

## Article

# Joint Resource Allocation for Frequency-Domain Artificial Noise Assisted Multiuser Wiretap OFDM Channels with Finite-Alphabet Inputs

Linhui Fan \*, Bo Tang, Qiuxi Jiang, Fangzheng Liu and Chengyou Yin

College of Electronic Engineering, National University of Defense Technology, Hefei 230037, China

\* Correspondence: fanlinhui17@nudt.edu.cn; Tel.: +86-0551-6592-7148

Received: 27 May 2019; Accepted: 20 June 2019; Published: 1 July 2019



**Abstract:** The security issue on the physical layer is of significant challenge yet of paramount importance for 5G communications. In some previous works, transmit power allocation has already been studied for orthogonal frequency division multiplexing (OFDM) secure communication with Gaussian channel inputs for both a single user and multiple users. Faced with peak transmission power constraints, we adopt discrete channel inputs (e.g., equiprobable Quadrature Phase Shift Keying (QPSK) with symmetry) in a practical communication system, instead of Gaussian channel inputs. Finite-alphabet inputs impose a more significant challenge as compared with conventional Gaussian random inputs for the multiuser wiretap OFDM systems. This paper considers the joint resource allocation in frequency-domain artificial noise (AN) assisted multiuser wiretap OFDM channels with discrete channel inputs. This security problem is formulated as nonconvex sum secrecy rate optimization by jointly optimizing the subcarrier allocation, information-bearing power, and AN-bearing power. To this end, with a suboptimal subcarrier allocation scheme, we propose an efficient iterative algorithm to allocate the power between the information and the AN via the Lagrange duality method. Finally, we carry out some numerical simulations to demonstrate the performance of the proposed algorithm.

**Keywords:** artificial noise (AN); finite-alphabet inputs; multiuser wiretap channels; orthogonal frequency-division multiplexing (OFDM); resource allocation

## 1. Introduction

Recent years have witnessed the rapid development of various 5G communication technologies provided with the high data rate. Wireless services, despite broad popularity, find it challenging to shield transmitted signals from eavesdroppers and are vulnerable to being overheard on the communication link. Therefore, users' privacy concerns and information security issues have received more and more considerable attention (see, e.g., [1–5], and the references therein).

In the realm of traditional wireless information security, encryption-based approaches such as symmetric key schemes (see, e.g., [6,7]) and public key schemes (see, e.g., [8–11]) at higher protocol layers are entrusted to improve the security of wireless networks. With the drastically increasing computation capability of an eavesdropper and the discovery of some encryption cracking algorithms, the basic assumption of “security based on computational complexity” is seriously challenged.

Toward this end, physical layer security has arisen as a novel and attractive alternative in wireless communications. The theoretical foundation for physical layer security techniques has been provided in [12–15]. A network, including a legitimate transmitter (LT), a legitimate receiver (LR) and a passive eavesdropper (PE), was referred to as the wiretap channel introduced by Wyner in [13]. The associated notion of secrecy rate was developed to characterize the achievable transmission rate at

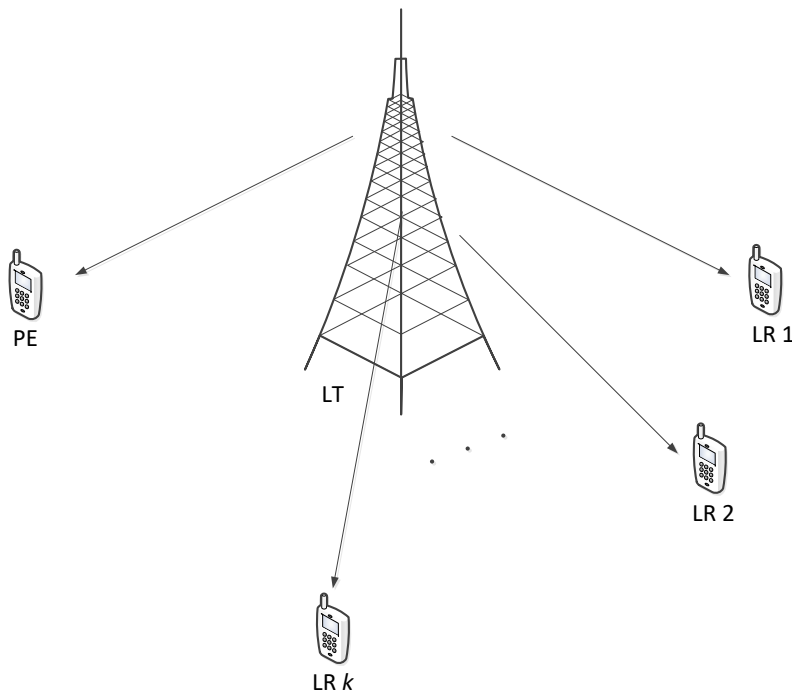
which one LT could reliably send a secret message to one LR while keeping one PE unable to obtain any information. Based on these works, various advanced techniques, such as beamforming, precoding, power allocation, and artificial noise design, have been developed to achieve the secrecy rate in multiple-input-multiple-output (MIMO) orthogonal frequency-division multiplexing (OFDM) systems (see, e.g., [16–19]). References [20–22] showed that the secrecy rate could be improved significantly via appropriate subcarrier (SC) assignment and power allocation in the multiuser wiretap OFDM channels.

As a quite efficient technique to improve physical layer security, artificial noise (AN), which is generated in the transmit design, was proposed to degrade eavesdroppers' receptions. The original AN scheme in [19] was presented for multiple-antenna transmission. Then, spatial AN [23–25], temporal AN [26,27], and frequency-domain AN [28,29] were developed to maximize the secrecy rate in the wiretap channel. Recently, a huge body of literature has been based on real interference alignment with non-Gaussian inputs. It turns out that interference alignment proposed in [30] plays a central role in achieving the optimal secure degrees of freedom (d.o.f.) and is an alternative but insightful technology for both Gaussian inputs and a discrete constellation. However, existing results for the multiuser wiretap OFDM channels focus on a simple scenario where the transmitter employs Gaussian distribution inputs. Moreover, Gaussian symbols are not realizable in practice because of the arbitrarily large peak transmit power and the infinite detection complexities. Thus, communication signals are likely to be finite alphabet symbols. This limitation reveals that the achievable secrecy rate for discrete inputs would significantly differ from that under the Gaussian input assumption (see, e.g., [31–34]). In [29], the sum secrecy rate for the random Gaussian codebook is optimized for the frequency-domain AN-aided multiuser OFDM systems, while the signals under finite-alphabet constellations constraint are not considered. Therefore, it is of importance to investigate the effect of arbitrary input distribution on the sum secrecy rate in multiuser wiretap OFDM channels.

In this paper, inspired by the reasons mentioned above, we consider the optimal resource allocation with discrete channel inputs in the AN-aided multiuser wiretap OFDM channels, as shown in Figure 1. Different from the Gaussian inputs [29], we develop a frequency-domain AN methodology with finite-alphabet symbols to jointly optimize the SC allocation and the power allocation of information signals and AN signals. Exploiting the transmission diversity provided by the frequency-domain AN addition and removal method, we aim at generating independent AN on each SC at the LT and canceling it at each LR such that only the PE is degraded. We make the assumption that the LT has public knowledge of instantaneous channel state information (CSI) associated with multiple LRs and the PE. This assumption may be valid in certain scenarios where the LRs and the PE are peer nodes in the system. The formulated problem can be treated as a mixed integer programming problem, which is non-convex. To cope with this question, we develop a joint design algorithm for information power, AN power, and SC allocation based on the Lagrange dual method. In the case of discrete finite-alphabet inputs, numerical results are presented to show that the proposed method can boost the secrecy rate considerably.

The rest of this paper is organized as follows. In Section 2, we establish the system model with finite-alphabet input constraints in the frequency-domain AN-aided multiuser wiretap OFDM channels and then formulate the optimization problem on the sum secrecy rate considered in this paper. In Section 3, a resource allocation algorithm for discrete inputs based on the Lagrange duality method is presented to tackle the optimization problem. Section 4 illustrates simulation results to demonstrate the performance of proposed algorithms. Finally, we draw the conclusion in Section 5.

We use bold lowercase letters and uppercase letters to denote vectors and matrices, respectively.  $\mathbb{C}$  represents the set of complex numbers.  $x \sim \mathcal{CN}(0, \sigma^2)$  denotes that  $x$  is a complex Gaussian random variable with zero mean and variance  $\sigma^2$ .  $\mathcal{I}(x; y)$  denotes the mutual information between random variables  $x$  and  $y$ .  $[x]^+$  is defined as  $\max\{x, 0\}$ , and  $f'(x_0)$  denotes the first derivative of  $f(x)$  at the point  $x_0$ .



**Figure 1.** Illustration of a multiuser wiretap orthogonal frequency-division multiplexing (OFDM) system, including one legitimate transmitter (LT),  $K$  legitimate receivers (LRs) and one passive eavesdropper (PE).

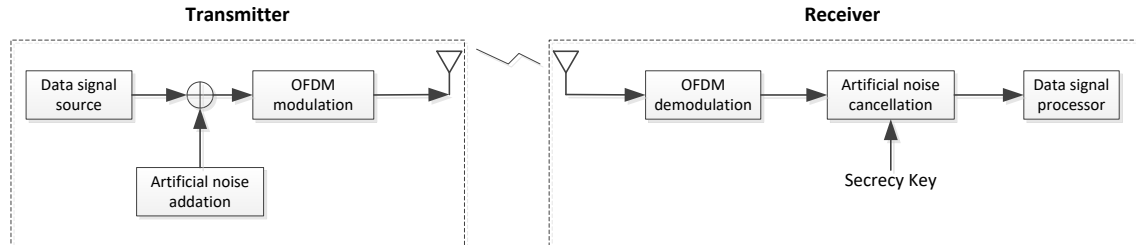
## 2. System Model and Problem Formulation

In this paper, we consider a frequency-domain AN-aided multiuser OFDM system with  $N$  SCs for finite-alphabet constellations in the wiretap channels, as illustrated in Figure 1. The system consists of one LT,  $K$  LRs and one PE, all with a single transmit antenna. We denote the sets of SCs and multiple users as  $\mathcal{N} = \{1, \dots, N\}$  and  $\mathcal{K} = \{1, \dots, K\}$ , respectively. It is assumed that the LT perfectly knows the CSIs on SC  $i \in \mathcal{N}$  of the LRs as well as the PE. This is practically valid in scenarios where the eavesdropper cooperates with its peer nodes at some time but is not trusted by the legitimate nodes during a certain time. In this situation, the CSI of the eavesdropper can be obtained by monitoring the possible transmission activities of the eavesdropper (see, e.g., [29,35] and the references therein for identical assumptions). We denote  $H_{k,i} \in \mathbb{C}$  and  $G_i \in \mathbb{C}$  as the frequency channel coefficients over SC  $i$  from the LT to the LR  $k$  and the PE, respectively. Since the redundancy is provided by the asymmetry between the filter shapes for the LT and the LR, we further consider the time slotted OFDM symbols by assuming that the wireless channel remains constant over each time slot, but can vary from one-time slot to another.

In this system, one LT sends confidential information to  $K$  LRs in the presence of one PE. As a control center, the LT performs the SC allocation and then notifies all LRs of the corresponding SCs for them by signals. We denote  $\pi_{k,i}$  as the SC assignment indicator for the LR  $k$  over the SC  $i$ , which means  $\pi_{k,i} = 1$  when the LR  $k$  can communicate on the SC  $i$ , while  $\pi_{k,i} = 0$ , otherwise. Herein, any SC only can be assigned to at most one LR, i.e.,  $\sum_{k=1}^K \pi_{k,i} = 1, \forall i \in \mathcal{N}$ .

To degrade the channel performance at the PE against its eavesdropping, the LT adds AN signals to the transmit signals. We adopt the “key” distribution method for generating and removing AN in the frequency domain with practical complexity, as shown in Figure 2 (see, e.g., [28,29,36–38] and the references therein for the similar setting). By leveraging the independence and short-term reciprocity of the wireless channels, the LT sends the corresponding keys with the secret method (see [39] for more details) at each time. This novel frequency domain AN scheme differs from the traditional AN in the

frequency domain, which cannot improve the secrecy rate of single-antenna wiretap channels (see, e.g., [26,29] and the references therein for the proof). With the distribution method, the key is secretly sent without being wiretapped by the PE. Accordingly, the PE does not have the ability to cancel AN used at each SC, but the LR does.



**Figure 2.** Block diagram of an OFDM transmitter and receiver with artificial noise (AN) addition and cancellation procedure in a wiretap channel.

As the sum of a confidential information signal  $s_{k,i}$  and an AN signal  $a_i$ , the transmitted signal  $x_{k,i}$  from the LT to the LR  $k$  over the SC  $i$  is expressed by

$$x_{k,i} = \pi_{k,i} \sqrt{p_{k,i}} s_{k,i} + \sqrt{\sigma_{a,i}^2} a_i, \quad (1)$$

where  $p_{k,i} \geq 0$  and  $\sigma_{a,i}^2 \geq 0$  denote the corresponding transmit power of  $s_{k,i}$  and  $a_i$ , respectively. It is apparent that  $p_{k,i} = 0$  when  $\pi_{k,i} = 0$ . Then we assume that  $s_{k,i}$  and  $a_i$  denote a complex discrete random variable and a complex Gaussian random variable with zero mean and unit variance, which are also statistically independent across the SC, respectively.

Then, following the system block diagram in Figure 2, the corresponding signals received by the LR  $k$  and the PE (which is wiretapping all the LRs) over the SC  $i$  can be expressed as

$$y_{k,i} = H_{k,i} x_{k,i} + w_{k,i} \quad (2)$$

$$= H_{k,i} \pi_{k,i} \sqrt{p_{k,i}} s_{k,i} + H_{k,i} \sqrt{\sigma_{a,i}^2} a_i + w_{k,i},$$

$$z_i = G_i \sum_{k=1}^K x_{k,i} + v_i \quad (3)$$

$$= G_i \sum_{k=1}^K \pi_{k,i} \sqrt{p_{k,i}} s_{k,i} + G_i \sqrt{\sigma_{a,i}^2} a_i + v_i,$$

where  $w_{k,i}$  and  $v_i$  denote zero-mean independently and identically distributed (i.i.d.) Additive White Gaussian Noise (AWGN) samples with variance  $\sigma_{w_k}^2$  and  $\sigma_v^2$ , respectively. Without loss of generality, it is assumed that  $\sigma_{w_k}^2 = \sigma_v^2 = 1$ .

Based on the above AN design scheme, the AN can be removed at the LR  $k$  over each SC before decoding the confidential information signal  $s_{k,i}$ , but not possibly at the PE. Then, after the AN removal, the received signals of the LR  $k$  and the PE over SC  $i$  can be equivalently written by

$$y_{k,i} = H_{k,i} \pi_{k,i} \sqrt{p_{k,i}} s_{k,i} + w_{k,i}, \quad (4)$$

$$z_i = G_i \sum_{k=1}^K \pi_{k,i} \sqrt{p_{k,i}} s_{k,i} + G_i \sqrt{\sigma_{a,i}^2} a_i + v_i. \quad (5)$$

According to [16], the achievable secrecy rate of the LR  $k$  associated with the signal model in Equations (4) and (5) can be obtained as

$$R_k(p_{k,i}, \pi_{k,i}, \sigma_{a,i}^2) \quad (6a)$$

$$= \sum_{i=1}^N [\mathcal{I}(s_{k,i}; H_{k,i} \pi_{k,i} \sqrt{p_{k,i}} s_{k,i} + w_{k,i}) - \mathcal{I}(s_{k,i}; G_i \pi_{k,i} \sqrt{p_{k,i}} s_{k,i} + G_i \sqrt{\sigma_{a,i}^2} a_i + v_i)]^+ \quad (6b)$$

$$= \sum_{i=1}^N [\mathcal{I}(s_{k,i}; \pi_{k,i} H_{k,i} \sqrt{p_{k,i}} s_{k,i} + w_{k,i}) - \mathcal{I}(s_{k,i}; \frac{\pi_{k,i} G_i}{\sqrt{|G_i|^2 \sigma_{a,i}^2 + 1}} \sqrt{p_{k,i}} s_{k,i} + \hat{v}_i)]^+, \quad (6c)$$

with  $\hat{v}_i = \frac{G_i \sqrt{\sigma_{a,i}^2} a_i + v_i}{\sqrt{|G_i|^2 \sigma_{a,i}^2 + 1}} \sim \mathcal{CN}(0, 1)$ .

Under the transmit power constraint, the sum secrecy rate optimization problem can be formulated as

$$\max_{\pi, \mathbf{p}, \sigma_a^2} R_{sum}(\pi, \mathbf{p}, \sigma_a^2) \quad (7a)$$

$$\text{s.t.} \sum_{i=1}^N \sum_{k=1}^K \pi_{k,i} p_{k,i} + \sum_{i=1}^N \sigma_{a,i}^2 \leq P \quad (7b)$$

$$p_{k,i} \geq 0, \forall i \in \mathcal{N}, k \in \mathcal{K} \quad (7c)$$

$$\sigma_{a,i}^2 \geq 0, \forall i \in \mathcal{N}, k \in \mathcal{K} \quad (7d)$$

$$\pi_{k,i} \in \{0, 1\}, \forall i \in \mathcal{N}, k \in \mathcal{K} \quad (7e)$$

$$\sum_{k=1}^K \pi_{k,i} = 1, \forall i \in \mathcal{N} \quad (7f)$$

where  $R_{sum}(\pi, \mathbf{p}, \sigma_a^2) \triangleq \sum_{k=1}^K R_k(p_{k,i}, \pi_{k,i}, \sigma_{a,i}^2)$  is denoted as the sum secrecy rate,  $\mathbf{p} = \{p_{k,i}\}$  is denoted as the power allocation of information signal,  $\pi \triangleq \{\pi_{k,i}\}$  is denoted as the SC allocation for LRs,  $\sigma_a^2 \triangleq \{\sigma_{a,i}^2\}$  is denoted as the power allocation of AN signal, and  $P$  in Equation (7b) is the achievable maximal transmit power.

### 3. Optimal Solution

Note that the optimization Equation (7) is a mixed integer programming and thus is non-convex, which is difficult to tackle. In order to reduce the complexity of solving the Equation (7), we adopt the suboptimal SC allocation scheme in [22] is given by

$$\pi_{k,i}^* = \begin{cases} 1, & \text{if } k = \arg \max\{|H_{k',i}|^2, k' \in \mathcal{K}\}; \\ 0, & \text{otherwise.} \end{cases}, \quad \forall i \in \mathcal{N}. \quad (8)$$

Then, considering the above SC allocation, we can recast the optimization problem in Equation (7) as

$$\max_{\mathbf{p}, \sigma_a^2} R_{sum}(\mathbf{p}, \sigma_a^2 | \pi^*) \quad (9a)$$

$$\text{s.t.} \sum_{i=1}^N \sum_{k=1}^K \pi_{k,i}^* p_{k,i} + \sum_{i=1}^N \sigma_{a,i}^2 \leq P \quad (9b)$$

$$p_{k,i} \geq 0, \forall i \in \mathcal{N}, k \in \mathcal{K} \quad (9c)$$

$$\sigma_{a,i}^2 \geq 0, \forall i \in \mathcal{N}, k \in \mathcal{K} \quad (9d)$$

where  $\pi^*$  is given by Equation (8).

Herein, we consider the Lagrange duality method to tackle the problem in Equation (9) asymptotically optimally. Using the result in [40,41], we can obtain that the duality gap becomes zero in the order of  $O(1/\sqrt{N})$  for OFDM-based power allocation Equation (9) as  $N$  goes to infinity, due to the mild condition that the channel has a finite delay spread. The partial Lagrange of the Equation (9) is formulated by

$$L(\mathbf{p}, \sigma_a^2, \lambda | \pi^*) = \sum_{i=1}^N \sum_{k=1}^K [\mathcal{I}(s_{k,i}; \pi_{k,i}^* H_{k,i} \sqrt{p_{k,i}} s_{k,i} + w_{k,i}) - \mathcal{I}(s_{k,i}; \frac{\pi_{k,i}^* G_i}{\sqrt{|G_i|^2 \sigma_{a,i}^2 + 1}} \sqrt{p_{k,i}} s_{k,i} + \hat{v}_i)]^+ + \lambda (P - \sum_{i=1}^N \sum_{k=1}^K \pi_{k,i}^* p_{k,i} - \sum_{i=1}^N \sigma_{a,i}^2), \quad (10)$$

where  $\lambda$  is the Lagrange multiplier associated with Equation (9b).

The dual problem is given by

$$D^* = \min_{\lambda \geq 0} D(\lambda), \quad (11)$$

where  $D^*$  denotes the optimal dual objective value and the dual function for the Equation (9) is expressed as

$$D(\lambda) = \max_{\sigma_a^2 \geq 0, \mathbf{p} \geq 0} L(\mathbf{p}, \sigma_a^2, \lambda | \pi^*). \quad (12)$$

Notice that  $D(\lambda)$  is a convex function in  $\lambda$  [42] and its subgradient

$$\nabla D(\lambda) \triangleq P - \sum_{i=1}^N \sum_{k=1}^K \pi_{k,i}^* p_{k,i}^* - \sum_{i=1}^N \sigma_{a,i}^{*2}, \quad (13)$$

where  $p_{k,i}^*$  and  $\sigma_{a,i}^{*2}$  are the optimal solutions to Equation (9) for fixed  $\lambda$ . We can update efficiently the dual variable  $\lambda^*$  with bisection method and the associated solution  $(p_{k,i}^*, \sigma_{a,i}^{*2})$  in Equation (12) with the obtained primal solution, respectively.

Then, we can observe that the maximization in Equation (12) can be decomposed into  $N$  independent subproblems, rewritten as

$$D(\lambda) = \sum_{i=1}^N B(p_{k,i}, \sigma_{a,i}^2 | \lambda, \pi_{k,i}^*) + \lambda P, \quad (14)$$

where  $B(p_{k,i}, \sigma_{a,i}^2 | \lambda, \pi_{k,i}^*)$  is obtained by

$$B(p_{k,i}, \sigma_{a,i}^2 | \lambda, \pi_{k,i}^*) = \max_{p_{k,i} \geq 0, \sigma_{a,i}^2 \geq 0} \sum_{k=1}^K [\mathcal{I}(s_{k,i}; \pi_{k,i}^* H_{k,i} \sqrt{p_{k,i}} s_{k,i} + w_{k,i}) - \mathcal{I}(s_{k,i}; \frac{\pi_{k,i}^* G_i}{\sqrt{|G_i|^2 \sigma_{a,i}^2 + 1}} \sqrt{p_{k,i}} s_{k,i} + \hat{v}_i)]^+ - \lambda (\sum_{k=1}^K \pi_{k,i}^* p_{k,i} + \sigma_{a,i}^2). \quad (15)$$

According to the constraint in Equation (7f), for fixed  $i$ , only one term among  $\{\mathcal{I}(s_{k,i}; \pi_{k,i}^* H_{k,i} \sqrt{p_{k,i}} s_{k,i} + w_{k,i}) - \mathcal{I}(s_{k,i}; \frac{\pi_{k,i}^* G_i}{\sqrt{|G_i|^2 \sigma_{a,i}^2 + 1}} \sqrt{p_{k,i}} s_{k,i} + \hat{v}_i), k \in \mathcal{K}\}$  is non-zero. Therefore, we can simplify the solution of the problem in Equation (15).

In what follows, since the objective function of the Equation (15) is not concave in  $(p_{k,i}, \sigma_{a,i}^2)$ , we exploit the coordinate descent method [43] to tackle the Equation (15). In particular, we obtain the maximization in Equation (15) with respect to (w.r.t.)  $p_{k,i}$  for  $\sigma_{a,i}^2$  given and that w.r.t.  $\sigma_{a,i}^2$  for  $p_{k,i}$  given. We present the details as follows.

### 3.1. Update of $p_{k,i}$ with Given $\sigma_{a,i}^2$

With  $\sigma_{a,i}^2$  given, the optimal  $p_{k,i}$  of the Equation (15) can be obtained via simple line search [42], expressed by

$$p_{k,i}^* = \arg \max_{p_{k,i} \geq 0} \{ [\mathcal{I}(s_{k,i}; \pi_{k,i}^* H_{k,i} \sqrt{p_{k,i}} s_{k,i} + w_{k,i}) - \mathcal{I}(s_{k,i}; \frac{\pi_{k,i}^* G_i}{\sqrt{|G_i|^2 \sigma_{a,i}^2 + 1}} \sqrt{p_{k,i}} s_{k,i} + \hat{v}_i)]^+ - \lambda \pi_{k,i}^* p_{k,i} \}. \quad (16)$$

### 3.2. Update of $\sigma_{a,i}^2$ with Given $p_{k,i}$

Next, we consider the optimization of Equation (15) for a given  $p_{k,i}$ . Since the solution  $p_{k,i}$  obtained by Equation (16) ensures the term  $\mathcal{I}(s_{k,i}; \pi_{k,i}^* H_{k,i} \sqrt{p_{k,i}} s_{k,i} + w_{k,i}) - \mathcal{I}(s_{k,i}; \frac{\pi_{k,i}^* G_i}{\sqrt{|G_i|^2 \sigma_{a,i}^2 + 1}} \sqrt{p_{k,i}} s_{k,i} + \hat{v}_i)$  is nonnegative, it is easy to verify that the optimization problem in Equation (15) is equivalent to

$$\min_{\sigma_{a,i}^2 \geq 0} \sum_{k=1}^K T_{k,i}(\sigma_{a,i}^2) + \lambda \sigma_{a,i}^2, \quad (17)$$

where

$$T_{k,i}(\sigma_{a,i}^2) \triangleq \mathcal{I} \left( s_{k,i}; \frac{\pi_{k,i}^* G_i}{\sqrt{|G_i|^2 \sigma_{a,i}^2 + 1}} \sqrt{p_{k,i}} s_{k,i} + \hat{v}_i \right). \quad (18)$$

Now we adopt a successive convex approximation (SCA) method where the original problem is converted into a sequence of semi-definite program (SDP) problems. The SCA method ensures the stability and the guarantee of the convergence.

Let  $t_i = (|G_i|^2 \sigma_{a,i}^2 + 1)^{-1}$  such that  $T_{k,i}(t_i) \triangleq T_{k,i}(\sigma_{a,i}^2)$ , then the first derivative of  $T_{k,i}(t_i)$  w.r.t.  $t_i$  is expressed as [44]

$$T'_{k,i}(t_i) = \pi_{k,i}^* |G_i|^2 p_{k,i} \text{mmse} \left( \pi_{k,i}^* |G_i|^2 p_{k,i} t_i \right). \quad (19)$$

Using the expression in Equation (19), we can obtain the first-order approximation to  $T_{k,i}(t_i)$  at the point  $\bar{t}_i$ :

$$\tilde{T}_{k,i}(t_i) = T_{k,i}(\bar{t}_i) + T'_{k,i}(\bar{t}_i) (t_i - \bar{t}_i), \quad (20)$$

with  $\bar{t}_i = (|G_i|^2 \sigma_a^2 + 1)^{-1}$  and  $\bar{t}_i$  denoting the one solved in the previous iteration. Therefore, Equation (17) can be reformulated with the above first-order approximation:

$$\min_{\sigma_{a,i}^2 \geq 0, t_i} \sum_{k=1}^K \tilde{T}_{k,i}(t_i) + \lambda \sigma_{a,i}^2 \quad (21a)$$

$$\text{s.t.} \quad t_i = (|G_i|^2 \sigma_{a,i}^2 + 1)^{-1}. \quad (21b)$$

Furthermore, we show that the approximated Equation (21) can be treated as a convex SDP. Omitting all the terms not depending on  $\sigma_{a,i}^2$  and  $t_i$ , Equation (21) can be equivalently cast as

$$\min_{\sigma_{a,i}^2 \geq 0, t_i} \sum_{k=1}^K \pi_{k,i}^* |G_i|^2 p_{k,i} \left[ \text{mmse} \left( \frac{\pi_{k,i}^* |G_i|^2 p_{k,i}}{|G_i|^2 \sigma_a^2 + 1} \right) \right] t_i + \lambda \sigma_{a,i}^2 \quad (22a)$$

$$\text{s.t.} \quad t_i = (|G_i|^2 \sigma_{a,i}^2 + 1)^{-1}. \quad (22b)$$



Considering nonnegative MMSE, we can recast the problem in Equation (22) as

$$\min_{\sigma_{a,i}^2 \geq 0, t_i} \sum_{k=1}^K \pi_{k,i}^* |G_i|^2 p_{k,i} \left[ \text{mmse} \left( \frac{\pi_{k,i}^* |G_i|^2 p_{k,i}}{|G_i|^2 \sigma_a^2 + 1} \right) \right] t_i + \lambda \sigma_{a,i}^2 \quad (23a)$$

$$\text{s.t.} \quad t_i \geq \left( |G_i|^2 \sigma_{a,i}^2 + 1 \right)^{-1}. \quad (23b)$$

According to Shur complement [42], Equation (23) can be rewritten by

$$\min_{\sigma_{a,i}^2 \geq 0, t_i} \sum_{k=1}^K \pi_{k,i}^* |G_i|^2 p_{k,i} \left[ \text{mmse} \left( \frac{\pi_{k,i}^* |G_i|^2 p_{k,i}}{|G_i|^2 \sigma_a^2 + 1} \right) \right] t_i + \lambda \sigma_{a,i}^2 \quad (24a)$$

$$\text{s.t.} \quad \begin{bmatrix} |G_i|^2 \sigma_{a,i}^2 + 1 & 1 \\ 1 & t_i \end{bmatrix} \succeq \mathbf{0}. \quad (24b)$$

It is easy to verify that we apply convex solvers (e.g., CVX [45]) to solve Equation (24) which is a standard SDP.

We prove the convergence of the proposed SCA algorithm. Let  $\tilde{T}_{k,i}$  in Equation (20) denote the first-order convex approximation of the function  $T_{k,i}$ . As a consequence, we can obtain that

$$T_{k,i}(\bar{t}_i) = \tilde{T}_{k,i}(\bar{t}_i) \quad (25a)$$

$$\geq \tilde{T}_{k,i}(t_i) \quad (25b)$$

$$\geq T_{k,i}(t_i), \quad (25c)$$

where Equation (25a) holds by substituting  $t_i$  with  $\bar{t}_i$  in Equation (20), Equation (25b) is due to the optimality of  $t_i$  at the next iteration, and Equation (25c) is due to the concavity of  $T_{k,i}$  w.r.t.  $t_i$  [46]. Hence, according to [47], the proposed SCA algorithm will converge to a point leading to a locally optimal solution of Equation (17), which satisfies KKT conditions of the original Equation (17). Finally, Algorithm 1 summarizes the joint power allocation algorithm of artificial noise and information signals for solving Equation (9) based on the Lagrange dual method and the SCA algorithm is summarized in step 2.2 of the Algorithm 1.

---

**Algorithm 1:** Joint power allocation of artificial noise and information signals for solving Equation (9).

---

**Input:**  $\lambda_h > \lambda_l = 0, \pi^*$

**Output:**  $\mathbf{p}, \sigma_a^2$ .

1 **repeat**

2     Step 1: update  $\lambda = \frac{1}{2}(\lambda_h + \lambda_l)$

3     Step 2:

4         **repeat**

5             Step 2.1: obtain  $\mathbf{p}$  by solving Equation (16)

6             Step 2.2: obtain the optimal  $\sigma_a^2$

7             **repeat**

8                 Step 2.2.1: solve Equation (24) by CVX

9                 Step 2.2.2: set  $\bar{\sigma}_a^2 = \sigma_a^2$

10             **until** a specified convergence criterion is satisfied.;

11     **until**  $L(\mathbf{p}, \sigma_a^2, \lambda | \pi^*)$  meets a specified convergence criterion.;

12     Step 3: if  $\sum_{i=1}^N \sum_{k=1}^K \pi_{k,i}^* p_{k,i} + \sum_{i=1}^N \sigma_{a,i}^2 < P$ , then update  $\lambda_h = \lambda$ , else update  $\lambda_l = \lambda$ .

13 **until**  $\lambda$  meets a specified convergence criterion.;

---



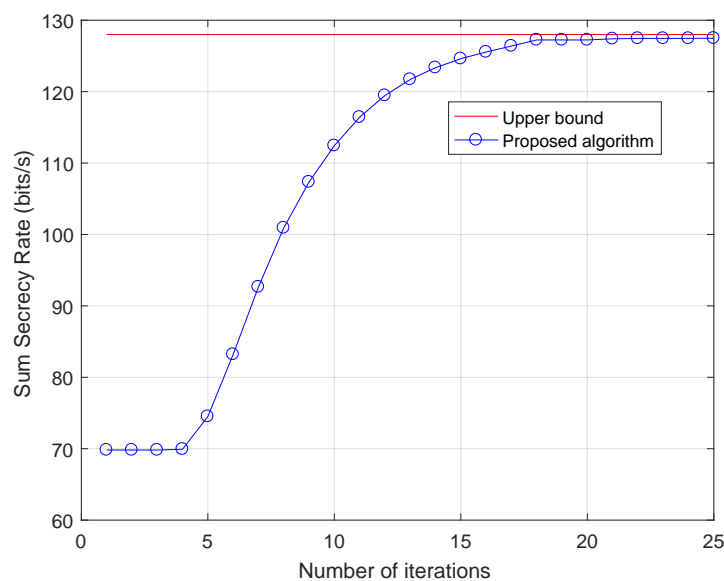
### 3.3. Computational Complexity Analysis

In this subsection, we analyze the computational complexity of the proposed algorithm. The computational complexity of the proposed depends on the number of iterations and the complexity involved at each iteration. Precisely, in every iteration, the computational complexity is mainly due to Equation (24). In addition, the optimization of  $\sigma_a^2$  through solving the SDP in Equation (24) requires  $O(N^{4.5})$  operations [48].

## 4. Numerical Results

In this section, we provide some numerical results to demonstrate the efficacy of our proposed algorithm, including the effects of AN and the multiuser diversity. Then, we consider that the OFDM system has  $N = 64$  SCs with both Gaussian (denoted by “Gau”) and Quadrature Phase Shift Keying (QPSK) inputs. In the simulation setup, the channel coefficients only consist of small-scale fading, which is modeled as Rayleigh fading. Each channel realization is assumed to be composed of 8 i.i.d. Rayleigh fading paths with the maximum time delay of 7 samples and the unit channel power. The numerical results are averaged over 50 channel realizations for each simulation point, with  $\text{SNR} = P$  in which artificial noise power is included in the total transmit power  $P$ . Finally, all the numerical results are performed on a standard PC with CPU CoRe i7-770 3.6 GHz and 16 GB memory.

First, we analyze the convergence of the proposed algorithm and compare it with the upper bound, which is obtained by the classical water-filling [49] under the transmission without PE. From Figure 3, the result shows a monotonically increasing behavior of the devised algorithm with increasing number of iterations. Meanwhile, the sum secrecy rate of the proposed algorithm is about 0.52 away from the upper bound. This is because there are some LR’s channels which are worse than the PE’s channels (i.e.,  $\{i ||H_{k,i}|^2 < |G_i|^2, i \in \mathcal{N}, k \in \mathcal{K}\}$ ).



**Figure 3.** The convergence of the proposed algorithm,  $K = 10$ ,  $P = 25$  dB.

Second, we analyze the sum secrecy rate performance for the proposed algorithm. The proposed suboptimal SC assignment in Equation (8) is compared with the fixed SC assignment, while the joint power allocation of artificial noise and data signals is optimized by Algorithm 1 for QPSK inputs (denoted by “QPSK, AN”). Moreover, we compare the proposed algorithm with Algorithm 2 in [22] for Gaussian inputs (denoted by “Gau, AN”). For performance comparison, we also consider the transmissions without PE (denoted by “QPSK, no PE” for QPSK inputs and “Gau, no PE” for Gaussian) which is the upper bound obtained by the classical water-filling [49] and without using AN which can be easily obtained by  $\sigma_a^2 = 0$  in Step 2.2 of the Algorithm 1 for discrete inputs (denoted by “QPSK,

no AN”) and by  $\sigma_a^2 = 0$  of the Algorithm 2 in [22] for Gaussian inputs (denoted by “Gau, no AN”), as benchmarks, respectively.

Figure 4 illustrates the sum secrecy rate of various LRs’ number versus the SNR for QPSK and Gaussian inputs obtained by the different algorithms in the case of suboptimal SC assignment scheme. As expected, Figure 4a depicts that compared to Gaussian inputs, discrete inputs for current practical systems suffer a significant loss in secrecy performance. Then, Figure 4b shows the zoomed version associated with Figure 4a for only QPSK inputs. As shown in Figure 4b, we can observe a monotonically increasing sum secrecy rate of the proposed algorithm with SNR increasing. Furthermore, at all the SNR region, the sum secrecy rate of 10 LR is among the best, better than that of 4 LR, significantly outperforming that of 2 LR. In addition, for 2 LR, 4 LR, and 10 LR, the amount of performance difference between “QPSK, no PE” and “QPSK, AN” have almost identical behavior as the sum secrecy rate. This is because that, the multiuser diversity, gained by suboptimal SC assignment scheme, makes the LR’s channels better than the PE’s channels (i.e.,  $\{i||H_{k,i}|^2 > |G_i|^2, i \in \mathcal{N}, k \in \mathcal{K}\}$ ). In addition, the sum secrecy rate of 10 LR almost reaches the performance of “no PE” in the high SNR area. Moreover, the performance of the devised Algorithm is expectantly better than that of the “no AN” algorithm, especially in high SNR regime. The reason for this is that the use of AN can degrade the CSI of the LT-PE link to improve LR’s secrecy rates. These are also identical to the observations in [20,22]. Figure 4c presents the zoomed version of 10 LR associated with Figure 4a for QPSK inputs and Gaussian inputs. It can be observed from this figure that the amount of performance difference between “no PE” and “AN” for Gaussian inputs saturates in the high SNR regime, but it tends to be smaller for QPSK inputs.

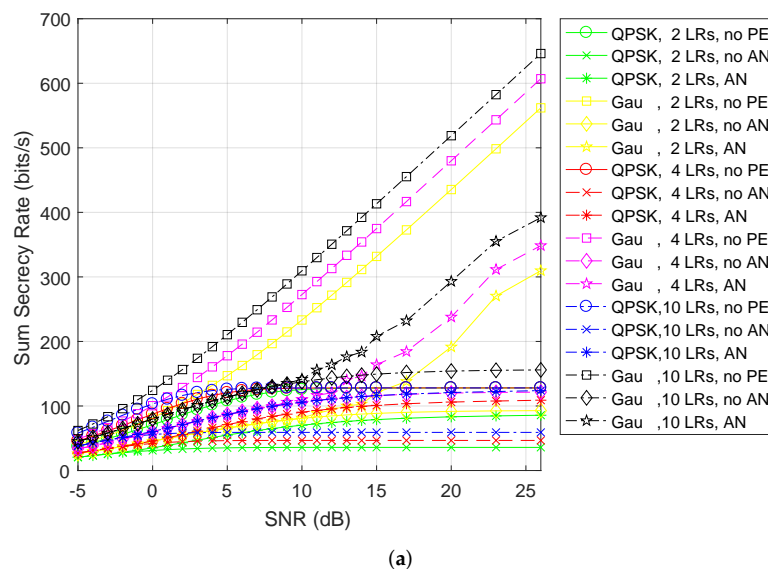
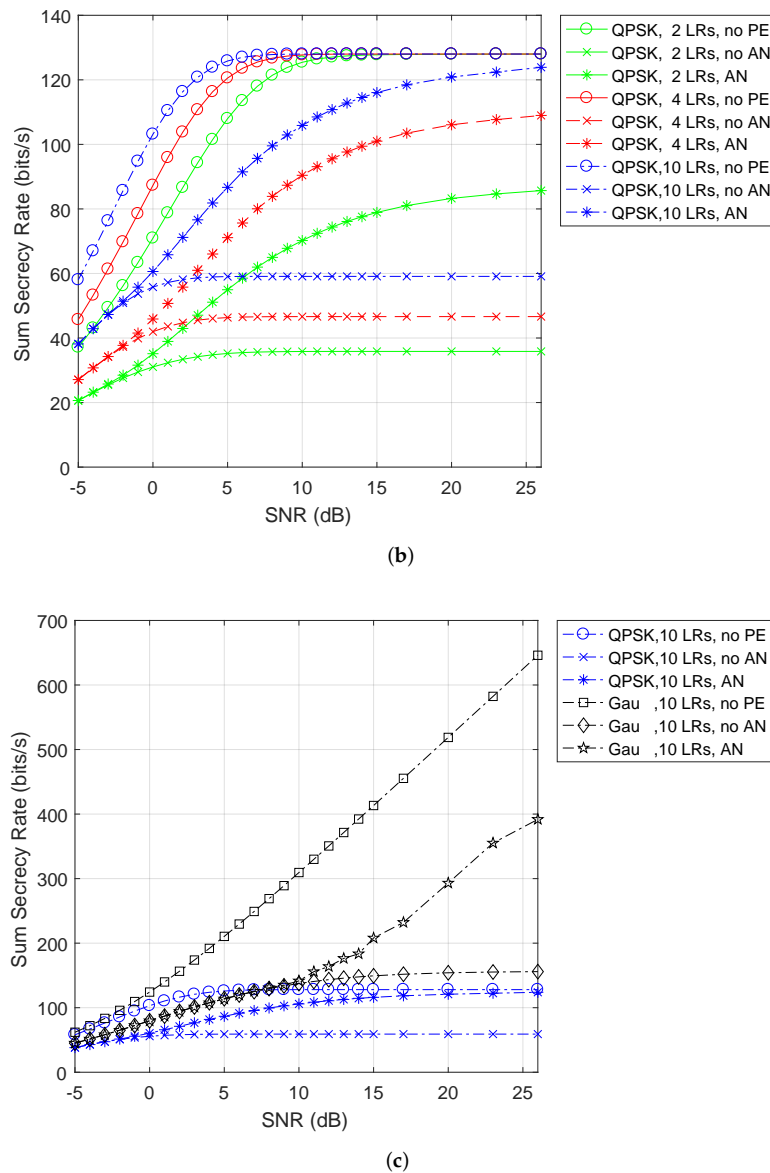


Figure 4. Cont.



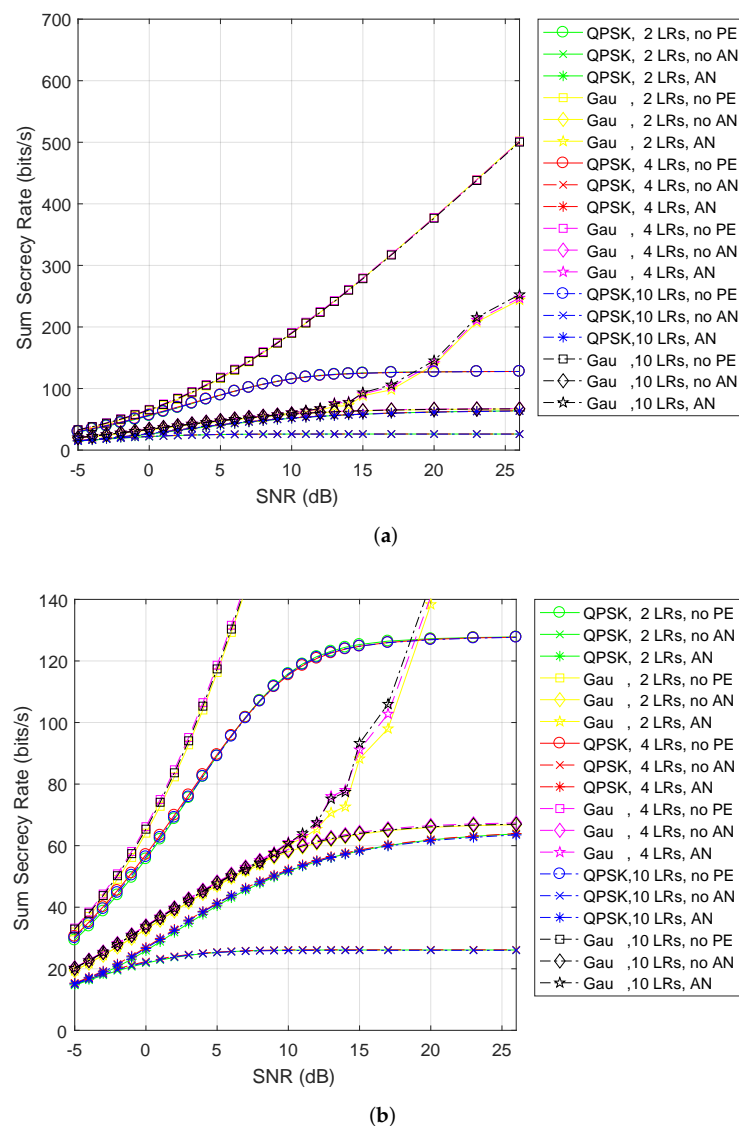
**Figure 4.** (a) Sum secrecy rate for both Gaussian and Quadrature Phase Shift Keying (QPSK) inputs. (b) Sum secrecy rate of various LRs' number for QPSK inputs. (c) Sum secrecy rate of 10 LRs for Gaussian and QPSK inputs. The SC assignment scheme in Equation (8).

Next, if we consider the fixed SC assignment, shown as in Figure 5, we can observe that the performance of sum secrecy rate corresponding to 2 LRs, 4 LRs and 10 LRs for various algorithms are almost identical, respectively. This also verifies the penalty for ignorance of the SC allocation can be quite large in practice.

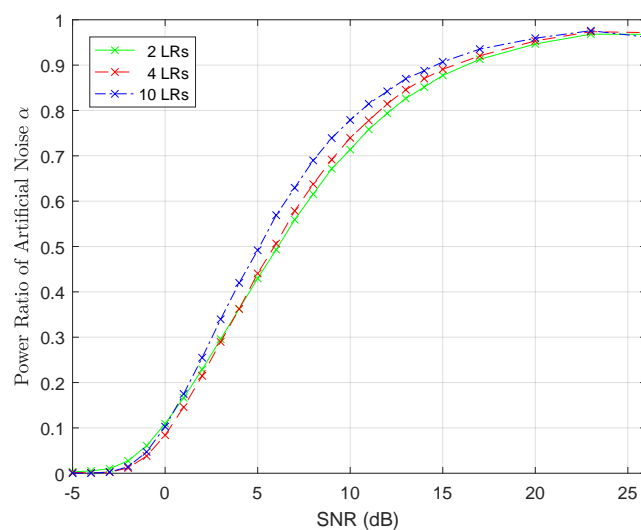
Finally, Figure 6 further presents the power ratio of artificial noise calculated using the devised algorithm. Besides, the power ratio of artificial noise is denoted by

$$\alpha = \frac{\sum_{i=1}^N \sigma_{a,i}^2}{P}. \quad (26)$$

We can observe from this figure that, for any number of LRs, the power ratio allocated to artificial noise increases monotonically as SNR increases. The results indicate that the frequency-domain AN can degrade the performance of the PE.



**Figure 5.** (a) Sum secrecy rate for both Gaussian and QPSK inputs. (b) Low sum secrecy rate for both Gaussian and QPSK inputs. The fixed subcarrier (SC) assignment scheme.



**Figure 6.** The AN ratio in the total transmit power for Algorithm 1.

## 5. Conclusions

In this paper, we investigate the multiuser wiretap OFDM channels with AN in the frequency domain under the discrete input constraints, which are deployed in current practical wireless systems. Within the generation and removal framework of the frequency-domain AN, we maximize the sum secrecy rate associated with all LRs for finite-alphabet inputs by jointly optimizing the SC allocation as well as the transmit power for information signals and AN signals over SCs. We have presented a Lagrange dual algorithm to tackle the non-convex joint optimization problem. Numerical results suggest that the proposed algorithm further improves the sum secrecy rate for finite-alphabet inputs, mainly due to the AN and multiuser diversity gain, especially in the high SNR region.

**Author Contributions:** Conceptualization, L.F., B.T., Q.J. and F.L.; Methodology, L.F. and B.T.; Software, L.F. and C.Y.; Validation, L.F. and C.Y.; Formal analysis, L.F. and C.Y.; Investigation, L.F., F.L. and C.Y.; Resources, B.T., Q.J. and F.L.; Data Curation, L.F. and F.L.; Writing—Original Draft Preparation, L.F. and B.T.; Writing—Review & Editing, L.F., B.T., Q.J., F.L. and C.Y.; Visualization, L.F. and B.T.; Supervision, B.T. and Q.J.; Project Administration, B.T. and Q.J.; Funding Acquisition, B.T.

**Funding:** This work was supported in part by the National Natural Science Foundation of China under Grant 61671453, in part by the Anhui Provincial Natural Science Foundation under Grant 1608085MF123, and in part by the Young Elite Scientist Sponsorship Program under Grant 17-JCJQ-QT-041.

**Acknowledgments:** L.F. would like to thank Haohao Qin in [20] for the helpful comments on their research stimulations. L.F. wishes to thank Xiang Chen in [22] for the valuable contact with Haohao Qin. L.F. also wants to thank Yongpeng Wu in [50] and Meng Zhang in [29] for pointing his attention to the works of Weiliang Zeng et al. [51] and the subgradient method, respectively.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Renna, F.; Laurenti, N.; Poor, H.V. Physical-Layer Secrecy for OFDM Transmissions Over Fading Channels. *IEEE Trans. Inf. Forensic Secur.* **2012**, *7*, 1354–1367. [\[CrossRef\]](#)
2. Tsai, S.H.; Poor, H.V. Power Allocation for Artificial-Noise Secure MIMO Precoding Systems. *IEEE Trans. Signal Process.* **2014**, *62*, 3479–3493. [\[CrossRef\]](#)
3. Jameel, F.; Wyne, S.; Kaddoum, G.; Duong, T.Q. A Comprehensive Survey on Cooperative Relaying and Jamming Strategies for Physical Layer Security. *IEEE Commun. Surv. Tutor.* **2018**. [\[CrossRef\]](#)
4. Jang, U.; Lim, H.; Kim, H. Privacy-Enhancing Security Protocol in LTE Initial Attack. *Symmetry* **2014**, *6*, 1011–1025. [\[CrossRef\]](#)
5. Liu, Y.; Li, L.; Alexandropoulos, G.C.; Pesavento, M. Securing Relay Networks with Artificial Noise: An Error Performance-Based Approach. *Entropy* **2017**, *19*, 384. [\[CrossRef\]](#)
6. Alvarez, R.; Andrade, A.; Zamora, A. Optimizing a Password Hashing Function with Hardware-Accelerated Symmetric Encryption. *Symmetry* **2018**, *10*, 705. [\[CrossRef\]](#)
7. Rajesh, S.; Paul, V.; Menon, V.G.; Khosravi, M.R. A Secure and Efficient Lightweight Symmetric Encryption Scheme for Transfer of Text Files between Embedded IoT Devices. *Symmetry* **2019**, *11*, 293. [\[CrossRef\]](#)
8. Massey, J.L. An Introduction to Contemporary Cryptology. *IEEE Proc.* **1988**, *76*, 533–549. [\[CrossRef\]](#)
9. Wallace, J.W.; Sharma, R.K. Automatic Secret Keys From Reciprocal MIMO Wireless Channels: Measurement and Analysis. *IEEE Trans. Inf. Forensic Secur.* **2010**, *5*, 381–392. [\[CrossRef\]](#)
10. Fan, C.I.; Tseng, Y.F. Anonymous Multi-Receiver Identity-Based Authenticated Encryption with CCA Security. *Symmetry* **2015**, *7*, 1856–1881. [\[CrossRef\]](#)
11. Ahmad, M.; Al Solami, E.; Wang, X.Y.; Doja, M.N.; Beg, M.M.S.; Alzaidi, A.A. Cryptanalysis of an Image Encryption Algorithm Based on Combined Chaos for a BAN System, and Improved Scheme Using SHA-512 and Hyperchaos. *Symmetry* **2018**, *10*, 266. [\[CrossRef\]](#)
12. Shannon, C.E. Communication Theory of Secrecy Systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [\[CrossRef\]](#)
13. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [\[CrossRef\]](#)
14. Leung-yan-cheong, S.K.; Hellman, M.E. The Gaussian wire-tap channel. *IEEE Trans. Inf. Theory* **1978**, *24*, 451–456. [\[CrossRef\]](#)
15. Csiszar, I.; Korner, J. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory* **1978**, *24*, 339–348. [\[CrossRef\]](#)

16. Li, Z.; Yates, R.; Trappe, W. Secrecy Capacity of Independent Parallel Channels. In *Securing Wireless Communications at the Physical Layer*; Springer: Boston, MA, USA, 2010; pp. 1–18.
17. Khisti, A.; Wornell, G.W. Secure Transmission With Multiple Antennas I: The MISOME Wiretap Channel. *IEEE Trans. Inf. Theory* **2010**, *56*, 3088–3104. [[CrossRef](#)]
18. Jorswieck, E.A.; Wolf, A. Resource allocation for the wire-tap multi-carrier broadcast channel. In Proceedings of the 2008 International Conference on Telecommunications, St. Petersburg, Russia, 16–19 June 2008; pp. 1–6. [[CrossRef](#)]
19. Goel, S.; Negi, R. Guaranteeing secrecy using artificial noise. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 2180–2189. [[CrossRef](#)]
20. Qin, H.H.; Chen, X.; Zhong, X.F.; He, F.; Zhao, M.; Wang, J. Joint Power Allocation and Artificial Noise Design for Multiuser Wiretap OFDM Channels. In Proceedings of the 2013 IEEE International Conference on Communications, Budapest, Hungary, 9–13 June 2013. [[CrossRef](#)]
21. Karachontzitis, S.; Timotheou, S.; Krikidis, I.; Berberidis, K. Security-Aware Max-Min Resource Allocation in Multiuser OFDMA Downlink. *IEEE Trans. Inf. Forensic Secur.* **2015**, *10*, 529–542. [[CrossRef](#)]
22. Chen, X.; Qin, H.H.; Xiao, L.M. Joint Resource Allocation and Artificial Noise Design for Multiuser Wiretap OFDM Channels. *J. Commun. Netw.* **2017**, *19*, 451–460. [[CrossRef](#)]
23. Zhou, X.Y.; McKay, M.R. Secure Transmission with Artificial Noise over Fading Channels: Achievable Rate and Optimal Power Allocation. *IEEE Trans. Veh. Technol.* **2010**, *59*, 3831–3842. [[CrossRef](#)]
24. Li, Q.; Ma, W.K. Optimal and Robust Transmit Designs for MISO Channel Secrecy by Semidefinite Programming. *IEEE Trans. Signal Process.* **2011**, *59*, 3799–3812. [[CrossRef](#)]
25. Liao, W.C.; Chang, T.H.; Ma, W.K.; Chi, C.Y. QoS-Based Transmit Beamforming in the Presence of Eavesdroppers: An Optimized Artificial-Noise-Aided Approach. *IEEE Trans. Signal Process.* **2011**, *59*, 1202–1216. [[CrossRef](#)]
26. Qin, H.H.; Sun, Y.; Chang, T.H.; Chen, X.; Chi, C.Y.; Zhao, M.; Wang, J. Power Allocation and Time-Domain Artificial Noise Design for Wiretap OFDM with Discrete Inputs. *IEEE Trans. Wirel. Commun.* **2013**, *12*, 2717–2729. [[CrossRef](#)]
27. Cheng, D.H.; Gao, Z.Z.; Liu, F.; Liao, X.W. A General Time-domain Artificial Noise Design for OFDM AF Relay Systems. In Proceedings of the 2015 IEEE/CIC International Conference on Communications, Shenzhen, China, 2–4 November 2015; pp. 1–6. [[CrossRef](#)]
28. Xing, H.; Liu, L.; Zhang, R. Secrecy Wireless Information and Power Transfer in Fading Wiretap Channel. *IEEE Trans. Veh. Technol.* **2016**, *65*, 180–190. [[CrossRef](#)]
29. Zhang, M.; Liu, Y.; Zhang, R. Artificial Noise Aided Secrecy Information and Power Transfer in OFDMA Systems. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 3085–3096. [[CrossRef](#)]
30. Motahari, A.S.; Oveis-Gharan, S.; Maddah-Ali, M.A.; Khandani, A.K. Real Interference Alignment: Exploiting the Potential of Single Antenna Systems. *IEEE Trans. Inf. Theory* **2014**, *60*, 4799–4810. [[CrossRef](#)]
31. Xiao, C.S.; Zheng, Y.R.; Ding, Z. Globally Optimal Linear Precoders for Finite Alphabet Signals Over Complex Vector Gaussian Channels. *IEEE Trans. Signal Process.* **2011**, *59*, 3301–3314. [[CrossRef](#)]
32. Atallah, M.; Kaddoum, G. Secrecy Analysis in Wireless Network with Passive Eavesdroppers by Using Partial Cooperation. *IEEE Trans. Veh. Technol.* **2019**. [[CrossRef](#)]
33. Vuppala, S.; Tolossa, Y.J.; Kaddoum, G.; Abreu, G. On the Physical Layer Security Analysis of Hybrid Millimeter Wave Networks. *IEEE Trans. Commun.* **2018**, *66*, 1139–1152. [[CrossRef](#)]
34. Fan, L.H.; Tang, B.; Huang, Z.R.; Jiang, Q.X. Designing Constant-Envelope Transmissions for Secret Communications in MISO Wiretap Channels. *IEEE Access* **2019**, *7*, 17791–17797. [[CrossRef](#)]
35. Li, L.X.; Chen, Z.; Petropulu, A.P.; Fang, J. Linear Precoder Design for an MIMO Gaussian Wiretap Channel With Full-Duplex Source and Destination Nodes. *IEEE Trans. Inf. Forensic Secur.* **2018**, *13*, 421–436. [[CrossRef](#)]
36. Al-Talabani, A.; Deng, Y.S.; Nallanathan, A.; Nguyen, H.X. Enhancing Secrecy Rate in Cognitive Radio Networks via Stackelberg Game. *IEEE Trans. Commun.* **2016**, *64*, 4764–4775. [[CrossRef](#)]
37. Xu, D.; Li, Q. Improving physical-layer security for primary users in cognitive radio networks. *IET Commun.* **2017**, *11*, 2303–2310. [[CrossRef](#)]
38. Moon, J.; Lee, H.; Song, C.; Lee, S.; Lee, I. Proactive Eavesdropping With Full-Duplex Relay and Cooperative Jamming. *IEEE Trans. Wirel. Commun.* **2018**, *17*, 6707–6719. [[CrossRef](#)]
39. Koorapaty, H.; Hassan, A.A.; Chennakeshu, S. Secure information transmission for mobile radio. *IEEE Commun. Lett.* **2000**, *4*, 52–55. [[CrossRef](#)]

40. Seong, K.; Mohseni, M.; Cioffi, J.M. Optimal Resource Allocation for OFDMA Downlink Systems. In Proceedings of the 2006 IEEE International Symposium on Information Theory, Seattle, WA, USA, 9–14 July 2006; pp. 1394–1398. [\[CrossRef\]](#)
41. Yu, W.; Lui, R. Dual methods for nonconvex spectrum optimization of multicarrier systems. *IEEE Trans. Commun.* **2006**, *54*, 1310–1322. [\[CrossRef\]](#)
42. Boyd, S.; Vandenberghe, L. *Convex Optimization*; Cambridge University Press: New York, NY, USA, 2013.
43. Bertsekas, D. *Nonlinear Programming*; Athena Scientific: Belmont, MA, USA, 1999.
44. Guo, D.N.; Shamai, S.; Verdu, S. Mutual information and minimum mean-square error in Gaussian channels. *IEEE Trans. Inf. Theory* **2005**, *51*, 1261–1282. [\[CrossRef\]](#)
45. Grant, M.; Boyd, S. CVX: Matlab Software for Disciplined Convex Programming. 2017. Available online: <https://cvxr.com/cvx> (accessed on 27 May 2019).
46. Guo, D.N.; Wu, Y.H.; Shamai, S.; Verdu, S. Estimation in Gaussian Noise: Properties of the Minimum Mean-Square Error. *IEEE Trans. Inf. Theory* **2011**, *57*, 2371–2385. [\[CrossRef\]](#)
47. Marks, B.R.; Wright, G.P. A general inner approximation algorithm for nonconvex mathematical programs. *Oper. Res.* **1978**, *26*, 681–683. [\[CrossRef\]](#)
48. Luo, Z.Q.; Ma, W.K.; So, A.M.C.; Ye, Y.Y.; Zhang, S.Z. Semidefinite Relaxation of Quadratic Optimization Problems. *IEEE Signal Process. Mag.* **2010**, *27*, 20–34. [\[CrossRef\]](#)
49. Lozano, A.; Tulino, A.M.; Verdu, S. Optimum power allocation for parallel Gaussian channels with arbitrary input distributions. *IEEE Trans. Inf. Theory* **2006**, *52*, 3033–3051. [\[CrossRef\]](#)
50. Wu, Y.; Ng, D.W.K.; Wen, C.K.; Schober, R.; Lozano, A. Low-Complexity MIMO Precoding for Finite-Alphabet Signals. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 4571–4584. [\[CrossRef\]](#)
51. Zeng, W.L.; Xiao, C.S.; Wang, M.X.; Lu, J.H. Linear Precoding for Finite-Alphabet Inputs Over MIMO Fading Channels With Statistical CSI. *IEEE Trans. Signal Process.* **2012**, *60*, 3134–3148. [\[CrossRef\]](#)



© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).