Parameters Optimization of Decoy-State Phase-Matching Quantum Key Distribution Based on the Nature-Inspired Algorithms

Chang Liu(刘畅), Yue Li(李悦), Haoyang Wang(王浩洋), Kaiyi Shi(石开毅), Duo Ma(马铎), Yujia Zhang(张育嘉) and Haiqiang Ma(马海强)*

State Key Laboratory of Information Photonics and Optical Communications, School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China

(Received 14 September 2024; accepted manuscript online 9 December 2024)

Phase-matching quantum-key distribution (PM-QKD) has achieved significant results in various practical applications. However, real-time communication requires dynamic adjustment and optimization of key parameters during communication. In this letter, we predict the PM-QKD parameters using nature-inspired algorithms (NIAs). The results are obtained from an exhaustive traversal algorithm (ETA), which serves as a benchmark. We mainly study the parameter optimization effects of the two NIAs: ant colony optimization (ACO) and the genetic algorithm (GA). The configuration of the inherent parameters of these algorithms in the decoy-state PM-QKD is also discussed. The simulation results indicate that the parameters obtained by the ACO exhibit superior convergence and stability, whereas the GA results are relatively scattered. Nevertheless, more than 97% of the key rates predicted by both algorithms are highly consistent with the optimal key rate. Moreover, the relative error of the key rates remained below 10%. Furthermore, NIAs maintain power consumption below 8 W and require three orders of magnitude less computing time than ETA.

DOI: 10.1088/0256-307X/42/1/010301 CSTR: 32039.14.0256-307X.42.1.010301

1. Introduction. Quantum key distribution (QKD) is based on the principles of quantum mechanics,[1] which allow the unconditional and secure sharing of keys between trusted communication parties without limiting the computing power of potential eavesdroppers. The BB84-QKD protocol lays the foundation for the development of QKD.[2] Various protocols have been proposed over the past 40 years. Among them, the decoy-state-QKD protocol addresses the problem of multiphoton security vulnerability at the source side in practical QKD systems.[3] The measurement-device-independent QKD (MDI-QKD) protocol is designed to withstand all attacks against the detector side,[4,5] such as time-shift attacks,[6,7] faked states attacks,[8,9] and detector blinding attacks.[10,11] However, all these protocols share a common challenge: the key rate cannot exceed the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound without the use of a quantum repeater.[12,13] The twin-field QKD (TF-QKD) protocol, proposed by Lucamarini *et al.*, addresses this limitation.[14] Based on the principle of single-photon interference, the security key rate of TF-QKD is proportional to the square root of the transmittance of the channel. This feature is particularly critical in long-distance communication scenarios, significantly extending the effective coding distance and demonstrating significant advantages over traditional MDI-QKD. However, a later announcement of the phase information in TF-QKD causes security loopholes, and many variants of TF-QKD have been proposed to close these loopholes. Among them, decoy-state phase-matching QKD (PM-QKD) offers a quadratic improvement in the key rate without requiring basic selection. It eliminates the requirement for phase locking or pre-phase feedback, thereby obviating the need for a phase post-compensation technique.[15]

With the deepening of QKD theory research, its practical application has made remarkable progress, including constructing large-scale intercity QKD networks and realizing space-to-ground integrated QKD systems.[16–21] Nevertheless, the deployment of decoy-state PM-QKD in practical settings inevitably confronts multifaceted challenges such as encompassing electromagnetic interference,[22] light source defects,[23] and environmental noise[24]. These factors directly affect the key rate of the decoy-state PM-QKD, which may endanger the security and efficiency of communication. To address these challenges, optimizing the parameter settings of the decoy-state PM-QKD protocol is crucial to reducing the impact of external interference on system performance through precise adjustments. Traditionally, parameter optimization has adopted exhaustive traversal algorithms (ETA) and local search algorithms (LSA).[25] Although these methods can obtain the optimal parameter values, their optimization process is time-consuming and fails to meet the high real-time demands of modern communication systems. Therefore, exploring and developing more efficient and fast parameter optimization algorithms is necessary to ensure that the decoy-state PM-QKD system can maintain stable performance and efficient security key generation ability in various application

*Corresponding author. Email: hqma@bupt.edu.cn

scenarios.

Nature-inspired algorithms (NIAs) are a class of algorithms designed to draw inspiration from natural biological phenomena and patterns.[26,27] These algorithms embody the survival strategies, group behaviors, and evolutionary mechanisms of organisms in nature. They are known for their adaptive distributed computation and powerful global search capabilities. Over the past few decades, NIAs such as ant colony optimization (ACO) and genetic algorithm (GA),[28–31] have been widely applied to solve the problem of optimal parameter setting.[32–34] These algorithms can efficiently explore the entire solution space with a certain probability within a specified range, ultimately identifying the optimal solution owing to their inherent characteristics. Importantly, these approaches do not alter the fundamental principles or underlying logic of QKD protocols, making them suitable for various QKD protocols, including subsequent variants of TF-QKD and MP-QKD.[4,35–38]

In this letter, we study the effects of ACO and GA on parameter optimization in decoy-state PM-QKD. ACO is commonly used to solve the traveling salesman problem (TSP),[39] with its pheromone renewal strategy typically associated with the distances between cities. In QKD parameter optimization, we consider the key rate to be a crucial metric in the pheromone update strategy. To comprehensively evaluate the performance of these two algorithms in decoy-state PM-QKD parameter optimization, we conduct a comparative analysis of three key dimensions: the accuracy of the parameter prediction, size of the relative error value of the key rate, and computational cost. The results show that both NIAs perform well across all three categories. Moreover, the parameters predicted by the ACO demonstrate greater accuracy.

2. Decoy-State PM-QKD. Alice and Bob each generate a coherent state $|\sqrt{s}e^{i(\phi_{\mathrm{A(B)}}+\pi\kappa_{\mathrm{A(B)}})}\rangle_{\mathrm{A(B)}}$, where $\kappa_{\mathrm{A(B)}}$ denotes the random key, $\phi_{\mathrm{A(B)}}$ denotes the random phase, and $s\in\{\mu,\nu,\omega\}$ denotes the random intensity (μ,ν,ω represent the signal state, decoy state, and vacuum state, respectively). Alice and Bob then send the modulated pulses to an untrusted third party, Eve, who conducts the interferometry and records the responses from the detectors. After Eve announces the detection results, Alice and Bob announce the phase slice index where the random phase is located and sift the key based on Eve's published detection success events (noticing that only one of the two detectors responded). Finally, a secure key is extracted from the filtered bits through key extraction, parameter estimation, and postprocessing.

Using Gottesman, Lo, Lütkenhaus and Preskill (GLLP) theory,[40] the gain obtained is as follows:

$$Q_s = 1 - e^{-s\eta_{\mathrm{d}}\eta} + 2P_{\mathrm{dc}}e^{-s\eta_{\mathrm{d}}\eta},\ s\in\{\mu,\nu,\omega\}, \tag{1}$$

where P_{dc} denotes the dark count rate, η_{d} denotes the detection efficiency of the detector and $\eta = 10^{-\alpha L/20}$ with α and L denoting the fiber loss factor and transmission distance, respectively.

The quantum bit error rate (QBER) in the Z basis is as follows:

$$E_s^Z = \frac{(P_{\mathrm{dc}} + s\eta_{\mathrm{d}}\eta e_\delta)e^{-s\eta_{\mathrm{d}}\eta}}{Q_s}, \tag{2}$$

where e_δ denotes the misalignment error rate.

The phase-error rate is[41]

$$E_\mu^X = q_1 e_1^Z + q_0 + e_0^Z + (1 - q_0 - q_1), \tag{3}$$

where q_k represents the ratio of the $k$photon signal to fully detected signal, and e_k^Z represents the quantum bit error rate of the k-photon signal.

In Eq. (3), the upper bound of the single-photon signal error is as follows:

$$e_1^Z = \frac{E_\nu^Z Q_\nu e^\nu - E_\omega^Z Q_\omega e^\omega}{(\nu-\omega)Y_1}, \tag{4}$$

where Y_1 denotes the single-photon yield.

The key rate of decoy-state PM-QKD in the asymptotic scenario is:

$$R = \frac{2}{M}Q_\mu[1 - fH(E_\mu^Z) - H(E_\mu^X)], \tag{5}$$

where M denotes the number of slices, f denotes the error correction efficiency, and $H(x)$ denotes the binary entropy, expressed as $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$.

From the above analysis, it is evident that inherent statistical fluctuations in the observed values must be considered when employing decoy state analysis to estimate the contribution of a single photon. Consequently, selecting an appropriate strength value to optimize key rate generation is essential. Here, we mainly optimize μ and ν, which are constrained to lie within the range of [0.01, 1], under the condition that $\mu > \nu$ and $\omega = 0$. Subsequently, ACO and GA are employed to search for the optimal solution within this range using their respective computational techniques. The principles underlying these methods are as follows.

3. ACO and GA. ACO, a metaheuristic algorithm inspired by the foraging behavior of ants, has demonstrated remarkable effectiveness in solving complex optimization problems. This fundamental concept is based on the efficient collective intelligence exhibited by ants when locating food sources. Particularly the route selection mechanisms and information transmission through releasing and detecting pheromones. Australian scholars Marco Dorigo *et al.* proposed an ACO algorithm based precisely on the foraging behavior of ants.[29] Subsequently, the ant cycle, quantity, and density systems were derived according to the characteristics of releasing pheromones $\Delta\tau$, among which the most commonly used is the ant cycle system. Now, we utilize the concept of the ant cycle system (i.e., ants release pheromones after only one cycle) and combine it with the characteristics of the decoy-state PM-QKD protocol to obtain $\Delta\tau = R_{\mathrm{TF-QKD}}$. The specific solution process for ACO is shown in Fig. 1. The key steps of the ACO are as follows:

(1) Updated pheromone concentrations

$$\tau_i(\mathrm{iter}+1) = \tau_i(\mathrm{iter}) \times (1-\rho) + \Delta\tau_i(\mathrm{iter}), \tag{6}$$

where the subscript i represents the ith ant, and iter denotes the number of iterations; τ denotes the pheromone concentration correspondingly; ρ denotes the pheromone

volatilization factor; $\Delta\tau$ is the value of the fitness function, which is denoted as $R_{\mathrm{TF-QKD}}$.

(2) State transfer probability

$$P_i(\mathrm{iter}) = (\tau_{\mathrm{best}}(\mathrm{iter}) - \tau_i(\mathrm{iter}))/\tau_{\mathrm{best}}(\mathrm{iter}), \tag{7}$$

where P denotes the state transfer probability and τ_{best} denotes the maximum pheromone concentration.

$$X_i(\mathrm{iter}+1) = \begin{cases} X_i(\mathrm{iter}) + (2\times\mathrm{rand}-1)/\max\_\mathrm{iter} & P_i(\mathrm{iter}) < P_0, \\ X_i(\mathrm{iter}) + (\mathrm{Up}-\mathrm{Low})\times(\mathrm{rand}-0.5) & P_i(\mathrm{iter}) > P_0, \end{cases} \tag{8}$$

where X indicates the positional coordinates of the ant, rand denotes a pseudo-random number between 0 and 1, Up and Low are the upper and lower bounds of the ant's coordinates, respectively, and P_0 denotes the transfer probability constant.

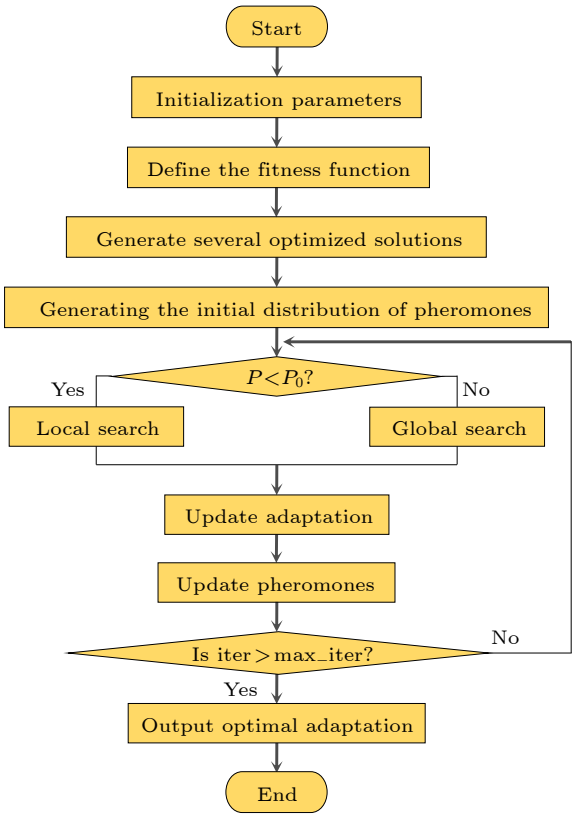

Fig. 1. Flowchart of the ACO.

Concurrently, we combine the GA with decoy-state PM-QKD to study its optimization performance. The following is a brief introduction to this principle. John Holland originally proposed the GA as a heuristic solution search or optimization technique based on the natural selection of Darwin's biological evolution theory and the biological evolution process of genetic mechanisms.[31] Holland's schema theorem and the related building block hypothesis provide the theoretical and conceptual foundation for the design of an efficient GA. In GA, each solution instance is regarded as an "individual", and the entire solution space forms a "population". Each individual is represented by a "chromosome", in which binary numbers typically represent the information on the chromosome. Then, a fitness-based selection and recombination process is performed to generate a subsequent population, that is, the next generation. As the population iterates, fitness continuously improves until the optimal solution is reached. Its core steps include selection, crossover [as shown in Fig. 2(a)], and mutation [as shown in Fig. 2(b)].[31]

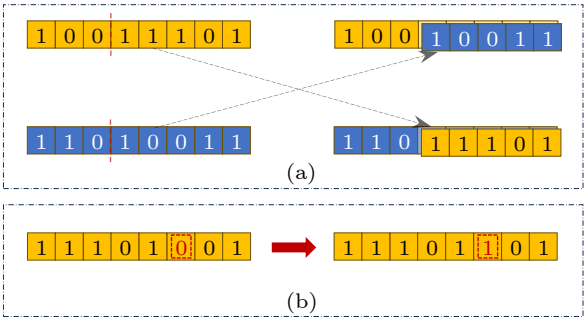

Fig. 2. Crossover and mutation processes of GA. (a) Single-point crossover process. According to a certain crossover probability, two-parent individuals select a crossover point on their chromosomes. Subsequently, they produce two new offspring by exchanging gene segments. (b) Mutation process. Certain individual loci with a specific probability of mutation are selected. Subsequently, the values of these loci are altered, which may involve changes in the locus value from 0 to 1 or from 1 to 0.

4. Numerical Simulation. Considering the impact of the algorithm's internal parameters on the computational performance, we analyzed the simulation results under different parameter combinations and selected the optimal internal parameter configuration accordingly. In this study, we regarded the prediction results obtained by the ETA as the optimal values. We selected 145,800 data sets with channel distances within 600 km to carefully study the parameters listed in Table 1. Simultaneously, the standard deviations of μ and ν were calculated for each parameter combination, which were used as indicators to evaluate the proximity between the predicted and optimal results.

The data analysis shows that after selecting the parameter s_1 in the ACO, the maximum difference in the standard deviation across various combinations of ρ and P_0 is 0.0027. This finding underscores the high robustness of the ACO with respect to ρ and P_0. However, as s_1 increased, the standard deviation decreased, whereas the running time increased significantly. By contrast, the GA was less sensitive to the parameters s_2 and P_{c}, yielding satisfactory results when $s_2 \geqslant 20$. Specifically, when P_{c} and P_{m} are fixed, increasing s_2 from 20 to 300 decreased the standard deviation by only 8.2%. It is important to note that the GA is highly sensitive to variations in the parameter P_{m}, and reducing the probability of variation can significantly enhance the accuracy of the results. Therefore, after considering key factors such as running time, power consumption, and accuracy, we opted for a trade-off, sacrificing accuracy to optimize the overall performance. The selected parameters are presented in Table 2.

Table 1. The inherent parameters and the test range. s_1, ρ, and P_0 represent the population number, pheromone volatilization factor, and the ACO transfer probability constant, respectively. s_2, P_c, and P_m represent the population size, crossover probability, and mutation probability of the GA, respectively.

Inherent parameters	s_1	ρ	P_0	s_2	P_c	P_m
Test range	[10, 300]	[0.1, 0.9]	[0.1, 0.9]	[10, 300]	[0.1, 0.9]	[0.1, 0.9]

Table 2. Inherent parameters of ACO and GA.

Inherent parameters	s_1	ρ	P_0	s_2	P_c	P_m
Value	70	0.8	0.2	20	0.8	0.1

Table 3. Simulation parameters.

Parameters	f	M	α	P_{dc}	η_d
Value	1.15	16	0.2	8×10^{-8}	0.145

Table 4. Comparison of the computational cost by ACO, GA, and ETA.

	Time (s)	CPU (%)	Power consumption (W)
ACO	32.54	10%	< 8
GA	34.11	10%	< 8
ETA	13835.93	11%	1000

After selecting the inherent parameters of the algorithms, we predicted the decoy-state PM-QKD parameters. The decoy-state PM-QKD system parameters are listed in Table 3. Initially, we compared the computational costs of the three algorithms (CPU: 13th Gen Intel(R) Core(TM) i7-13700 @ 2.10 GHz; RAM: 16.0 GB), as shown in Table 4. NIAs take approximately 33 s, which is three orders of magnitude shorter than the ETA. In addition, NIAs consume less power, allowing them to save on electricity costs in the long run.

Figure 3 shows the prediction performance of ACO and the GA for parameter μ under different distance conditions. The results indicate that the predicted values generated by ACO were closely aligned with the optimal predicted values. In addition, the data points are tightly clustered around the optimal value, demonstrating high consistency and accuracy. In contrast, although the predicted values from the GA also exhibited a trend similar to the optimal values, some data points were widely dispersed, indicating significant variability. This discrepancy is particularly evident for longer distances. Figure 4 further highlights the prediction performance of the two algorithms for the parameter ν at different distances, revealing that the values predicted by the GA exhibit greater dispersion. In summary, ACO clearly outperformed the GA regarding parameter prediction accuracy.

Additionally, given the significance of the key rate in evaluating protocol quality, we conducted a specific analysis of the key rate calculated by these two algorithms to assess their effectiveness and impact in practical applications comprehensively. Comparing the data accuracy of the algorithms, ACO showed remarkable superiority. The experimental results are shown in Fig. 5, where 98.7% of the ACO calculation results fall within the 10% relative error range. By contrast, the GA achieved a data accuracy of 97.6%. Although its numerical results are good, the ACO clearly offers greater advantages in scenarios that demand higher accuracy.

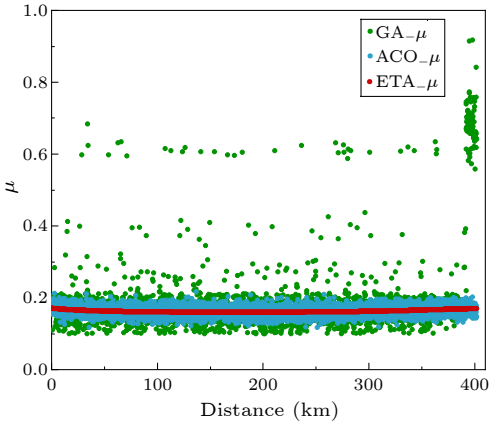

Fig. 3. Comparison of the performance of GA and ACO in predicting μ. The green and blue dots represent μ obtained by GA and ACO, respectively, whereas the red dots denote the optimal μ obtained by ETA.

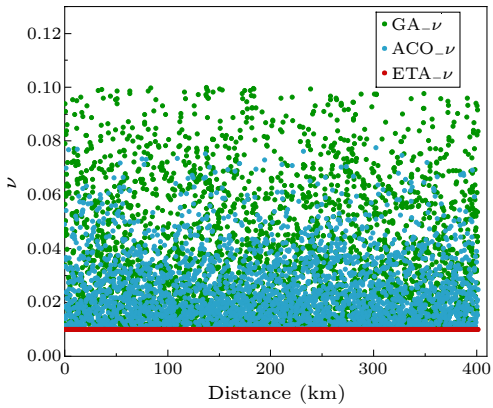

Fig. 4. Comparison of the performance of GA and ACO in predicting ν. The green and blue dots represent ν obtained by GA and ACO, respectively, whereas the red dots denote the optimal ν obtained by ETA.

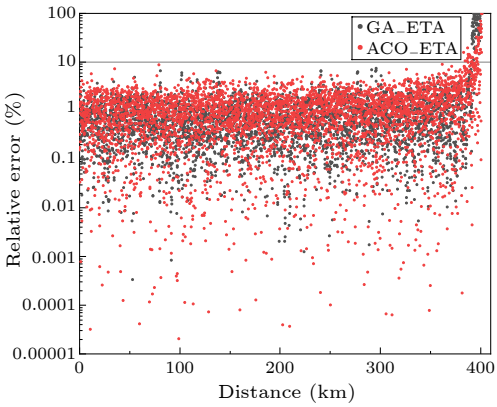

Fig. 5. Relative error values of key rates from ACO and GA. Black dots represent the relative errors between the GA and ETA, and red dots represent those between the ACO and ETA.

5. Conclusion. In this study, the parameter optimization strategy of a decoy-state PM-QKD system was comprehensively analyzed. Initially, we researched the inherent parameter settings of ACO and the GA, recognizing that varying parameter configurations can lead to different operational outcomes. Subsequently, we systematically evaluated the performances of the two NIAs in predicting the parameters using the classical optimization method, ETA, as a benchmark. The results demonstrated that NIAs operate three orders of magnitude faster than ETA while maintaining a power consumption below 8 W. The accuracy of the obtained key rate exceeded 97% (98.7% for ACO and 97.6% for GA). However, the different NIAs exhibited variations in the accuracy of parameter predictions. The ACO displayed remarkable stability, with its optimized parameter values fluctuating around the optimal value, indicating excellent convergence characteristics. In contrast, the GA showed considerable fluctuations in the parameter predictions, resulting in a more scattered data distribution. Therefore, NIAs can be effectively employed for parameter prediction in decoy-state PM-QKD application scenarios with stringent low-latency requirements. Additionally, ACO or GA can be judiciously selected based on a comprehensive computational efficiency assessment and prediction accuracy assessment.

Acknowledgement. This work is supported by the State Key Laboratory of Information Photonics and Optical Communications (Beijing University of Posts and Telecommunications) No. IPOC2021ZT10, BUPT Excellent Ph.D. Students Foundation (Grant No. CX2023207), and the BUPT innovation and entrepreneurship support program No. 2024-YC-A188.

References

[1] Wootters W K and Zurek W H 1982 *Nature* **299** 802
[2] Bennett C H and Brassard G 2014 *Theor. Comput. Sci* **560** 7
[3] Lo H K, Ma X, and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[4] Lo H K, Curty M, and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[5] Tang G Z, Sun S H, and Li C Y 2019 *Chin. Phys. Lett.* **36** 070301
[6] Qi B, Fred Fung C H, Lo H K, and Ma X F 2007 *Quantum Inf. Comput.* **7** 73
[7] Zhao Y, Fred Fung C H, Qi B, Chen C, and Lo H K 2008 *Phys. Rev. A* **78** 042333
[8] Makarov V and Hjelme D R 2007 *J. Mod. Opt.* **52** 691
[9] Iwakoshi T 2015 *Proceedings of the SPIE* **9505** 950504
[10] Makarov V 2009 *New J. Phys.* **11** 065003
[11] Chistiakov V, Huang A Q, Egorov V, and Makarov V 2019 *Opt. Express* **27** 32253
[12] Pirandola S, Laurenza R, Ottaviani C, and Banchi L 2017 *Nat. Commun.* **8** 15043
[13] Li Z D, Zhang R, Yin X F *et al.* 2019 *Nat. Photonics* **13** 644
[14] Lucamarini M, Yuan Z L, Dynes J F, and Shields A J 2018 *Nature* **557** 400
[15] Ma X F, Zeng P, and Zhou H Y 2018 *Phys. Rev. X* **8** 031043
[16] Liu H, Jiang C, Zhu H T *et al.* 2021 *Phys. Rev. Lett.* **126** 250502
[17] Chen T Y, Jiang X, Tang S B *et al.* 2021 *npj Quantum Inf.* **7** 134
[18] Liu Y, Zhang W J, Jiang C *et al.* 2023 *Phys. Rev. Lett.* **130** 210801
[19] Yin J, Li Y H, Liao S K *et al.* 2020 *Nature* **582** 501
[20] Chen Y A, Zhang Q, Chen T Y *et al.* 2021 *Nature* **589** 214
[21] Liao S K, Lin J, Ren J G *et al.* 2017 *Chin. Phys. Lett.* **34** 090302
[22] Li F Y, Wang D, Wang S *et al.* 2014 *Chin. Phys. B* **23** 124201
[23] Gu J, Cao X Y, Fu Y *et al.* 2022 *Sci. Bull.* **67** 2167
[24] Bertaina G *et al.* 2024 *Nature* **7** 2400032
[25] Xu F H, Xu H, and Lo H K 2014 *Phys. Rev. A* **89** 052333
[26] Kumar A, Nadeem M, and Banka H 2022 *Evolving Systems* **14** 141
[27] Darvishpoor S, Darvishpour A, Escarcega M, and Hassanalian M 2023 *Drones* **7** 427
[28] Fidanova S 2021 *Ant Colony Optimization and Applications* (Switzerland: Springer cham)
[29] Dorigo M and Stützle T 2019 *Ant colony optimization: overview and recent advances* (Berlin: Springer) pp. 311
[30] Anwaar A, Ashraf A, Bangyal W H K, and Iqbal M 2022 *Genetic Algorithms: Brief review on Genetic Algorithms for Global Optimization Problems* (America: IEEE) pp. 1
[31] Holland J H 1992 *Adaptation in natural and systems: an introductory analysis with applications to biology, control, and artificial intelligence* (America: Massachusetts Institute of Technology Press)
[32] Razavi S and Jalali-Farahani F 2010 *J Petrol. Sci. Eng.* **74** 147
[33] Vassiliadis V and Dounias G 2008 *Int. J. Artif. Intell.* **18** 487
[34] Lin Z L and Zhang Z C 2020 *Eur. J. Remote Sens* **53** 124
[35] Wang X B, Yu Z W, and Hu X L 2018 *Phys. Rev. A* **98** 062323
[36] Zeng P, Zhou H Y, Wu W J, and Ma X F 2022 *Nat. Commun.* **13** 3903
[37] Xie Y M, Weng C X, Lu Y S, Fu Y, Wang Y, Yin H L, and Chen Z B 2023 *Phys. Rev. A* **107** 042603
[38] Li B H, Xie Y M, Li Z, Weng C X, Li C L, Yin H L, and Chen Z B 2021 *Opt. Lett.* **46** 5529
[39] Lu Y L, Hao J k, and Wu Q H 2022 *PeerJ Comput. Sci.* **8** e972
[40] Liu B, Liu X R, and Jia W G 2024 *Eur. Phys. J. Plus* **137** 412
[41] Song Z A, Huang G Q, Dong Q, and Jiao R Z 2021 *Eur. Phys. J. D* **75** 298