Quantum Key Distribution Random Access Network

Yao Zhang, Qiang Ni
{y.zhang70, q.ni}@lancaster.ac.uk
School of Computing and Communications
InfoLab 21, Lancaster University
LA1 4WA, Lancaster, United Kingdom

***Abstract*—This paper proposes a possible application of quantum key distribution in multi-user network. In modern networks, variety of multiple access technologies are being used for multi-user access purposes. In this paper, we focus on a type of widely used MAC (Media Access Control) protocol—CSMA/CA, and analyse its use for the quantum key distribution in the network. This work is based on a successful experiment that implemented the quantum key distribution over 200 km by using the decoy-state method. The secret key generation rate as the main indicator of the performance is given, including the relationship between it and the number of stations in the network, and the relationship between the key generation rate and the transmission distance under the multiple access condition as well.**

***Index Terms*—Quantum key distribution, random access, CSMA/CA.**

I. Introduction

Quantum key distribution (QKD) is a method of key distribution that is able to provide the absolute security in communications, and it has already been developed for decades of years. Since the first quantum key distribution was proposed by Bennett and Brassard in 1984 (which is known as BB84 protocol) [1], several different quantum key distribution protocols had come up in last years. Some of them are based on the mode of quantum comparing and mearsuring, such as the well known BB84 protocol, while some are based on the entanglement of quantum pairs, such as the E91 protocol [2] and BBM92 protocol [3]. All of these protocols are proved that the quantum key distribution based on principles of quantum mechanics is theoretically secure [4], [5]. However, due to imperfect devices in the QKD's implementation, there still can be some kinds of attack in this process. For instance, photon-number splitting (PNS) attacks, which use the leaked photon sent by the transmitter to intercept the information [6]. For overcoming this issue, some of modified protocols are addressed. Here, we focus on an experiment that successfully implemented the secure quantum key distribution over 200 km by using one of the modified QKD protocol—decoy state quantum key distribution, and we propose and design a potential multiple users access network.

Our main contribution in this paper is to design a multi-user QKD network using CSMA/CA protocol. In addition, we analyse its performance by utilising Markov chain mathematical model and the decoy state QKD method. The relationship between the key generation rate, number of stations and transmission distance are obtained and demonstrated for the multiple access condition.

The rest of this paper is organised as follows. In section II, we review the original BB84 protocol and the decoy state protocol, which is used in real experiments. In section III, a communication protocol designed for random access is reviewed. It is used for the combination of our quantum key distribution and classical networks. In section IV, we analyse the suggested QKD network and two relations that related to the secret key generation rate are given. Finally, the conclusion is given in section V.

II. Decoy state quantum key distribution

The original BB84 protocol is the first quantum key distribution protocol. It was proposed by Bennett and Brassard in 1984 [1]. The main idea of BB84 protocol can be described as follows:

1. The transmitter (Alice) generates a quantum bit (qubit) from 4 types of photon polarisation (vertical, horizontal, 45 degree and -45 degree) randomly and sends it to the receiver (Bob), then the state of the qubit has been determined.
2. Bob receives the qubit and measures this qubit that Alice sent to him by using two types of measuring basis (vertical-horizontal and 45/-45 degree) randomly to decode the qubit. Since Bob's measuring basis is chosen randomly, there is half chance to use the wrong basis. It is obvious that there must be some incorrect measurements. The incorrect rate can be calculated as $50\%(wrong\ basis) * 50\%(correct\ rate\ in\ wrong\ basis) = 25\%$.
3. Bob feeds back to Alice what type of measuring basis he used for each encoded qubit via the public channel which is the classical channel and can be eavesdropped by the eavesdropper (Eve). Then, according to this public information, Alice is able to know which bases are right and which are wrong from comparing with her own polarisation of photons she just sent.
4. Finally, Alice tells Bob which results of wrong basis need to be discarded via the public channel. The remained results Bob measured are the final sifted results. These two remained sequences are all the same in both Alice's and Bob's sides, and the same sequence is the generated secret key.

According to the description above, it is clear that even though Eve intercepts all the information from the public channel, she needs to eavesdrop the quantum channel as well to get the whole information restored. However, if she did so, the state of the transmitted photon would be destroyed and this would result in that the error rate increases rapidly and becomes much higher than the threshold, so that legal users in the communication are able to perceive its existance. Thus, benefitting from the no-cloning theorem of quantum mechanics, the BB84 protocal can build an absolutely secure communication system theoretically.

In contrast with the principle's simplicity, the implementation of QKD in real-life is really difficult. Since the BB84 protocol requires exact single-photon as the quantum source, it can hardly achieve this requirement due to devices' imperfection. Obviously, single photon cannot be splitted, but if the light that sent by the quantum source contains more than one photon, it is quite possible to make PNS attacks. That is, the eavesdropper can intercept one of photons in the light and make the rest of photons pass to the receiver. Due to the high loss of the channel, the eavesdropper may not be found by pretending that the lost photon is annihilated by the channel. This description is detailed in [6].

Although there exists a lower bound of the key generation rate to make sure the QKD's security in the environment with small imperfections [7], a modified protocol using decoy state provides better performance. The decoy state method was originally addressed in 2003 [6], and more detailed analyses are in [8]–[10]. The basic idea of the decoy state method is illustrated as follows. Insert the decoy state pulse into the signal pulse sequence randomly and send it to the receiver. The average numbers of the photon in the decoy state pulse and the signal pulse are different. Thus the counting rates (also called "yield" in some papers [8]) of single-photon pulses and multi-photon pulses must be quite different. Because of these two kinds of pulses are the same except the number of photons, Eve cannot distinguish the pulse she intercepted if it is the signal state or the decoy state. After the quantum communication processing, whether there exists the PNS attack can be detected by comparing counting rates of these two different pulses.

From the analysis of the decoy state method, the secure key generation rate is given by [8]:

$$R \geq q\{-Q_\mu f(E_\mu)H_2(E_\mu) + Q_1[1 - H_2(e_1)]\}, \qquad (1)$$

where μ represents the average number of photons in a pulse, q is a factor that represents the protocol's efficiency, for example, for BB84 protocol, this factor is 0.5 because of there is 50% chance that Alice and Bob use different measuring bases. Q_μ is the ratio of the number signal state detections to the total number of sent signal state pulses, which is also called the gain of the signal state. In addition, Q_1 is the gain of single-photon pulses, e_1 is the error rate associated with single-photon pulses, E_μ is signal state quantum bit error (QBER), H_2 is the binary Shannon entropy which is given by $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$, and $f(E_\mu)$ is another factor that represents the error correction efficiency which is usually determined by the specific experiment [8], [9].

III. Random Access Network

In data communication networks, there is a widely used method to access the shared channel for multiple users, which is associated with random access protocols. For instance, in the 802.11 standard, it adopts a fundamental mechanism called distributed coordination function (DCF) to access the medium. This is a random access scheme and based on the carrier sense multiple access with collision avoidance (CSMA/CA) protocol [11]. The CSMA/CA protocol is designed for the wireless local area network (WLAN), but the basic mechanism is really able to be used on all types of shared channels. In this paper, we use this medium access control (MAC) protocol for reference to analyse the performance of the multi-access QKD network.

Collisions that come from more than one signals sent by different stations at the same time cannot be detected on wireless network. Thus, the CSMA/CA protocol is right for this kind of networks (collisions cannot be detected). The completed and detailed information of the CSMA/CA protocol can be found in 802.11 standards. Here in this paper, we just focus on the performance analysis.

In data communications, one of the most significant indicators of the performance is the throughput. However, in our work, only the collision probability is expected. A valuable saturation throughput analysis is given in [11]. In this throughput analysis, the probability that a station transmits in a randomly chosen slot time is given as

$$\tau = \frac{2(1-2p)}{(1-2p)(W+1) + pW(1-(2p)^m)}, \qquad (2)$$

where W is the backoff window, m is the maximum backoff stage which determines the maximum backoff window by $CW_{max} = 2^m W$, and p is the conditional collision probability which means that this is the probability of a collision seen by a packet being transmitted on the channel. Actually, the probability p depends on the probability of remaining station transmits a packet, which is τ. Because p represents that in a time slot, when a station is transmitting a packet, at least one of the $n-1$ remaining stations is transmitting as well. With the assumption that each transmission "sees" the system in the same state (Markov chain mathematical model, detailed in [11]), it gives the p as

$$p = 1 - (1-\tau)^{n-1}. \qquad (3)$$

These two unknowns τ and p of independent equations (2) and (3) can be solved by using numerical techniques.

When the probability τ has been achieved, consider another probability that there is at least one transmission in the considered slot time, which is denoted by P_{tr}. Obviously it is

$$P_{tr} = 1 - (1-\tau)^n. \qquad (4)$$

In addition, the probability that a successful transmission given by the probability that exactly one station transmits on the channel, denoted as P_s, is given by

$$P_s = \frac{n\tau(1-\tau)^{n-1}}{P_{tr}}. \qquad (5)$$

Now all the definitions of different cases are obtained: with the probability $1 - P_{tr}$, the time slot is empty; with the probability $P_{tr}P_s$, there is a successful transmission; and with the probability $P_{tr}(1 - P_s)$, the time slot contains a collision.

IV. QKD IN RANDOM ACCESS NETWORK

From 2005, many experiments have successfully performed the decoy state QKD [12]–[15]. The experiment in [15] is a typical experiment that implements the QKD over 200 km with photon polarisation transmitted by optical fiber cable by using a 3-state decoy state protocol proposed by Wang [16]. All the specifications in this experiment are treated as assumptions in our work and the data for simulation is from the result of this experiment.

As the weak coherent light is used as the quantum source, the state emitted from Alice is given by

$$\rho = \sum_{n=0}^{\infty} \frac{\mu^n e^{-\mu}}{n!} \left|n\right\rangle \left\langle n\right| .$$

Thus, states with average photon number 0, μ and μ' (represent the vacuum pulses, signal pulses and decoy pulses separately) are denoted by ρ_0 (which is 0), ρ_μ and ρ'_μ, and corresponding number of counts are C_0, C_μ and C'_μ. With another set of numbers, N_0, N_μ and N'_μ, which are the pulse numbers of intensity 0, μ and μ' that Alice sent out, the counting rates of each different intensity pulses can be calculated as $S_0 = \frac{C_0}{N_0}$, $S_\mu = \frac{C_\mu}{N_\mu}$ and $S'_\mu = \frac{C'_\mu}{N'_\mu}$.

Another concept or definition distinguished from the counting rate $S(S_0, S_\mu, S'_\mu)$ is the counting rates of vacuum pulses, single-photon pulses and multi-photon pulses from signal states (decoy) states, which are denoted as $s_0(s'_0), s_1(s'_1)$ and $s_c(s'_c)$. Particularly, the single-photon counting rate is important for the calculation. The relationship between these two types of counting rate can be expressed by a set of equations which is detailed in [15]. Actually, the counting rate S and s are corresponding to the concept of "Gain" and "Yield" in previous paper of the decoy state method theory [8]–[10].

For simplifying the explanation, here we focus on the notation of signal states (the decoy states can be easily denoted by adding the "prime"). Then the theoretical key generation rate is given directly here, as

$$R_\mu = qS_\mu\{-H(E_\mu) + \Delta_1^\mu[1 - H(E_1^\mu)]\}. \tag{6}$$

This equation is based on Eq. (1) and proposed by Wang in his work [9], [16], where q and function $H(\cdot)$ have the same meanings as Eq. (1), and Δ_1^μ is the remaining bits in the sifted key that defined in [7]. However, Eq. (6) is a theoretical value of the key generation rate under the condition of that the QBER has been known. In the real experiment, the value of the QBER needs to be estimated by using a part of the whole qubits. Therefore, the final key generation rate should be updated to

$$K_\mu = R_\mu \cdot \delta_e, \tag{7}$$

where δ_e represents the length of the bits that is used for generating the actual quantum key, and it can be expressed as

$$\delta_e = \frac{(1 - L_\mu)\frac{C_\mu}{S_\mu}}{T}, \tag{8}$$

where L_μ is the fraction of the count bits in signal states used for QBER tests, which is provided by the experiment; C_μ and S_μ are the number of counts which comes from the intensity μ and the counting rate of pulses of intensity μ. According to the previous talk in this paper, δ_e includes all the neccessary information for the calculation with the data of the experiment. The useful data for the calculation from the experiment [15] is listed in the table.

TABLE I
SPECIFICATIONS OF THE EXPERIMENT.

Parameters	Description	Values
l	Transmission distance.	200
η_{Detect}	Detection efficiency.	0.75
S_0	Counting rate from vacuum states.	1.3204×10^{-8}
C_0	Number of counts from vacuum pulses.	3263
s_1	Single photon counting rate from signal states.	1.2788×10^{-6}
s'_1	Single photon counting rate from decoy states.	1.3707×10^{-6}
C_μ	Number of counts from μ photons pulses.	449467
C'_μ	Number of counts from μ' photons pulses.	77157
L_μ	Fraction of count bits in signal states.	0.1
L'_μ	Fraction of count bits in decoy states.	0.1
S_μ	Counting rate from signal states.	9.0941×10^{-7}
S'_μ	Counting rate from decoy states.	3.1223×10^{-7}
μ	Average photon number of signal states.	0.6
μ'	Average photon number of decoy states.	0.2
E^U_μ	QBER upper bound of signal states.	0.0263
$E^U_{\mu'}$	QBER upper bound of decoy states.	0.6
E_μ	Tested (observed) QBER of signal states.	0.0196
E'_μ	Tested (observed) QBER of decoy states.	0.0404

Suppose that this peer-to-peer QKD will be used in a channel shared network to satisfy multiple users' access requirements, see Fig. 1. In this network, we are trying to analyse the performance of QKD used by multiple users. Assume that there are finite number of terminals in the network and connected each other by an ideal channel, so it is reasonable to assume there exists a constant and independent collision probability of a packet transmitted by each stations. Thus from our previous talk, it can be achieved that the secret key

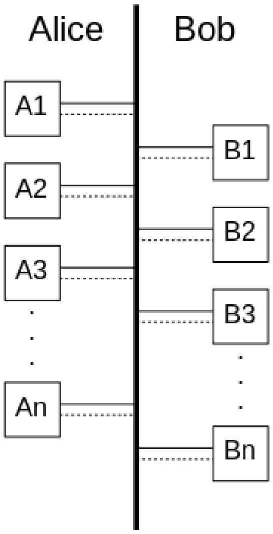


Fig. 1. Topology of all optical fiber connected QKD network. The line is the logical classical channel, and the dash line is the logical quantum channel. Usually, the channel will be multi-used since the quantum source is also the weak coherent light.

generation rate per user should be expressed as

$$K_{CSMA} = K_{QKD} * P, \tag{9}$$

where K_{QKD} is the key generation rate of two-terminals QKD, P is the probability of a successful transmission. Combine the QKD protocol that experiment used with the CSMA protocol, the secret key generation can be expressed as

$$K_{CSMA} = K_{\mu} P_{tr} P_s, \tag{10}$$

and the numerical result is shown as Fig. 2.

Follow this result, we will discuss the relationship between the key generation rate and the communication distance under the multi-access condition. Even though some parameters are not given in the experiment [15], the analysis is still able to be done according to the principle of the decoy method. Refer to [9], there is an internal correlation between S_n and s_n, which is

$$S_n = s_n \frac{\mu^n}{n!} e^{-\mu},$$

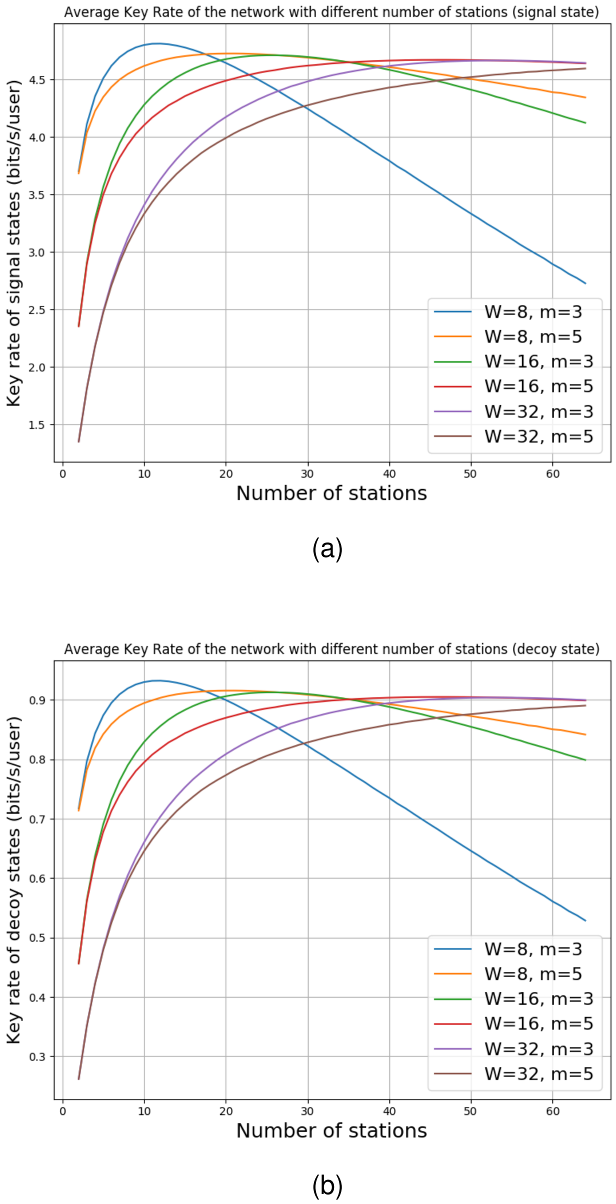
the overall counting rate and overall QBER can be expressed as

$$\begin{aligned} S_{\mu} &= \sum_{n=0}^{\infty} s_n \frac{\mu^n}{n!} e^{-\mu} \\ &= s_0 + 1 - e^{-\eta\mu} \end{aligned} \tag{11}$$

and

$$E_{\mu} = E_0 s_0 + e_{detector}(1 - e^{-\eta\mu}), \tag{12}$$

where n is the photon numbers included in pulses, S_n is the counting rate of n-photon pulses, s_n is the counting rate of n-photon pulses from signal states, η is the transmission efficiency that depends on the transmittance and the detection efficiency η_{Detect}, and $e_{detector}$ is the probability that a photon is detected by the imperfect detector. The parameters η and $e_{detector}$ can be calculated by solving Eq. (11) and (12).



(a)

(b)

Fig. 2. The average key generation rate (bits/s/user) with different numbers of stations.

The parameter η affects most observed data in an experiment, such as the counting rate S and the QBER E. Meanwhile, η is affected by the loss coefficient α, which represents the light pulse attenuation with the increment of the distance. The relation between them can be expressed as

$$\eta = 10^{-\frac{\alpha l}{10}} \cdot \eta_{Detect}, \tag{13}$$

where l is the transmission distance in km and α is the loss coefficient in dB/km.

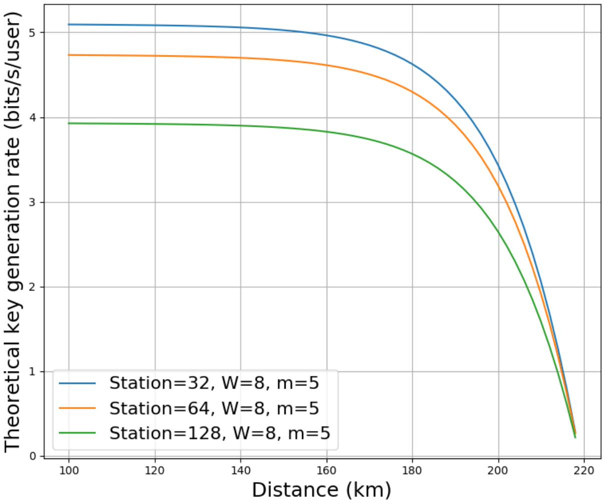


Fig. 3. Relationship between the transmission distance and the key generation rate. This is a calculated theoretical result based on the experiment [15] partly, since some estimated values instead of parameters not given in that experiment.

After calculating these parameters not given directly, the QBER E_μ can be re-estimated by using Eq. (14), which is independent with Eq. (12), and Eq. (15), which is an approximate estimate of s_μ.

$$E_\mu = \frac{e_0 s_0 + e_{detector}\eta}{s_\mu}, \tag{14}$$

$$s_\mu \doteq s_0 + \eta. \tag{15}$$

For simplifying the analysis, Eq. (11)-(15) simply connects the transmission distance and the counting rate and the QBER. Thus, by using Eq. (6), (7), (8) and (10), the relationship between the transmission distance and the key generation rate will be found. The numerical result is shown in Fig. 3.

V. Conclusion

Based on the theory of random access network and the successful experiment of the decoy state quantum key distribution, a possible scheme of QKD random access network is proposed and the main performance of QKD—key generation rate is analysed in this paper. Because of the difference between tha classical data packets and quantum source pulses, all the methods rely on the physical implementation cannot be simply used in quantum communications except the methods of logical analysis. In this paper, because of the method of the accessing refers to the classical communications, which is CSMA protocol, the quantum secret key generation rate is related to the pulse transmitting, so that it is affected by the probability of successful transmissions in the channel. The relationship between the quantum secret key generation rate and the number of stations on a shared channel random access network is studied. Since most work on QKD tries to enhance the distance of quantum communications, the relationship between the transmission distance and the secret key generation rate under the multi-access condition is considered as well.

References

[1] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in *Proc. 1984 IEEE International Conf. Comput. Syst. Signal Process.*, 1984, pp. 175–179.

[2] A. K. Ekert, “Quantum cryptography based on bell’s theorem,” *Phys. Rev. Lett.*, vol. 67, no. 6, p. 661, 1991.

[3] C. H. Bennett, G. Brassard, and N. D. Mermin, “Quantum cryptography without bells theorem,” *Phys. Rev. Lett.*, vol. 68, no. 5, p. 557, 1992.

[4] H.-K. Lo, H. F. Chau, and M. Ardehali, “Efficient quantum key distribution scheme and a proof of its unconditional security,” *J. Crypto.*, vol. 18, no. 2, pp. 133–165, 2005.

[5] E. Waks, A. Zeevi, and Y. Yamamoto, “Security of quantum key distribution with entangled photons against individual attacks,” *Phys. Rev. A*, vol. 65, no. 5, p. 052310, 2002.

[6] W.-Y. Hwang, “Quantum key distribution with high loss: toward global secure communication,” *Physical Review Letters*, vol. 91, no. 5, p. 057901, 2003.

[7] D. Gottesman, H. Lo, N. Lutkenhaus, and J. Preskill, “Security of quantum key distribution with imperfect devices,” *Quantum Inf. Comput.*, vol. 4, no. 5, pp. 325–360, 2004.

[8] H.-K. Lo, X. Ma, and K. Chen, “Decoy state quantum key distribution,” *Phys. Rev. Lett.*, vol. 94, no. 23, p. 230504, 2005.

[9] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, “Practical decoy state for quantum key distribution,” *Phys. Rev. A*, vol. 72, no. 1, p. 012326, 2005.

[10] L. O. Mailloux, M. R. Grimaila, D. D. Hodson, R. Engle, C. McLaughlin, and G. Baumgartner, “Modeling, simulation, and performance analysis of decoy state enabled quantum key distribution systems,” *Applied Sciences*, vol. 7, no. 2, p. 212, 2017.

[11] G. Bianchi, “Performance analysis of the ieee 802.11 distributed coordination function,” *IEEE Journal on selected areas in Comms.*, vol. 18, no. 3, pp. 535–547, 2000.

[12] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, “Experimental quantum key distribution with decoy states,” *Phys. Rev. Lett.*, vol. 96, no. 7, p. 070502, 2006.

[13] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, “Long-distance decoy-state quantum key distribution in optical fiber,” *Phys. Rev. Lett.*, vol. 98, no. 1, p. 010503, 2007.

[14] A. Tanaka, M. Fujiwara, S. W. Nam, Y. Nambu, S. Takahashi, W. Maeda, K.-i. Yoshino, S. Miki, B. Baek, Z. Wang *et al.*, “Ultra fast quantum key distribution over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronization,” *Opt. Express*, vol. 16, no. 15, pp. 11 354–11 360, 2008.

[15] Y. Liu, T.-Y. Chen, J. Wang, W.-Q. Cai, X. Wan, L.-K. Chen, J.-H. Wang, S.-B. Liu, H. Liang, L. Yang *et al.*, “Decoy-state quantum key distribution with polarized photons over 200 km,” *Opt. Express*, vol. 18, no. 8, pp. 8587–8594, 2010.

[16] X.-B. Wang, “Beating the photon-number-splitting attack in practical quantum cryptography,” *Phys. Rev. Lett.*, vol. 94, no. 23, p. 230503, 2005.