Long-distance continuous-variable measurement-device-independent quantum key distribution with discrete modulation

Hong-Xin Ma,1,2,3 Peng Huang,3 Dong-Yun Bai,3 Tao Wang,3 Shi-Yu Wang,3 Wan-Su Bao,1,2 and Gui-Hua Zeng3

1Zhengzhou Information Science and Technology Institute, Zhengzhou 450004, China
2Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China
3State Key Laboratory of Advanced Optical Communication Systems and Networks and Center of Quantum Information Sensing and Processing, Shanghai Jiao Tong University, Shanghai 200240, China

(Dated: December 17, 2018)

We propose a long-distance continuous-variable measurement-device-independent quantum key distribution (CV-MDI-QKD) protocol with discrete modulation. This kind of discrete-modulated schemes have good compatibility with efficient error correction code, which lead to higher reconciliation efficiency even at low signal-to-noise ratio (SNR). Security analysis shows that the proposed protocol is secure against arbitrary collective attacks in the asymptotic limit with proper use of decoy states. And with the using of discrete modulation, the proposed CV-MDI-QKD protocol has simpler implementation and outperform previous protocols in terms of achievable maximal transmission distance, which precisely solve the bottleneck of the original Gaussian-modulated CV-MDI-QKD protocol.

PACS numbers: 03.67.Hk, 03.67.-a, 03.67.Dd

I. INTRODUCTION

Quantum key distribution (QKD) [1] allows two distant authenticated users to establish secure key through untrusted quantum and classical channels. QKD has two main categories: one is discrete-variable (DV)QKD protocols [2–4], and the alternative is continuous-variable (CV) QKD protocols [5–8]. Compared with DVQKD protocols (such as BB84 protocol), CVQKD protocols have unique potentials of being effectively compatible with existing optical communication systems and using lower cost light sources and detectors. In addition, CVQKD allow users to approximate the ultimate limit of repeater-less communication, which is known as the PLOB bound [9].

In recent decades, research on CVQKD has evolved rapidly. The Gaussian-modulated CVQKD protocol employing coherent state [6] has been theoretically proved to be secure under arbitrary collective attack [10] and coherent attacks [11], even taking finite-size regime into account [12–13]. What’s more, its composable security has been fully proven [14]. Furthermore, this protocol has been experimentally proved to be feasible both in laboratory [17–18] and field tests [16]. A recent demonstration of all-fiber Gaussian-modulated CVQKD protocol has extended the secure transmission distance of CVQKD over 100 km in the laboratory [17], which showing its potential of being an appealing solution for metropolitan quantum networks.

Theoretically, the security analysis of CVQKD relies on some ideal assumptions, which is hard to satisfy in the experimental implementation [18–20]. The imperfect devices lead to the practical security loopholes, which will be utilized by eavesdroppers to take quantum attack strategies, such as local oscillator (LO) fluctuation attack [21], calibration attack [22], LO wavelength attack [23] and detector saturation attack [24]. Most of these attack strategies mainly focus on the loopholes of the practical imperfect detectors. The attackers employ these loopholes to reduce the estimated additional noise by manipulating the measurement results of the detector, causing Alice to overestimate the security key rate, which in turn hides the extra noise introduced by the attack process.

In order to eliminate all the security hazard of the detector end effectively, continuous-variable measurement-device-independent (CV-MDI) QKD has been proposed by several groups independently [25–28]. In CV-MDI-QKD protocol, two legitimate parties, Alice and Bob, are both senders. An untrusted third party, Charlie, is introduced to receive quantum states sent by Alice and Bob, performing Bell-State Measurement (BSM) and communicating the measurement result to generate the secure keys. Since the measurement part of the protocol is performed by an untrusted third party, the security of the protocol no longer counts on the perfect detector. Therefore, CV-MDI-QKD can remove all known or unknown side-channel attacks on detectors, which means higher practical security. In recent years, several significant results have been achieved in the theoretical research field of CV-MDI-QKD [29–32].

Unfortunately, in practical implementation, the maximal transmission distance of CV-MDI-QKD is unsatisfactory [28]. One of the key problems is that the reconciliation efficiency $\beta$ is quite low for Gaussian-modulated protocols in the case of long distance transmission with low signal-to-noise ratio. The best error correction codes presently available, such as LDPC codes [37] or turbo codes, work well with discrete (e.g. binary) value under low SNR condition, but have poor performance with continuous (e.g. Gaussian-modulated) value under the same condition.

In order to solve this problem, many efforts are being dedicated. The mainstream approach is to programming an error
FIG. 1: (Color online). Schematic diagram of the CV-MDI-QKD protocol with discrete modulation. $|\psi_4\rangle_{A_1 A_2}$ and $|\psi_4\rangle_{B_1 B_2}$ are all two-mode squeezed states. Het is heterodyne detection. Hom is homodyne detection. $D(\beta)$ is displacement operation.

correction code with higher efficiency under low SNR conditions. This approach is consistent with the way to solve this problem in one-way protocol, such as the code proposed in [38], which can be combined with a multidimensional reconciliation scheme [39] and work well in the regime of low SNR. However, this type of error correction codes is designed and implemented with high complexity, and the cost of hardware required is high. What's more, the probability that such codes will succeed in achieving high reconciliation efficiency is quite low [38].

Interestingly, it has been found that the discrete modulation, such as four-state modulation, allows for a much better reconciliation efficiency at low SNR, which lead to longer transmission distance in CVQKD protocol [40, 41]. In discrete-modulated protocols [40–42], the senders prepare a certain number of nonorthogonal coherent states (for four-state scheme, the number is four), and exploit the sign of measured quadratures of each state to encode the bits of secret key rate, while the Gaussian-modulated protocols exploit the quadratures itself to encode information. The sign of measured quadratures is already discrete values, which works well with high efficient error correction codes even at low SNR. The discrete-modulated protocols are particularly suited in long-distance transmission, whereas they are hard to obtain high key rate at short distance. Surprisingly, a recent work [43] shows the 256 modes discrete-modulated protocol is able to obtain almost the same high key rate with the Gaussian-modulated protocol. Furthermore, discrete modulation is more convenient for experimental implementation and specific operation than Gaussian modulation. Inspired by the aforementioned advantages, we propose a CV-MDI-QKD protocol by employing discrete modulation, which could apparent extent the maximal transmission distance of CV-MDI-QKD protocol without taking additional security vulnerability.

The paper is structured as follows. In Sec. II we first introduce the original CV-MDI-QKD protocol, then introduce the model of the CV-MDI-QKD protocol with discrete modulation and the use of decoy states. In Sec. III we derive the secret key of the CV-MDI-QKD protocol with discrete modulation. In Sec. IV we give the numerical simulation and performance analysis. Conclusion and discussion are drawn in Sec. V.

II. CV-MDI-QKD PROTOCOL WITH DISCRETE MODULATION

In this section, we first review the CV-MDI-QKD protocol, especially the entanglement-based (EB) version. Then, we present the CV-MDI-QKD protocol with discrete modulation. In addition, we introduce the use of decoy states for CV-MDI-QKD protocol with discrete modulation, which guarantee the security of this protocol.

A. CV-MDI-QKD Protocol

Generally, for CV-MDI-QKD protocol, the prepare-and-measure (PM) version is applied to implementation in practice as it is easy to apply, while the equivalent EB version is used for security analysis. The construction of CV-MDI-QKD protocol is illustrated in Fig. 1. The main steps of EB version can be depicted as follows:

Step 1: Alice and Bob prepare two-mode squeezed states $|\psi_4\rangle_{A_1 A_2}$ and $|\psi_4\rangle_{B_1 B_2}$ independently. Mode $A_1$ and $B_1$ are retained by Alice and Bob respectively, and mode $A_2$ and $B_2$ are sent to an untrusted third part Charlie through the quantum channel with length $L_{AC}$ and $L_{BC}$, respectively.

Step 2: After receive modes $A'$ and $B'$, Charlie interferes the two modes at a beam splitter (BS) and get two output modes $C$ and $D$. After the $x$ quadrature of mode $C$ and $p$ quadrature of mode $D$ are measured by homodyne detections,
Charlie announced the measurement results \( \{ X_C, P_D \} \) publicly.

Step 3: Bob uses the received measurement results to modifies mode \( B_1 \) through displacement operation \( D(\beta) \) and obtains

\[
\rho_{B_1} = D(\beta) \rho_{B_1} D^\dagger(\beta),
\]
where \( \rho_{B_1} \) is the density matrix of mod \( B_1 \), \( \beta = g(X_C + iP_D) \), and \( g \) is the gain of the displacement. Through heterodyne detection, Bob measures mode \( B'_1 \) to get \( \{ X_B, P_B \} \), and Alice measures mode \( A_1 \) to get \( \{ X_A, P_A \} \).

Step 4: Alice and Bob implement parameter estimation, information reconciliation and privacy amplification, finally obtaining a string of secret key.

Through the BSM and Bob’s displacement operation, modes modes \( A_1 \) and \( B'_1 \) are entangled \([44]\), and \( \{ X_B, P_B \} \) and \( \{ X_A, P_A \} \) are correlated.

In the PM scheme, Alice and Bob prepare coherent states independently and send them to Charlie for BSM. After Charlie announce the measurement results, Bob modifies his data according to the measurement results, while Alice keeps her data unchanged. There is no displacement operation for Bob in the PM scheme. Alice and Bob extract a string of secret key by using parameter estimation, information reconciliation and privacy amplification.

**B. Discrete modulation in CV-MDI-QKD**

In CV-MDI-QKD protocol with discrete modulation, Alice and Bob perform discrete modulation operations simultaneously. For the sake of specificity and simplicity, we mainly focus on four-state scheme \([40, 42]\). In this scheme, the modulated coherent states consist of four types: \( |\alpha e^{i\pi/4}\rangle \), \( |\alpha e^{-3i\pi/4}\rangle \), \( |\alpha e^{-i\pi/4}\rangle \), and \( |\alpha e^{i\pi/4}\rangle \), where \( \alpha \) is a positive number related to the modulation variance of coherent states. The four types are shown in Fig. 1. The modulation variance of coherent state is \( \lambda^2 = 2\alpha^2 \).

First, we consider the discrete modulation operation in Alice. In PM version, the mixture state \( \rho_4^A \), which is send by Alice to Charlie through the quantum channel, is given by

\[
\rho_4^A = \frac{1}{4} \sum_{k=0}^{3} \left| \alpha_k^A \right\rangle \left\langle \alpha_k^A \right|.
\]

In EB version, the two-mode squeezed state prepares by Alice is \( |\Psi_4\rangle_{A_1A_2} \), and the variances of the quadrature components of the two modes \( A_1 \) and \( A_2 \) are all \( \lambda^2 \). The two-mode squeezed state prepares by Bob is \( |\Psi_4\rangle_{B_1B_2} \), and the variances of the quadrature components of the two modes \( B_1 \) and \( B_2 \) are all \( \lambda^2 \), and \( \lambda^2 = V_M \). The modes of \( |\Psi_4\rangle_{A_1A_2} \) and \( |\Psi_4\rangle_{B_1B_2} \) is illustrated in Fig. 1. the two-mode entangled state prepares by Alice is

\[
|\Psi_4\rangle_{A_1A_2} = \sum_{k=0}^{3} \sqrt{\lambda_k} |\phi_k^A\rangle |\phi_k^A\rangle = \frac{1}{2} \sum_{k=0}^{3} |\psi_k\rangle_{A_1} |\alpha_k^A\rangle_{A_2},
\]
where the non-Gaussian states \( |\psi_k\rangle_{A_1} \) is given by

\[
|\psi_k\rangle_{A_1} = \frac{1}{2} \sum_{m=0}^{3} e^{i(1+2k)m\pi/4} |\phi_m^A\rangle,
\]
with \( m \in \{ 0, 1, 2, 3 \} \) and

\[
|\phi_k^A\rangle = \frac{1}{\sqrt{2}} \sum_{n=0}^{\infty} (-1)^n \frac{\alpha^{4n+k}}{\sqrt{(4n+k)!}} |4n+k\rangle,
\]
for \( k \in \{ 0, 1, 2, 3 \} \), and

\[
\lambda_{0,2} = \frac{1}{2e^{\pi\alpha^2}} \left[ \cosh(\alpha^2) \pm \cos(\alpha^2) \right],
\]
\[
\lambda_{1,3} = \frac{1}{2e^{\pi\alpha^2}} \left[ \sinh(\alpha^2) \pm \sin(\alpha^2) \right].
\]

As the PM version is equivalent to the EB vision for this protocol, the mixture state \( \rho_4 \) can be calculated as

\[
\rho_4 = \text{Tr} \left( |\Psi_4\rangle_{A_1A_2} \langle \Psi_4|_{A_1A_2} \right) = \sum_{k=0}^{3} \lambda_k |\phi_k^A\rangle \langle \phi_k^A|.
\]

The covariance matrix \( \gamma_{A_1A_2} \) of the bipartite state \( |\Psi_4\rangle_{A_1A_2} \) can be expressed by

\[
\gamma_{A_1A_2} = \begin{pmatrix}
XI_2 & Z_4\sigma_z \\
Z_4\sigma_z & YI_2
\end{pmatrix},
\]
where \( I_2 \) is a \( 2 \times 2 \) identity matrix, \( \sigma_z = \text{diag}(1, -1) \), and

\[
X = \langle \Psi_4 | 1 + a_1^\dagger a_1 | \Psi_4 \rangle = 1 + 2\alpha^2,
\]
\[
Y = \langle \Psi_4 | 1 + a_2^\dagger a_2 | \Psi_4 \rangle = 1 + 2\alpha^2,
\]
\[
Z_4 = \langle \Psi_4 | a_1 a_2 + a_1^\dagger a_2^\dagger | \Psi_4 \rangle = 2\alpha^2 \sum_{k=0}^{3} \lambda_{k-1}^{3/2} \lambda_k^{-1/2}.
\]

Similarly, we set the modulation variance in Bob is still \( \lambda^2 = 2\beta^2 = 2\alpha^2 \), and the two output modes of the bipartite state \( |\Psi_4\rangle_{B_1B_2} \) are \( B_1 \) and \( B_2 \). As Alice and Bob perform the same discrete modulation, the covariance matrix \( \gamma_{B_1B_2} \) of \( |\Psi_4\rangle_{B_1B_2} \) is the same as \( \gamma_{A_1A_2} \). Displacement operation does not affect the covariance matrix.

To summarize, in PM version of our protocol, Alice randomly prepares four nonorthogonal coherent states and send one of them to Charlie, Bob randomly prepares another four nonorthogonal coherent states and send one of them to Charlie. After Charlie performs the BSM on the received two states and announced the measurement results, Alice keeps her sign of quadratures and Bob modifies his sign based on these results. In EB version of our protocol, when Alice performs projection measurement on mode \( A_1 \), she only discriminates which coherent state is sent to Charlie, which shows the sign of quadratures of the state. And Bob performs projection measurement on mode \( B'_1 \) to get the sign of quadratures, which is associated with the sign obtained by Alice. Both the PM version and EB version use the signs of measured quadratures of states to extract a string of secret key.
FIG. 2: (Color online). Equivalent one-way protocol of the CV-MDI-QKD protocol with discrete modulation in EB version, where Eve is aware of Charlie, channels, the two-mode squeezed state $|\Psi_i\rangle_{B_1B_2}$ and the displacement operation $D(\beta)$.

C. Decoy states

In EB version of our protocol, Alice (Bob) performs the projection measurement, which just makes Alice (or Bob) to discriminate which state is sent to Charlie, but not aware of the quadratures of her (his) quantum mode. Therefore, the two legitimate users cannot use these experimental data to construct the covariance matrix of the mixed state $\rho_{AB}$ without the linear channel assumption (LCA) [42]. In other words, LCA is a necessary condition for the security of the protocol.

In order to solve this problem, we introduce decoy states to modify our protocol, which refer to the idea of A. Leverrier et al. [41]. The use of decoy state can be expressed as

$$p\sigma_{\text{key}} + (1-p)\sigma_{\text{decoy}} = \sigma_G,$$  

where $\sigma_{\text{key}}$ is the states used for the key distillation, $\sigma_{\text{decoy}}$ is the decoy states, and $p$ is a weight between 0 and 1. $\sigma_G$ is the states satisfying Gaussian distribution and meeting

$$p_{\text{est}}\sigma_{\text{est}} + (1-p_{\text{est}})\sigma_G = \sigma_{\text{All}},$$

where $\sigma_{\text{est}}$ is the states used for parameter estimation, $\sigma_{\text{All}}$ are all the states sent through quantum channel. $\sigma_{\text{est}}$ and $\sigma_{\text{All}}$ are all follow Gaussian distribution. $p_{\text{est}}$ denote the fraction of $\sigma_{\text{est}}$. In practice, Alice randomly prepares $\sigma_{\text{key}}^A$, $\sigma_{\text{decoy}}^A$ and $\sigma_{\text{est}}^A$ with probability $p(1-p_{\text{est}})$, $(1-p)(1-p_{\text{est}})$ and $p_{\text{est}}$ respectively. The three types of states can be given as

$$\sigma_{\text{key}}^A = \int p_{\text{key}}(\alpha) \langle \alpha | \alpha \rangle d\alpha,$$

$$\sigma_{\text{decoy}}^A = \int p_{\text{decoy}}(\alpha) \langle \alpha | \alpha \rangle d\alpha,$$

$$\sigma_{\text{est}}^A = \int p_{\text{est}}(\alpha) \langle \alpha | \alpha \rangle d\alpha,$$

where the probability distribution $p_{\text{key}}(\alpha)$ is chosen as $p(1-p_{\text{est}})$, $p_{\text{decoy}}(\alpha)$ is chosen as $(1-p)(1-p_{\text{est}})$ and $p_{\text{est}}(\alpha)$ is chosen as $p_{\text{est}}$. Obviously, the mixed state sent by Alice to Charlie is Gaussian, denoted as $\sigma_{\text{All}}^A$. Bob prepares a Gaussian state $\sigma_{\text{All}}^B$ and sends it to Charlie through quantum channel, taking BSM with $\sigma_{\text{All}}^A$. After these quantum process, Alice tell Bob $p$, $p_{\text{est}}$ and which state is $\sigma_{\text{key}}^A$, $\sigma_{\text{decoy}}^A$ or $\sigma_{\text{est}}^A$ through the classical channel. Then Alice and Bob can establish secure keys through our protocol without LCA. In addition, the use of decoy states can also eliminate the vulnerability exploited by state-discrimination attack [45], since the discrimination receiver is noneffective for Gaussian states and Eve cannot distinguish whether the state is $\sigma_{\text{key}}$, $\sigma_{\text{decoy}}$ or $\sigma_{\text{est}}$. Otherwise, this method still has certain defects. In practice, these operations will increase the complexity of the system, and the decoy states is hard to be precisely prepared.

III. CALCULATION OF THE SECRET KEY RATE

In this section, we mainly focus on the secret key rate under collective attacks, since they are optimal in the asymptotic limit. The EB scheme of CV-MDI-QKD protocol can be converted into a common one-way CVQKD protocol, where we assume that the two-mode squeezed state $|\Psi_i\rangle_{B_1B_2}$ and the displacement operation $D(\beta)$ are untrusted. The equivalent one-way protocol is shown in Fig. 2. We denote the secure key rate of the CV-MDI-QKD protocol with discrete modulation and the equivalent one-way protocol are $K_{DM}$ and $K_{one}$, respectively. It is obvious that $K_{DM} \geq K_{one}$. Hence, the lower bound of $K_{DM}$ can be estimated by using similar covariance matrix of the equivalent one-way protocol. In PM version of our protocol, the quantum states sent by Alice and Bob are all non-Gaussian states. According to the optimality of Gaussian attack [45], we can use the method of calculating secret key rate under collective Gaussian attacks to get the low bound of the secret key rate of our protocol under collective attacks. In order to facilitate the analysis, we use the method of calculating $K_{one}$ under collective Gaussian attacks to obtain $K_{DM}$.

In addition, we assume the quantum channels from Alice to Charlie and Bob to Charlie are two independent Markovian memoryless Gaussian quantum channels [47]. This assumption is based on that the two quantum channels are come from different directions in practical CV-MDI-QKD system, which means that the ambient noise of the two channels should have weak connection. Under this assumption, the optimal collective Gaussian attack is taking entangling cloner attacks on each quantum channel independently [10, 26]. The following calculation and simulation are all based on this attack strategy.

The excess noise and the transmittance of the quantum channel between Alice (Bob) and Charlie are $\varepsilon_A$ ($\varepsilon_B$) and $\eta_A$ ($\eta_B$). We set both quantum channel losses are $l = 0.2$ dB/km, then the transmittance can be given as $\eta_A = 10^{-\frac{4l}{\lambda}}$, $\eta_B = 10^{-\frac{4l_{BC}}{\lambda}}$. $\varepsilon$ refers to the equivalent excess noise of the equivalent one-way protocol, which can be calculated as

$$\varepsilon = 1 + \chi_A + \frac{\eta_B}{\eta_A} (\varepsilon_B - 1)$$

$$+ \frac{\eta_B}{\eta_A} \left( \sqrt{\frac{2}{\eta_B}} - 1 - \sqrt{\frac{1}{\eta_B} + 1} \right)^2,$$

where $\chi_A = \frac{1}{\eta_A} - 1 + \varepsilon_A$, $\chi_B = \frac{1}{\eta_B} - 1 + \varepsilon_B$, $g$ is the gain of the displacement operation in Bob. We adopt $g^2 = \frac{2(\sqrt{g^2 - 1})}{\eta_B}$ to minimize $\varepsilon$, then we obtain

$$\varepsilon = \frac{\eta_B}{\eta_A} (\varepsilon_B - 1) + 1 + \chi_A$$

$$= \frac{\eta_B}{\eta_A} (\varepsilon_B - 2) + \varepsilon_A + \frac{2}{\eta_A},$$

where $\chi_A = \frac{1}{\eta_A} - 1 + \varepsilon_A$. Therefore, $\chi_A$ and $\chi_B$ can be directly calculated as

$$\chi_A = \frac{1}{\eta_A} - 1 + \varepsilon_A,$$

$$\chi_B = \frac{1}{\eta_B} - 1 + \varepsilon_B.$$
We suppose the homodyne detectors in Charlie are ideal apparatuses, then the total channel-added noise expressed in shot noise units is
\[
\rho = \frac{\text{paratuses, then the total channel-added noise expressed in shot noise units is}}{20 \text{ km}, 25 \text{ km} \text{ and } 30 \text{ km}.}
\]
\[
\text{Parameters are fixed as follows: excess noise } \varepsilon_A = \varepsilon_B = 0.002, \text{ reconciliation efficiency } \beta = 90\%.
\]

The secure key rate of the CV-MDI-QKD protocol with discrete modulation can be calculated by
\[
\kappa_{1,2} = \frac{1}{2} \left( A + \sqrt{A^2 - 4B^2} \right),
\]
with the notations
\[
A = a^2 + b^2 - 2c^2 = X^2 + \eta^2(Y + \chi_t)^2 - 2\eta Z_i^2,
\]
\[
B = ab - c^2 = \eta(XY + X\chi_t - Z_i^2).
\]

The symplectic eigenvalues \(\chi_{M}^{A_i}\) is given by
\[
\gamma_{M}^{A_i} = a I_2 - c \sigma_z(b I_2 + I_2)^{-1} \sigma_z = [a - c^2/(b + 1)] I_2.
\]

Then the symplectic eigenvalues \(\kappa_3\) is obtained as
\[
\kappa_3 = a - c^2/(b + 1) = X - \eta Z_i^2/[(\eta(Y + \chi_t) + 1].
\]

IV. PERFORMANCE ANALYSIS

In this section, we show the performance of CV-MDI-QKD protocol with discrete modulation compared with the original CV-MDI-QKD protocol. It has been proven that the configuration with the optimal performance for CV-MDI-QKD protocol is the extreme asymmetric case [28], where Charlie infinitely close to Bob. In our analysis, we are mainly concerned about this case. In this case, \(L_{BC} = 0\), the transmission distance is equal to \(L_{AC}\).

The modulation variance \(V_M\) is a parameter that will profoundly affect the performance of the proposed protocol. In order to extract the optimal secret key rate, we plot the secret key rates as a function of the modulation variance \(V_M\) with different transmission distance in extreme asymmetric case, which is shown Fig. [5]. It is obvious that the optimal areas of \(V_M\) are gradually compressed when transmission distance increases, and the secret key rate decreases evidently with the increase of transmission distance. The practicable \(V_M\) values of our protocol are quite low than the original CV-MDI-QKD protocol.
It seems clear that the maximum transmission distance of discrete-modulated CV-MDI-QKD protocol is always longer than that of the original Gaussian-modulated one under both excess noises. Compared with the original CV-MDI-QKD protocol, the discrete modulation combined with CV-MDI-QKD protocol can obviously extend the maximum transmission distance, which can effectively expand the scope of application of such protocols. Moreover, when the transmission distance is longer than 21.7 km with the excess noise $\varepsilon_A = \varepsilon_B = 0.002$, the performance of discrete-modulated CV-MDI-QKD protocol is much closer to the PLOB bound than that of the original Gaussian-modulated CV-MDI-QKD protocol, and the performance gap between the two protocols will become larger and larger with the increase of transmission distance. As the discrete-modulated protocol works well with efficient error correction code in reconciliation process, even in extremely low SNR conditions [40], the maximal transmission distance of the discrete-modulated CV-MDI-QKD protocol can be much longer than that of original Gaussian-modulated CV-MDI-QKD protocol in practice.

There is a phenomenon that deserves our attention: within a shorter transmission distance, the performance of the CV-MDI-QKD protocols with discrete modulation is worse than that of original CV-MDI-QKD protocol. This case is caused by the lower modulation variance of the quantum signal in discrete-modulated CV-MDI-QKD protocol (almost below 1 units of shot noise), which leads to the secret key rate of discrete-modulated protocol is much lower than the original one in the condition of low-channel-loss. In addition, as shown in the figure 4, when the excess noise increases, the secret key rate of discrete-modulated CV-MDI-QKD protocol decreases faster than that of the original CV-MDI-QKD protocol. This means that our protocol is more sensitive to the excess noise. The reason for this phenomenon is that the quantum signal intensity and the SNR in discrete-modulated CV-MDI-QKD protocol is much lower than these of original CV-MDI-QKD protocol. However, these defects can be corrected effectively with the participation of noiseless linear
amplifier. Otherwise, Z. Li et al. have proved that discrete-modulated coherent state protocol with 256 modes can reach the high secret key rate almost the same as Gaussian modulation case [43].

Fig. 5 depicts a performance comparison of the CV-MDI-QKD protocol with discrete modulation and the original CV-MDI-QKD protocol with Gaussian modulation for different reconciliation efficiency $\beta$ in the extreme asymmetric case, where $L_{BC} = 0$. $V_{M}$ of both protocols are all the ones provide optimal performance in practice, which is the same as the $V_{M}$ in Fig. 4.

For the CV-MDI-QKD protocol with discrete modulation, the usable range of $\beta$ narrows with the increase of transmission distance. When the transmission distance are 20km, the secret key rate of the CV-MDI-QKD protocols with discrete modulation are lower than that of the original CV-MDI-QKD protocol when the reconciliation efficiency $\beta$ values in 0.892 to 1. This is also caused by the lower quantum signal modulation variance in discrete modulation. Nevertheless, with $\beta$ decrease, the secret key rate of the original protocol decrease faster than that of the protocol with discrete modulation. When $\beta$ is lower than 0.892, the secret key rate of the protocols with discrete modulation get higher than that of the original one. Moreover, the original CV-MDI-QKD protocol will have no secret key when $\beta$ is lower than 0.889, but the lower bound of $\beta$ to obtaining secret key for the CV-MDI-QKD protocols with discrete modulation is 0.761. All this means the CV-MDI-QKD protocol with discrete modulation are more tolerant of the reconciliation efficiency. What’s more, the protocol with discrete modulation have better combination with efficient error correction code. This will further widen the performance gap between our protocol and the original CV-MDI-QKD protocol over long-distance transmission.

V. CONCLUSION AND DISCUSSIONS

In this paper, we have introduced a CV-MDI-QKD protocol with discrete modulation, which can obviously improve the maximal transmission distance. We focus on the analysis of four-state scheme as the representative of discrete modulation scheme. The security of this protocol under arbitrary collective attacks is established with the appropriate use of decoy states. The discrete-modulated CV-MDI-QKD protocol have commendable cooperation with efficient reconciliation error correction codes, even in extremely low SNR conditions, which leads to longer secure transmission distance. This property exactly right remedies the defect in the transmission distance of CV-MDI-QKD protocol. The secret key rate simulation results under the asymptotic case shows that the proposed protocol has obvious advantages over the original Gaussian-modulated CV-MDI-QKD protocol in maximal transmission distance, even with the same reconciliation efficiency. What’s more, compared with the original Gaussian-modulated CV-MDI-QKD protocol, the experimental implementation of our protocol is more simple and convenient in practice.

In the above analysis, Charlie’s homodyne detectors are assumed to be perfect, where the electronic noise $\nu_{el}$ of homodyne detector is 0 and the quantum efficiency $\eta_{hom}$ of homodyne detector is 1. However, the practical homodyne detectors in Charlie are not the always ideal apparatuses. We express the detection-added noise in shot noise units as $\chi_{hom} = \nu_{el} + (1 - \eta_{hom})\chi_{el}$. The total noise referred to the channel input with imperfect detectors can be calculated as $\chi_{t}^\prime = \chi_{t} + 2\chi_{hom}/\eta_{A}$. Obviously, the imperfection of the detectors will great increase the total noise. Since the quantum signal intensity of our protocol is much lower than these of the original Gaussian-modulated one, our protocol is more sensitive to the total noise and, especially, the imperfection of the detectors. But fortunately, through the rational use of noiseless linear amplifier and state-discrimination detection, we will significantly improve the robustness of our protocol to the imperfections of detectors. Moreover, it would be meaningful to improve the initial secret key rate of the proposed protocol and carry out the experimental implementation in further research.

Acknowledgments

This work was supported the National key research and development program (Grants No. 2016YFA0302600), the National Basic Research Program of China (Grant No. 2013CB338002) and the National Natural Science Foundation of China (Grants No. 11304397, 61332019, 61505261, 61675235, 61605248, 61671287).

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. 74, 145 (2002).
[2] C. H. Bennett and G. Brassard, in Proceedings IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York, 1984), pp. 175C179.
[3] A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991).
[4] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. A. Smolin, J. Cryptol. 5, 3 (1992).
[5] T. C. Ralph, Phys. Rev. A 61, 010303(R)(1999).
[6] F. Grosshans and P. Grangier, Phys. Rev. Lett. 88, 057902 (2002).
[7] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf and P. Grangier, Nature(London) 421, 238 (2003).
[8] C. Weedbrook, S. Pirandola, R. Garcia-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. 84, 621 (2012).
[9] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. 8, 15043 (2017).
[10] M. Navascues, F. Grosshans, and A. Acín, Phys. Rev. Lett. 97, 190502 (2006).
[11] R. Renner and J. I. Cirac, Phys. Rev. Lett. 102, 110504 (2009).
[12] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, Phys. Rev. Lett. 110, 030502 (2013).
[13] A. Leverrier Phys. Rev. Lett. 118, 200501 (2017).
[14] A. Leverrier, Phys. Rev. Lett. 114, 070501 (2015).
[15] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photon. 7, 378 (2013).
[16] D. Huang, P. Huang, H. Li, T. Wang, Y. Zhou, and G. Zeng, Opt. Lett. 41, 3511 (2016).
[17] D. Huang, P. Huang, D. Lin, and G. Zeng, Sci. Rep. 6, 19201 (2016).
[18] G. Brassard, N. Lutkenhaus, T. Mor and B. C. Sanders, Phys. Rev. Lett. 85, 1330 (2000).
[19] R. Filip, Phys. Rev. A 77, 022310 (2008).
[20] Z. L. Yuan, J. F. Dynes and A. J. Shields, Nat. Photon. 4, 800-801 (2010).
[21] X. C. Ma, S. H. Sun, M. S. Jiang, and L. M. Liang, Phys. Rev. A 87, 062339 (2013).
[22] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, Phys. Rev. A 87, 062313 (2013).
[23] X. C. Ma, S. H. Sun, M. S. Jiang, and L. M. Liang, Phys. Rev. A 87, 052309 (2013).
[24] H. Qin, R. Kumar, and R. Alléaume, Phys. Rev. A 94, 012325 (2016).
[25] X.-C. Ma, S.-H. Sun, M.-S. Jiang, M. Gui, and L.-M. Liang, Phys. Rev. A 89, 042335 (2014).
[26] Z. Li, Y.-C. Zhang, F. Xu, X. Peng, and H. Guo, Phys. Rev. A 89, 052301 (2014).
[27] Y. C. Zhang, Z. Li, S. Yu, W. Gu, X. Peng, and H. Guo, Phys. Rev. A 89, 052325 (2014).
[28] S. Pirandola, C. Ottaviani, G. Spedalieri, et al, Nat. Photon. 9, 397-402 (2015).
[29] C. Ottaviani, G. Spedalieri, S. Braunstein, and S. Pirandola, Phys. Rev. A 91, 022320 (2015).
[30] X. Zhang, Y. Zhang, Y. Zhao, X. Wang, S. Yu, and H. Guo, Phys. Rev. A 96, 042334 (2017).
[31] P. Papanastasiou, C. Ottaviani, and S. Pirandola, Phys. Rev. A 96, 042332 (2017).
[32] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, Phys. Rev. A 97, 052327 (2018).
[33] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, Phys. Rev. Lett. 120, 220505 (2018).
[34] Z. Chen, Y. Zhang, G. Wang, Z. Li, and H. Guo, Phys. Rev. A 98, 012314 (2018).
[35] Y. Zhao, Y. Zhang, B. Xu, S. Yu, and H. Guo, Phys. Rev. A 97, 042328 (2018).
[36] H. Ma, P. Huang, D. Bai, S. Wang, W. Bao, and G. Zeng, Phys. Rev. A 97, 042329 (2018).
[37] T. Richardson M. Shokrollahi, and R. Urbanke, IEEE Trans. Inf. Theory 47, 619 (2001).
[38] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Phys. Rev. A 84, 062317 (2011).
[39] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, Phys. Rev. A 77, 042325 (2011).
[40] A. Leverrier and P. Grangier, Phys. Rev. Lett. 102, 180504 (2009).
[41] A. Leverrier and P. Grangier, Phys. Rev. A 83, 042312 (2011).
[42] J. Yang, B. Xu, X. Peng, and H. Guo, Phys. Rev. A 85, 052302 (2012).
[43] Z. Li, Y. Zhang, and H. Guo, arXiv:1805.04249
[44] R. E. S. Polkinghorne and T. C. Ralph, Phys. Rev. Lett. 83, 2095 (1999).
[45] P. Huang, J. Fang, and G. Zeng, Phys. Rev. A 89, 042330 (2014).
[46] R. García-Patrón, and N. J. Cerf, Phys. Rev. Lett. 97, 190503 (2006).
[47] S. Pirandola, New J. Phys. 15, 113046 (2013).
[48] A. S. Holevo, Probl. Inf. Transm. 9, 177 (1973).
[49] R. García-Patrón, Ph.D. thesis, Universite Libre de Bruxelles, 2007.