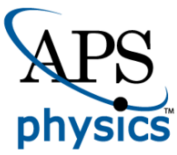

This is the accepted manuscript made available via CHORUS. The article has been published as:

Quantum Key Distribution Over a Channel with Scattering

Qi-Hang Lu, Fang-Xiang Wang, Kun Huang, Xin Wu, Ze-Hao Wang, Shuang Wang, De-Yong He, Zhen-Qiang Yin, Guang-Can Guo, Wei Chen, and Zheng-Fu Han

Phys. Rev. Applied **17**, 034045 — Published 16 March 2022

DOI: 10.1103/PhysRevApplied.17.034045

Quantum key distribution (QKD) over scattering channel

Qi-Hang Lu[1,2], Fang-Xiang Wang[1,2,*], Kun Huang[3], Xin Wu[1,2], Ze-Hao Wang[1,2], Shuang Wang[1,2], De-Yong He[1,2], Zhen-Qiang Yin[1,2], Guang-Can Guo[1,2], Wei Chen[1,2,†], and Zheng-Fu Han[1,2,§]

[1] *CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China*

[2] *CAS Center For Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*

[3] *Department of Optics and Optical Engineering, University of Science and Technology of China, Hefei 230026, China*

[*] *Corresponding author: fxwung@ustc.edu.cn*

[†] *Corresponding author: weich@ustc.edu.cn*

[§] *Corresponding author: zfhan@ustc.edu.cn*

(Dated: March 1, 2022)

Scattering of light by cloud, haze, and fog decreases the transmission efficiency of communication channels in quantum key distribution (QKD), reduces the system's practical security, and thus constrains the deployment of free-space QKD. Here, we employ the wavefront shaping technology to compensate distorted optical signals in high-loss scattering quantum channels and fulfill a polarization-encoded BB84 QKD experiment. With this quantum channel compensation technology, we achieve a typical enhancement of about 250 in transmission efficiency and build a secure communication link even considering finite key length effect, while the link is impossible to share secure keys before optimization. The method applied in QKD system shows the potential to expand the application range of QKD systems from lossless channels to highly scattered ones and therefore enhances the deployment ability of global quantum communication network.

PACS numbers: Valid PACS appear here

I. INTRODUCTION

Quantum key distribution (QKD) [1, 2] paves the way for two legitimate parties (conventionally called Alice and Bob) to share secret keys. For decades, QKD has developed rapidly from proof-of-principle experiments to commercial applications [3–16]. QKD is mainly implemented over fiber-based [5–8] and free-space channels [9–17], which is the essential part of establishing a global secure quantum network. The free space QKD channel easily suffers from the influence of atmospheric turbulence and optical noise [13, 15, 17–20]. Different from classical optical communication systems, the influence of a quantum channels cannot be compensated by enhancing the transmitted photon number, which decreases communication security. Previous studies used the adaptive tracking, atmospheric phase correction or post-processing methods to mitigate the influence of atmospheric turbulence and optical noise to QKD systems [13, 15, 17–20] and have achieved significant progress during the last twenty years and have been successfully demonstrated between satellite and ground over a channel length from 10 km to 1000 km [9–17].

However, most free-space QKD systems were implemented under the conditions that the channel is clearly seen without haze or fogs and the channel loss is relatively low and mostly between 10 to 40 dB [10, 12, 13, 15–17]. In more complicated practical channel conditions with, such as, cloud, dust, haze or fogs, strong scattering effects may exist and leads to the large transmission loss [21–26], which can be 60 dB or larger. Distributing secure key through the scattering-induced high-loss quantum channel remains to be verified for free-space QKD systems. In the strong scattering channel, the beam deformation is much stronger and the beam may even be destructed into speckles, making the performance of QKD system decline and even be difficult to share secret keys [21, 25–28]. Therefore, an effective method for compensating the strong scattering effects and improving the channel performance is vital to free-space QKD systems.

For classical systems, wavefront shaping methods have been developed to deal with light field propagation through scattering media. Wavefront shaping can modulate the optical field by phase and (or) amplitude and hence compensate the scattering effect. Commonly used wavefront shaping methods include transmission matrix (TM) measurement [29, 30], digital optical phase conjugation (DOPC) [31], and iterative algorithms [32, 33]. Hao et al. proposed a DOPC scheme to increase the channel efficiency of a classical optical communication system in 2014 [34]. Also the task of shaping or monitoring quantum states after scattering media has attracted much attention recently [35, 36]. However, applying the wavefront shaping methods in QKD through scattering channels has rarely been studied.

Free space based QKD systems often work under low signal-to-noise ratio (SNR) and unstable environmental condition [19, 20]. Because of its simplicity and opti-

mization robustness against noise [33], the genetic algorithm (GA) developed by John Holland [37] has shown its advantage and has been applied to various of applications [33, 38–41], e.g., shaping the focused spots through the scattering medium [33]. In this article, we implement QKD experiments through strong scattering quantum channels by utilizing the GA wavefront-shaping compensation approach. We applied the anti-noise merits of GA by monitoring the single-photon detecting signals of a QKD system, which means there is no need to increase the system complexity. Experimental results show that the channel transmission efficiency can be enhanced by about 250 times via the compensation. As a result, a secure communication link has been constructed even considering the finite key length effect while there is no secure key rate before optimization. Our work experimentally verifies the feasibility of distributing secret quantum keys through a strong scattering channel and will expand its application range.

II. GENETIC ALGORITHM AND DEMONSTRATION SYSTEMS

A. Scheme of Algorithm and QKD system

To make QKD process possible or enhance the QKD performance through strong scattering media, transmission efficiency over scattering channels should be improved while keeping a relatively low quantum bit error rate (QBER). The solution of this problem will be to gather the transmitted photons inside a predefined area and to keep the spot shape as close to Gaussian distribution as possible. The GA wavefront shaping method has the anti-noise stability and does not need sophisticated apparatus with careful calibration. It searches for a better solution by emulating the evolution process by natural selection among the generations in nature. Thus, GA is a valuable tool to compensate the channel effect and to optimize the optical field through scattering media [33, 42]. The fitness function in GA is used to evaluate the fitness of solution and decides the direction of the evolution, thus it needs to be chosen to reflect the quality of each pattern of the population directly. As is shown in Fig. 1, the primary process of this wavefront-shaping GA can be divided into four steps:

1. Initialization. At the beginning of optimization, a group of random patterns that offers the random initial search of the solution space is generated.

2. Evaluation and ranking. All the patterns are evaluated by the fitness function (each pattern gets a score F_i). Then the patterns are ranked in an ascending order according to their scores.

3. Breeding. The process of generating offspring patterns from initial patterns (the so-called parent patterns) is then executed. Firstly the parents are selected by using a roulette method, which randomly selects two among all parent patterns in the group with the selecting probability according to the equation below:

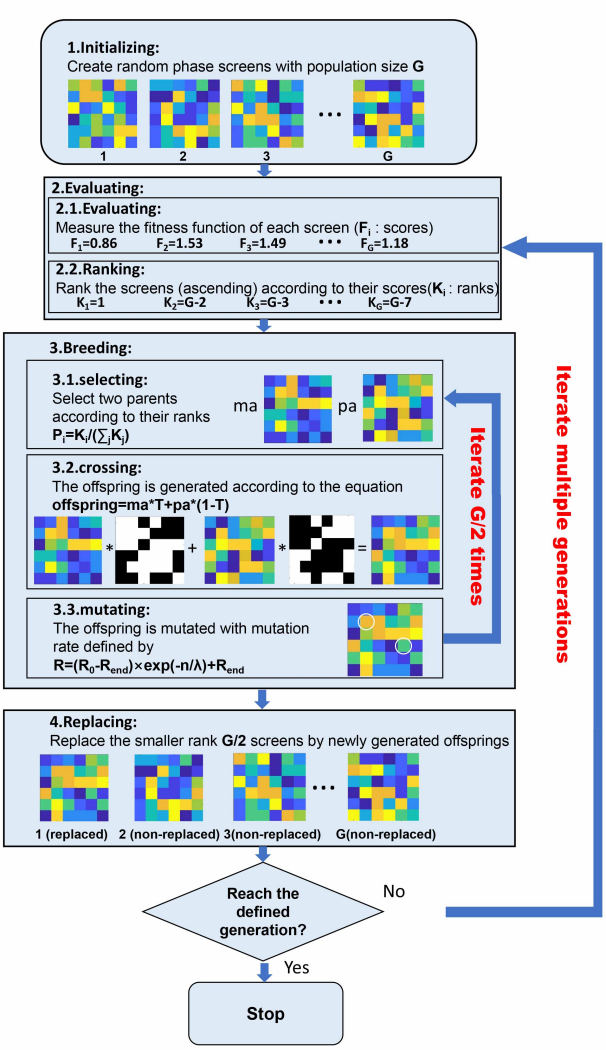

FIG. 1. Flowchart of the GA-based wavefront-shaping compensation method.

$$P_i = \frac{K_i}{\sum_j K_j}, \tag{1}$$

where K_i is the rank of the i-th pattern. At each time, one offspring pattern is generated according to the equation $offspring = T \times ma + (1 - T) \times pa$, where T is a random binary template and ma and pa are the parent patterns selected. The generated offspring, which combines the possible excellent parts of the parents, is then mutated by randomly changing the values of a few pixels of the pattern to expand the searching ability of the algorithm. In order to compromise between optimization speed and global searching ability, the mutation rate R is set to be exponentially decaying, following $R = (R_0 - R_{end}) \times \exp(-n/\lambda) + R_{end}$, where R_0, R_{end}, and λ are the initial mutation rate, the final mutation rate, and the decay factor, respectively.

4. Replacement. The parent patterns of the last half ranks are replaced by the newly generated offspring ones. The iterations are performed cyclically until a prefixed number of optimization.

B. Experimental setup

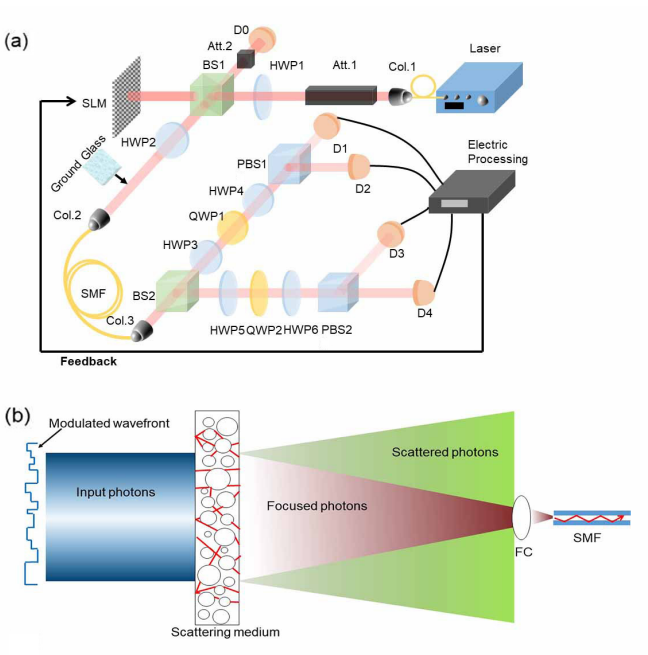

FIG. 2. (a) Experimental setup for proof-of-principle QKD experiment. (b) Conceptual illustration of optimization in our scheme. Att., optical attenuator; HWP, half-wave plate; QWP, quarter-wave plate; PBS, polarization beam splitter; BS, beam splitter; SLM, spatial light modulator; Col., fiber collimators; SMF, single-mode fiber; D_0-D_4, single-photon detectors; FC, fiber collimator.

We verify the validity of the method by two experiments. Firstly, we implement a proof-of-principle BB84 QKD system without scattering medium in the quantum channel (Fig. 2(a)). Two mutually unbiased bases (MUBs), the orthogonal (Z) basis and diagonal (X) basis, are chosen as $|H\rangle, |V\rangle$ and $|+\rangle, |-\rangle$, respectively. $|H\rangle, |V\rangle, |+\rangle, |-\rangle$ corresponded to horizontal, vertical, 45° and 135° linear polarization, respectively. These MUBs are encoded using polarization of photons and realized by a half-wave plate (HWP2) in the system. We use a coherent laser at the wavelength of 780 nm and a 2.1 mm diameter waist. The laser pulses are attenuated to the single-photon level before transmitted into the quantum channel using an attenuator (Att.1). Another attenuator (Att.2) and a single-photon detector (SPD, D_0) are placed at the reflecting port of a beam splitter (BS1) to monitor the average photon number per pulse into the quantum channel. A collimator collects the single-photon signals over the scattering channels to SMF (Col.2), then the photons are incident into the decoding and detection module of Bob. The beam splitter (BS2) of Bob is used to choose measurement basis passively. The upper and down paths performed the Z basis and X basis measurements, respectively. In each path, two HWPs and a quarter-wave plate (QWP) are used to compensate for the polarization variation by the SMF. We measure the total counting rate of the single-photon detectors in Bob (D_1-D_4) and the QBER of each polarization state to characterize the QKD system's performance. The average detection efficiency and dark count rate of the SPD are about 55% and 8.4 Hz, respectively.

Then, we use ground glass diffusers with 120 and 600 grits (Thorlabs, DG20-120 and DG20-600) to simulate scattering channels with different scattering strength. For the QKD system with scattering channels, we realize a single-photon level modulation of the spatial optical field to optimize the transmission efficiency. For free-space QKD systems, the single-mode-fiber (SMF) is usually used as a spatial mode filter to suppress background noise for the receiver [43, 44]. To improve the performance of the quantum channel, the coupling efficiency of the fiber receiver should also be enhanced. As is shown in Fig. 2(b), by modulating the spatial field distribution of transmitted photons, the channel-transmission and fiber-coupling efficiencies to the single-photon signals can be optimized generation by generation using GA.

We use a spatial light modulator (SLM, Holoeye, LETO, with the precision of 0.2π) to compensate the scattering effect of the quantum channel by pre-modulating the spatial phase of the photon state according to the estimated results of GA. A half-wave plate (HWP1) is adopted to rotate the incident polarization to match the SLM's polarization axis. The effective pre-modulation area of the SLM is divided into 60×60 blocks, each of which is $51.6\mu m \times 51.6\mu m$. In the initialization step of the algorithm, we generate 20 random patterns (population size) as the parent group, among which a blank pattern is introduced to make sure that the initial maximum coupling efficiency will not be less than that without the GA optimization. The blank pattern speeds up the optimization procedure and provides a fairer evaluation of the algorithm's optimization ability. As proposed in Section II. A, the total single-photon count rate of Bob reflects the channel efficiency directly and is selected as the fitness function, which is defined as follows,

$$F \equiv \frac{D_1 + D_2 + D_3 + D_4}{D_0}, \tag{2}$$

where $D_0 - D_4$ are the single-photon counting rate of the corresponding SPDs. By choosing the total counting rate of the four SPDs, we can calculate the relative ratio of the fitness function over that of the blank pattern to evaluate the system efficiency enhancement with the optimization procedure. By dividing the transmitted photon count D_0, we are able to mitigate intensity fluctuation of the light source and make the relative ratio coming from single-photon detection be more accurate.

After optimization, we execute the QKD procedure and compare the performance with that before optimization to evaluate the effectiveness of GA procedure.

III. RESULTS AND DISCUSSION

When there is no scattering medium in the quantum channel, the overall transmission efficiency of the quantum channel between Alice and Bob is 64.5% (about 1.9 dB), which is mainly contributed by the coupling efficiency of the fiber collimator (Col.2 in Fig. 2(a)). After transmitting through the quantum channel with a 120-grit scattering medium, the overall transmission loss increased to 62.1 dB. However, the transmission loss over the scattering channel decreases to 38.0 dB after the optimization using the GA with 3000 generations, and the evolution process of optimization is shown in Fig. 3(a). By replacing the strong scattering medium with a weaker one (600 grit), the overall transmission loss of the quantum channel becomes 16.8 dB. After optimized by GA with 7000 generations, the transmission loss decreases to 14.6 dB. The enhancement of the optimization is shown in Fig. 3(b).

From the results above, we can see that the channel

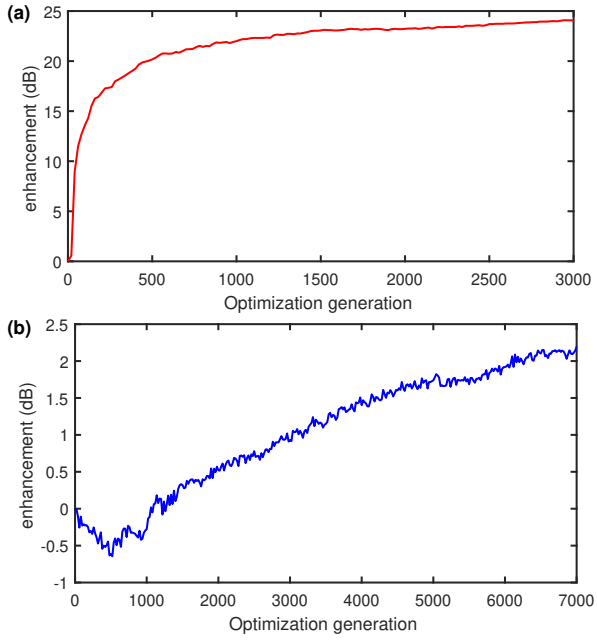

FIG. 3. Optimization results of the scattering channel. (a) The enhancement of the total photon count of D_1-D_4 in the optimization process after a 120-grit scattering medium was added. GA algorithm has made the transmitted power coupling to the SMF a converging curve, indicating the increase of the transmission efficiency. The horizontal axis is the generation. (f) The enhancement of the total photon count of D_1-D_4 in the optimization process after a 600-grit scattering medium was added.

transmission loss under the 600-grit scattering medium without optimization is much lower than that under the 120-grit scattering medium, which indicates that the scattering effect decreases significantly. Therefore, the corresponding enhancement under a 600-grit scattering medium is much lower as well. The evolution processing show that there exists random fluctuation for adjacent generations (Figs. 3(a)-3(b)), which is majorly due to the background noise. However, benefiting from the robustness of GA, this fluctuation only affects the optimization performance slightly.

We then carry out QKD sessions after evaluating the optimization performance of the light pulses. According to Gottesman-Lo-Lütkenhaus-Preskill (GLLP) equation [45], the asymptotic secure key generation rate of BB84 QKD is

$$R = max\{qQ_\mu[-f_{EC}H_2(E_\mu) + \Delta_1(1 - H_2(e_1))], 0\}, \quad (3)$$

where q depends on the QKD protocol and is 1/2 in our experiment; Q_μ and e_μ are the gain and QBER of the signal state; f_{EC} is the error correction efficiency and is set as 1.15; H_2 is the binary Shannon entropy, which is defined as $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$; Δ_1 and e_1 are the fraction and QBER of single-photon signals, respectively. We estimate the values of Δ_1 and e_1 by adopting the "vacuum + weak decoy-state" method [46–48], and the photon numbers of the signal state μ and decoy state ν are set as 0.6 and 0.2, respectively. Although the decoy states have not been randomly modulated pulse by pulse in this proof-of-principle experiment, the effectiveness of this evaluation-optimization method is verified since the comparisons are under the same conditions.

We have also considered the finite-key effect by adopting the analysis method proposed by C.C.W.Lim et al. [49]. Additionally, by calculating the upper bound for the phase error rate of the single photon events in the Z basis, the secure key rate can be improved further [50]. The secure key rate formula is [49, 50]

$$l = s_{z,0} + s_{z,1} - s_{z,1}H_2(\phi_z) - \lambda_{EC} - 6\log_2(\frac{21}{\epsilon_{sec}}) - \log_2(\frac{2}{\epsilon_{cor}}), \quad (4)$$

where $s_{z,0}$ is the number of vacuum events and $s_{z,1}$ is the number and ϕ_z is the phase error rate (upper bound) of single photon events in the Z basis, respectively; ϵ_{sec} and ϵ_{cor} are the security parameters of correctness and secrecy, respectively; the parameter λ_{EC} is the size of the information exchanged during the error-correction step, which is set as $n_z f_{EC} h(e_{obs})$, where e_{obs} is the average of the observed error rates in basis Z. From equation (4) we can calculate the secure key rate $R = l/N$, where N is the sample size sent by Alice (block length) and is set as $N = 4.5 \times 10^{10}$ in our experiment (In the 120 grit case we have also considered the case when N increases to 1×10^{12} in simulation).

The simulation and experimental secure key rates in both the asymptotic limit and finite length method without scattering media, for 120-grit and 600-grit scattering media are shown in Fig. 4(a), (b) and (c), respectively, all under different channel losses for the scattering channel. More details of the experimental parameters and results are shown in the appendix. As shown in Fig. 4, the introducing of the scattering media leads to a significant decrease of SKR. Especially, for strong scattering channel (120 grit), when there is no optimization, the transmission loss is higher than 60 dB and the scattered signal photons barely propagate through quantum channel so that secure key cannot be generated (thus there is no corresponding curve in Fig. 4(c)). After optimization, QKD becomes usable and the SKR is shown by the black triangles. The asymptotic simulation curve (black dashed line) shows that the QKD system can support secure key distribution over 70-dB loss channel. However, when considering finite-length effect, the extreme channel loss decreases to 64 dB with $N = 4.5 \times 10^{10}$. By increasing the sample size to 10^{12}, the system can support a secure key distribution over 67 dB. That is, an effective QKD channel has been built up through the optimization process for the strong scattering channel. For weak scattering channel (600 grit), the SKR enhancement is relatively small. However, it will be crucial for limit-distance communication.

In order to quantify the optimization effectiveness, we also measure the beam profiles of transmitted optical fields through the quantum channel with and without the scattering medium using a charge-coupled-devices (CCD) camera. The beam profile and intensity distribution along x axis in front of Col.2 without scattering medium are shown in Fig. 5(a) and the black triangle line of Fig. 5(b), respectively. The intensity distribution along the x axis approximates to the Gaussian distribution. After transmitting through the quantum channel with a 120-grit scattering medium, the beam profile in front of Col.2 is shown in Fig. 5(c), which demonstrates that the optical field is seriously scattered and the intensity distribution is relatively "flat" (the blue square line in Fig. 5(b)). After optimization with GA, the beam profile has been shaped to a sharp spot with a high contrast of about 100 to the around the area (Fig. 5(d)). The intensity distribution of the spot is Gaussian-like (red circle line in Fig. 5(b)), which indicates a good matching of the spatial mode to the SMF fiber and hence the transmission loss is reduced from 62.1 dB to 38.0 dB.

The speed of proposed optimization process is mainly limited by the frame rate of the SLM. For free-space based systems under some practical channel conditions, such as some types of haze, fog or cloud, the variance of the channel characteristics are in the time scale of 1s to 1min [22–24]. By replacing the SLM with digital micro-mirror devices (DMD, with a frame rate of 10kHz or faster), the GA method can achieve an optimization from chaos within several seconds (for 1000 optimization generation). After an optimized solution has achieved, a feedback with 10-generation optimization can be fulfilled within 100 ms to track the slow changes of the scattering characteristic.Some other wavefront shaping methods like TM method could also require no previous knowledge of the scattering characteristic. In fact, the patterns needed to measure of GA and TM are at the same level [29, 33]. For example, for a pattern with 100×100 elements, the measurement time of TM method is at the level of 10^4, which corresponds to 500 generations of GA method with a population of 20 patterns. TM method also needs software based computation algorithm to get TM elements, which depends on particular algorithm and is resource and time-consuming [51, 52]. Comparing with TM method, GA requires much less computation resource and is simpler to realize. At the same time, when there exists large background noise, GA can give a more robust result than that by the TM method [33]. In free-space QKD system, optical and electrical noise may become significant in daylight and high-loss-channel scenario [19, 20]. Therefore, the GA optimization method is hopeful to achieve a real-time correction of the practical complex scattering channel and to improve the performance of practical free-space QKD systems.

The ratio of receiver aperture over scattered beam size of present system is nearly 100%, which can support QKD over 1 km to 10 km free-space channel. For remote distance QKD, especially the satellite-to-ground QKD, the received beam size will be broadened to 10-1000 m [12, 53]. This is because of the ultra long channel length (100-1000 km) and the turbulence effects of atmosphere [53]. The ratio of receiver aperture over scattered beam size will be less than 1%. The system needs further development to be applied to such a smaller ratio of receiver aperture over scattered beam size. The satellite-to-ground QKD faces another challenge that the effective detected signal block size is too small to overcome the finite-length effect [50]. This can be improved by using satellites with middle or high orbit (1 thousand to 10 thousand km). In the middle or high-orbit satellite-to-ground channel, the transmission loss will become much higher due to the larger beam divergence. To solve this problem, fast and powerful adaptive methods, such as GA method with further significant improvement, will be a potential tool to improve the effective signal count rate and may make it possible to share secure keys between satellite and ground.

IV. SUMMARY

We have applied the waveform shaping method to the QKD system through scattering quantum channels using GA based on the single-photon-level signals and optimization processing. The proof-of-principle QKD experiment clearly shows that an effective quantum link can be built through a strong scattering channel using this method, which can even make the key generation sessions from impossible to possible even considering finite

length effects, which will be crucial for practical QKD under extreme field conditions. By using modulation devices with higher speed in this method, the system can be used to provide a real-time correction to the more practical strong scattering media, such as haze or fogs in the free space QKD channel. Additionally, this system has the potential to improve the performance of satellite-to-ground QKD by further developments. Our study shows the potentiality to expand the application range of practical QKD systems and can potentially enhance the global quantum communication network's deployment ability.

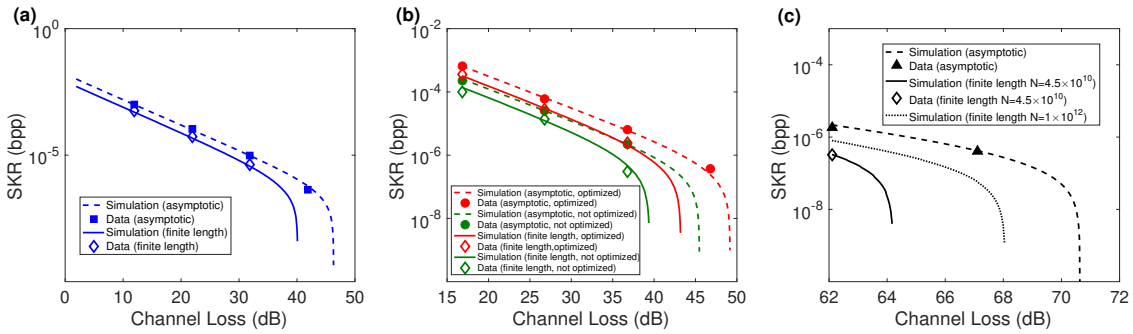

FIG. 4. Secure key rates (SKRs) in bit per pulse (bpp) of the proof-of-principle QKD experiment with the channel loss (where scattering loss is already included). The lines are the simulation SKRs for the quantum channels without (blue lines in (a)) and with 600-grit before optimization (red lines in (b)) and after optimization (green lines in (b)) and 120-grit scattering media (black lines in (c)), respectively. The solid lines are the finite length SKRs while the dashed lines (long dash length) are the asymptotic SKRs. The squares, filled and hollow circles, triangles and diamonds are the corresponding experimental SKRs. The dashed line in (c) with a shorter dash length is the simulated SKR under block length $N = 10^{12}$.

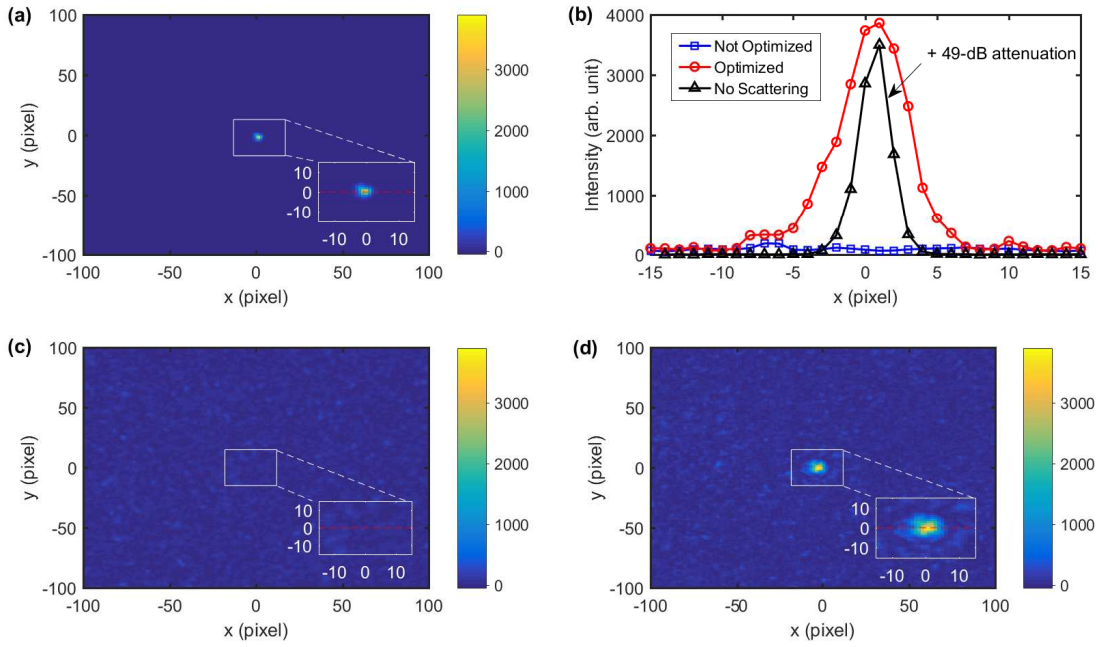

FIG. 5. The beam profile of the optical fields transmitted through scattering quantum channels. (a) The beam profile without scattering medium. (b) The transverse intensity distribution of the beam without and with a scattering medium of 120 grit. (c)-(d), the transmitted beam profiles through the 120-grit scattering medium without and with GA optimization, respectively. Red, blue and black lines in (b): the intensity distribution along X axis (the red dashes) of the beam profiles in (a), (c) and (d), respectively. All the beam profiles are measured with a lens (the focus length is 5cm), and when measuring without scattering medium a 49-dB attenuation is added to avoid overexposure. Arb. unit: arbitrary unit. Color bars in (a), (c) and (d): Intensity (pixel value of the CCD). Pixel size: 6.4 μm. CCD exposure time in (a), (c), and (d) is 0.2 ms. Subfigures in (a), (c), and (d): The magnified intensity distribution of 30×30 pixels around the spot.

FUNDING INFORMATION

This work has been supported by the National Key Research and Development Program of China (Grant No. 2018YFA0306400), National Natural Science Foundation of China (Grant Nos. 61627820, 61905235, 61675189, 61622506, 61822115, 61875181), Anhui Initiative in Quantum Information Technologies(Grant No. AHY030000) and the University of Science and Technology of Chinas Centre for Micro and Nanoscale Research and Fabrication. K.H. also thanks CAS Pioneer Hundred Talents Program, the Fundamental Research Funds for the Central Universities in China, USTC Research Funds of the Double First-Class Initiative (Grant YD2030002003). F.-X.W. also thanks the support of China Postdoctoral Science Foundation (2019M652179).

ACKNOWLEDGMENTS

The authors thank Lei. Gong for fruitful discussion and Zhao-Di. Liu for technical support on wavefront shaping techniques.

DISCLOSURES

The authors declare no conflicts of interest.

Appendix A: Specific Experimental Data and Secure Key Rates in the Asymptotic Limit

We realized a proof-of-principle decoy-state BB84 QKD experiment over a strong scattering quantum channel. In the experiment, two mutually unbiased bases (MUBs), the orthogonal (Z) basis and diagonal (X) basis, were chosen as $|H\rangle, |V\rangle$ and $|+\rangle, |-\rangle$, respectively. $|H\rangle, |V\rangle, |+\rangle, |-\rangle$ corresponded to horizontal, vertical, 45° and 135° linear polarization, respectively. In the asymptotic limit, we utilized the "vacuum + weak decoy state" method [46–48]. The lower bound of yield Y_1 and the upper bound of QBER e_1 of the single photon signals were estimated from the experimental yield and QBER of signal and decoy states, respectively. The 0.6 and 0.2 photon per pulse were selected as the signal state μ and decoy state ν, respectively.

$$Y_1 \geq Y_1^{L,\nu,0} = \frac{\mu}{\mu\nu - \nu^2}(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0) \tag{A1}$$

$$e_1 \leq \frac{E_\nu Q_\nu e^\nu - e_0 Y_0}{Y_1^{L,\nu,0}\nu} \tag{A2}$$

Then we calculated the lower bound of average single photon fraction Δ_1 in the GLLP formula (Eq.3 in the main text) by

$$\Delta_1 \geq \frac{Y_1^{L,\nu,0}\mu e^{-\mu}}{Q_\mu}, \tag{A3}$$

where Q_μ, E_μ, Q_ν and E_ν are the average yields and QBERs of the signal and decoy states. The experimental data with/without optimization and with different channel losses were measured under each scattering length. The specific experimental values of the losses, Q_μ, E_μ, Q_ν, E_ν and the secure key rates under different scattering lengths are shown in the table below.

TABLE I. **The experimental data of the QKD procedure with the decoy-state method. Labels: Scatt Loss: Scattering-induced channel loss. Total Loss: The total loss in the channel including the scattering-induced channel loss and the simulated channel loss by the attenuator. No Scatt: No scattering media. R: Secure Key Rate.**

	Optimization	Scatt Loss(dB)	Total Loss(dB)	Q_μ	Q_ν	$E_\mu(\%)$	$E_\nu(\%)$	R (per pulse) (asymptotic)	R (per pulse) (finite length)
120grit	Without	62.1	62.1	2.2×10^{-7}	1.2×10^{-7}	24	37	None	None
	With	38.0	38.0	1.34×10^{-5}	4.50×10^{-6}	1.63	2.79	1.85×10^{-6}	3.17×10^{-7}
		38.0	43.0	4.67×10^{-6}	1.71×10^{-6}	2.95	6.84	3.96×10^{-7}	None
600grit	Without	16.8	16.8	1.8989×10^{-3}	6.2211×10^{-4}	1.72	2.51	2.29×10^{-4}	1.00×10^{-4}
		16.8	26.8	1.862×10^{-4}	6.26×10^{-5}	1.87	1.99	2.55×10^{-5}	1.39×10^{-5}
		16.8	36.8	1.93×10^{-5}	6.49×10^{-6}	2.27	3.14	2.19×10^{-6}	2.99×10^{-7}
		16.8	46.8	1.99×10^{-6}	8.0×10^{-7}	6.00	12.56	None	None
	With	14.6	14.6	3.2224×10^{-3}	1.0862×10^{-3}	0.80	0.77	6.43×10^{-4}	3.57×10^{-4}
		14.6	24.6	3.259×10^{-4}	1.069×10^{-4}	0.77	0.81	6.13×10^{-5}	2.86×10^{-5}
		14.6	34.6	3.15×10^{-5}	1.10×10^{-5}	1.00	1.54	6.36×10^{-6}	2.45×10^{-7}
		14.6	44.6	3.38×10^{-6}	1.28×10^{-6}	3.37	7.17	3.68×10^{-7}	None
No Scatt.	-	0	11.9	5.8597×10^{-3}	1.9355×10^{-3}	1.02	1.14	1.02×10^{-3}	5.73×10^{-4}
		0	21.9	5.764×10^{-4}	1.961×10^{-4}	1.05	0.97	1.10×10^{-4}	5.53×10^{-5}
		0	31.9	5.87×10^{-5}	1.94×10^{-5}	1.13	1.44	9.86×10^{-6}	4.26×10^{-6}
		0	41.9	6.13×10^{-6}	2.07×10^{-6}	2.68	6.22	4.37×10^{-7}	None

Appendix B: Finite Size Analysis of the Secure Key Rates

When considering the finite length effects, we adopted the method used by [49, 50]. The secure key rates are calculated based on equation (4), with the lower bound of the vacuum events of Z basis calculated as,

$$s_{z,0} \geq \tau_0 \frac{\nu n^-_{z,0}}{\nu}, \tag{B1}$$

where $\tau_n = \sum_{k\in\kappa} e^{-k} k^n \frac{P_k}{n!}$, $\kappa = \{\mu, \nu, 0\}$; P_k is the sending probability of the corresponding state (the probabilities of the signal, decoy and vacuum state were set equally as 1/3); $n^{\pm}_{z,k} = \frac{e^k}{P_k}[n_{z,k} \pm \sqrt{\frac{n_z}{2}\ln\frac{21}{\epsilon_{sec}}}], \forall k \in \kappa$ is the upper and lower bounds of the number of count of Z basis, where $n_{z,k}$ is the number of count at Z basis with the corresponding k state and $n_z = \sum_{k\in\kappa} n_{z,k}$.

The lower bounds of the single photon count number of Z basis and X basis are calculated respectively as,

$$s_{z,1} \geq \frac{\tau_1\mu[n^-_{z,\nu} - n^+_{z,0} - \frac{\nu^2}{\mu^2}(n^+_{z,\mu} - \frac{s_{z,0}}{\tau_0})]}{\mu\nu - \nu^2} \tag{B2}$$

and

$$s_{x,1} \geq \frac{\tau_1\mu[n^-_{x,\nu} - n^+_{x,0} - \frac{\nu^2}{\mu^2}(n^+_{x,\mu} - \frac{s_{x,0}}{\tau_0})]}{\mu\nu - \nu^2}, \tag{B3}$$

where $n^{\pm}_{z,k}$ and $n^{\pm}_{x,k}$ are the upper and lower bounds of the number of count of Z basis and X basis, respectively.

At the same time, the upper bound of the X basis bit error rate is calculated as,

$$\nu_{x,1} \leq \tau_1 \frac{m^+_{x,\nu} - m^-_{x,0}}{\nu}, \tag{B4}$$

where $m^{\pm}_{x,k} = \frac{e^k}{P_k}[m_{x,k} \pm \sqrt{\frac{m_x}{2}\ln\frac{21}{\epsilon_{sec}}}], \forall k \in \kappa$ is the upper and lower bounds of the corresponding states in X basis and $m_x = \sum_{k\in\kappa} m_{x,k}$.

Then, the upper bound of phase error rate of single photon events of Z basis can be calculated as,

$$\phi_z \leq \frac{\nu_{x,1}}{s_{x,1}} + \gamma(\epsilon, \frac{\nu_{x,1}}{S_{x,1}}, S_{x,1}, S_{z,1}), \tag{B5}$$

where $\gamma(a,b,c,d) = \min_{\xi}\{\xi + \frac{1}{d}\sqrt{1 - \frac{\ln[a^2 - \exp\left(-\frac{2(c+d)c\xi^2}{d+1}\right)]}{2\Gamma_c(b+\xi)}}\}$ and $\epsilon = \frac{\epsilon_{sec}}{21}$. In the expression above $\Gamma_c(b+\xi) = \frac{1}{c(b+\xi)+1} + \frac{1}{c-c(b+\xi)+1}$ and $\xi \in (0, \gamma), c(b+\xi) \in R^+, d^2(\gamma-\xi)^2 > 1$.

The average of the observed error rates in basis Z is calculated by $e_{obs} = \frac{m_z}{n_z}$, where $m_z = \sum_{k\in\kappa} m_{z,k}$ and $m_{z,k}$ is the error rate of corresponding state in Z basis.

[1] C. H. Bennett and G. Brassard, Proceedings of the IEEE international conference on computers, systems and signal processing (1984).

[2] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Reviews of Modern Physics **92**, 025002 (2020).

[3] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Experimental quantum cryptography, in *Workshop on the Theory and Application of of Cryptographic Techniques* (Springer, 1990) pp. 253–265.

[4] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. Dynes, *et al.*, The SECOQC quantum key distribution network in vienna, New Journal of Physics **11**, 075001 (2009).

[5] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, *et al.*, Field test of quantum key distribution in the Tokyo QKD network, Optics express **19**, 10387 (2011).

[6] S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang, *et al.*, Field and long-term demonstration of a wide area quantum key distribution network, Optics express **22**, 21739 (2014).

[7] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, *et al.*, Secure quantum key distribution over 421 km of optical fiber, Physical review letters **121**, 190502 (2018).

[8] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. Sharpe, A. Dixon, E. Lavelle, J. Dynes, A. Murakami, *et al.*, 10-Mb/s quantum key distribution, Journal of Lightwave Technology **36**, 3427 (2018).

[9] B. Jacobs and J. Franson, Quantum cryptography in free space, Optics Letters **21**, 1854 (1996).

[10] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, *et al.*, Experimental demonstration of free-space decoy-state quantum key distribution over 144 km, Physical Review Letters **98**, 010504 (2007).

[11] R. Bedington, J. M. Arrazola, and A. Ling, Progress in satellite quantum key distribution, npj Quantum Information **3**, 1 (2017).

[12] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, *et al.*, Satellite-to-ground quantum key distribution, Nature **549**, 43 (2017).

[13] S.-K. Liao, H.-L. Yong, C. Liu, G.-L. Shentu, D.-D. Li, J. Lin, H. Dai, S.-Q. Zhao, B. Li, J.-Y. Guan, *et al.*, Long-distance free-space quantum key distribution in daylight towards inter-satellite communication, Nature Photonics **11**, 509 (2017).

[14] J. Yin, Y.-H. Li, S.-K. Liao, M. Yang, Y. Cao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, S.-L. Li, *et al.*, Entanglement-based secure quantum cryptography over 1,120 kilometres, Nature **582**, 501 (2020).

[15] Y. Cao, Y.-H. Li, K.-X. Yang, Y.-F. Jiang, S.-L. Li, X.-L. Hu, M. Abulizi, C.-L. Li, W. Zhang, Q.-C. Sun, *et al.*, Long-distance free-space measurement-device-independent quantum key distribution, Physical Review Letters **125**, 260503 (2020).

[16] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, *et al.*, An integrated space-to-ground quantum communication network over 4,600 kilometres, Nature **589**, 214 (2021).

[17] E. Moschandreou, B. J. Rollick, B. Qi, and G. Siopsis, Experimental decoy-state Bennett-Brassard 1984 quantum key distribution through a turbulent channel, Physical Review A **103**, 032614 (2021).

[18] C. Erven, B. Heim, E. Meyer-Scott, J. Bourgoin, R. Laflamme, G. Weihs, and T. Jennewein, Studying free-space transmission statistics and improving free-space quantum key distribution in the turbulent atmosphere, New Journal of Physics **14**, 123018 (2012).

[19] C. Liorni, H. Kampermann, and D. Bruß, Satellite-based links for quantum key distribution: beam effects and weather dependence, New Journal of Physics **21**, 093055 (2019).

[20] S. Pirandola, Limits and security of free-space quantum communications, Physical Review Research **3**, 013279 (2021).

[21] A. Deepak, U. O. Farrukh, and A. Zardecki, Significance of higher-order multiple scattering for laser beam propagation through hazes, fogs, and clouds, Applied optics **21**, 439 (1982).

[22] C. Colvero, M. Cordeiro, and J. Von der Weid, Real-time measurements of visibility and transmission in far-, mid- and near-IR free space optical links, Electronics Letters **41**, 610 (2005).

[23] S. S. Muhammad, B. Flecker, E. Leitgeb, and M. Gebhart, Characterization of fog attenuation in terrestrial free space optical links, Optical engineering **46**, 066001 (2007).

[24] M. Ijaz, Z. Ghassemlooy, J. Pesek, O. Fiser, H. Le Minh, and E. Bentley, Modeling of fog and smoke attenuation in free space optical communications link under controlled laboratory conditions, Journal of Lightwave Technology **31**, 1720 (2013).

[25] D. Vasylyev, A. Semenov, W. Vogel, K. Günthner, A. Thurn, Ö. Bayraktar, and C. Marquardt, Free-space quantum links under diverse weather conditions, Physical Review A **96**, 043856 (2017).

[26] M. Grabner and V. Kvicera, Multiple scattering in rain and fog on free-space optical links, Journal of lightwave technology **32**, 513 (2013).

[27] O. Katz, E. Small, and Y. Silberberg, Looking around corners and through thin turbid layers in real time with scattered incoherent light, Nature photonics **6**, 549 (2012).

[28] J. Zhao, Y. Zhou, B. Braverman, C. Liu, K. Pang, N. K. Steinhoff, G. A. Tyler, A. E. Willner, and R. W. Boyd, Performance of real-time adaptive optics compensation in a turbulent channel with high-dimensional spatial-mode encoding, Optics express **28**, 15376 (2020).

[29] S. Popoff, G. Lerosey, R. Carminati, M. Fink, A. Boccara, and S. Gigan, Measuring the transmission matrix in optics: an approach to the study and control of light propagation in disordered media, Physical review letters **104**, 100601 (2010).

[30] L. Gong, Q. Zhao, H. Zhang, X.-Y. Hu, K. Huang, J.-M. Yang, and Y.-M. Li, Optical orbital-angular-momentum-multiplexed data transmission under high scattering,

Light: Science & Applications **8**, 1 (2019).
[31] Z. Yaqoob, D. Psaltis, M. S. Feld, and C. Yang, Optical phase conjugation for turbidity suppression in biological samples, Nature photonics **2**, 110 (2008).
[32] I. M. Vellekoop and A. Mosk, Focusing coherent light through opaque strongly scattering media, Optics letters **32**, 2309 (2007).
[33] D. B. Conkey, A. N. Brown, A. M. Caravaca-Aguirre, and R. Piestun, Genetic algorithm optimization for focusing through turbid media in noisy environments, Optics express **20**, 4840 (2012).
[34] X. Hao, L. Martin-Rouault, and M. Cui, A self-adaptive method for creating high efficiency communication channels through random scattering media, Scientific reports **4**, 5874 (2014).
[35] H. Defienne, M. Barbieri, B. Chalopin, B. Chatel, I. Walmsley, B. Smith, and S. Gigan, Nonclassical light manipulation in a multiple-scattering medium, Optics letters **39**, 6090 (2014).
[36] O. Lib, G. Hasson, and Y. Bromberg, Real-time shaping of entangled photons by classical control and feedback, Science Advances **6**, eabb6298 (2020).
[37] J. H. Holland, *Adaptation in natural and artificial systems: an introductory analysis with applications to biology, control, and artificial intelligence* (MIT press, 1992).
[38] K. Deb, A. Pratap, S. Agarwal, and T. Meyarivan, A fast and elitist multiobjective genetic algorithm: NSGA-II, IEEE transactions on evolutionary computation **6**, 182 (2002).
[39] G. Jones, P. Willett, R. C. Glen, A. R. Leach, and R. Taylor, Development and validation of a genetic algorithm for flexible docking, Journal of molecular biology **267**, 727 (1997).
[40] C.-L. Chiang, Improved genetic algorithm for power economic dispatch of units with valve-point effects and multiple fuels, IEEE transactions on power systems **20**, 1690 (2005).
[41] U. Mahlab, J. Shamir, and H. J. Caulfield, Genetic algorithm for optical pattern recognition, Optics Letters **16**, 648 (1991).
[42] I. M. Vellekoop, Feedback-based wavefront shaping, Optics express **23**, 12189 (2015).
[43] Y.-P. Li, W. Chen, F.-X. Wang, Z.-Q. Yin, L. Zhang, H. Liu, S. Wang, D.-Y. He, Z. Zhou, G.-C. Guo, *et al.*, Experimental realization of a reference-frame-independent decoy BB84 quantum key distribution based on sagnac interferometer, Optics letters **44**, 4523 (2019).
[44] M. T. Gruneisen, M. B. Flanagan, and B. A. Sickmiller, Modeling satellite-earth quantum channel downlinks with adaptive-optics coupling to single-mode fibers, Optical Engineering **56**, 126111 (2017).
[45] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Security of quantum key distribution with imperfect devices, Quantum Information & Computation **4**, 325 (2004).
[46] X.-B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, Physical review letters **94**, 230503 (2005).
[47] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, Physical review letters **94**, 230504 (2005).
[48] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Practical decoy state for quantum key distribution, Physical Review A **72**, 012326 (2005).
[49] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Concise security bounds for practical decoy-state quantum key distribution, Physical Review A **89**, 022307 (2014).
[50] C. C.-W. Lim, F. Xu, J.-W. Pan, and A. Ekert, Security analysis of quantum key distribution with small block length and its application to quantum space communications, Physical Review Letters **126**, 100501 (2021).
[51] J. Yoon, K. Lee, J. Park, and Y. Park, Measuring optical transmission matrices by wavefront shaping, Opt. Express **23**, 10158 (2015).
[52] H. Yu, K. Lee, and Y. Park, Ultrahigh enhancement of light focusing through disordered media controlled by mega-pixel modes, Optics express **25**, 8036 (2017).
[53] A. Scriminich, G. Foletto, F. Picciariello, G. Vallone, P. Villoresi, and F. Vedovato, Optimal design and performance evaluation of free-space quantum key distribution systems, arXiv preprint arXiv:2109.13886 (2021).