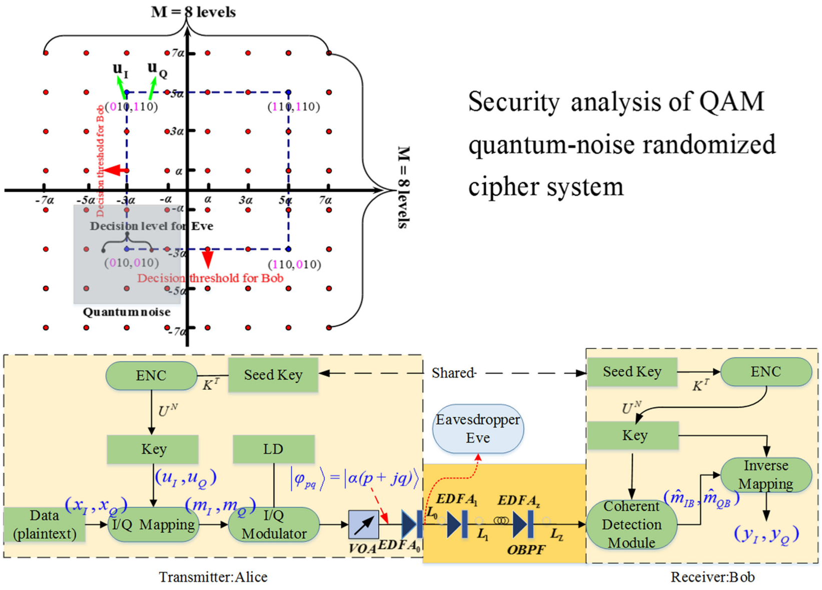
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Security Analysis of QAM Quantum-Noise Randomized Cipher System

Volume 12, Number 4, August 2020

Yukai Chen
Haisong Jiao
Hua Zhou
Jilin Zheng
Tao Pu



Security analysis of QAM quantum-noise randomized cipher system

DOI: 10.1109/JPHOT.2020.3009252

Security Analysis of QAM Quantum-Noise Randomized Cipher System

Yukai Chen,[1] **Haisong Jiao**,[1] **Hua Zhou**,[1] **Jilin Zheng**,[1]
and Tao Pu[1]

[1]College of Communications Engineering, Army Engineering University of PLA, Nanjing
210007, China

DOI:10.1109/JPHOT.2020.3009252

Manuscript received May 8, 2020; revised July 9, 2020; accepted July 11, 2020. Date of publication July 15, 2020; date of current version July 28, 2020. This work was supported by the National Natural Science Foundation of China under Grants 61974165 and 61901480. Corresponding author: Tao Pu (e-mail: nj_putao@163.com).

Abstract: Applying the quadrature amplitude modulation (QAM) format, quantum-noise randomized cipher (QNRC) systems hide the signal states in quantum phase noise and amplitude noise to prevent eavesdropping. In this paper, based on the traditional wire-tap channel model analysis method, the physical-layer security of QAM-QNRC system is investigated quantitatively under the metric of secrecy rate. The general expressions of secrecy rates of the data and key are derived separately. Furthermore, the maximum reachable secrecy rate of a QAM-QNRC system is put forward, under which the data and key are both safe in the view of mutual information evaluation. Finally, the variation trend of secrecy rate with various system parameters is discussed in detail. The simulation results show that we can obtain a higher secrecy rate by setting reasonable parameters, such as the level of ciphertext, mesoscopic signal power, and inner gain at the transmitter. Meanwhile, the security of the key is the main constraint of the maximum reachable secrecy rate.

Index Terms: Quantum secure communication, quantum-noise randomized cipher, secrecy rate, physical-layer security.

1. Introduction

Network services such as high-definition video, virtual reality, Big Data, and cloud computing have emerged in recent years. With increasingly more confidential information being carried on optical fiber networks, the security of optical fiber communication has become extremely important. However, due to enhanced computational ability, especially the proposed quantum computer [1], the traditional anti-interception methods based on computational complexity, such as the Advanced Encryption Standard (AES), have lost their security foundation. Thus, enhancing the security of physical layer in optical communication is becoming increasingly more important [2]. Quantum key distribution (QKD), which generates a secure key stream, together with the “one-time pad” (OTP) cryptosystem [3], has been regarded as an effective method with which to guarantee secure communication theoretically. Unfortunately, the limited QKD rate (e.g., 2.38 Mbps) [4] cannot support the high-speed data stream of the OTP. Therefore, fiber-optic anti-interception communication must provide not only ideal security, but also a high transmission rate.

A quantum-noise randomized cipher (QNRC) system, based on Heisenberg’s uncertainty principle and employing the Y-00 protocol, has been investigated recently to realized high-speed secure communications [5]. By employing inherent quantum noise to mark the signal level, the signal is hidden in the noise in a Y-00 system and it increases the difficulty for an eavesdropper to intercept signals. There are three major implementation schemes for QNRC: phase shift keying (PSK) [6], intensity shift keying (ISK) [7], and quadrature amplitude modulation (QAM) [8]. QAM is currently becoming the mainstream modulation format due to its improved spectral efficiency and bit rate [9]. Until now, QAM-QNRC systems with their dimension of ciphertext symbols reaching 1024 × 1024, a communication distance achieving 480 km, and a rate of data peaking at 70 Gb/s have been reported [10], [11].

How to evaluate the security of the Y-00 protocol is an essential topic that has been a subject of intense debate [12]–[15]. However, it is difficult to verify the security of the Y-00 protocol because the physical parameters for a Y-00 system are finite [16]. Employing the wire-tap channel approach, Mihaljevic proposed a generic framework to evaluate the security of the Y-00 protocol for the first time [17]. In Refs. [18] and [19], based on the wire-tap channel (WTC) model [20], the Y-00 protocol is regarded as the channel advantage of the main channel over the wire-tap channel. Then, the physical-layer security of a PSK-QNRC system is analyzed with secrecy capacity as the security performance metric. In Ref. [21], the WTC model of an ISK-QNRC system is established and the security performance metric is the secrecy rate. However, the signal structure of a coherent state and encryption mechanism of the QAM-QNRC system are more complex than those of the PSK-QNRC or ISK-QNRC systems. Moreover, unlike the PSK-QNRC system, both the wire-tap channel and main channel of a QAM-QNRC system are not discrete symmetric channels. And the probability density function of the QAM-QNRC system is more difficult than those of the PSK-QNRC and ISK-QNRC systems. These aspects cant be ignored when the security of a QAM-QNRC system is analyzed. So in this sense, the quantitative security analysis of a QAM-QNRC system is difficult, which has rarely been discussed before. Thus, it is extremely necessary to study the physical-layer security of the QAM-QNRC system by considering the Y-00 protocol as physical-layer superiority in the WTC model.

In this paper, the security of a QAM-QNRC system is analyzed quantitatively with secrecy rate serving as the security performance metric. Considering the unique properties of the QAM-QNRC system, the wire-tap channel model that fits the QAM-QNRC system can be established and its security analyzed quantitatively. The simulation results will benefit the configuration of a QAM-QNRC system for specific security promotion. The rest of this paper is organized as follows. In Section 2, the encryption method of a QAM-QNRC system by the Y-00 protocol is provided and the wire-tap channel models of the key and data are established separately. In Section 3, the general expressions of secrecy rates are derived, including the key and data. Moreover, the maximum reachable secrecy rate of a QAM-QNRC system is put forward. In Section 4, the variation trend of secrecy rates with various system parameters is assessed and compared in detail. In Section 5, main conclusions are summarized.

2. Wire-Tap Channel Model for QAM-QNRC System

2.1 Encryption Method of QAM-QNRC by Y-00 Protocol

Figure 1 is a schematic of a QAM-QNRC system based on the WTC model. A seed key K^T is shared by two legal parties (Alice and Bob) through a secure key channel. Applying the key expansion module, an N-bit key U is generated, which will be separated into n subkeys soon afterward; namely,

$$U^N = ENC\left(K^T\right) = (u_{Ii}, u_{Qi}), i = 1, 2, \ldots n. \tag{1}$$

There are $2l$ bits per subkey with $l = \log_2(M_b)$ bits for the in-phase(I) channel and l bits for the quadrature-phase(Q) channel, where M_b is the level of per subkey on I channel or Q channel. The data stream X^{2n}, namely the plaintext, is also separated into n symbols:

$$X^{2n} = (x_{Ii}, x_{Qi}), i = 1, 2, \ldots n. \tag{2}$$

There are 2 bits per symbol with 1 bit for the I channel and a 1 bit for the Q channel [22]. Subsequently, the key stream U^N is used to encrypt the data stream X^{2n}, where the $2l$ bit (u_{Ii}, u_{Qi})

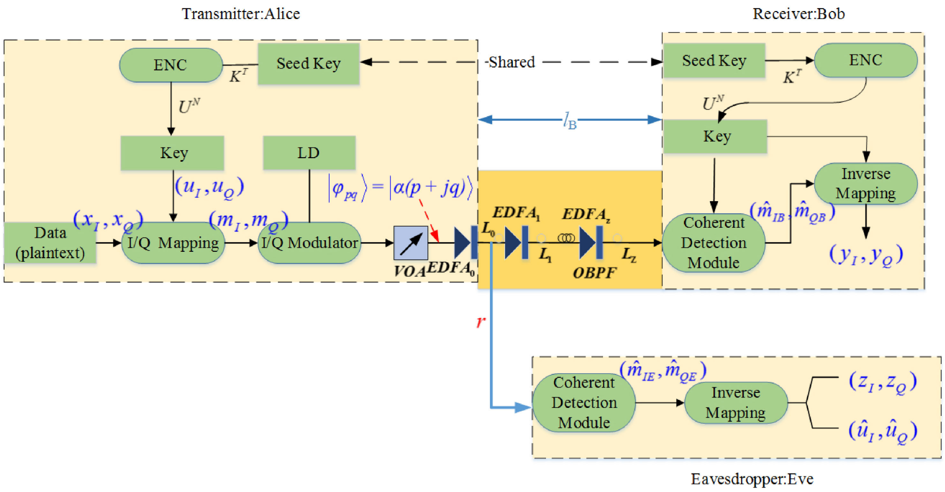


Fig. 1. Schematic of QAM-QNRC system based on WTC model.

is used to encrypt the 2 bit (x_{Ii}, x_{Qi}). Thus, the ciphertext is

$$\begin{aligned} m_I &= f(x_I, u_I) = u_I + [x_I \oplus Pol(u_I)] \bullet M_b, \\ m_Q &= f(x_Q, u_Q) = u_Q + [x_Q \oplus Pol(u_Q)] \bullet M_b, \end{aligned} \tag{3}$$

where Pol(•) is a parity function that takes the value of 1 or 0 when • is odd or even, respectively. Then, (m_I, m_Q) will be modulated into the phase and intensity of QAM quantum signals. The multiplicity $M = 2M_b$ is the level of ciphertext m_I or m_Q. Consider $M \times M$-ary QAM signals with coherent states:

$$\left|\varphi_{pq}\right\rangle = \left|\alpha(p + jq)\right\rangle, (p, q) \in \Omega, \tag{4}$$

where α is the basic amplitude and $p = -(M-1) + 2m_I$, $q = -(M-1) + 2m_Q$. The symbol set Ω is [23]:

$$\Omega = \{-(M-1) + 2k | k = 0, 1, \ldots, M-1\}. \tag{5}$$

Furthermore, the average number of photons is [24]

$$\begin{aligned} N &= |\alpha|^2 \frac{1}{M^2} \sum_{p\in\Omega} \sum_{q\in\Omega} (p^2 + q^2) \\ &= \frac{2}{3}(M^2 - 1)|\alpha|^2. \end{aligned} \tag{6}$$

As shown by the blue square in Fig. 2, aware of the key in advance, Bob must only discriminate four states, i.e., $|\varphi_{p_1 q_1}\rangle$, $|\varphi_{p_2 q_2}\rangle$, $|\varphi_{p_3 q_3}\rangle$, and $|\varphi_{p_4 q_4}\rangle$, where

$$\begin{aligned} p_1 &= -(M-1) + 2u_I,\ q_1 = -(M-1) + 2u_Q, \\ p_2 &= -(M-1) + 2(u_I + M_b),\ q_2 = -(M-1) + 2u_Q, \\ p_3 &= -(M-1) + 2u_I,\ q_3 = -(M-1) + 2(u_Q + M_b), \\ p_4 &= -(M-1) + 2(u_I + M_b),\ q_4 = -(M-1) + 2(u_Q + M_b). \end{aligned} \tag{7}$$

The symbol distance of the four states is large enough. However, since there is no key information, the M^2-ary quantum states must be discriminated by the eavesdropper (named Eve). Because of Heisenberg's uncertainty principle, the difference between adjacent quantum states will be covered with quantum noise. It ensures that the key or data are not intercepted.

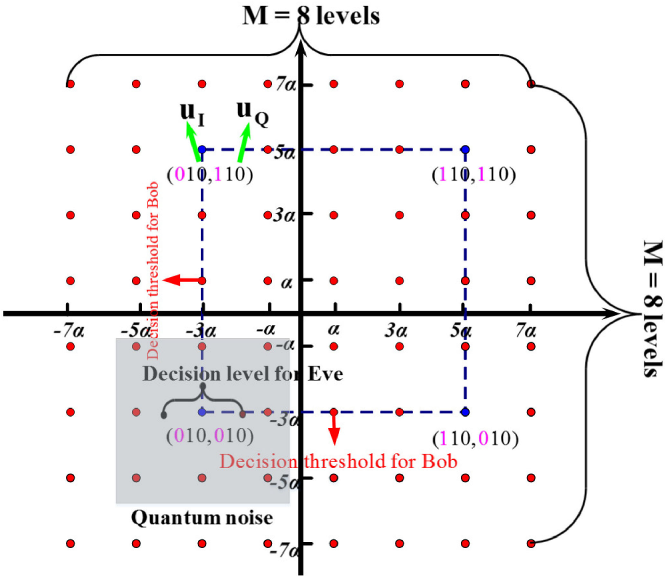


Fig. 2. Constellation diagram of 64QAM-QNRC; two-bit data are encrypted using a four-bit key.

2.2 Wiretap Channel Model

As Fig. 1 shows, when Alice communicates with Bob by the main channel, Eve intercepts some signals by bending the fiber with the eavesdropping rate r. Suppose that the signal passing rate of the main channel is t. In Ref. [19], generally $r = t = 1$ or $r + t = 1 (0 < r < 1)$. To adapt to long-haul optical fiber transmission, an erbium-doped fiber amplifier $EDFA_0$ is used to amplify the mesoscopic signal to a conventional signal level at the transmitter. Moreover, $EDFA_0$ will bring classical amplified spontaneous emission (ASE) noise. The main channel is an optical amplifying link relayed by the erbium-doped fiber amplifier (EDFA). We define z as the number of EDFAs and L_B as the transmission distance. The received signal powers of Bob and Eve are [25]

$$\begin{cases} P_B = tP_{S0}G_0L_0\prod_{i=1}^{z} G_iL_i, \\ P_E = rP_{S0}G_0L_E, \end{cases} \tag{8}$$

respectively, where P_{S0} is the power of the mesoscopic signal $|\varphi_{pq}\rangle$, L_i the transmission loss of the fiber span behind $EDFA_i$, G_i $EDFA_i$'s gain, and L_E the eavesdropping distance. To facilitate the next stage of the analysis, the received signal powers of Bob and Eve in terms of average number of photons per symbol are

$$\begin{cases} N_B = \frac{2}{3}(M^2 - 1)|\alpha_B|^2 = (tP_{S0}G_0L_0\prod_{i=1}^{z} G_iL_i)/h\nu R, \\ N_E = \frac{2}{3}(M^2 - 1)|\alpha_E|^2 = rP_{S0}G_0L_E/h\nu R, \end{cases} \tag{9}$$

respectively, where R is the symbol rate, Planck's constant is $h = 6.626 \times 10^{-34} J\,.\,s$, ν the photon frequency, and α_E and α_B are the basic amplitudes of Eve and Bob, respectively. According to the Nyquist first criterion, it is necessary to ensure that the optical bandwidth $B_0 \geq R$. In this paper, let $B_0 = 2R$, so the ASE noise variances of Bob and Eve are given respectively by [21]:

$$\begin{aligned} \delta^2_{Ase,Bob} &= 4tL_0n_{sp}(G_0 - 1) + \sum_{i=1}^{z} 4L_in_{sp}(G_i - 1), \\ \delta^2_{Ase,Eve} &= 4rL_En_{sp}(G_0 - 1), \end{aligned} \tag{10}$$

where the spontaneous radiation factor $n_{sp} = 1.4$.

The signal intercepted by Eve is $|\alpha_E(p + jq)\rangle$. According to Eq. (9), $\alpha_E = \sqrt{N_E/[\frac{2}{3}(M^2 - 1)]}$. The heterodyne measurement is the pivotal step in evaluating the security of QNRC systems [16].

Owing to the inevitable effect of quantum noise and ASE noise, Eve is unavailable to get its exact position from the QAM constellation. The QAM quantum heterodyne receiver's probability density function is given by [24], [26]:

$$p_e(x_c, x_s|p, q) = \frac{1}{2\pi\delta_E^2}\exp\left[\frac{-(x_c - p\alpha_E)^2 - (x_s - q\alpha_E)^2}{2\delta_E^2}\right], \tag{11}$$

where (x_c, x_s) is the output of the quantum heterodyne receiver. In addition, σ_E^2 is the total noise for Eve. In the wire-tap channel model, the total noise for Eve should include quantum shot noise and classical ASE noise. In Ref. [23], the variance of the quantum noise is defined as unity, so the total noise for Eve is

$$\sigma_E^2 = \sigma_{shot}^2 + \sigma_{Ase,Eve}^2 = 1 + 4rL_E n_{sp}(G_0 - 1). \tag{12}$$

Consequently, the probability density function of Eve has been determined. Based on the measured (x_c, x_s), Eve will make a judgment on the original coherent state $|\varphi_{pq}\rangle$, and then estimate (p, q). According to the Bayes strategy, Eves decision regions are [24]

$$D_{p',q'} = \left\{(x_c, x_s)\left|\begin{cases}-\infty < x_c < (p'+1)\alpha_E & p' < -(M-2)\\ (p'-1)\alpha_E < x_c < +\infty & p' > (M-2)\\ (p'-1)\alpha_E < x_c < (p'+1)\alpha_E & \text{else}\end{cases}\right\};\right.$$
$$\left.\begin{cases}-\infty < x_s < (q'+1)\alpha_E & q' < -(M-2)\\ (q'-1)\alpha_E < x_s < +\infty & q' > (M-2)\\ (q'-1)\alpha_E < x_s < (q'+1)\alpha_E & \text{else}\end{cases}\right\} \tag{13}$$

where

$$\begin{aligned}&p' = -(M-1) + 2\hat{m}_I, q' = -(M-1) + 2\hat{m}_Q,\\ &\hat{m}_I = 0, 1, \ldots M-1; \hat{m}_Q = 0, 1, \ldots M-1.\end{aligned} \tag{14}$$

When $(x_c, x_s) \in D_{p',q'}$, Eve will make a judgment of (p', q'); that is, make a choice of $(\hat{m}_I, \hat{m}_Q)$. Therefore, the ciphertext symbol transition probability of Eve can be expressed as

$$P_E(p', q'|p, q) = \iint_{D_{p',q'}} p_e(x_c, x_s|p, q)\mathrm{d}x_c\mathrm{d}x_s. \tag{15}$$

For Bob, the basic amplitude is $\alpha_B = \sqrt{N_B/[\frac{2}{3}(M^2 - 1)]}$. In addition, the noise variance is $\sigma_B^2 = 1 + \sigma_{Ase,Bob}^2$. By replacing α_E and σ_E^2 with the obtained α_B and σ_B^2 in formula (11), Bob's probability density function $p_b(x_c, x_s|p, q)$ is obtained. In addition, Bob knows the key in advance, so his work is to make a decision of four quantum states $\{|\varphi_{p_1q_1}\rangle, |\varphi_{p_2q_2}\rangle, |\varphi_{p_3q_3}\rangle, |\varphi_{p_4q_4}\rangle\}$, which have the same key. Therefore, Bob's decision regions are

$$D'_{p',q'} = \left\{(xc, xs)\left|\begin{cases}-\infty < xc < (p'+M_b)\alpha_B & p' < 0\\ (p'-M_b)\alpha_B < xc < +\infty & p' \geq 0\end{cases}\right\};\right.$$
$$\left.\times\begin{cases}-\infty < xs < (q'+M_b)\alpha_B & q' < 0\\ (q'-M_b)\alpha_B < xs < +\infty & q' \geq 0\end{cases}\right\}, \tag{16}$$

where

$$\begin{aligned}&p' = -(M-1) + 2\hat{m}_I, q' = -(M-1) + 2\hat{m}_Q,\\ &\hat{m}_I = m_I \text{ or } m_I + M_b; \hat{m}_Q = m_Q \text{ or } m_Q + M_b.\end{aligned} \tag{17}$$

Furthermore, Bob's ciphertext symbol transmission probability is

$$P_B(p', q'|p, q) = \iint_{D_{p',q'}} p_b(x_c, x_s|p, q)\mathrm{d}x_c\mathrm{d}x_s. \tag{18}$$

The ciphertext symbol transmission probabilities of Eve and Bob are obtained separately, and then the WTC models of the key and data will be established separately.

The key U is considered the information source. Because Bob knows the key in advance, there are no errors in the main channel. However, serious interference exists in the wire-tap channel because of the noise's effect. More concretely, this wiretap channel is

$$\begin{aligned}(u_I, u_Q) &\xrightarrow{P(m_I, m_Q|u_I, u_Q) = P(x_I, x_Q)} (m_I, m_Q) \xrightarrow{P_E(\hat{m}_I, \hat{m}_Q|m_I, m_Q)} (\hat{m}_I, \hat{m}_Q) \\ &\xrightarrow{P(\hat{u}_I, \hat{u}_Q\left|\hat{m}_I, \hat{m}_Q\right.) = 1} (\hat{u}_I, \hat{u}_Q),\end{aligned} \tag{19}$$

where $(\hat{m}_I, \hat{m}_Q)$ is the ciphertext symbol intercepted by Eve, and

$$\hat{m}_I = f(z_I, \hat{u}_I), \hat{m}_Q = f(z_Q, \hat{u}_Q). \tag{20}$$

Here, $(\hat{u}_I, \hat{u}_Q)$ and (z_I, z_Q) denote the key and data, respectively, intercepted by Eve, so Eve's key transition probability is derived as follows:

$$\begin{aligned}&P(\hat{u}_I, \hat{u}_Q|u_I, u_Q) \\ &= \sum_{m_I, m_Q} \sum_{\hat{m}_I, \hat{m}_Q} P(\hat{u}_I, \hat{u}_Q|\hat{m}_I, \hat{m}_Q) P_E(\hat{m}_I, \hat{m}_Q|m_I, m_Q) P(m_I, m_Q|u_I, u_Q) \\ &= \sum_{x_I=0}^{1} \sum_{x_Q=0}^{1} \sum_{z_I=0}^{1} \sum_{z_Q=0}^{1} P_E(\hat{m}_{z_I, \hat{u}_I}; \hat{m}_{z_Q, \hat{u}_Q}|m_{x_I, u_I}; m_{x_Q, u_Q}) P(x_I, x_Q) \\ &= \frac{1}{4} \sum_{x_I=0}^{1} \sum_{x_Q=0}^{1} \sum_{z_I=0}^{1} \sum_{z_Q=0}^{1} P_E(\hat{m}_{z_I, \hat{u}_I}; \hat{m}_{z_Q, \hat{u}_Q}|m_{x_I, u_I,}; m_{x_Q, u_Q}).\end{aligned} \tag{21}$$

Likewise, the quantum state $|\varphi_{pq}\rangle$ carries the data information that will also be intercepted by Eve. The wire-tap channel for data is also noisy. Moreover, there are errors in the main channel for data because of the degradation in signal-to-noise ratio after channel transmission. Specifically, the wire-tap channel and main channel for data are derived as follows:

$$\begin{aligned}(x_I, x_Q) &\xrightarrow{P(m_I, m_Q|x_I, x_Q) = P(u_I, u_Q)} (m_{x_I, u_I}; m_{x_Q, u_Q}) \xrightarrow{P_E(\hat{m}_{IE}, \hat{m}_{QE}|m_I, m_Q)} \\ &(\hat{m}_{z_I, \hat{u}_I}; \hat{m}_{z_Q, \hat{u}_Q}) \xrightarrow{P_E(z_I, z_Q\left|\hat{m}_{z_I, \hat{u}_I}; \hat{m}_{z_Q, \hat{u}_Q}\right.) = 1} (z_I, z_Q),\end{aligned} \tag{22}$$

$$\begin{aligned}(x_I, x_Q) &\xrightarrow{P(m_I, m_Q|x_I, x_Q) = P(u_I, u_Q)} (m_{x_I, u_I}; m_{x_Q, u_Q}) \xrightarrow{P_B(\hat{m}_{IB}, \hat{m}_{QB}|m_I, m_Q)} \\ &(\hat{m}_{y_I, u_I}; \hat{m}_{y_Q, u_Q}) \xrightarrow{P_B(y_I, y_Q\left|\hat{m}_{y_I, u_I}; \hat{m}_{y_Q, u_Q}\right.) = 1} (y_I, y_Q),\end{aligned} \tag{23}$$

respectively, where (y_I, y_Q) and (z_I, z_Q) are the data received by Bob and Eve, respectively, and $(\hat{m}_{IB}, \hat{m}_{QB})$ and $(\hat{m}_{IE}, \hat{m}_{QE})$ are the respective ciphertext symbols intercepted by Bob and Eve. Hence, the data transition probabilities of Eve and Bob, are obtained as follows, respectively:

$$\begin{aligned}&P_E(z_I, z_Q|x_I, x_Q) \\ &= \sum_{m_I} \sum_{m_Q} \sum_{\hat{m}_{IE}} \sum_{\hat{m}_{QE}} P_E(z_I, z_Q|\hat{m}_{IE}, \hat{m}_{QE}) P_E(\hat{m}_{IE}, \hat{m}_{QE}|m_I; m_Q) P(m_I; m_Q|x_I, x_Q) \\ &= \sum_{u_I=0}^{M_b-1} \sum_{u_Q=0}^{M_b-1} \sum_{\hat{u}_I=0}^{M_b-1} \sum_{\hat{u}_Q=0}^{M_b-1} P_E(\hat{m}_{z_I, \hat{u}_I}; \hat{m}_{z_Q, \hat{u}_Q}|m_{x_I, u_I}; m_{x_Q, u_Q}) P(u_I, u_Q)\end{aligned}$$

$$= \frac{1}{(M_b)^2} \sum_{u_I=0}^{M_b-1} \sum_{u_Q=0}^{M_b-1} \sum_{\hat{u}_I=0}^{M_b-1} \sum_{\hat{u}_Q=0}^{M_b-1} P_E(\hat{m}_{z_I,\hat{u}_I}; \hat{m}_{z_Q,\hat{u}_Q} | m_{x_I,u_I}; m_{x_Q,u_Q}), \tag{24}$$

$$\begin{aligned} & P_B(y_I, y_Q | x_I, x_Q) \\ & = \sum_{m_I} \sum_{m_Q} \sum_{\hat{m}_{IB}} \sum_{\hat{m}_{QB}} P_B(y_I, y_Q | \hat{m}_{IB}, \hat{m}_{QB}) P_B(\hat{m}_{IB}, \hat{m}_{QB} | m_I; m_Q) P(m_I; m_Q | x_I, x_Q) \\ & = \sum_{u_I=0}^{M_b-1} \sum_{u_Q=0}^{M_b-1} P_B(\hat{m}_{y_I,u_I}; \hat{m}_{y_Q,u_Q} | m_{x_I,u_I}; m_{x_Q,u_Q}) P(u_I, u_Q) \\ & = \frac{1}{(M_b)^2} \sum_{u_I=0}^{M_b-1} \sum_{u_Q=0}^{M_b-1} P_B(\hat{m}_{y_I,u_I}; \hat{m}_{y_Q,u_Q} | m_{x_I,u_I}; m_{x_Q,u_Q}). \end{aligned} \tag{25}$$

3. Secrecy Rates of QAM-QNRC System

Exactly like the ISK scheme, both the wire-tap channel and main channel of a QAM-QNRC system are not discrete symmetric channels. The secrecy rate R_S is defined as the difference in mutual information between Alice-Bob and Alice-Eve for a specific probability distribution of source symbols [20]. In this section, the security of a QAM-QNRC system is analyzed quantitatively with the secrecy rate serving as the security performance metric. The general expressions of secrecy rate of the key and data are based on the WTC models built above. Moreover, taking into account the secrecy restrictions of the key and data simultaneously, the maximal achievable secrecy rate of a QAM-QNRC system is put forward.

3.1 Secrecy Rate of the Key

Based on the key transition probability of Eve, $P(\hat{u}_I, \hat{u}_Q | u_I, u_Q)$, obtained in Section 2, the secrecy rate of the key R_{su} is

$$\begin{aligned} R_{Su} &= [I_{AB}(u_I, u_Q; u_I, u_Q) - I_{AE}(\hat{u}_I, \hat{u}_Q; u_I, u_Q)]_{P(u_I,u_Q)=\frac{1}{(M_b)^2}} \\ &= [H(u_I, u_Q) - H(u_I, u_Q | u_I, u_Q)] - [H(\hat{u}_I, \hat{u}_Q) - H(\hat{u}_I, \hat{u}_Q | u_I, u_Q)] \\ &= 2I - [H(\hat{u}_I, \hat{u}_Q) - H(\hat{u}_I, \hat{u}_Q | u_I, u_Q)]_{P(u_I,u_Q)=\frac{1}{(M_b)^2}}, \end{aligned} \tag{26}$$

where $I(\mathbf{.}, \mathbf{.})$ denotes the mutual information, $H(\mathbf{.})$ the Shannon entropy function, and $H(\mathbf{.}|\mathbf{.})$ equivocation. Herein, the equivocation $H(\hat{u}_I, \hat{u}_Q | u_I, u_Q)$ is

$$\begin{aligned} & [H(\hat{u}_I, \hat{u}_Q | u_I, u_Q)]_{P(u_I,u_Q)=\frac{1}{(M_b)^2}} \\ & = -\sum_{u_I=0}^{M_b-1} \sum_{u_Q=0}^{M_b-1} \sum_{\hat{u}_I=0}^{M_b-1} \sum_{\hat{u}_Q=0}^{M_b-1} P(u_I, u_Q) P(\hat{u}_I, \hat{u}_Q | u_I, u_Q) \bullet \log P(\hat{u}_I, \hat{u}_Q | u_I, u_Q) \\ & = -\frac{1}{(M_b)^2} \sum_{u_I=0}^{M_b-1} \sum_{u_Q=0}^{M_b-1} \sum_{\hat{u}_I=0}^{M_b-1} \sum_{\hat{u}_Q=0}^{M_b-1} P(\hat{u}_I, \hat{u}_Q | u_I, u_Q) \bullet \log P(\hat{u}_I, \hat{u}_Q | u_I, u_Q), \end{aligned} \tag{27}$$

and the Shannon entropy function $H(\hat{u}_I, \hat{u}_Q)$ is

$$[H(\hat{u}_I, \hat{u}_Q] = -\sum_{\hat{u}_I=0}^{M_b-1} \sum_{\hat{u}_Q=0}^{M_b-1} P(\hat{u}_I, \hat{u}_Q) \bullet \log P(\hat{u}_I, \hat{u}_Q), \tag{28}$$

where the probability distribution of the key received by Eve, $P(\hat{u}_I, \hat{u}_Q)$, is

$$\begin{aligned} P(\hat{u}_I, \hat{u}_Q) &= \sum_{u_I=0}^{M_b-1} \sum_{u_Q=0}^{M_b-1} P(u_I, u_Q) P(\hat{u}_I, \hat{u}_Q | u_I, u_Q) \\ &= \frac{1}{(M_b)^2} \sum_{u_I=0}^{M_b-1} \sum_{u_Q=0}^{M_b-1} P(\hat{u}_I, \hat{u}_Q | u_I, u_Q). \end{aligned} \tag{29}$$

Then, the secrecy rate of the key is normalized to I_{AB}, i.e., $R_{su0} = R_{su}/(2I)$.

3.2 Secrecy Rate of Data

Likewise, based on the data transition probabilities of Eve and Bob, $P_E(z_I, z_Q | x_I, x_Q)$ and $P_B(y_I, y_Q | x_I, x_Q)$, respectively, obtained in Section 2, the secrecy rate of the data R_{Sx} is

$$\begin{aligned} R_{sx} &= \{I_{AB}(y_I, y_Q; x_I, x_Q) - I_{AE}(z_I, z_Q; x_I, x_Q)]\}_{P(x_I, x_Q)=1/4} \\ &= [H(y_I, y_Q) - H(y_I, y_Q | x_I, x_Q)] - [H(z_I, z_Q) - H(z_I, z_Q | x_I, x_Q)], \end{aligned} \tag{30}$$

where the Shannon entropy functions $H(z_I, z_Q)$ and $H(y_I, y_Q)$ are given by

$$H(z_I, z_Q) = -\sum_{z_I=0}^{1} \sum_{z_Q=0}^{1} P(z_I, z_Q) \bullet logP(z_I, z_Q), \tag{31}$$

$$H(y_I, y_Q) = -\sum_{y_I=0}^{1} \sum_{y_Q=0}^{1} P(y_I, y_Q) \bullet logP(y_I, y_Q), \tag{32}$$

respectively, where the probability distributions of the data received by Eve and Bob, namely $P(z_I, z_Q)$ and $P(y_I, y_Q)$, respectively, are derived as follows:

$$\begin{aligned} P(z_I, z_Q) &= \sum_{x_I=0}^{1} \sum_{x_Q=0}^{1} P_E(z_I, z_Q | x_I, x_Q) P(x_I, x_Q) \\ &= \frac{1}{4} \sum_{x_I=0}^{1} \sum_{x_Q=0}^{1} P_E(z_I, z_Q | x_I, x_Q), \end{aligned} \tag{33}$$

$$\begin{aligned} P(y_I, y_Q) &= \sum_{x_I=0}^{1} \sum_{x_Q=0}^{1} P_B(y_I, y_Q | x_I, x_Q) P(x_I, x_Q) \\ &= \frac{1}{4} \sum_{x_I=0}^{1} \sum_{x_Q=0}^{1} P_B(y_I, y_Q | x_I, x_Q), \end{aligned} \tag{34}$$

respectively. Furthermore, the equivocation of the wire-tap channel and main channel, i.e., $H(z_I, z_Q | x_I, x_Q)$ and $H(y_I, y_Q | x_I, x_Q)$, respectively, can be derived as

$$\begin{aligned} &H(z_I, z_Q | x_I, x_Q) \\ &= -\sum_{x_I=0}^{1} \sum_{x_Q=0}^{1} \sum_{z_I=0}^{1} \sum_{z_Q=0}^{1} P(x_I, x_Q) P_E(z_I, z_Q | x_I, x_Q) \bullet logP_E(z_I, z_Q | x_I, x_Q) \\ &= -\frac{1}{4} \sum_{x_I=0}^{1} \sum_{x_Q=0}^{1} \sum_{z_I=0}^{1} \sum_{z_Q=0}^{1} P_E(z_I, z_Q | x_I, x_Q) \bullet logP_E(z_I, z_Q | x_I, x_Q), \end{aligned} \tag{35}$$

$$
\begin{aligned}
&H(y_I, y_Q|x_I, x_Q)\\
&= -\sum_{x_I=0}^{1}\sum_{x_Q=0}^{1}\sum_{y_I=0}^{1}\sum_{y_Q=0}^{1} P(x_I, x_Q)P_B(y_I, y_Q|x_I, x_Q) \bullet logP_B(y_I, y_Q|x_I, x_Q)\\
&= -\frac{1}{4}\sum_{x_I=0}^{1}\sum_{x_Q=0}^{1}\sum_{y_I=0}^{1}\sum_{y_Q=0}^{1} P_B(y_I, y_Q|x_I, x_Q) \bullet logP_B(y_I, y_Q|x_I, x_Q).
\end{aligned} \tag{36}
$$

3.3 System Maximum Reachable Secrecy Rate

Above, the secrecy rates of the key and data, which provided security restrictions for the transmission of key and data, respectively, were obtained. The data and key are simultaneously carried in the Y-00 quantum state for transmission, so both security restrictions must be considered to ensure the strictness of the entire system's safety. Specifically, it is assumed that the transmission bit rates of the data and key are defined, respectively, as R_x and R_u. The quantum state $|\varphi_{pq}\rangle$ contains a $2l$-bit key (u_I, u_Q) and two-bit data (x_I, x_Q), so $R_u = lR_x$. According to Wyner theory,

$$
\begin{cases} R_x \le R_{sx} \\ R_u = lR_x \le R_{su} \end{cases} \Rightarrow R_x \le \min\left\{R_{sx}, \frac{R_{su}}{l}\right\} = \min\left\{R_{sx}, 2R_{su0}\right\}. \tag{37}
$$

We define $R_s = \min\{R_{sx}, 2R_{su0}\}$ as the maximum reachable secrecy rate of a QAM-QNRC system. Under this rate, the key and the data are both safe from the perspective of mutual information evaluation.

4. Results and Discussion

According to Section 3, the secrecy rate is dependent on pivotal system parameters, such as the multiplicity M (the level of ciphertext m_I or m_Q); mesoscopic signal power P_{S0}, inner gain at the transmitter, G_0; transmission distance for Bob, L_B; eavesdropping distance for Eve, L_E; eavesdropping ratio r; and signal passing rate of the main channel t. The above-mentioned system have been calculated numerically by MATLAB software. The values of general numerical simulation parameters are the following: The fiber loss factor is $u = 0.2\ dB/km$, coherent light center wavelength is $\lambda = 1550\ nm$, gain of the optical amplifier $EDFA_i$ is $G_i = 20\ dB$, transmission loss of fiber span behind $EDFA_i$ is $L_i = -20\ dB$, and symbol rate is $R = 2.5\ Gsymbol/s$.

4.1 Secrecy Rate of Key

The effect of eavesdropping distance L_E on the security of the key is illustrated in Fig. 3 for the case of $M = 8$, $G_0 = 30\ dB$, $P_{S0} = -45\ dBm$ and $r = \{0.01, 0.1, 0.5, 1\}$. Obviously, the secrecy rate of the key increases with increasing eavesdropping distance and decreases with increasing eavesdropping ratio. Therefore, to steal more messages, Eve will bring the eavesdropping position as close as possible to Alice inevitably, and intercept the signal as much as possible according to its own eavesdropping ability.

After determining Eve's optimal eavesdropping position, attention is directed to the effect of the inner gain at the transmitter, G_0, on the security of the key. The secrecy rate of the key (normalized to I_{AB}), R_{su0}, versus the inner gain is illustrated in Fig. 4 for the case of $r = \{0.01, 0.1, 0.18, 0.5, 1\}$, $M = \{8, 16\}$, and $P_{S0} = \{-45\ dBm, -40\ dBm\}$. It can be seen that the trend of R_{su0} with G_0 depends on r. Faced with Eve having strong eavesdropping ability (r is larger), the increase of G_0 is beneficial to improving security. However, amplifying the signal at the transmitter will degrade the security of the key for Eve with normal ability. Regardless of the trend, the greater the eavesdropping ratio, the worse the security of the key becomes. Moreover, when the inner gain is large sufficiently; that is, $G_0 \ge 29dB$ and R_{su0} will stabilize to a value that is related to P_{S0} and M, and no longer varies with G_0 and r. For the above change law, first, to complete the long-distance communication, it is necessary

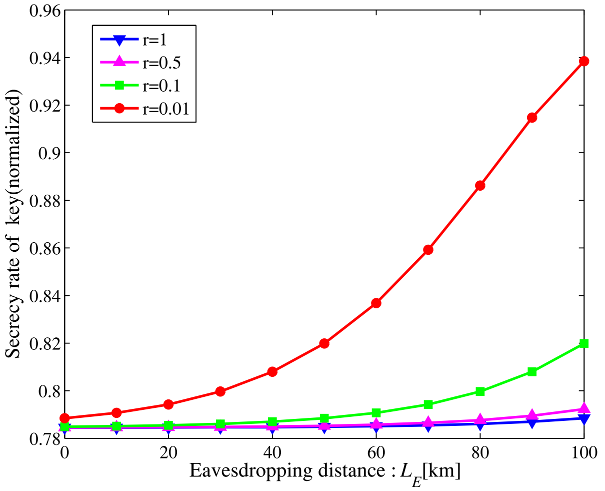


Fig. 3. Secrecy rate of key (normalized) R_{su0} *vs* L_E for different eavesdropping ratios *r*, with $M = 8$, $G_0 = 30\ dB$, and $P_{S0} = -45\ dBm$.

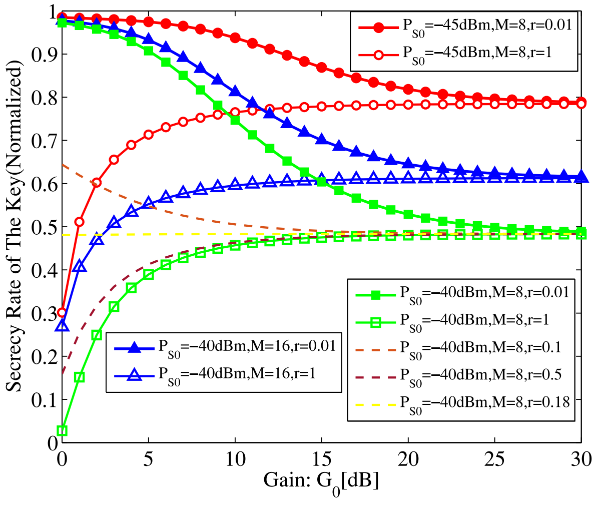


Fig. 4. R_{su0} *vs* G_0 for different P_{S0}, *M*, and *r* values with $L_E = 0\ km$.

to amplify the Y-00 quantum state. Meanwhile, even if Alice does not use $EDFA_0$ to enhance the key's security against Eve with normal ability, the amplifier will be introduced by Eve to steal more messages. Therefore, the use of $EDFA_0$ is always necessary.

Then, R_{su0} versus the mesoscopic signal power P_{S0} for the case of $M = \{8, 16, 32\}$, $r = 1$, $G_0 = 30\ dB$, $L_E = 0km$ is shown in Fig. 5. As P_{S0} decreases or *M* increases, the secrecy rate of the key (normalized) R_{su0} increases. This is because, by increasing the multiplicity *M*, the signal constellation density will be further increased and can limit Eve to intercept the key. Moreover, the basic amplitude of Eve, α_E, decreases with decreasing P_{S0}, leading to the result that the signal is susceptible to the effect of noise. Thus, Eve finds it more difficult to intercept useful information.

4.2 Secrecy Rate of Data

The secrecy rate of the data, R_{sx}, versus the transmission distance, L_B, is shown in Fig. 6 for the case of the signal passing rate $t = \{0.5, 0.8, 0.99\}$, $M = 8$, $G_0 = 30\ dB$, and $P_{S0} = -45\ dBm$. As L_B

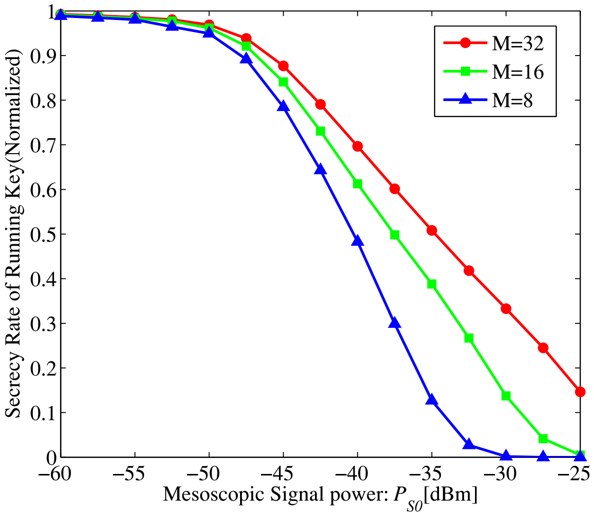


Fig. 5. Secrecy rate of key (normalized) R_{su0} *vs* P_{S0}, with $r = 1$, $G_0 = 30$ *dB*, and $L_E = 0$ *km*.

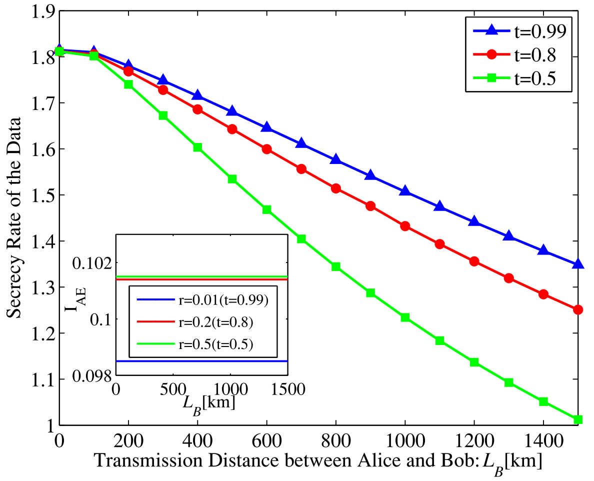


Fig. 6. Secrecy rate of data R_{sx} *vs* L_B, with $M = 8$, $G_0 = 30$ *dB*, and $P_{S0} = -45$ *dB*.

increases, R_{sx} decreases continuously. This is because the accumulated noise is so large that even Bob's measurement is influenced. Meanwhile, R_{sx} decreases along with decreasing t. However, despite the change of L_B, the mutual information of Alice-Eve, I_{AE}, remains a small constant that increases slightly with increasing $r = 1 - t$. This is because the data are protected by noise at the source and Eve can only intercept a small, almost negligible, amount information. Actually, it is the reduction of the mutual information of Alice-Bob I_{AB} that leads to the decrease of R_{sx}. Furthermore, it can be found that a QAM-QNRC system is suitable for long-distance transmission.

Then, as Fig. 7 shows, the secrecy rate of the data as a function of G_0 is illustrated for the case of an eavesdropping ratio $r = \{0.01, 1\}$, $M = \{8, 16\}$, $L_B = 500$ *km*, and $P_{S0} = -45$ *dBm*. Obviously, the secrecy rate of the data, R_{sx}, grows with increasing G_0. When G_0 is small, R_{sx} in the presence of Eve with normal ability ($r = 0.01, t = 0.99$) is higher than that of Eve with her strongest ability ($r = t = 1$). This is because the change trend of the mutual information of Alice-Eve, I_{AE}, versus G_0 is similar to $R_{su0} - G_0$ in Fig. 4. The growth of G_0 is beneficial to the security of Eve with her strongest ability, while it is detrimental to the security of Eve with normal ability. Meanwhile, with

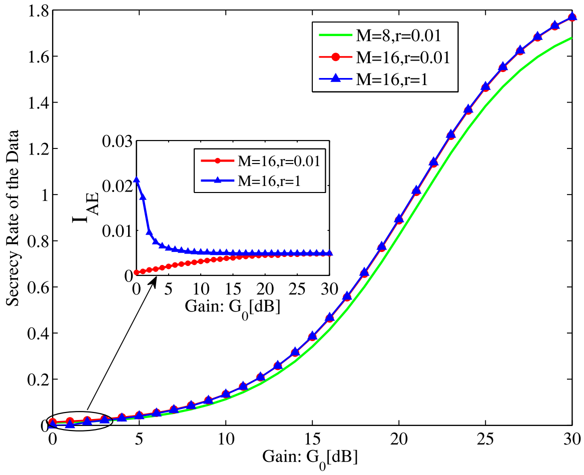


Fig. 7. Secrecy rate of data R_{sx} *vs* G_0 for different parameters (M and r), with $L_E = 0$ *km*, $L_B = 500$ *km*, and $P_{S0} = -45$ *dBm*.

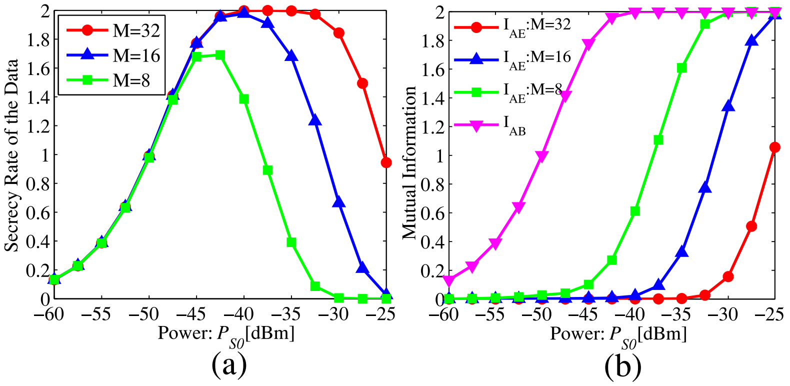
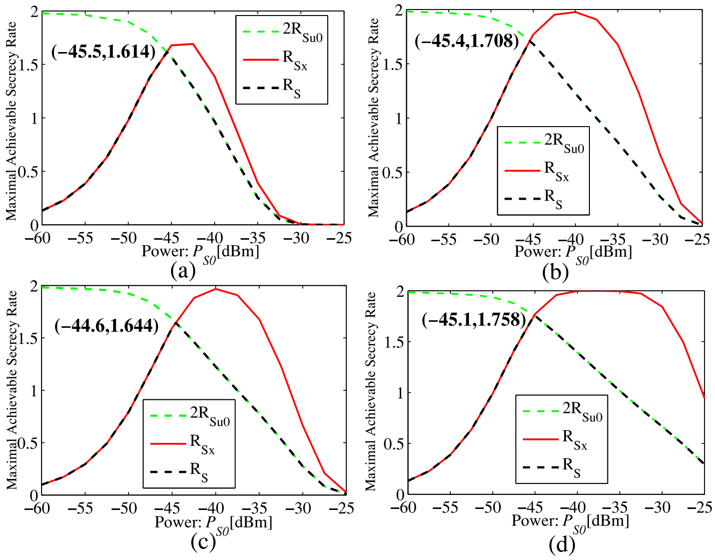


Fig. 8. For $r = 1$, $G_0 = 30$ *dB*, and $L_B = 500$ *km*: (a) Secrecy rate of data, R_{sx}, *vs* P_{S0}; (b) mutual information of Alice-Bob, I_{AB}, and mutual information of Alice-Eve, I_{AE}, *vs* P_{S0}.

increasing multiplicity M, R_{sx} will increase. In fact, M has little influence on the mutual information of Alice-Bob, I_{AB}, while I_{AE} reduces as M increases. Generally, it is beneficial to use the optical amplifier at the transmitter.

Figure 8(a) illustrates the effect of mesoscopic signal power P_{S0} on the secrecy rate of the data R_{sx} for the case $r = 1$, $G_0 = 30$ *dB*, and $L_B = 500$ *km*. Along with the increase of P_{S0}, R_{sx} increases at first, and then maintains a peak value at a certain point or for an interval, and then finally decreases. As M increases, the peak value of R_{sx} increases. For further analysis, the corresponding mutual information of Alice-Bob, I_{AB}, and mutual information of Alice-Eve, I_{AE}, versus P_{S0} is shown in Fig. 8(b). It is observed that I_{AB}, which is irrelevant to M, increases from the beginning until reaching 2, and then keeps the peak value along with the increase of P_{S0}. Moreover, I_{AE} starts to increase only when the mesoscopic signal power is large enough; that is, the basic amplitude α_E is large enough. The turning point (I_{AE} starting to increase) is defined as A. It can be seen that the larger M is, the larger the value taken by A is. The reason is that, as M increases, the wire-tap channel is more sensitive to noise. Therefore, α_E should be larger to better degrade the effect of noise.



(a) (b) (c) (d)

Fig. 9. Maximal reachable secrecy rate R_s and comparison between $2R_{su0}$ and R_{sx} as functions of P_{S0}: (a) $M = 8$, $L_B = 500$ *km*; (b) $M = 16$, $L_B = 500$ *km*; (c) $M = 16$, $L_B = 1000$ *km*; (d) $M = 32$, $L_B = 500$ *km* with $G_0 = 30$ *dB*, and $L_E = 0$ *km* for (a)–(d).

4.3 System Maximum Reachable Secrecy Rate

Finally, the maximum reachable secrecy rate of the system is analyzed by comparing the secrecy rates of the key and the data, i.e., $R_s = \min\{R_{sx}, 2R_{su0}\}$. Fig. 9 plots the variation of R_s, $2R_{su0}$, and R_{sx} versus the mesoscopic signal power P_{S0} in different cases. When P_{S0} is smaller, $R_{sx} < 2R_{su0}$, so R_s is determined by R_{sx} here. In addition, when P_{S0} is large enough, $2R_{su0} < R_{sx}$, so in this case $2R_{su0}$ is the restriction of R_s. From an implementation point of view, it is more practical for actual long-distance transmission when the mesoscopic signal power P_{S0} is higher. Thus, R_s is constrained mainly by $2R_{su0}$. It can be seen that R_s has a peak value in all Fig. 9(a)–(d), which indicate the best scheme for system configuration to optimize the system's security performance under certain conditions.

Through Fig. 9(a)–(d), it can be seen that with increasing multiplicity M the maximum value of R_s increases. This is because $2R_{su0}$ is higher with a larger M, but the increase of R_{sx} is unfortunately irrelevant to M. Therefore, to achieve a higher maximal reachable secrecy rate, more attention should be paid to improving the secrecy rate of the key. Furthermore, comparing Fig. 9(b) and (c), although the cumulative ASE noise, R_s, degrades, the QNRC system can still achieve a very high level of the maximum security rate. For example, the optimal R_S can achieve 1.644 bit/symbol for the case of $M = 16$, $L_B = 1000$ *km*, which means a symbol can carry up to 1.644 bits of information to achieve safe transmission. So if the symbol rate of the QAM-QNRC system is 2.5 Gsymbol/s, the secrecy rate can approach up 4.11 Gbit/s with the key and data both being safe from the perspective of mutual information evaluation.

5. Conclusion

Based on traditional wire-tap channel model analysis method, the security of a QAM-QNRC system is evaluated quantitatively with secrecy rate as a basic performance metric. The wire-tap channel model is established for the key and data separately. Furthermore, taking the secrecy constraints of both the key and data into consideration, the maximum reachable security rate of the system is proposed.

Detailed simulation results show that setting suitable values of pivotal system parameters, such as M (the level of ciphertext m_I or m_Q), inner gain at the transmitter, and mesoscopic signal power, a higher secrecy rate of a QAM-QNRC system can be obtained. Increasing M (the level of ciphertext m_I or m_Q) is a good way to enhance the security of the data or key. Increasing the inner gain at the transmitter will enhance the security of data, and it is also beneficial to improving the security of key against Eve with her strongest ability, while weakening the security of key against Eve with normal ability. As the mesoscopic signal power increases, the secrecy rate of the key decreases, while the secrecy rate of the data first increases, maintains a peak value at a certain point or for an interval, and then finally decreases. Moreover, for the certain system parameters, an optimal value of the mesoscopic signal power to optimize the system's security performance exists. From an implementation point of view, the limitation of the secrecy rate of the key is more critical for the improvement of the system's maximum reachable secrecy rate.

References

[1] M. Schuld and N. Killoran, "Quantum machine learning in feature Hilbert spaces," *Phys. Rev. Lett.*, vol. 122, no. 4, 2019, Art. no. 040504.

[2] J Ji *et al.*, "Improvement of physical-layer security and reliability in coherent time-spreading OCDMA wiretap channel," *Opt. Quantum Electron.*, vol. 50, no. 5, pp. 215.1–215.11, 2018.

[3] F. G. Deng and G. L. Long, "Secure direct communication with a quantum one-time pad," *Phys. Rev. A.*, vol. 69, no. 5, 2004, Art. no. 052319.

[4] K. A. Patel *et al.*, "Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks," *Appl. Phys. Lett.*, vol. 104, no. 5, pp. 1-4, 2014, Art. no. 051123.

[5] R. Nair *et al.*, "Quantum-noise randomized ciphers," *Phys. Rev. A.*, vol. 74, no. 5, 2006, Art. no. 052309.

[6] G. S. Kanter, D. Reilly, and N. Smith, "Practical physical-layer encryption: The marriage of optical noise with traditional cryptography," *IEEE Commun. Mag.*, vol. 47, no. 11, pp. 74–81, Nov. 2009.

[7] Hirota *et al.*, "Quantum stream cipher by the Yuen 2000 protocol: Design and experiment by an intensity-modulation scheme," *Phys. Rev. A.*, vol. 72, no. 2, 2005, Art. no. 022335.

[8] M. Yoshida *et al.*, "Real-time 10 Gbit/s-16 QAM quantum stream cipher transmission over 320 km with FPGA-based transmitter and receiver," in *Proc. OFC/IEEE Opt. Fiber Commun. Conf. Exhib.* 2015, pp. 1-3.

[9] X. K. Yang *et al.*, "Single-carrier QAM/QNSC and PSK/QNSC transmission systems with bit-resolution limited DACs," *Opt. Commun.*, vol. 445, pp. 29–35, 2019.

[10] N. Masataka *et al.*, "QAM quantum noise stream cipher transmission over 100 km with continuous variable quantum key distribution," *IEEE J. Quantum Electron.*, vol. 53, no. 4, Aug. 2017, Art. no. 8000316.

[11] M. Yoshida *et al.*, "Single-channel 40 Gbit/s digital coherent QAM quantum noise stream cipher transmission over 480 km," *Opt. Express.*, vol. 24, no. 1, pp. 652–661, 2016.

[12] G. A. Barbosa *et al.*, "Secure communication using mesoscopic coherent states," *Phys. Rev. Lett.*, vol. 90, no. 22, 2003, Art. no. 227901.

[13] Z L. Yuan *et al.*, "Comment on "Secure Communication using Mesoscopic coherent states"," *Phys. Rev. Lett.*, vol. 94, no. 4, 2005, Art. no. 048901.

[14] S. Tetsuya *et al.*, "Running key mapping in a quantum stream cipher by the Yuen 2000 protocol," *Phys. Rev. A.*, vol. 77, no. 3, 2008, Art. no. 034305.

[15] T. Iwakoshi, "Guessing probability under unlimited known-plaintext attack on secret keys for Y00 quantum stream cipher by quantum multiple hypotheses testing," *Opt. Eng.*, vol. 57, no. 12, 2018, Art. no. 126103.

[16] M. Sohma and O. Hirota, "Coherent pulse position modulation quantum cipher supported by secret key," 2010, *arXiv:Quantum Physics*.

[17] M. J. Mihaljević, "Generic framework for the secure Yuen 2000 quantum-encryption protocol employing the wire-tap channel approach," *Phys. Rev. A.*, vol. 75, no. 5, 2007, Art. no. 052334.

[18] H. S. Jiao *et al.*, "Physical-layer security analysis of PSK quantum-noise randomized cipher in optically amplified links," *Quantum Inf. Process.*, vol. 16, no. 8, 2017, Art. no. 189.

[19] H. S. Jiao *et al.*, "Physical-layer security analysis of a quantum-noise randomized cipher based on the wire-tap channel model," *Opt. Express.*, vol. 25, no. 10, pp. 10947–10960, 2017.

[20] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[21] Y. T. Tan *et al.*, "Performance analysis of physical-layer security in ISK quantum-noise randomized cipher based on wiretap channel," *Opt. Commun.*, vol. 461, 2019, Art. no. 125151.

[22] X. K. Yang *et al.*, "DFTs-OFDM based quantum noise stream cipher system," *Opt. Fiber. Technol.*, vol. 52, 2019, Art. no. 101939.

[23] K. Kato and O. Hirota, "Quantum quadrature amplitude modulation system and its applicability to coherent-state quantum cryptography," *Proc. SPIE - Int. Soc. Opt. Eng.*, vol. 5893, 2005, Art. no. 589303.

[24] K. Kato, M. Osaki, M. Sasaki, and O. Hirota, "Quantum detection and mutual information for QAM and PSK signals," *IEEE Trans. Commun.*, vol. 47, no. 2, pp. 248–254, Feb. 1999.

[25] C. R. Giles *et al.*, "Propagation of signal and noise in concatenated erbium-doped fiber optical amplifiers," *J. Lightw. Technol.*, vol. 9, no. 2, pp. 147–154, Feb. 1991.

[26] Donnet *et al.*, "Security of Y-00 under heterodyne measurement and fast correlation attack," *Phys. Lett. A.*, vol. 356, no. 6, pp. 406–410, 2006.