

Optimization and Performance Analysis of 16-APSK constellations for discrete modulation CV-QKD

Seonguk Kim
School of Electrical Engineering
Korea University
Seoul, Korea
djm06145@korea.ac.kr

Jun Heo
School of Electrical Engineering
Korea University
Seoul, Korea
junheo@korea.ac.kr

Abstract—This paper proposes a 16-APSK constellation optimization method for discrete modulated CV-QKD. The method adjusts the ring spacing and ring probability of a two-ring constellation. As a result, it improves the finite-size secret key rate compared with conventional fixed APSK structures. Fidelity between the discrete and Gaussian average states is also used as an analysis metric. This metric provides a clearer structural interpretation of the secret key rate trend than the correlation parameter alone.

Keywords—QKD, CV-QKD, discrete modulation, secret key rate, constellation, fidelity

I. INTRODUCTION

Quantum key distribution (QKD) is a technology that distributes a secret key between two users based on the measurement disturbance and the no-cloning property of quantum states. In conventional data communication, information is protected by using a secret key that has already been shared. QKD aims to distribute the secret key itself in a secure way. The main performance metric in QKD is the amount of secure information unknown to an eavesdropper, which is called the secret key rate [1]–[4]. This paper focuses on continuous variable quantum key distribution (CV-QKD).

QKD can be divided into discrete variable QKD (DV-QKD) and continuous variable QKD (CV-QKD), depending on how the quantum states are represented. DV-QKD uses discrete quantum states such as polarization, phase, or time bin states, and it usually requires single photon detectors. On the other hand, CV-QKD modulates the quadrature components of coherent states and measures them by using homodyne or heterodyne detection. Since CV-QKD can be implemented with coherent detection, it has good compatibility with conventional optical communication systems and can use high speed optical components. For this reason, CV-QKD has been actively studied as a QKD scheme that can be connected to practical optical communication infrastructure [5], [6].

The standard modulation scheme in CV-QKD is Gaussian modulation. Gaussian modulation uses continuous

constellation points and a Gaussian probability distribution, so it can provide a high theoretical secret key rate and has a well established security analysis. However, in practical systems, it is difficult to generate infinitely many constellation points with perfect accuracy and reconciliation can become complicated in a low signal to noise ratio (SNR) regime. To reduce these limitations, Discrete modulation (non-Gaussian) CV-QKD has been studied. Discrete modulation uses a finite number of constellation points, which can make implementation simpler. However, due to the finite use of constellation points, its performance is inferior to Gaussian modulation [7]–[11].

The goal of this study is to improve the secret key rate of Discrete modulation CV-QKD by designing a finite constellation that becomes closer to Gaussian modulation. This paper considers only the 16-APSK (4+12) structure as a representative low order APSK constellation. A low order discrete modulation structure is relatively simple to implement and preserves the practical advantage of discrete modulation. It has a larger difference from Gaussian modulation, so there is more possibility for performance improvement through constellation shaping. The main contributions of this paper are summarized as follows. First, we jointly optimize the inner-ring radius ratio and inner ring probability of the 16-APSK constellation under a finite-size CV-QKD setting. Second, we compare the optimized constellation with conventional uniform and binomial APSK structures in terms of the secret key rate and maximum transmission distance. Third, we use the fidelity between the discrete and Gaussian average modulation states as an additional structural indicator to interpret the performance improvement beyond the correlation parameter alone.

II. PRELIMINARY

A. CV-QKD secret key rate

The secret key rate of CV-QKD is evaluated from the Devetak–Winter bound [12]:

$$K = I(A:B) - \chi(B:E) \quad (1)$$

where $I(A:B)$ is the mutual information between Alice and Bob and $\chi(B:E)$ is the Holevo information between Bob and Eve. The Holevo information gives an upper bound on Eve's accessible information from Bob's data. Thus, the secret key

This work was supported in part by the Institute of Information & Communications Technology Planning & Evaluation (IITP)-ITRC (Information Technology Research Center) grant funded by the Korea government (MSIT) (IITP-2026-RS-2021-II211810, 50%) and in part by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. RS-2023-00242396, 50%).

rate represents the amount of secure information that can be extracted between Alice and Bob.

Since practical information reconciliation is not perfectly efficient, the reconciliation efficiency β is included in the mutual information term. In this work, we use the finite-size secret key rate [7], [8], [13]:

$$K = \frac{m}{N}(\beta I_{BA} - \chi_{BE} - \Delta m) \quad (2)$$

where N is the total number of transmitted quantum states and m is the number of data used for information reconciliation. The parameter Δm is the finite-size correction term associated with privacy amplification. In the finite-size regime, the channel parameters are estimated from a limited number of samples. It assumes a normal linear channel model between Alice's and Bob's data $y_{Bob} = tx_{Alice} + z$, where t is related to the channel transmittance and z is a zero-mean Gaussian noise term. The noise variance includes the effect of excess noise and receiver thermal noise. Due to the finite number of samples, the estimated channel parameters have statistical uncertainty. Therefore, the secret key rate is calculated using worst case parameters within the confidence interval, namely the lower bound of the transmittance and the upper bound of the excess noise.

B. Parameter Z^* and Constellation

A key parameter in the secret key rate calculation is the correlation parameter Z^* , which describes the correlation between Alice and Bob in the covariance matrix. Since the Holevo information χ_{BE} is calculated from the covariance matrix, Z^* directly affects the final secret key rate. Following [8], Z^* is given by:

$$Z^*(T, \xi, \tau) = 2\sqrt{T} \text{Tr} \left(\tau^{\frac{1}{2}} \hat{a} \tau^{\frac{1}{2}} \hat{a}^\dagger \right) - \sqrt{2T\xi w} \quad (3)$$

$$w = \sum_k p_k (\langle \alpha_k | \hat{a}_\tau^\dagger \hat{a}_\tau | \alpha_k \rangle - |\langle \alpha_k | \hat{a}_\tau | \alpha_k \rangle|^2) \quad (4)$$

where $\hat{a}_\tau = \tau^{1/2} \hat{a} \tau^{-1/2}$. The average modulation state is defined as:

$$\tau = \sum_k p_k |\alpha_k\rangle \langle \alpha_k| \quad (5)$$

p_k is the probability of the k -th constellation point and $|\alpha_k\rangle$ is the corresponding coherent state. Thus, τ represents the average state of the modulation, which includes both the constellation points and their probabilities. The operators $\hat{a}$ and $\hat{a}^\dagger$ are the annihilation and creation operators.

Although Z^* is useful for evaluating the performance of a modulation format, it does not reflect only the constellation structure. It is also affected by channel parameters such as the transmittance T and the excess noise ξ . Therefore, an improvement in Z^* cannot be interpreted only as a structural improvement of the constellation. To analyze the effect of the constellation structure more directly, this work also considers the average modulation state τ .

III. METHOD AND ANALYSIS

Previous work showed that binomial probabilistic shaping can improve the secret key rate of APSK based CV-QKD [7]. However, in that study, the APSK constellation was used with a fixed equally spaced ring structure and only limited probability distributions, such as uniform and binomial distributions. In addition, the performance improvement was mainly analyzed using the correlation parameter Z^* . However, since Z^* is affected not only by the constellation structure but also by channel parameters such as transmittance and excess noise, it is difficult to isolate the effect of the constellation structure itself.

Based on this observation, this work investigates the possibility of further optimization of the ring radius and ring probability in the 16-APSK (4+12) constellation. In addition, to analyze the structural change caused by the optimization, we use the fidelity between average modulation states and examine the relationship between the structural change and the improvement in the secret key rate.

A. Ring Radius and Probability Optimization

In this work, we optimize the ring radius and ring probability of the 16-APSK (4+12) constellation. The 16-APSK (4+12) constellation has a two ring structure, where four constellation points are placed on the inner ring and twelve constellation points are placed on the outer ring. The ring probabilities and radius ratios are defined as follows:

$$P_{\text{in}} = p, P_{\text{out}} = 1 - p \quad (6)$$

$$R_{\text{in}} = r, R_{\text{out}} = 1 \quad (7)$$

Here, p denotes the total probability assigned to the inner ring and r denotes the relative radius ratio of the inner ring with respect to the outer ring. The constellation points within each ring are assumed to have equal probability. In practice, the target ring probability can be generated digitally using distribution matching before applying the corresponding amplitude and phase sequence to an I/Q modulator.

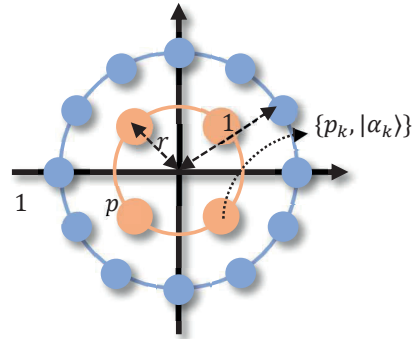


Fig. 1. 16-APSK (4+12) constellation

In CV-QKD, the modulation variance V_A is generally optimized for each transmission distance to maximize the secret key rate. The modulation variance is related to the mean photon number $\langle n \rangle$ as:

$$V_A = 2\langle n \rangle \quad (8)$$

$$\langle n \rangle = \sum_{k=0}^{15} p_k |\alpha_k|^2 \quad (9)$$

The parameter V_A determines the overall average energy of the constellation. In conventional CV-QKD analysis, V_A is optimized for each transmission distance. As V_A increases, the mutual information between Alice and Bob I_{AB} increases and the Holevo information of Eve χ_{BE} also increases. Therefore, the secret key rate is not a monotonically increasing function of V_A . It increases to an optimal modulation variance and then decreases beyond that point.

In this work, we extend this optimization from V_A to the ring radius ratio r and the ring probability p . To this end, r and p are swept from 0 to 1 with a step size of 0.03. For each transmission distance, we search for the combination (V_A, r, p) that maximizes the secret key rate. The optimization procedure is performed by evaluating the finite size secret key rate for all candidate combinations of V_A , r , and p . For each pair of r and p , the modulation variance V_A is swept to find the maximum key rate. The final optimized structure at each distance is selected as the parameter set that gives the largest secret key rate among all candidates. Since the dependence of the secret key rate on V_A , r , and p is not known a priori, a grid search is used to examine the overall performance landscape over the considered parameter ranges. This procedure allows geometrical and probabilistic shaping to be evaluated simultaneously. The total number of candidate evaluations is given by the product of the numbers of grid points for V_A , r , and p , i.e., N_{V_A}, N_r, N_p , and is computationally manageable for the present two ring optimization. For higher order constellations, the increased search complexity can be reduced using coarse-to-fine searches or more efficient optimization algorithms.

B. Fidelity

To analyze the effect of constellation structure changes more directly, we compare the average modulation state τ . The average state τ , defined in Eq. (5), is determined by the constellation points $|\alpha_k\rangle$ and their probabilities p_k . Therefore, it does not directly include channel parameters such as the transmittance T or excess noise ξ . By comparing the average modulation states, the structural effect caused by changes in the ring radius and ring probability can be separately analyzed.

In CV-QKD, Gaussian modulation is used as a reference modulation scheme that theoretically provides a high secret key rate. Therefore, in this work, we compare how similar the average state of the discrete modulation is to that of Gaussian modulation before and after optimization. For this comparison, we use fidelity, which measures the similarity between quantum states or density matrices. Fidelity is defined as:

$$F(\rho, \sigma) = \left(\text{Tr} \sqrt{\sqrt{\rho} \sigma \sqrt{\rho}} \right)^2 \quad (10)$$

ρ and σ denote the two density matrices to be compared. The fidelity value ranges from 0 to 1. It approaches 1 when the two density matrices are identical, and approaches 0 when they are highly distinguishable.

In this work, we set ρ as the average state of Gaussian modulation τ_G and σ as the average state of discrete modulation τ_D . The average state of Gaussian modulation is represented as a thermal state and is given by:

$$\tau_G = \frac{1}{1 + \langle n \rangle} \sum_{m=0}^{\infty} \left(\frac{\langle n \rangle}{1 + \langle n \rangle} \right)^m |m\rangle \langle m| \quad (11)$$

A higher fidelity between τ_D and τ_G indicates that the discrete constellation forms an average state closer to Gaussian modulation. Therefore, we compare the fidelity before and after optimization to analyze the structural change caused by ring radius and ring probability optimization and to examine how this change is related to the improvement in the secret key rate.

C. Results

In this work, we compare the 16-APSK (4+12) constellation using the same secret key rate calculation parameters as in [7]. The comparison includes the uniform distribution, the binomial distribution, and the proposed r, p optimized structure. For the uniform distribution, the same probability is assigned to each ring, and the probability of the q -th ring is given by:

$$P_q = \frac{1}{R}, q = 1, \dots, R \quad (12)$$

For the binomial distribution, the probability assigned to the q -th ring is defined as:

$$P_q = \frac{2}{2^{2R-1}} \binom{2R-1}{q-1}, q = 1, \dots, R \quad (13)$$

R is the total number of rings and q denotes the ring index from the outer ring to the inner ring. Since the 16-APSK (4+12) constellation has a two ring structure, the probabilities of the inner and outer rings are set to 0.5 and 0.5 respectively for the uniform distribution. For the binomial distribution, the probabilities of the inner and outer rings are set to 0.75 and 0.25 respectively. The constellation points within each ring equally share the probability assigned to that ring.

In the proposed r, p optimized structure, the inner ring probability p and the inner ring radius ratio r are treated as optimization variables. For each transmission distance, we search for the combination (V_A, r, p) that maximizes the secret key rate. Based on this optimal combination, we compare the fidelity, Z^* , the optimal modulation variance V_A , and the secret key rate. From the optimized structures at different transmission distances, the optimal inner-ring radius ratio r remains relatively stable, while the inner-ring probability p tends to increase with transmission distance. Specifically, r remains approximately 0.42, whereas p varies from 0.57 to 0.72. In this work, 30km is selected as the representative distance because the performance difference among the structures is clearly observed, while the secret key rate has not yet entered the rapidly decreasing region. The structure parameters at 30km are summarized in Table I.

TABLE I. STRUCTURE PARAMETERS AT 30KM

Structure	Inner ring radius ratio r	Inner ring probability p
Uniform [7]	0.5	0.5
Binomial [7]	0.5	0.75
Proposed	0.42	0.69

Through the r, p sweep, the optimal (V_A, r, p) combination is obtained for each transmission distance. Table I summarizes the optimized constellation parameters at 30km. The optimized structure combines a smaller inner-ring radius with a relatively high inner-ring probability, concentrating more states in the low amplitude region while maintaining a less probable high amplitude outer ring. This radial shaping more closely resembles the characteristics of Gaussian modulation, which is consistent with the increased average state fidelity. The exact optimal values, however, depend on the system considered and channel parameters.

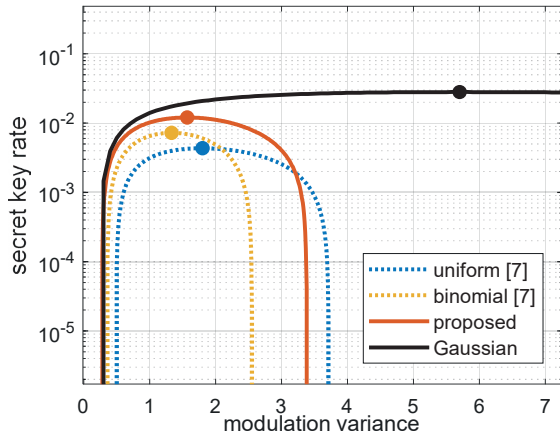


Fig. 2. Secret key rate versus modulation variance at 30km

Fig. 2 shows the secret key rate as a function of the modulation variance V_A for the structures listed in Table I. The r, p optimized structure achieves a higher maximum secret key rate than the conventional uniform and binomial structures, while maintaining a positive key rate over a comparable V_A range.

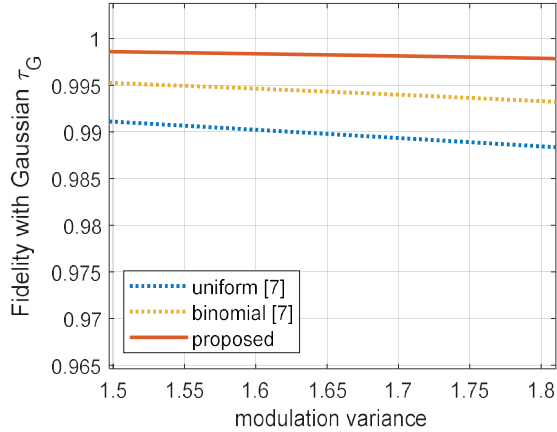
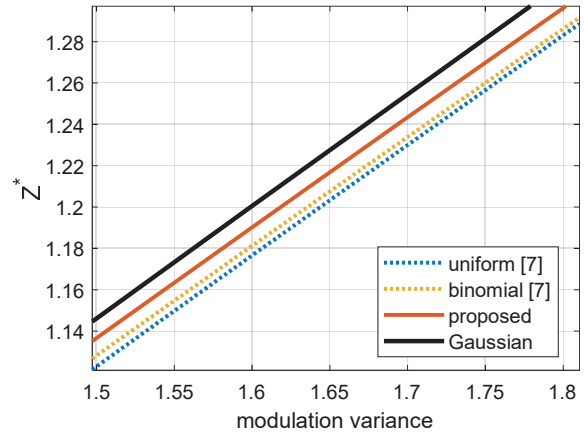


Fig. 3. Fidelity comparison at 30km

Fig. 3 shows the fidelity comparison for each structure at 30km. Since the optimal modulation variance V_A at this

distance lies in the range of 1.5 to 1.8, the structural advantage shown in Fig. 3 and Fig. 4 is analyzed within this range. The r, p optimized structure shows higher fidelity than the uniform and binomial structures, indicating that the optimized ring radius and ring probability make the average state of discrete modulation closer to that of Gaussian modulation.

Fig. 4 shows the comparison of Z^* for each structure at 30km. The r, p optimized structure shows a higher Z^* value than the uniform and binomial structures. Since Z^* represents the correlation between Alice and Bob and is directly used in the secret key rate calculation, this result indicates that the optimized constellation provides a more favorable correlation structure. This result shows a similar tendency to the fidelity comparison in Fig. 3. For the considered structures, higher fidelity is accompanied by a higher Z^* , suggesting that a constellation whose average state is closer to Gaussian modulation can provide a more favorable correlation structure.

Fig. 4. Z^* comparison at 30km

However, fidelity does not directly determine Z^* or the secret key rate and is used only as a complementary structural indicator.

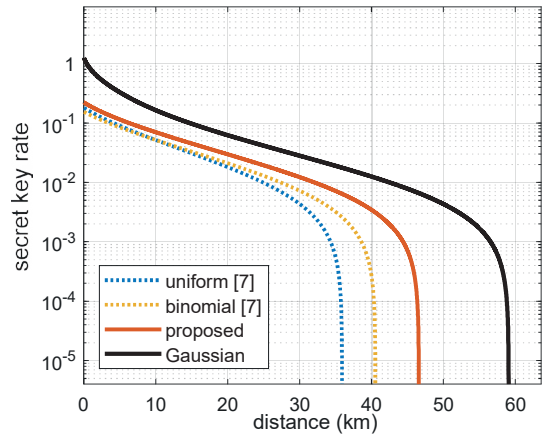


Fig. 5. Secret key rate versus transmission distance

Fig. 5 shows the secret key rate as a function of transmission distance. For the uniform and binomial structures, V_A is optimized at each distance, while V_A, r and p are jointly optimized for the proposed structure. The r, p optimized structure maintains a positive secret key rate over a longer

transmission distance than the uniform and binomial structures. This result shows that the joint optimization of the ring radius and ring probability improves not only the secret key rate at a fixed distance but also the maximum achievable transmission distance.

In addition, the results in Fig. 3 - Fig. 5 show a consistent tendency. The structures with higher fidelity also exhibit larger Z^* , higher secret key rates, and longer transmission distances. This consistent tendency suggests that fidelity can be used as a complementary structural indicator for interpreting performance improvement. Therefore, fidelity can be used as a structural indicator for interpreting the performance improvement of the proposed constellation.

TABLE II. MAXIMUM TRANSMISSION DISTANCE

Structure	Max distance [km]	V_A	r	p
Uniform [7]	35.90	1.6	0.5	0.5
Binomial [7]	40.54	1.2	0.5	0.75
Proposed	46.59	1.3	0.42	0.72

Table II summarizes the maximum transmission distance and the corresponding parameter set for each structure. The uniform structure maintains a positive secret key rate up to 35.90 km, while the binomial structure reaches 40.54 km. In contrast, the proposed r, p optimized structure maintains a positive secret key rate up to 46.59 km.

Compared with the uniform structure, the proposed structure extends the maximum transmission distance by 10.69 km, corresponding to a 29.78% improvement. In addition, compared with the binomial structure used in [7], the maximum transmission distance is increased by 6.05 km, corresponding to a 14.92% improvement. These results show that the joint optimization of the ring radius and ring probability effectively improves the transmission distance performance of the 16-APSK (4+12) constellation. The improvement over the binomial structure is particularly important because the binomial distribution already provides probabilistic shaping with a fixed ring geometry. Therefore, the additional gain of the proposed structure indicates that probability shaping alone is not sufficient to fully exploit the performance potential of the APSK constellation. By jointly adjusting the ring spacing and the ring probability, the proposed method changes both the geometrical distribution of coherent states and their statistical weights. This combined effect leads to a constellation structure that is more favorable for finite-size secret key generation.

IV. CONCLUSION

In this work, we proposed a method to improve the secret key rate of discrete-modulated CV-QKD by adjusting the ring radius and ring probability of the constellation. Specifically, we considered the 16-APSK (4+12) constellation and used the equally spaced ring structure with uniform and binomial probability distributions in [7] as reference structures. The inner-ring radius ratio r and inner ring probability p were swept to find the constellation structure that maximizes the secret key rate at each transmission distance.

In previous work, the structural advantage was mainly analyzed using the correlation parameter Z^* . However, Z^* includes not only the effect of the constellation structure but also the effects of channel parameters such as

transmittance and excess noise. Therefore, in this work, we additionally used the fidelity between average modulation states to examine whether the optimized discrete modulation becomes closer to the average state of ideal Gaussian modulation.

The results show that the proposed r, p optimized structure achieves higher fidelity and a larger Z^* than the uniform and binomial structures and this tendency lead to an improvement in the secret key rate. In terms of the maximum transmission distance, the proposed structure extends the achievable distance by 6.05 km compared with the binomial structure used in [7], corresponding to a 14.92% improvement. These results indicate that fidelity can be used as a useful auxiliary indicator for interpreting the structural change of discrete constellations.

For future work, a finer r, p sweep can be considered to examine the possibility of further performance improvement. However, based on the observed trend, the additional gain is expected to be limited. Although this work focuses on 16-APSK (4+12), the proposed framework can be extended to higher-order multi-ring constellations by jointly optimizing multiple ring radius and probabilities. Future work will investigate its application to 32-APSK and 64-APSK. The reconciliation efficiency β is fixed in this work, although changes in the probability distribution, ring spacing, and modulation variance may affect practical reconciliation performance. Their impact will be investigated in future work.

REFERENCES

- [1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7–11, 2014.
- [2] V. Scarani et al., "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, 2009.
- [3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, 2002.
- [4] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nat. Photon.*, vol. 8, no. 8, pp. 595–604, 2014.
- [5] S. P. Kish, P. J. Gleeson, A. Walsh, P. K. Lam, and S. M. Assad, "Comparison of discrete variable and continuous variable quantum key distribution protocols with phase noise in the thermal-loss channel," *Quantum*, vol. 8, Art. no. 1382, 2024.
- [6] S. Pirandola et al., "Advances in quantum cryptography," *Adv. Opt. Photon.*, vol. 12, no. 4, pp. 1012–1236, 2020.
- [7] M. Almeida et al., "Secret key rate of multi-ring M-APSK continuous variable quantum key distribution," *Opt. Express*, vol. 29, no. 23, pp. 38669–38682, 2021.
- [8] A. Denys, P. Brown, and A. Leverrier, "Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation," *Quantum*, vol. 5, Art. no. 540, 2021.
- [9] C. Weedbrook et al., "Gaussian quantum information," *Rev. Mod. Phys.*, vol. 84, no. 2, pp. 621–669, 2012.
- [10] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, no. 5, Art. no. 057902, 2002.
- [11] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, "Asymptotic security of continuous-variable quantum key distribution with a discrete modulation," *Phys. Rev. X*, vol. 9, no. 2, Art. no. 021059, 2019.
- [12] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," *Proc. R. Soc. A, Math. Phys. Eng. Sci.*, vol. 461, no. 2053, pp. 207–235, 2005.
- [13] A. Leverrier, F. Grosshans, and P. Grangier, "Finite-size analysis of a continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 81, no. 6, Art. no. 062343, 2010.