Optimizing Quantum Key Distribution Protocols using Decoy State Techniques and Experimental Validation

Sellami Ali
Faculty of Science and Technology, University of Tamanghasset, Tamanghasset, Algeria | Materials and Energy Research Laboratory, University of Tamanghasset, Tamanghasset, Algeria
sellamiali2023@gmail.com (corresponding author)

Benlahcene Djaouida
Faculty of Science and Technology, University of Tamanghasset, Tamanghasset, Algeria
sellami2003@hotmail.com

Received: 16 April 2024 | Revised: 3 May 2024 and 19 May 2024 | Accepted: 19 May 2024

 DOI: https://doi.org/10.48084/etasr.7521

ABSTRACT

This paper simulated the operation of vacuum state and single decoy state protocols in the BB84 and SARG04 QKD schemes by utilizing the features of the commercial ID-3000 QKD system. Numerical modeling identified an optimal signal-to-decoy state ratio of 0.95:0.05 and an intensity of μ=0.85 for the signal state and v_1=0.05 for the decoy state, ensuring the highest key generation rate and a secure distance of up to 50 km. These protocols were validated experimentally over various transmission distances with standard telecom fiber, using the ID-3000 QKD system in a conventional bi-directional plug-and-play setup. Simulations predicted secure key rates of 1.2×10^5 bits/s for SARG04 and 8.5×10^4 bits/s for BB84 at 10 km, with secure distances of 45 km and 35 km, respectively. The experimental results confirmed these predictions, showing a 30% higher key rate and 20% longer secure distance compared to non-decoy methods. The SARG04 protocol surpassed BB84 in key rate and secure distance, highlighting the two-photon component's role in key generation. This study concludes that the decoy-state method significantly enhances key generation rates and secure distances, optimizing QKD protocols for secure quantum communication.

Keywords-optical communication; decoy state method; quantum cryptography; quantum key distribution

I. INTRODUCTION

The current state of affairs highlights the critical need for extremely secure communication methods. With the prevalent transmission of sensitive information, the risk of unauthorized access and data breaches is heightened. Quantum cryptography emerges as a promising solution to this pressing demand for secure communication. Bennett and Brassard pioneered the concept of Quantum Key Distribution (QKD) as a secure communication technology in 1984 [1, 43], which promises absolute security due to its grounding in the inviolable laws of quantum mechanics [2, 44]. However, practical implementations of QKD protocols, such as the seminal BB84 protocol, face significant challenges due to the limitations of the current technology. Notably, the inability to generate ideal single-photon sources necessitates the use of attenuated laser pulses, introducing vulnerabilities to eavesdropping attacks like the photon number splitting technique [3, 34]. In this attack, an eavesdropper can intercept and split multi-photon signals while allowing single-photon transmissions to pass undetected, compromising the security of the system.

Recognizing these vulnerabilities, Hwang [4] proposed an innovative solution by introducing the concept of decoy states. These additional test states, transmitted alongside the key-generating signal, enable the determination of channel parameters and the detection of potential eavesdropping attempts. Building upon this foundation, authors in [5] demonstrated that the integration of decoy states with the entanglement distillation method could significantly enhance the key generation rate and secure distance of QKD systems compared to non-decoy methods. Several techniques have been suggested to enhance the effectiveness of QKD using decoy states [6]. The SARG04 protocol was designed with decoy states in mind and may offer higher secure key rates than BB84 without decoy states, but this does not necessarily mean that it will be faster than all the other protocols (like B92 or E91) when they also incorporate decoy states. The actual performance and speed of the protocols depend on the specific implementation details, channel conditions, and other optimizations employed. These methods include adding extra decoy states [7], following a non-orthogonal decoy-state approach [8], detecting individual photons [9], utilizing a

heralded single photon source [10, 11], adjusting the coherent state source [12], and varying the laser pulse intensities [13, 14]. Some prototypes of QKD with decoy states have already been developed and tested [15–22]. More recently, decoy-state QKD has been successfully implemented in both optical fiber [23, 24] and free space [25]. Numerous field-test QKD networks [26, 27] have been developed employing decoy-state QKD systems. When combined with Measurement-Device-Independent (MDI) methodology [28, 29], which eliminates all detector side-channel attacks, decoy-state QKD systems surpassed the repeaterless secret key capacity [30, 31], becoming more practical for real-world applications [32, 33].

In practice, all decoy-state QKD experiments are conducted over a finite period, meaning the number of emitted signals is limited. Consequently, estimating single-photon contributions by adopting the decoy-state method, a researcher must consider statistical fluctuations, a process known as finite-key analysis of QKD [34]. When dealing with a finite data size, optimizing the intensity choices of signal and decoy states, along with the probabilities of sending these states, is crucial for improving system performance. Therefore, comprehensive optimization is necessary to determine these parameters based on specific experimental conditions, such as optical misalignment, data size, and channel loss. Numerous studies have been conducted on improving channel performance [35-38].

In general, performing full optimization typically involves a brute-force global search, which is difficult due to limited computational resources. Therefore, it is only feasible for functions with a small number of parameters. Authors in [39] introduced the Local Search Algorithm (LSA) of Coordinate Descent (CD), which greatly enhances the optimization speed for symmetric MDI-QKD, which involves a larger number of parameters. This algorithm has since proven to be an effective tool for optimization in various QKD protocols, including asymmetric MDI-QKD [40, 41] and twin-field QKD [42]. Despite these promising theoretical advancements, the practical implementation of decoy state QKD protocols presents substantial challenges. Determining the optimal intensities and proportions of signal and decoy states, while accounting for statistical fluctuations and experimental imperfections, is crucial for maximizing the performance of these protocols. Additionally, the integration of decoy state techniques into existing commercial QKD systems requires careful consideration of system parameters and the development of specialized hardware and software components.

This study addresses challenges in decoy state QKD protocols through extensive numerical simulations and experiments with a commercial QKD system. The former examines vacuum and one decoy state protocols in BB84 and SARG04 schemes, optimizing signal-to-decoy state ratios and intensities to enhance secure key generation rates and practical secure distances. By incorporating additional optical and electronic components, these protocols are experimentally validated across various transmission distances using standard telecom fiber. This work demonstrates the effectiveness of decoy state techniques in countering eavesdropping and advancing their practical application in secure quantum communication systems.

II. THE DECOY STATE METHOD

A. Protocol for the Vacuum State

In this step, Alice first turns off her photon source to perform a vacuum decoy state. Through this decoy state, Alice and Bob can estimate the background rate, $Q_0 = y_0$ and $E_{vacuum} = e_0 = \frac{1}{2}$. A simple decoy state protocol with only a vacuum state and a signal state will be presented. For the vacuum state protocol, the lower bound of the gain of single photon state is given by:

$$Q_1^{L,0,\mu} = e^{-\mu}\left[\hat{Q}_\mu e^{\mu} + \hat{Q}_0\right] \quad (1)$$

The upper bound of e_1 is given by:

$$e_1^{U,0,\mu} = \hat{E}_\mu\left(\frac{\hat{Q}_\mu}{Q_1^{L,0,\mu}}\right) \quad (2)$$

The lower bound of the gain of the two photon state is:

$$Q_2^{L,0,\mu} = e^{-\mu}\left(\hat{Q}_\mu e^{\mu} + \hat{Q}_0\right) \quad (3)$$

The upper bound of e_2 is:

$$e_2^{U,0,\mu} = \frac{1}{Q_2^{L,0,\mu}}\left(\hat{E}_\mu\hat{Q}_\mu - e_1^{U,0,\mu}Q_1^{L,0,\mu}\right) \quad (4)$$

B. Protocol for a Single Photon State

The goal of this protocol is to determine the lower bounds for the single-photon Q_1 and two-photon gain Q_2 and the upper bounds for the single-photon e_1 and two-photon e_2 Quantum Bit Error Rate (QBER). It is hypothesized that using only one decoy state is adequate for estimating these bounds. The focus of the analysis is on figuring out a method to leverage a single decoy state to estimate the stated bounds. The proposal is that Alice randomly varies the intensity of her pump light between 2 values (one decoy state and one signal state). Specifically, the intensity of one mode of the two-mode source is randomly changed between v_1 and μ, which satisfies the inequality $v_1 < \mu$, where v_1 represents the expected photon number of the decoy state and μ denotes the expected photon number of the signal state. The lower bound of the gain of the single photon state for one decoy state protocol is given by:

$$Q_1^{L,v_1,\mu} = \frac{\mu e^{-\mu}}{(\mu - v_1)}\left[\hat{Q}_\mu e^{\mu} - \hat{Q}_{v_1} e^{v_1} + \hat{Q}_0\right] \quad (5)$$

The upper bound of e_1 is given by:

$$e_1^{U,v_1,\mu} = \frac{\mu}{(\mu - v_1)Q_1^{L,v_1,\mu}e^{\mu}}\left[\hat{E}_\mu\hat{Q}_\mu e^{\mu} - \hat{E}_{v_1}\hat{Q}_{v_1} e^{v_1}\right] \quad (6)$$

The lower bound of the gain of the two photon state is:

$$Q_2^{L,\nu_1,\mu} = \frac{\mu^2 e^{-\mu}}{\left(\mu^2 - \nu_1^2\right)}\left(\hat{Q}_\mu e^\mu - \hat{Q}_{\nu_1} e^{\nu_1} + \left(\hat{Q}_0 + Q_1^{L,\nu_1,\mu}\right)\right) \quad (7)$$

The upper bound of e_2 is:

$$e_2^{U,\nu_1,\mu} = \frac{\mu^2}{(\mu^2 - \nu_1^2)Q_2^{L,\nu_1,\mu} e^\mu} \times \left(\hat{E}_\mu \hat{Q}_\mu e^\mu - \hat{E}_{\nu_1}\hat{Q}_{\nu_1} e^{\nu_1} - \left(\frac{\mu - \nu_1}{\mu}\right) e_1^{L,\nu_1,\mu} Q_1^{L,\nu_1,\mu} e^\mu\right) \quad (8)$$

in which:

$$\hat{Q}_\mu = Q_\mu\left(1 \pm \frac{\sigma}{\sqrt{N_\mu Q_\mu}}\right)$$

$$\hat{E}_\mu = E_\mu\left(1 \pm \frac{\sigma}{\sqrt{N_\mu E_\mu}}\right)$$

$$\hat{Q}_{\nu_1} = Q_{\nu_1}\left(1 \pm \frac{\sigma}{\sqrt{N_{\nu_1} Q_{\nu_1}}}\right) \quad (9)$$

$$\hat{E}_{\nu_1} = E_{\nu_1}\left(1 \pm \frac{\sigma}{\sqrt{N_\mu E_{\nu_1}}}\right)$$

$$\hat{Q}_0 = y_0\left(1 \pm \frac{\sigma}{\sqrt{N_0 y_0}}\right)$$

where $\hat{Q}_\mu, \hat{Q}_0, \hat{Q}_{\nu_1}$ are the gains of $\mu, 0, \nu_1$, respectively with statistical fluctuations. N_μ, N_0, N_{ν_1} are the numbers of pulses used as signal and decoy states ($\mu, 0, \nu_1$), and σ is the standard deviation.

After doing estimations for the lower bounds of Q_1 and Q_2, as well as the upper bounds of e_1 and e_2 for each decoy state protocol, the ensuing equation can be employed to compute the ultimate key generation rate of the proposed QKD system, encompassing both the BB84 and SARG04 protocols [4].

$$R_{BB84} \geq R_{BB84}^L = q\{-Q_\mu f(E_\mu) H_2(E_\mu) + Q_1^L[1 - H_2(e_1^U)]\} \quad (10)$$

$$R_{SARG04} \geq R_{SARG04}^L = -Q_\mu f(E_\mu) H_2(E_\mu) + Q_1^L[1 - H_2(e_1^U)] + Q_2^L[1 - H_2(e_2^U)] \quad (11)$$

where q is a factor related to the implementation (equal to 1/2 for the standard BB84 protocol since Alice and Bob use incompatible bases half the time, or approximately 1 for the efficient BB84 protocol [45]), $f(x)$ represents the bi-directional error correction efficiency as a function of error rate (normally $f(x) \geq 1$ with the Shannon limit $f(x) = 1$), and $H_2(x)$ is the binary Shannon information function given by $H_2(x) = -x \log_2(x) - (1 - x) \log_2(1 - x)$. Specifically, q accounts for the protocol being used, $f(x)$ models the efficiency of error correction, and $H_2(x)$ refers to the binary entropy function. The key generation rate R depends on these factors as well as the observed gain and QBER.

C. Numerical Simulatios

Numerical simulations were performed to find the optimal experimental parameters and the required distance for implementing a specific decoy state protocol. The underlying principle of numerical simulation is the ability to replicate the performance of a QKD system by accurately modeling the expected gains and QBERs for all potential states. This can be achieved by knowing the intensities and proportions of the signal and decoy states utilized. This simulation step is crucial within the experimental context. This analysis evaluates the gains obtained from the signal and decoy states ($\hat{Q}_0, \hat{Q}_\mu, \hat{Q}_{\nu_1}$, $\hat{Q}_{\nu 2}$) as well as the overall QBERs associated with those states ($\hat{E}_\mu$, $\hat{E}_{\nu 1}$, $\hat{E}_{\nu_2}$). Then, the lower bound gains for single-photon and two-photon events, along with the upper bound QBERs for single-photon and two-photon pulses are determined. The obtained values are finally substituted into (10) and (11) to derive a lower bound for the key generation rate of both the BB84 and SARG04 protocols.

The decoy state mechanism employed in the present study aims to simulate the functionality of an optical fiber-based QKD system, specifically for the SARG04 and BB84 protocols. The calculation of losses in the quantum channel can be performed by utilizing the loss coefficient α (dB/km), in conjunction with the length of the fiber l (km). The expression for the channel transmittance can be represented as $\eta_{AB} = 10^{-\frac{\alpha l}{10}}$, where the total transmission between Alice and Bob is denoted by $\eta = \eta_{Bob}\eta_{AB}$, with loss coefficient $\alpha = 0.21$ dB/km in the performed experimental configuration, and η_{Bob} corresponds to the transmittance on Bob's side. The intrinsic parameters of the ID-3000 commercial QKD system, as specified in its data sheet, include the detection efficiency $\eta = 4.5 \times 10^{-2}$, the detectors' dark count rate ($y_0 = 5 \times 10^{-5}$), the probability of a photon hitting an erroneous detector ($e_{detector}$ = 0.01), the wavelength (λ = 1550 nm), the repetition rate of 5 MHz, and the total number of pulses sent by Alice (N = 100Mbit). In order to attain an optimal key generation rate and the greatest secure distance, optimal parameters are sought through the implementation of numerical simulations. The mean photon numbers of the signal state and decoy states, denoted as μ, ν_1, and ν_2, respectively, are systematically adjusted within the interval [0, 1] with an increment of 0.001. A comparable approach is employed to modify the proportion of each state.

The simulation results presented in Figure 1 illustrate the relationship between the key generation rate and the distance of the fiber link for different decoy state protocols. The provided figure depicts the outcomes acquired through the utilization of the inherent characteristics of the ID-3000 commercial QKD system. Curve (a) portrays the optimal rate at which secure

keys can be generated using the SARG04 protocol in the absence of decoy states. Curve (b) depicts the optimal rate of secure key generation for the BB84 protocol while employing decoy states, with a specified value of μ equal to 0.48 as determined by the method outlined in [46]. Curves (c) and (d) exhibit the secure key generation rate achieved by the vacuum state protocol for the BB84 and SARG04 protocols, respectively. The secure key generation rate of the one decoy state protocol for both the BB84 and SARG04 protocols is depicted by curves (e) and (f), accordingly. The comparison reveals that the utilization of the recommended method in fiber-based QKD systems for BB84 and SARG04 protocols yields superior results in terms of secret key rate and secure distance compared to previous methods. The analysis of these curves further suggests that the fiber-based QKD system, deploying the proposed method for the SARG04 protocol, achieves a superior secret key rate and a larger secure distance in comparison to the BB84 protocol. This implies that the contribution of the two-photon component is of utmost importance in determining the rate of key generation over all distances. Through the implementation of the suggested decoy state technique, it is possible to attain an elevated rate of key generation as well as an extended secure distance.

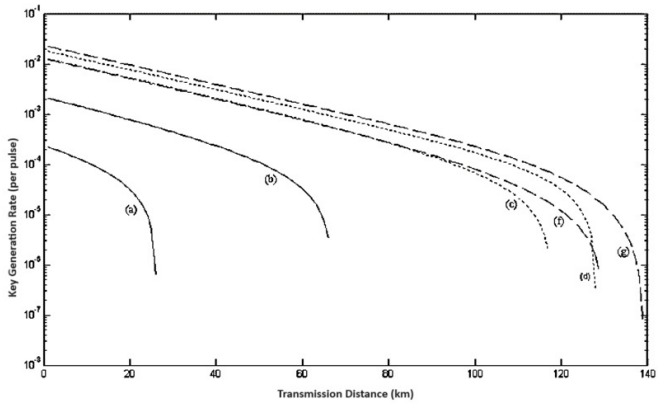

Fig. 1. Relationship between the key generation rate and the distance of the fiber link for different decoy state protocols.

III. EXPERIMENTAL SETUP

In order to implement the decoy state protocols, the system incorporates further optical and electronic elements. These additions facilitate the random attenuation of each signal to match the intensity of either the signal state, weak decoy, or vacuum state. The process of attenuation is achieved through the utilization of a Variable Optical Attenuator (VOA) located on Alice's side. It is imperative for the VOA to possess polarization-independent characteristics to ensure an equal attenuation of both pulses. The experiment deploys an Intensity Modulator (IM) to dynamically attenuate signals.

Numerical simulation plays a crucial role in the determination of ideal experimental parameters and the necessary distance for implementing a specific decoy protocol. The simulation incorporates the intensities, signal and decoy state percentages, and calculates the gains and QBERs for all states. The outcomes of the simulation are implemented in the computation of the lower bound for the gains of single and two-photon signals, the upper bound for QBER of single and two-photon pulses, and eventually, the lower bound for the rate of generating cryptographic keys in both the BB84 and SARG04 protocols.

The prototype of the QKD system is detailed in [47]. A brief explanation follows: The key is encoded within the phase difference of two pulses that propagate from Bob to Alice and then return. The system seen in Figure 2 is commonly known as a plug and play self-compensating configuration. Bob produces a high-intensity laser pulse with a wavelength of 1550 nm. This pulse is divided equally into two beams using a Beam Splitter (BS), with one beam traveling through a short arm containing a phase modulator, and the other beam passing through a long arm with a Delay Line (DL) of 50 ns.

All fiber optics and components utilized at Bob have been designed specifically to effectively preserve polarization. The short arm induces a 90-degree change in linear polarization, resulting in both pulses exiting Bob's Polarizing Beam Splitter (PBS) through the same port. The pulses are subsequently transmitted to Alice, where they undergo reflection, attenuation, and are subsequently returned as beams with orthogonal polarization by the use of a Faraday mirror. At the location known as Bob, the two pulses experience a reversal in direction and proceed to return to the originating point, referred to as BS. At this point, the pulses interact with each other, leading to interference. Subsequently, the pulses pass via a circulator denoted as C1, and are ultimately detected either at D1 or D2. Due to the fact that the two pulses traverse an identical path in reverse within Bob, the interferometer exhibits self-compensation.

In order to implement the Vacuum State Protocol and the One Decoy State Protocol, the pulse amplitudes are adjusted to two distinct levels: μ, *0* and μ, v_1, respectively. Generating a genuine "vacuum" state poses a significant challenge for high-speed amplitude modulators, mostly attributable to their constrained resolution capabilities. Nevertheless, if the magnitude of the "vacuum" state's gain is in proximity, within a few standard deviations, to the dark count rate, it can be deemed an acceptable approximation.

In the implemented system, Alice employs a Variable Optical Attenuator (VOA) to decrease the strength of the pulses. Figure 2 presents a schematic depiction of the optical and electrical constituents of the introduced system. The decoy state experiment conducted in this study utilizes a commercially available QKD system manufactured by id Quantique SA. The experimental setup consists of two components, namely Bob and Jr. Alice. In the conducted experiment, the term "Alice" denotes the system employed by the sender, encompassing Jr. Alice as well as supplementary optical and electronic components integrated by the authors. To implement the decoy state method, a decoy Intensity Modulator (IM) was positioned in front of Jr. Alice, denoted as DA in Figure 2. The modulator is designed to provide optimal transmission when it is in its idle state. When Bob transmits a frame, the decoy IM is in idle state. The classical detector is responsible for detecting the initial pulse subsequent to its transmission through coupler C2. This detection event prompts

the generation of a synchronization signal, which in turn triggers the Decoy Generator (DG). Upon triggering, the DG depicted in Figure 2 undergoes a delay period prior to emitting the modulation voltages. These voltages serve the purpose of dynamically modifying the intensity of the NP signals, aligning them with either the signal state or the decoy state as dictated by the Decoy Profile. The Decoy Profile is prepared in advance of the experiment and thereafter transferred from a computer to the DG in the form of an arbitrary waveform. In order to generate the Decoy Profile, a sequence of integers is generated $\{1 \le n_i \le 100\}$, with each integer representing the number of pulses contained within a frame. According to the optimal pulse distribution, a subset of the integers is designated as signal states, while the remaining integers are designated as decoy states. In the conducted experiment, Bob produces a sequence of NP pulses, where NP represents the numerical value of 624, and subsequently transmits this sequence to Alice. The temporal duration separating signals inside a frame is 200 ns. The subsequent frame is not produced until the entirety of the preceding frame has been returned to Bob. In an attempt to prevent Rayleigh scattering, the implementation of a lengthy delay line inside the communication system of Jr. Alice is employed to ensure the avoidance of signal overlap in the channel between Bob and Jr. Alice.

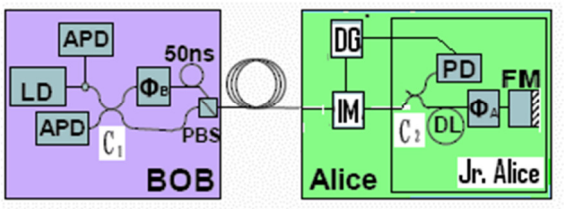

Fig. 2. Experimental setup.

IV. RESULTS AND DISCUSSION

Numerical simulations were conducted in order to determine the best settings. In the context of the vacuum state protocol, it is established that a specific value is assigned to μ = 0.85. The number of pulses employed to represent the signal state and vacuum state are denoted as N_μ=0.95 N and N_0=0.05 N, respectively. In the one decoy state protocol, the values of μ = 0.85 and v_1 = 0.05 are set. The numbers representing the signal state, the weak decoy state, and the total number of pulses (N = 100 Mbit) emitted by Alice in this experiment are $N_\mu = 0.95$ N and $N_{v_1} = 0.05$ N, accordingly. Alice transmitted the distribution of decoy states and base information to Bob subsequent to the transmission of all N signals. Bob subsequently proceeded to delineate the signals he had received on a correct basis. It is assumed that Alice and Bob have disclosed the measurement outcomes of all decoy states, as well as a subset of the signal states. The experimental results of the implementation of the vacuum state and one decoy state protocols in the QKD system have been documented and are illustrated in Figures 3-5. The provided figures display the variations in the gain and QBER of the signal state inside the vacuum state protocol, specifically for the BB84 and SARG04 protocols. These variations are observed as the transmission distance is progressively increased, as depicted in Figures 3 and 4. The findings of the gain and QBER for both the signal and decoy states in the SARG04 protocol are portrayed in Figure 5, demonstrating the variations as the transmission distance is extended. The data indicates that with an increase in the transmission distance, there is a simultaneous decrease in the gain of the signal and decoy states. Additionally, the QBER of the signal and the decoy states also experiences a decrease. The findings suggest that the utilization of both the vacuum state and one decoy state protocols has successfully attained low QBERs for the signal state over distances ranging from 10 to 50 km. The obtained signal gains were observed to be greater in magnitude compared to the gains associated with the decoy state. Additionally, the signal QBERs were discovered to be lower in magnitude compared to the QBERs of the decoy state.

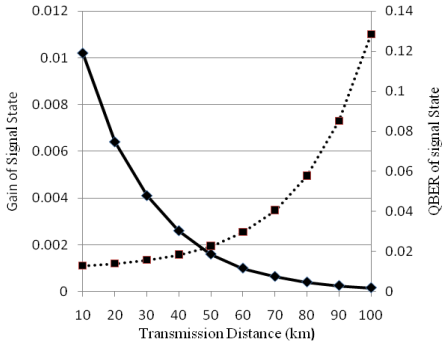

Fig. 3. The experimental results of the vacuum state for BB84 versus transmission distance. The solid line illustrates the gain of the signal state. The dotted line represents the QBER of the signal state.

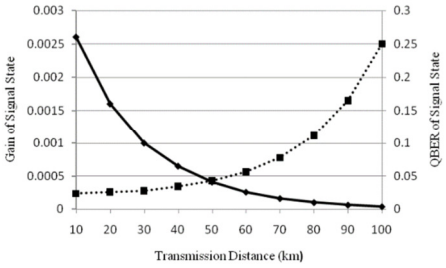

Fig. 4. The experimental findings of the vacuum state for SARG04 versus transmission distance. The solid line illustrates the gain of the signal state. The dotted line represents the QBER of the signal state.

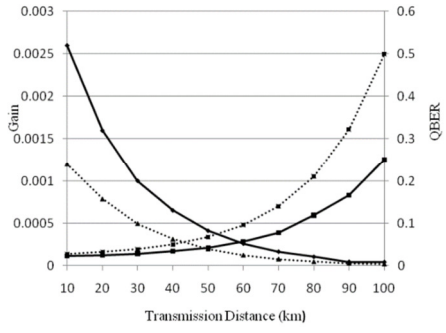

Fig. 5. The experimental findings of one SARG04 decoy state versus transmission distance. The solid line depicts the signal state's gain and QBER. The dotted line depicts the decoy state's gain and QBER.

Based on the presented experimental results, Alice and Bob have successfully determined the lower bound of gain achievable for single-photon and two-photon states. Additionally, they have identified the upper bound of the QBER for both single-photon and two-photon pulses. Furthermore, they have evaluated the lower bound rate of key generation for both BB84 and SARG04 protocols. In order to regulate the influence of Eve in a PNS assault scenario, the calculation of the ratio between the gain of the decoy state and the gain of the signal state is performed. An anticipated gain ratio for decoy states to achieve for signal states is expected for every transmission distance. The presence of a substantial departure from the anticipated value in the measured ratio serves as an indication of a potential attack on the peripheral nervous system (PNS) by an adversary named Eve. Figures 6 and 7 manifest the efficacy of the vacuum state and one decoy state protocols in managing the presence of Eve (PNS) in both the BB84 and SARG04 cryptographic schemes.

Figure 5 displays the theoretical ratio $\left(y_0 / Q_\mu\right)$ (solid line (a)) and the maximum fluctuation ratio $\left(y_0 / Q_\mu\right)$ (line (b)) for the vacuum state protocol (SARG04) at each distance. The same figure also showcases the theoretical ratio for the vacuum state protocol (BB84) (line (b)) and the maximum fluctuation ratio for the same protocol (dotted line (c)) at each distance. Figure 6 presents the secure areas of the vacuum state protocol for both BB84 and SARG04. The green area is the secure range of the vacuum state protocol for SARG04 while the blue area represents the secure range of the same protocol for BB84. This implies that when the ratio is less than expected, no secure bit rate is achievable, emphasizing the cost of privacy amplification to eliminate the information leaked by the PNS attack. Figure 7 discloses two secure regions from Eve's (PNS attack) perspective in the one decoy state protocol. The green region symbolizes the secure area of the one decoy state protocol for BB84, while the green and blue regions depict the secure area of the one decoy state protocol for SARG04. Both the vacuum state and the one decoy state protocols demonstrate that the secure region for SARG04 is larger than the one for BB84. As noticed in Figures 8 and 9, the maximum deviation between the decoy state gain and signal state gain increases with increasing transmission distance, in both vacuum protocols.

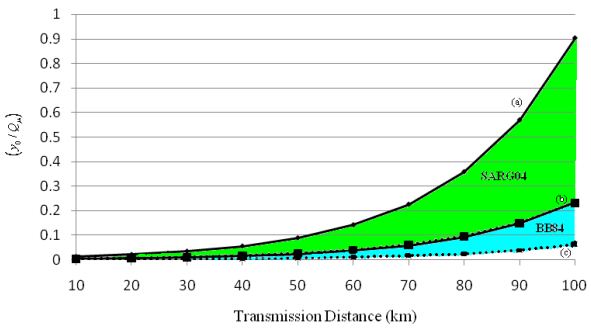

Fig. 6. The ratio y_0 / Q_μ of vacuum state protocol against transmission distance.

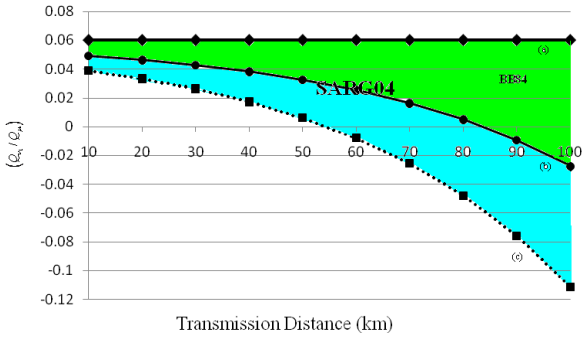

Fig. 7. The ratio Q_{ν_1} / Q_μ of a single decoy state protocol to the transmission distance. The (a) solid line represents the theoretical Q_{ν_1} / Q_μ ratio of a single decoy state protocol for both BB84 and SARG04. The (b) solid line illustrates the maximum fluctuation ratio Q_{ν_1} / Q_μ of a single decoy state protocol for BB84. The (c) dotted line depicts the maximum fluctuation ratio Q_{ν_1} / Q_μ of a single decoy state protocol for SARG04.

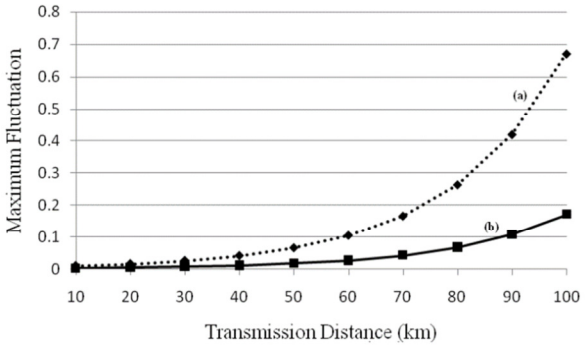

Fig. 8. Maximum fluctuation of the ratio y_0 / Q_μ for vacuum state protocol versus the transmission distance for: (a) SARG04, (b) BB84.

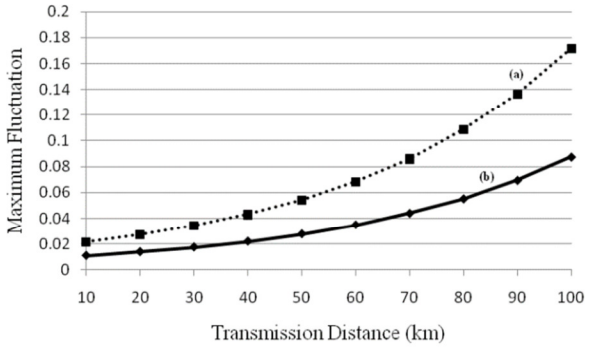

Fig. 9. Maximum fluctuation of the ratio Q_{ν_1} / Q_μ for one decoy state protocol versus the transmission distance at each distance for: (a) SARG04, (b) BB84.

Figure 10 presents the experimental results for the quantum key generation rate as a function of fiber link distance using different decoy state methods. Curve (a) shows the maximum theoretically achievable secure key rate for SARG04 without decoy states. Following the approach from reference [46], curve (b) gives the optimal key rate for BB84 without decoy

states at μ = 0.48. Curves (c) and (d) present the secure key rates obtained with the recommended vacuum state technique applied to BB84 and SARG04, respectively. Similarly, curves (e) and (f) display the secure key rates attained with the suggested one decoy state method on BB84 and SARG04. The experimental results match the simulations well. As expected, the key rate decays with an increasing transmission distance. Compared to previous approaches, the results disclose that fiber-based QKD systems, leveraging the method proposed for BB84 and SARG04, produce higher secret key rates and longer secure distances. Additionally, SARG04 outperforms BB84 in terms of secret key rate and secure distance, indicating two-photon signals which contribute to key generation at all distances. Applying the introduced decoy state approach further enhances the key rate and distance.

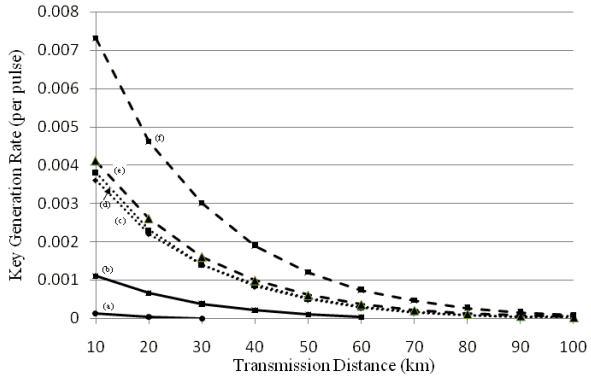

Fig. 10. Experimental results for the quantum key generation rate as a function of fiber link distance using different decoy state methods. (a) SARG04 without decoy states, (b) BB84 with decoy states at μ = 0.48, (c) SARG04-vacuum state, (d) BB84- vacuum state, (e) BB84 one decoy state, (f) SARG04-one decoy state.

V. CONCLUSION

In summary, this study investigates the optimization of Quantum Key Distribution (QKD) protocols using decoy state techniques. The research focused on developing and validating efficient decoy state protocols to enhance secure key generation rates and communication distances, addressing the limitations and vulnerabilities of the current QKD systems. Through rigorous numerical simulations, optimal signal-to-decoy state ratios and intensities for the BB84 and SARG04 protocols were determined, predicting maximum secure key rates of 1.2×10^5 bits/s for SARG04 and 8.5×10^4 bits/s for BB84 at 10 km, with secure distances of 45 km and 35 km, respectively. These predictions were experimentally validated, aligning closely with the simulated outcomes. The proposed decoy state strategy showed a 30% increase in the secret key rate and a 20% extension in secure distance compared to non-decoy methods. The SARG04 protocol outperformed BB84, highlighting the importance of the two-photon component in key generation. The successful implementation of decoy state techniques facilitates practical applications in secure quantum communication, enabling robust and efficient QKD networks with improved security and extended transmission distances. This work suggests future research directions, including integrating additional decoy states and advanced photon sources to further optimize decoy state QKD protocols and advance quantum cryptography.

ACKNOWLEDGEMENT

This study was funded by the Ministry of Higher Education and Scientific Research, Algeria (Grant Reference Number A10N01UN110120230001). We extend our sincere gratitude to our Research Laboratory for their invaluable assistance in facilitating a portion of this work.

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, Dec. 1984, pp. 175–179.

[2] H. Inamori, N. Lutkenhaus, and D. Mayers, "Unconditional security of practical quantum key distribution," *The European Physical Journal D*, vol. 41, no. 3, pp. 599–627, Mar. 2007, https://doi.org/10.1140/epjd/e2007-00010-4.

[3] B. Huttner, N. Imoto, N. Gisin, and T. Mor, "Quantum cryptography with coherent states," *Physical Review A*, vol. 51, no. 3, pp. 1863–1869, Mar. 1995, https://doi.org/10.1103/PhysRevA.51.1863.

[4] W.-Y. Hwang, "Quantum Key Distribution with High Loss: Toward Global Secure Communication," *Physical Review Letters*, vol. 91, no. 5, Aug. 2003, Art. no. 057901, https://doi.org/10.1103/PhysRevLett.91.057901.

[5] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," *Quantum Information & Computation*, vol. 4, no. 5, pp. 325–360, 2004, https://doi.org/10.26421/QIC4.5-1.

[6] H.-K. Lo, X. Ma, and K. Chen, "Decoy State Quantum Key Distribution," *Physical Review Letters*, vol. 94, no. 23, Jun. 2005, Art. no. 230504, https://doi.org/10.1103/PhysRevLett.94.230504.

[7] X.-B. Wang, "Decoy-state protocol for quantum cryptography with four different intensities of coherent light," *Physical Review A*, vol. 72, no. 1, Jul. 2005, Art. no. 012322, https://doi.org/10.1103/PhysRevA.72.012322.

[8] X.-B. Wang, "Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography," *Physical Review Letters*, vol. 94, no. 23, Jun. 2005, Art. no. 230503, https://doi.org/10.1103/PhysRevLett.94.230503.

[9] Q. Cai and Y. Tan, "Photon-number-resolving decoy-state quantum key distribution," *Physical Review A*, vol. 73, no. 3, Mar. 2006, Art. no. 032305, https://doi.org/10.1103/PhysRevA.73.032305.

[10] T. Horikiri and T. Kobayashi, "Decoy state quantum key distribution with a photon number resolved heralded single photon source," *Physical Review A*, vol. 73, no. 3, Mar. 2006, Art. no. 032331, https://doi.org/10.1103/PhysRevA.73.032331.

[11] Q. Wang *et al.*, "Experimental Decoy-State Quantum Key Distribution with a Sub-Poissionian Heralded Single-Photon Source," *Physical Review Letters*, vol. 100, no. 9, Mar. 2008, Art. no. 090501, https://doi.org/10.1103/PhysRevLett.100.090501.

[12] M. Bortz and J. Stolze, "Exact dynamics in the inhomogeneous central-spin model," *Physical Review B*, vol. 76, no. 1, Jul. 2007, Art. no. 014304, https://doi.org/10.1103/PhysRevB.76.014304.

[13] X.-B. Wang, C.-Z. Peng, and J.-W. Pan, "Simple protocol for secure decoy-state quantum key distribution with a loosely controlled source," *Applied Physics Letters*, vol. 90, no. 3, Jan. 2007, Art. no. 031110, https://doi.org/10.1063/1.2431718.

[14] X. B. Wang, "Secure and efficient decoy-state quantum key distribution with inexact pulse intensities," *Physical Review A*, vol. 75, no. 5, May 2007, Art. no. 052301, https://doi.org/10.1103/PhysRevA.75.052301.

[15] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, "Experimental Quantum Key Distribution with Decoy States," *Physical Review Letters*, vol. 96, no. 7, Feb. 2006, Art. no. 070502, https://doi.org/10.1103/PhysRevLett.96.070502.

[16] T. Schmitt-Manderbach *et al.*, "Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km," *Physical Review Letters*, vol. 98, no. 1, Jan. 2007, Art. no. 010504, https://doi.org/10.1103/PhysRevLett.98.010504.

[17] A. Boaron *et al.*, "Secure Quantum Key Distribution over 421 km of Optical Fiber," *Physical Review Letters*, vol. 121, no. 19, Nov. 2018, Art. no. 190502, https://doi.org/10.1103/PhysRevLett.121.190502.

[18] S. Ali and M. R. B. Wahiddin, "Fiber and free-space practical decoy state QKD for both BB84 and SARG04 protocols," *The European Physical Journal D*, vol. 60, no. 2, pp. 405–410, Nov. 2010, https://doi.org/10.1140/epjd/e2010-00214-5.

[19] S. Ali, S. Mohammed, M. S. H. Chowdhury, and A. A. Hasan, "Practical SARG04 quantum key distribution," *Optical and Quantum Electronics*, vol. 44, no. 10, pp. 471–482, Sep. 2012, https://doi.org/10.1007/s11082-012-9571-2.

[20] S. Ali, O. Mahmoud, and R. A. Saeed, "Estimation of decoy state parameters for practical QKD," *Australian Journal of Basic and Applied Sciences*, vol. 5, no. 6, pp. 430–439, Jun. 2011.

[21] J. Teng *et al.*, "Twin-field quantum key distribution with passive-decoy state," *New Journal of Physics*, vol. 22, no. 10, Jul. 2020, Art. no. 103017, https://doi.org/10.1088/1367-2630/abbab7.

[22] B. Djaouida and S. Ali, "Theoretical and simulation investigation of practical QKD for both BB84 and SARG04 protocols," *International Journal of Quantum Information*, Dec. 2023, Art. no. 2350050, https://doi.org/10.1142/S0219749923500508.

[23] Z. Yuan *et al.*, "10-Mb/s Quantum Key Distribution," *Journal of Lightwave Technology*, vol. 36, no. 16, pp. 3427–3433, Aug. 2018.

[24] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, "Twin-field quantum key distribution with large misalignment error," *Physical Review A*, vol. 98, no. 6, Dec. 2018, Art. no. 062323, https://doi.org/10.1103/PhysRevA.98.062323.

[25] S.-K. Liao *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, Sep. 2017, https://doi.org/10.1038/nature23655.

[26] S. Wang *et al.*, "Field and long-term demonstration of a wide area quantum key distribution network," *Optics Express*, vol. 22, no. 18, pp. 21739–21756, Sep. 2014, https://doi.org/10.1364/OE.22.021739.

[27] J. F. Dynes *et al.*, "Cambridge quantum network," *npj Quantum Information*, vol. 5, no. 1, Nov. 2019, Art. no. 101, https://doi.org/10.1038/s41534-019-0221-4.

[28] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, no. 7705, pp. 400–403, May 2018, https://doi.org/10.1038/s41586-018-0066-6.

[29] X. Ma, P. Zeng, and H. Zhou, "Phase-Matching Quantum Key Distribution," *Physical Review X*, vol. 8, no. 3, Aug. 2018, Art. no. 031043, https://doi.org/10.1103/PhysRevX.8.031043.

[30] X.-T. Fang *et al.*, "Implementation of quantum key distribution surpassing the linear rate-transmittance bound," *Nature Photonics*, vol. 14, no. 7, pp. 422–425, Jul. 2020, https://doi.org/10.1038/s41566-020-0599-8.

[31] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, "Proof-of-Principle Experimental Demonstration of Twin-Field Type Quantum Key Distribution," *Physical Review Letters*, vol. 123, no. 10, Sep. 2019, Art. no. 100506, https://doi.org/10.1103/PhysRevLett.123.100506.

[32] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, "Experimental Demonstration of Polarization Encoding Measurement-Device-Independent Quantum Key Distribution," *Physical Review Letters*, vol. 112, no. 19, May 2014, Art. no. 190503, https://doi.org/10.1103/PhysRevLett.112.190503.

[33] K. Wei *et al.*, "High-Speed Measurement-Device-Independent Quantum Key Distribution with Integrated Silicon Photonics," *Physical Review X*, vol. 10, no. 3, Aug. 2020, Art. no. 031030, https://doi.org/10.1103/PhysRevX.10.031030.

[34] D. Rusca, A. Boaron, F. Grunenfelder, A. Martin, and H. Zbinden, "Finite-key analysis for the 1-decoy state QKD protocol," *Applied Physics Letters*, vol. 112, no. 17, Apr. 2018, Art. no. 171104, https://doi.org/10.1063/1.5023340.

[35] M. A. A. Humayun, M. A. Rashid, A. Kuwana, and H. Kobayashi, "Improvement of Absorption and Emission Phenomena of 1.55µm Quantum Dot Laser using Indium Nitride," *Engineering, Technology & Applied Science Research*, vol. 13, no. 1, pp. 10134–10139, Feb. 2023, https://doi.org/10.48084/etasr.5512.

[36] B. B. Yousif and E. E. Elsayed, "Performance Enhancement of an Orbital-Angular-Momentum-Multiplexed Free-Space Optical Link Under Atmospheric Turbulence Effects Using Spatial-Mode Multiplexing and Hybrid Diversity Based on Adaptive MIMO Equalization," *IEEE Access*, vol. 7, pp. 84401–84412, Jan. 2019, https://doi.org/10.1109/ACCESS.2019.2924531.

[37] E. E. Elsayed and B. B. Yousif, "Performance evaluation and enhancement of the modified OOK based IM/DD techniques for hybrid fiber/FSO communication over WDM-PON systems," *Optical and Quantum Electronics*, vol. 52, no. 9, Aug. 2020, Art. no. 385, https://doi.org/10.1007/s11082-020-02497-0.

[38] E. E. Elsayed, A. G. Alharbi, M. Singh, and A. Grover, "Investigations on wavelength-division multiplexed fibre/FSO PON system employing DPPM scheme," *Optical and Quantum Electronics*, vol. 54, no. 6, May 2022, Art. no. 358, https://doi.org/10.1007/s11082-022-03717-5.

[39] F. Xu, H. Xu, and H.-K. Lo, "Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution," *Physical Review A*, vol. 89, no. 5, May 2014, Art. no. 052333, https://doi.org/10.1103/PhysRevA.89.052333.

[40] X.-L. Hu, Y. Cao, Z.-W. Yu, and X.-B. Wang, "Measurement-Device-Independent Quantum Key Distribution over asymmetric channel and unstable channel," *Scientific Reports*, vol. 8, no. 1, Dec. 2018, Art. no. 17634, https://doi.org/10.1038/s41598-018-35507-z.

[41] W. Wang, F. Xu, and H.-K. Lo, "Asymmetric Protocols for Scalable High-Rate Measurement-Device-Independent Quantum Key Distribution Networks," *Physical Review X*, vol. 9, no. 4, Oct. 2019, Art. no. 041012, https://doi.org/10.1103/PhysRevX.9.041012.

[42] W. Wang and H.-K. Lo, "Simple method for asymmetric twin-field quantum key distribution," *New Journal of Physics*, vol. 22, no. 1, Jan. 2020, Art. no. 013020, https://doi.org/10.1088/1367-2630/ab623a.

[43] T.-T. Nguyen, N.-Q. Luc, and T. T. Dao, "Developing Secure Messaging Software using Post-Quantum Cryptography," *Engineering, Technology & Applied Science Research*, vol. 13, no. 6, pp. 12440–12445, Dec. 2023, https://doi.org/10.48084/etasr.6549.

[44] N. Q. Luc, T. T. Nguyen, D. H. Quach, T. T. Dao, and N. T. Pham, "Building Applications and Developing Digital Signature Devices based on the Falcon Post-Quantum Digital Signature Scheme," *Engineering, Technology & Applied Science Research*, vol. 13, no. 2, pp. 10401–10406, Apr. 2023, https://doi.org/10.48084/etasr.5674.

[45] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security," *Journal of Cryptology*, vol. 18, no. 2, pp. 133–165, Apr. 2005, https://doi.org/10.1007/s00145-004-0142-y.

[46] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Physical Review A*, vol. 72, no. 1, Jul. 2005, Art. no. 012326, https://doi.org/10.1103/PhysRevA.72.012326.

[47] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug&play system," *New Journal of Physics*, vol. 4, no. 1, Apr. 2002, Art. no. 41, https://doi.org/10.1088/1367-2630/4/1/341.