eta_2}p_{N2}, \tag{9}$$

where $x_{N2}, p_{N2} \sim N(0, \Sigma_2^2)$ and η_2 stands for the parameter of the quantum channel from sender to receiver. In order to compensate a_5 for lossy in quantum channel, a_5 has to be amplified with gain g before Bell Measurement, so,

$$x_6 = gx_5. \tag{10}$$

At last, receiver plays a measurement on a_1 and a_6 for capturing message $X^{A/B}$ and the results a_7, a_8 are

$$\begin{aligned} x_7 &= \frac{1}{\sqrt{2}}(x_6 + x_1), p_7 = \frac{1}{\sqrt{2}}(p_6 + p_1), \\ x_8 &= \frac{1}{\sqrt{2}}(x_6 - x_1), p_8 = \frac{1}{\sqrt{2}}(p_6 - p_1). \end{aligned} \tag{11}$$

If $r > 0$, using Equations (5), (7)–(11) and setting $g = \sqrt{\frac{1}{\eta_1\eta_2}}$, we obtain

$$x_8 = \frac{y}{\sqrt{2\eta_1}} + \frac{\sqrt{1-\eta_1}x_{N1}}{\sqrt{2\eta_1}} + \frac{\sqrt{1-\eta_2}x_{N2}}{\sqrt{2\eta_1\eta_2}} - e^{-r}\hat{x}_2^0. \tag{12}$$

Obviously, x_8 obeys a Gaussian distribution, so, the variance of signal distribution is

$$V_s = \frac{\sigma^2}{2\eta_1}, \tag{13}$$

and the variance of noise is

$$N_s = \frac{1-\eta_1}{2\eta_1}\Sigma_1^2 + \frac{1-\eta_2}{2\eta_1\eta_2}\Sigma_2^2 - e^{-2r}. \tag{14}$$

The signal-noise-ratio (SNR) between sender and receiver is

$$\gamma = \frac{V_s}{N_s}. \tag{15}$$

According to the Shannon information theory [25], the mutual information is expressed as

$$I(S,R) = \frac{1}{2}\log_2(1+\gamma). \tag{16}$$

As for the two-mode squeezed state, the amplitude and phase are symmetric and both can be used to transfer message, so, the total mutual information is $2I(S,R)$ and the channel capacity is also $2I(S,R)$, when there is no attack. But, for describing more briefly, the messages carried on amplitude and phase are the same in this paper, so, the security is discussed only based on the amplitude, also the channel capacity is seen as $C = I(S,R)$ accordingly. For satisfying the message transferring successfully, the channel capacity cannot be less than the information of $X_i^{A/B}$, expressed as $C \geq H(X_i^{A/B})$. According to the (2,2)-threshold CVQSS proposed above, suppose X_i is equally distributed in $\{0,1,\ldots,5\}$, so $P(X_i = 0) = P(X_i = 1) = \cdots = P(X_i = 5) = \frac{1}{6}, i = (1,2,...,L+L_1+L_2)$, From definition of CRT or Table 1, the share of Alice is $X_i^A \in \{0,1\}$ and its probability function is

$$\begin{cases} P(X_i^A = 0) = P(X_i = 0) + P(X_i = 2) + P(X_i = 4) = \dfrac{1}{2}, \\ P(X_i^A = 1) = P(X_i = 1) + P(X_i = 3) + P(X_i = 5) = \dfrac{1}{2}. \end{cases} \tag{17}$$

Similarly, the share of Bob is $X_i^B \in \{0,1,2\}$ and its probability function is

$$\begin{cases} P(X_i^A = 0) = P(X_i = 0) + P(X_i = 3) = \dfrac{1}{3}, \\ P(X_i^A = 1) = P(X_i = 1) + P(X_i = 4) = \dfrac{1}{3}, \\ P(X_i^A = 2) = P(X_i = 2) + P(X_i = 5) = \dfrac{1}{3}. \end{cases} \tag{18}$$

Therefore, the information entropy of X_i, X_i^A and X^B are $H(X_i) = log_2 6\ bit$, $H(X_i^A) = 1\ bit$ and $H(X_i^B) = \log_2 3\ bit$. Hence, the channel can succeed to send X^A and X^B, when $C = I(S,R) \geq \log_2 3\ bit \approx 1.6\ bit$. Suppose the two quantum channels are the same with $\eta_1 = \eta_2 = \eta$ and $\Sigma_1 = \Sigma_2 = \Sigma$, the information rate $I(S,R)$ is depicted in Figure 3 which shows that the increment of squeezed parameter r and the variance of message σ^2 can improve $I(S,R)$, especially, the growth of σ^2 can enhance the tolerance of low channel transmission efficiency. Under condition $I(S,R) = \log_2 3\ bit$, the relation between r and σ^2 is drawn in Figure 4. It is shown that the σ^2 decreases to a fixed value, when r increases to 3 from 1, under the conditions of $\eta = \{1, 0.9, 0.6\}$. To come over more loss in quantum channel, the more energy has to be afforded by increasing σ^2 in modulation.

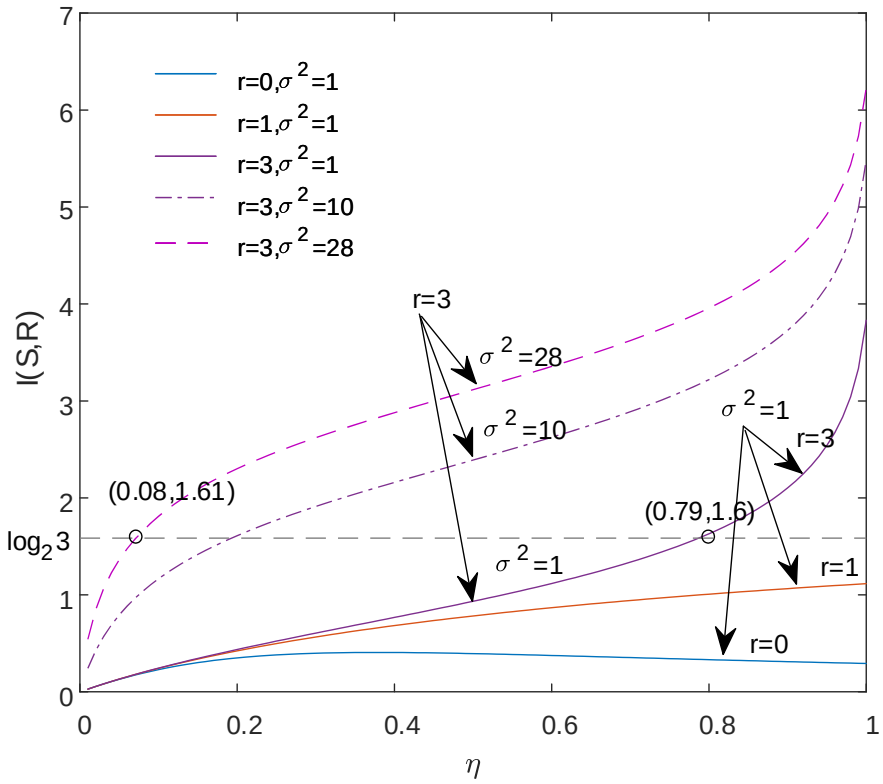

Figure 3. The information rate under different parameters ($\Sigma^2 = 1$).

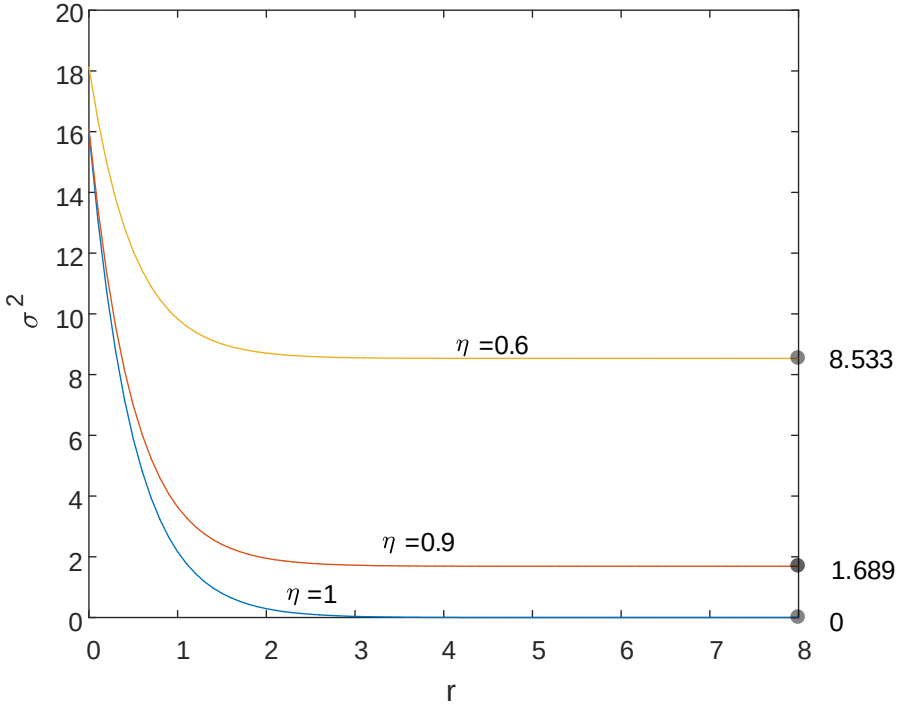

Figure 4. The relation between the squeezed parameter r and the variance of message σ^2, when $I(S,R) = \log_2 3$ bit.

3.2. Internal Attack

Generally, there are two kinds of attack considered in the QSS scheme. One is eavesdropping of Eve from outside, the other one is the dishonest participant attack from inside. However the dishonest participant has more superiorities to steal the secret than Eve from outside. Therefore, the scheme is secure with Eve's attack, so long as the protocol can resist inner attack. Consequently, the following security analysis primarily focuses on inner attack in noisy channel.

For curiousness, Alice and Bob may guess the original key S, which is hiden in X. Although each participant has one share $X^{A/B}$, they have no idea about the position of S in X, which means they should guess the right P^* at first, then recover S by guess. According to the Equation (2) or Table 1, the authorized set $X^A \cup X^B$ can recover the message X and from above caculations, $H(X_i) = H(X_i^A) + H(X_i^B)$, which means the unauthorized sets X_i^A and X_i^B are independent to each other. Apparently, $H(X_i) > H(X_i^B) > H(X_i^A) > 0$, so, curious member cannot deduce X_i from unauthorized set X_i^A or X_i^B, alone. Furthermore, from Table 1 and Equations (17) and (18), the conditional probabilities $P(X_i \mid X_i^A)$ and $P(X_i \mid X_i^B)$ can be concluded as Tables 2 and 3. Thus, according to Alice's share X_i^A, the successful probabilities of guessing P^* and S are $(\frac{1}{3})^{L_2}$ and $(\frac{1}{3})^L$, which approaches to *zero*, when $L, L_2 > 3$. Similarly, Bob can successfully guess P^* and S with probabilities $(\frac{1}{2})^{L_2}$ and $(\frac{1}{2})^L$. So, it is hardly to accurately locate S in X and then recover it for Alice and Bob. Therefore, dishonest participant has to perform attacks to acquire more information for secret recovery.

Table 2. The conditional probability of $P(X_i \mid X_i^A)$.

$P(X_i \mid X_i^A)$	$X_i = 0$	$X_i = 1$	$X_i = 2$	$X_i = 3$	$X_i = 4$	$X_i = 5$
$X_i^A = 0$	1/3	0	1/3	0	1/3	0
$X_i^A = 1$	0	1/3	0	1/3	0	1/3

Table 3. The conditional probability of $P(X_i \mid X_i^B)$.

$P(X_i \mid X_i^B)$	$X_i = 0$	$X_i = 1$	$X_i = 2$	$X_i = 3$	$X_i = 4$	$X_i = 5$
$X_i^B = 0$	1/2	0	0	1/2	0	0
$X_i^B = 1$	0	1/2	0	0	1/2	0
$X_i^B = 2$	0	0	1/2	0	0	1/2

In this protocol, the usage of coherent states can resist intercepting and re-sending attack, so, dishonest participant named Eve plays BS attack strategy [21,26], which is shown in Figure 2. To avoid being detected, Eve modulates the parameters of beam splitters to imitate the noisy quantum channels, i.e., the transmission coefficient of BS equals to the transmission efficiency of noisy quantum channel. In this way, the communicant may regard this attack as quantum channel lossy and noise. So, the mutual information between sender and receiver can be calculated as Equation (16). As for Eve, passing through the first BS, Eve can get

$$x_{E1} = \sqrt{\eta_1} x_{N1} - \sqrt{1-\eta_1} x_2, \quad p_{E1} = \sqrt{\eta_1} p_{N1} - \sqrt{1-\eta_1} p_2, \tag{19}$$

where η_1 is the transmission coefficient of BS, $a_{N1} = (x_{N1}, p_{N1})$ is a vacuum state and $x_{N1}, p_{N1} \sim N(0, \Sigma_1^2)$. Similarly, using the second BS, Eve can obtain

$$x_{E2} = \sqrt{\eta_2} x_{N2} - \sqrt{1-\eta_2} x_4, \quad p_{E2} = \sqrt{\eta_2} p_{N2} - \sqrt{1-\eta_2} p_4, \tag{20}$$

where η_2 is the transmission coefficient of BS, $a_{N2} = (x_{N2}, p_{N2})$ is a vacuum state and $x_{N2}, p_{N2} \sim N(0, \Sigma_2^2)$. Then, Eve performs a gain amplification on them to obtain

$$a'_{E1} = g_{E1} a_{E1}, \quad a'_{E2} = g_{E2} a_{E2}, \tag{21}$$

where $g_{E1} = \frac{1}{\sqrt{1-\eta_1}}$ and $g_{E2} = \frac{1}{\eta_1(\sqrt{1-\eta_2})}$. At last, Eve measures a'_{E1} and a'_{E2} and gets

$$a_E = \frac{1}{\sqrt{2}}(a'_{E1} - a'_{E2}). \tag{22}$$

According to the equations before, x_E can be expressed as

$$x_E = \frac{1}{\sqrt{2}}\left(\frac{\sqrt{\eta_1}}{\sqrt{1-\eta_2}} x_{N1} - \frac{\sqrt{\eta_2}}{\sqrt{\eta_1(1-\eta_2)}} x_{N2} - \frac{\sqrt{1-\eta_1}}{\sqrt{\eta}_1} x_{N2} + \frac{1}{\eta_1} y\right). \tag{23}$$

So, the signal variance of x_E is

$$V_E = \frac{\sigma^2}{2\eta_1} \tag{24}$$

and the noise variance of x_E is

$$N_E = \frac{1}{2}\left(\frac{\eta_1}{1-\eta_2}\Sigma_1^2 + \frac{\eta_2}{\eta_1(1-\eta_2)}\Sigma_2^2 + \frac{1-\eta_1}{\eta_1}\right)\Sigma_2^2. \tag{25}$$

So, the SNR of x_E is

$$\gamma_E = \frac{V_E}{N_E} \tag{26}$$

and the mutual information between sender and Eve is

$$I(S,E) = \frac{1}{2}\log_2(1+\gamma_E). \tag{27}$$

Therefore, the channel capacity C or the information rate ΔI is

$$C = \Delta I = I(S,R) - I(S,E). \tag{28}$$

Suppose the two quantum channels are the same with $\eta_1 = \eta_2 = \eta$ and $\Sigma_1 = \Sigma_2 = \Sigma$. According to the analysis above, the mutual information between sender and Eve is draw in Figure 5. It is obvious that setting lower noise variance of a_{N1} and a_{N2}, Σ_2^2, Eve can obtain more information. Moreover, the growth of σ^2 also can increase $I(S,E)$, but r has little effect on it.

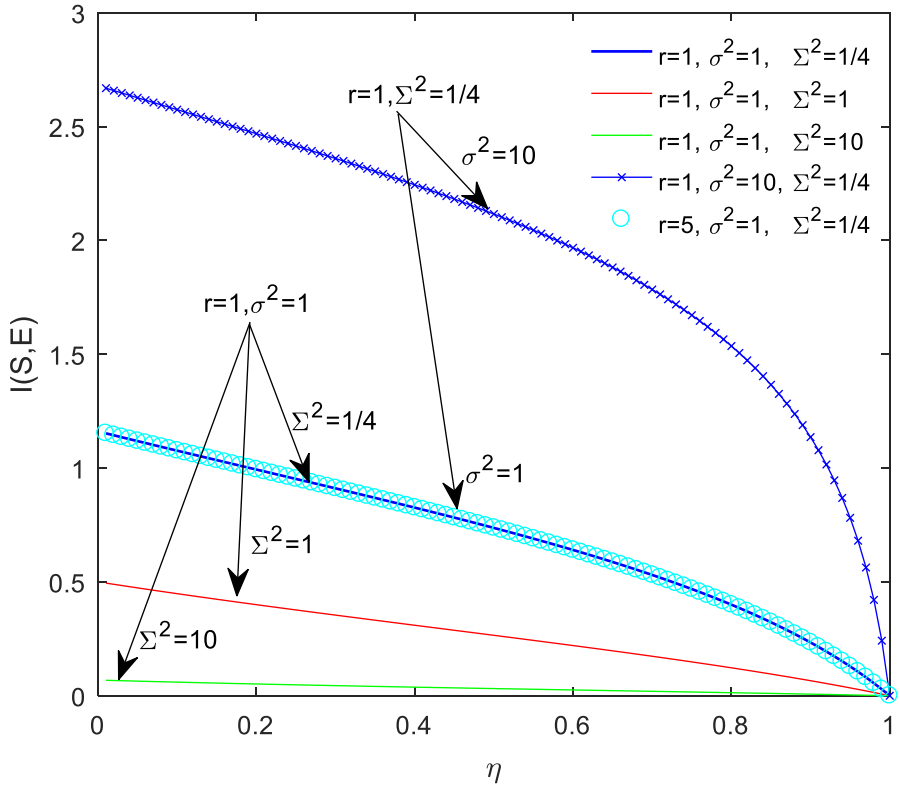

Figure 5. The mutual information of Eve.

Then, when $\Sigma^2 = 1$, the relationship between information rate ΔI and transmission efficiency η is exhibited in Figure 6. Under different conditions, such as $\sigma^2 = 1, r = 1, \sigma^2 = 1, r = 5, \sigma^2 = 28, r = 1$ and $\sigma^2 = 28, r = 5$, it is clear that the positions of $\Delta I = 0$ are all very closed to $(0.43, 0)$. When $\eta < 0.43$, $\Delta I < 0$ and Eve can acquire more information than legal communicators, so, the communication is insecure. When $\eta > 0.43$, $\Delta I > 0$ and ΔI increases with the growth of σ^2 or r, especially σ^2 can invite lots of improvement on ΔI. In order to transfer the secret shares successfully ($\Delta I \geq \log_2 3 \approx 1.6$), the requirement is rather more stringent, for example, when $\sigma^2 = 28, r = 5$, η need be greater than 0.79. Furthermore, Figure 7 depicts the relation between the squeezed parameter r and the variance of message σ^2 for satisfying $\Delta I = \log_2 3$, under conditions $\eta = \{1, 0.9, 0.8\}$. Obviously, when $r > 3$, the demand of σ^2 approaches to a stable value, which is seriously related with η of BSs. Compared with Figure 3, the requirement of σ^2 an r is much rougher. Because the loss of information is collected and used by Eve, rather than lost merely. Although the loss of channel is inevitable and Eve always exists, some strategies can be adopted to avoid Eve utilizing the lost or stolen information to infer the real secret. For example, encrypt the secret with one time pad generated by CVQKD [9], which is discussed in Ref. [26]. In this way, the $I(S, E)$ would be the same, but Eve can not exact any useful information about secret, which means no secret information leakage. So, the protocol would be feasible and secure under the low quantum channel transmission efficiency, only if the requirement of σ^2 an r can be achieved.

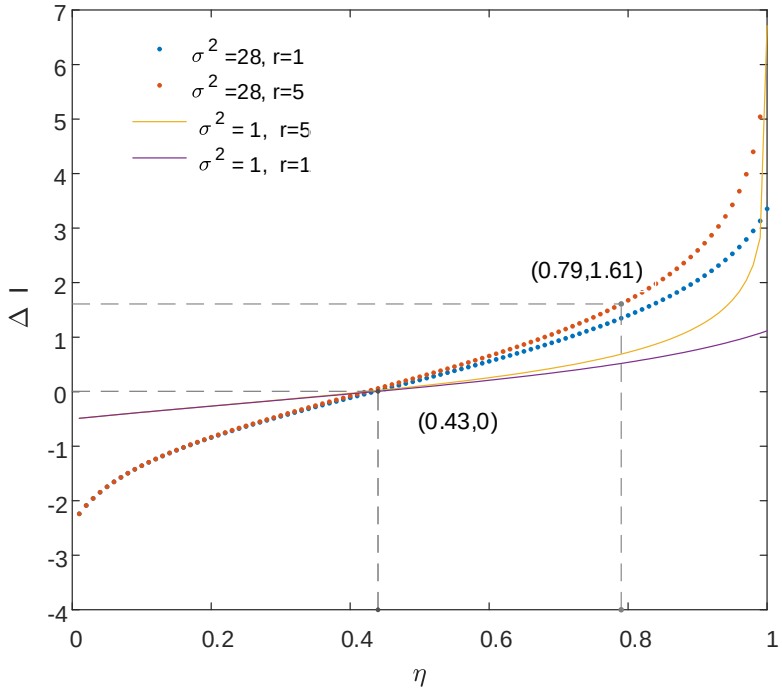

Figure 6. The information rate under attack ($\Sigma^2 = 1$).

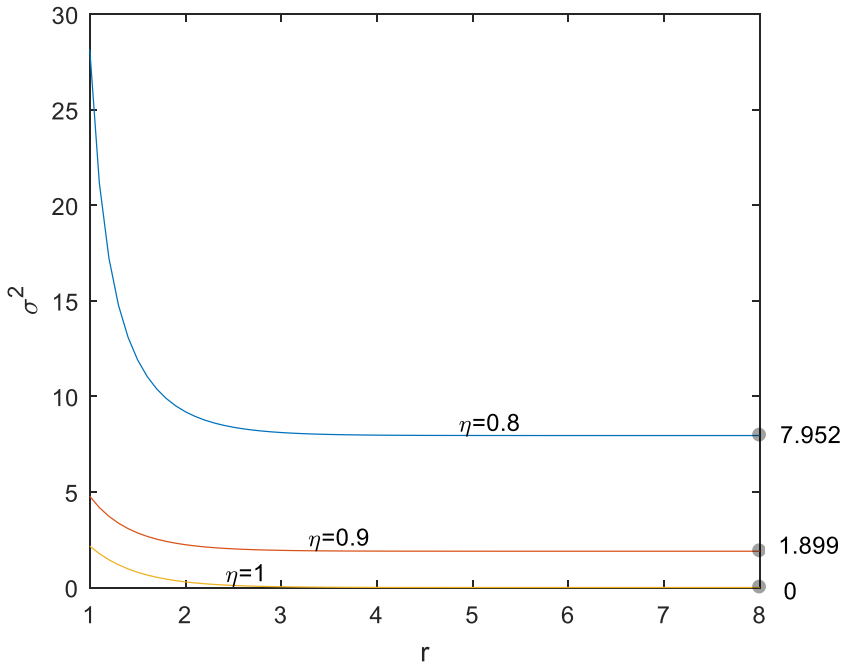

Figure 7. The relation between the squeezed parameter r and the variance of message σ^2, when $\Delta I = \log_2 3$ bit.

3.3. Fairness Property

In this protocol, the fairness property means Alice and Bob both can reconstruct the secret S or neither can recover it. According to the steps in recovery, the following situations would occur. (1) Suppose the position of the last secret S_L in message X is k. If Alice and Bob are both honest and follow the recovery steps to exchange their shares or the fake shares released at j_{th} round, $j > k + L_2$. After $(k + L_2)_{th}$ round, the determine pointer P^* appears, which means the secret S is recovered and can be picked out in front of P^* with length L. (2) If the fake shares released at j_{th} round, $1 \leq j < k$, the dishonest participant would be detected by message verification and the secret S has not been reconstructed before termination. (3) If the fake shares released at j_{th} round, $k < j < k + L_2$, the dishonest participant is checked out. At this moment, the secret S has been reconstructed and P^* does not appear completely. So, they both has possibility to guess right position and picks out S. (4) If the fake shares released at k_{th} round with probability $1/L_1$, dishonest participant he or she would reconstruct S and other participants are failed, but he or she can not assure this is the secret, because the right position is unknown. After this round, dishonest participant would be found. (5) If the fake shares released at $(k + L_2)_{th}$ round, dishonest participant, he or she, would reconstruct S and P^*, also honest participant would guess the position of S and pick it out correctly with great probability. Above all situations, both participants can recover or cannot recover the secret simultaneously, except in situation (4), dishonest participant may have little more advantage to acquire the whole secret, but, when the length of checking sequence R, L_1, is great enough, the probability of situation (4) is close to zero.

4. Conclusions

We have suggested a CVQSS scheme with fairness to resist dishonest participants keeping silence or returning error shares after receiving other ones' shares, which would be detected in verifying process. The participants release their shares interactively without simultaneity, but they can or can not reconstruct secret simultaneously. The above perspectives can be concluded from the discussion on fairness property, in which all five cases are enumerated and analyzed in detail. Of course, without loss of generality, participants cannot deduce the secret from their own shares independently.

The two-mode squeezed states are indispensable in our scheme and are exploited to transmit deterministic shares. As proved, this communication can send shares successfully, as long as setting proper the squeezing and modulation parameters according to the quantum channel transmission efficiency and the Shannon information of shares. Although, there must be eavesdropping in the channels, owing to the communication based on the two-mode squeezed states, legal communicators can detect the eavesdropper. In order to ensure the message directly transmitted succesfully, the channel transmission efficiency should be greater than 0.79. But, if the encrypted message is sent in the quantum channel, the infomation leakage of shares can be neglected, so that the demand of channel transmission efficiency can be regard as the conditon under no attack, that is lower to 0.08. However the increment of participants in the quantum network would greatly add the times of communication in this protocol. With the rapid development of n-particle CV entanglement, the CV GHZ can be invited to distribute shares which will make our scheme higher efficiency and more practical.

Author Contributions: Y.K. gave a general idea of the study, designed the concept of the study and wrote the article and completed the derivation of formulae and simulation analysis. H.Z. and G.C. provided practical recommendations for this study. Y.G. and X.J. revised some of the content in the paper. 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. 61572529, 61871407, 61872390, 61801522), and the Natural Science Foundation of the Jiangsu Higher Education Institutions of China (Grant No. 18KJB510045).

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

References

1. Hillery, M.; Bužek 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. [CrossRef]
3. Zhang, Z.; Man, Z. Multiparty quantum secret sharing of classical messages based on entanglement swapping. *Phys. Rev. A* **2005**, *72*, 022303. [CrossRef]
4. Li, Y.; Zhang, K.; Peng, K. Multiparty secret sharing of quantum information based on entanglement swapping. *Phys. Lett. A* **2004**, *324*, 420–424. [CrossRef]
5. Guo, Y.; Liao, Q.; Huang, D.; Zeng, G. Quantum relay schemes for continuous-variable quantum key distribution. *Phys. Rev. A* **2017**, *95*, 042326. [CrossRef]
6. Guo, Y.; Xie, C.; Huang, P.; Li, J.; Zhang, L.; Huang, D.; Zeng, G. Channel-parameter estimation for satellite-to-submarine continuous-variable quantum key distribution. *Phys. Rev. A* **2018**, *97*, 052326. [CrossRef]
7. Guo, Y.; Ye, W.; Zhong, H.; Liao, Q. Continuous-variable quantum key distribution with non-Gaussian quantum catalysis. *Phys. Rev. A* **2019**, *99*, 032327. [CrossRef]
8. Feng, Y.; Shi, R.; Guo, Y. Arbitrated quantum signature scheme with continuous-variable squeezed vacuum states. *Chin. Phys. B* **2018**, *27*, 020302. [CrossRef]
9. Guo, Y.; Feng, Y.; Zeng, G. Quantum anonymous voting with unweighted continuous-variable graph states. *Quantum Inf. Process* **2016**, *15*, 3327–3345. [CrossRef]
10. Lance, A.M.; Symul, T.; Bowen, W.P.; Tyc, T.; Sanders, B.C.; Lam, P.K. Continuous variable (2, 3) threshold quantum secret sharing schemes. *New J. Phys.* **2003**, *5*, 4. [CrossRef]
11. Shi, R.; Su, Q.; Guo, Y. Quantum secret sharing based on Chinese remainder theorem. *Commun. Theor. Phys.* **2011**, *55*, 573.
12. Guo, Y.; Zhao, Y. High-efficient quantum secret sharing based on the Chinese remainder theorem via the orbital angular momentum entanglement analysis. *Quantum Inf. Process.* **2013**, *12*, 1125–1139. [CrossRef]
13. Kang, Y.; Liao, Q.; Geng, J.; Guo, Y. Continuous Variable Quantum Secret Sharing with Chinese Remainder Theorem. *Int. J. Theor. Phys.* **2019**, *58*, 3986–3997. [CrossRef]
14. Liu, F.; Su, Q.; Wen, Q. Eavesdropping on multiparty quantum secret sharing scheme based on the phase shift operations. *Int. J. Theor. Phys.* **2014**, *53*, 1730–1737. [CrossRef]
15. Qin, S.J.; Gao, F.; Wen, Q.Y.; Zhu, F.-C. Cryptanalysis of the Hillery-Bužek-Berthiaume quantum secret-sharing protocol. *Phys. Rev. A* **2007**, *76*, 062324. [CrossRef]
16. Gao, F.; Qin, S.J.; Wen, Q.Y.; Zhu, F.-C. A simple participant attack on the protocol. *Quantum Inf. Comput.* **2007**, *7*, 329–334.
17. Lin, H.Y.; Harn, L. Fair reconstruction of a secret. *Inf. Process. Lett.* **1995**, *55*, 45–47. [CrossRef]
18. Liu, F.; Qin, S.J.; Wen, Q.Y. A quantum secret-sharing protocol with fairness. *Phys. Scr.* **2014**, *89*, 075104. [CrossRef]
19. Maitra, A.; De, S.J.; Paul, G.; Pal, A.K. Proposal for quantum rational secret sharing. *Phys. Rev. A* **2015**, *92*, 022305. [CrossRef]
20. He, G.; Zeng, G. Quantum encryption protocol based on continuous variable EPR correlations. *Commun. Theor. Phys.* **2006**, *46*, 61.
21. Gong, L.H.; Song, H.C.; He, C.S.; Liu, Y.; Zhou, N.-R. A continuous variable quantum deterministic key distribution based on two-mode squeezed states. *Phys. Scr.* **2014**, *89*, 035101. [CrossRef]
22. Ma, S.; Li, X.; Xie, J.; Li, F.-L. Two-mode squeezed states of two separated nitrogen-vacancy-center ensembles coupled via dissipative photons of superconducting resonators. *Phys. Rev. A* ***2019***, 99, 012325. [CrossRef]
23. Downing, C.A.; Carreño, J.C.L.; Laussy, F.P.; del Valle, E.; Fernández-Domínguez, A.I. Quasichiral interactions between quantum emitters at the nanoscale. *Phys. Rev. Lett.* ***2019***, 122, 057401. [CrossRef] [PubMed]

24. Asmuth, C.; Bloom, J. A modular approach to key safeguarding. *IEEE Trans. Informat. Theory* **1983**, *29*, 208. [CrossRef]
25. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
26. He, G.; Zhu, J.; Zeng, G. Quantum secure communication using continuous variable Einstein-Podolsky-Rosen correlations. *Phys. Rev. A* **2006**, *73*, 012314. [CrossRef]