An Encryption-Aware PHY Security Framework for 4-Node Gaussian Wiretap Channels With Joint Power Constraint

Tarig Sadig, *Student Member, IEEE*, Mehdi Maleki, *Member, IEEE*,
Nghi H. Tran, *Senior Member, IEEE*, and Hamid Reza Bahrami, *Senior Member, IEEE*

***Abstract*—In traditional physical layer security paradigm, no leakage of confidential information to the eavesdropper is tolerated regardless of whether the message is encrypted or not. This will result in an achievable secure transmission rate that is significantly smaller than the channel capacity. This article presents a novel approach that allows treatment of physical layer security in conjunction with encryption to achieve a flexible trade-off of system resources. We propose a novel framework to model the interplay between secured transmission rate and error probability in error prone ciphertexts. To this end, we use the concept of rate-equivocation region to establish such a connection. To clearly describe the application of our framework, we consider the case of 4-node Gaussian wiretap channel. For such a channel, we characterize the rate-equivocation region in different scenarios, and then use it to study the achievable rate of encryption-aware physical layer security. The obtained results show that, for a fixed transmission power, the prior knowledge of encryption can significantly increase the secured transmission rate. In addition, encryption-aware physical layer security can achieve a target transmission rate at a reduced transmission power compared to the conventional encryption-agnostic physical layer security.**

***Index Terms*—Physical layer security, encryption, rate-equivocation region, error prone ciphertext, Gaussian wiretap channels, encryption-aware physical layer security, encryption-agnostic physical layer security.**

I. Introduction

IN CONVENTIONAL communication systems, security is achieved by the means of cryptography, where information source encrypts the plain message using an encryption key to generate a cipher message that can only be decrypted at the intended receiver [1]. Each cryptography scheme can guarantee the security of the cipher message against an eavesdropper with a certain computational power. In fact, an eavesdropper with sufficient computational power can break the cipher to access the plain message. Physical layer (PHY) security can be considered as a strategy to guarantee secrecy in the presence of a computationally strong eavesdropper. The main objective of PHY security is to exploit the random nature of the communication channels to ensure that an eavesdropper cannot successfully decipher the confidential message, while, at the same time, guaranteeing a reliable transmission between the source and the legitimate destination [2].

PHY security schemes aim at preventing any leakage to the eavesdropper assuming plaintext transmission; i.e. no encryption. Whereas encryption schemes are designed to be robust against an attacker who has full access to error-free ciphertext [3]–[5]. However, both assumptions of plaintext transmission and error-free ciphertext are not practically sound. In fact, the presence of encryption can relax the design of PHY security schemes as some information leakage to the eavesdropper would be tolerable. On the other hand, the use of PHY security can relax the encryption design as it can guarantee errors in the ciphertext at the eavesdropper. Therefore, joint design of encryption and PHY security schemes can provide a flexible tool to tradeoff critical system resources, such as transmission and computational powers, and, at the same time, can arguably enhance the overall security of the system. Toward a more practical cryptographic design, the authors in [6]–[13] consider the concept of noisy ciphertexts and show its effectiveness from an application layer perspective. References [6]–[8] use tandem channel coding and cryptography to show that linear feedback shift register (LFSR) based cryptography is less susceptible to fast correlation attacks, when the ciphertexts are considered to be error-prone. In [9], the authors propose a practical physical layer coding scheme that fails to offer security in certain scenarios. Therefore, they suggest coupling the encoding with the cryptography to further enhance security. A new metric to measure the added complexity of attacks needed to break the joint coding and cryptography schemes over erasure channels is introduced in [10] and [11]. In the same context, even a simple substitution cipher [1] can enjoy an increased robustness when erasure-prone ciphertext is considered [12], and can also stand against the hidden Markov model (HMM) based attack developed in [3], when error-prone ciphertext is considered [13].

Encryption algorithms are typically designed to satisfy the generalized avalanche property [14]. This property indicates

Manuscript received March 9, 2020; revised July 3, 2020; accepted August 22, 2020. Date of publication September 21, 2020; date of current version December 16, 2020. This work was supported in part by the National Science Foundation (NSF) under award SaTC-1956110. The associate editor coordinating the review of this article and approving it for publication was I. Krikidis. *(Corresponding author: Hamid Reza Bahrami.)*

The authors are with the Department of Electrical and Computer Engineering, The University of Akron, Akron, OH 44325 USA (e-mail: th94@zips.uakron.edu; mm158@uakron.edu; nghi.tran@uakron.edu; hrb@uakron.edu).

Color versions of one or more of the figures in this article are available online at https://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCOMM.2020.3024825

that by slightly changing the ciphertext, the decrypted plaintext will change drastically. The avalanche property makes the ciphertext sensitive to the errors that occur at the physical layer. Stronger encryption will utilize its error sensitivity to make a successful cryptanalysis at the eavesdropper computationally burdensome. However, such an encryption will suffer from a high error rate, and hence requires more powerful channel coding to effectively detect and correct transmission errors [15]–[18]. In an effort to utilize this security-throughput tradeoff, [19] proposes an approach using encryption awareness to improve the security performance at the physical layer.

In this article, we propose a novel framework to study the joint effect of PHY security and encryption. Such a framework relies on the concept of rate-equivocation regions, and can be used to study the tradeoff between encryption strength, allowed leakage and transmission rate. As an application of our proposed framework, we consider a 4-node Gaussian wiretap channel. We will show that, by considering encryption, it is possible to achieve transmission rates beyond the secrecy capacity that is achievable by conventional PHY security. In the literature on PHY security, the transmission rate of a secured system is enhanced by introducing additional nodes to perform relaying [20]–[25], jamming [26]–[31], or both in a hybrid manner [32]–[34]. Jamming can also be used by the adversary as an attack mechanism in the physical layer to undermine the legitimate source-destination link [35], [36]. These papers [20]–[30], [32]–[36], however, consider the transmission of plaintext without encryption. We show that it is possible to significantly increase the secured transmission rate by factoring in the impact of the encryption. Toward our goal, we exploit the fact that cryptography undermines the ability of the eavesdropper to access the plaintext. We can then deliberately relax the constraint on PHY security without compromising the security of the system. As we demonstrate in the subsequent sections, even under a basic 4-node Gaussian wiretap channel, it is challenging to address the problem of encryption-aware secrecy rate maximization. Due to an additional constraint from encryption, an explicit characterization of the rate-equivocation region is needed, which will pose difficulties. It is because except for a few simple wiretap channels [2], [37], [38], analytical derivation of the rate-equivocation region remains a challenging task.

The significance and the main contributions of this article can be summarized as follows:

- We propose a novel framework relying upon the rate-equivocation region to study the joint impact of PHY security and encryption by making a connection between encryption strength and the tolerable amount of leakage to the eavesdropper at the physical layer. To the best of our knowledge, there does not exist any result in the literature that is related to our proposed joint security framework.
- We apply the proposed framework to a 4-node Gaussian wiretap channel, and derive the rate-equivocation regions in different scenarios. We then use our approach to maximize the secured transmission rate of the channel by taking into account the encryption strength. Compared to traditional PHY security, numerical results show that the secrecy rate can be significantly increased by taking into account the joint effect of PHY security and encryption, and beyond secrecy capacity performances can be achieved.
- We also formulate and solve a power minimization problem to minimize the transmitted power for a given encryption strength in the wiretap channel without compromising the secrecy. Equivalently, we can use significantly less transmission power while still achieving the same secrecy performance as in the unencrypted system.

The rest of the paper is organized as follows: In Section II, we present some preliminaries on encryption-aware PHY security. We briefly discuss the concept of rate-equivocation region, and introduce the problem of encryption-aware rate maximization with noisy ciphertext. In Section III, we consider the case study of a 4-node wiretap channel and formulate and solve the encryption-aware rate maximization for such a system. We derive the rate-equivocation regions for different channel conditions, and study the conditions where secured transmission rates beyond secrecy capacity is achievable. We also formulate and solve a rate maximization problem to optimally extract the advantage of encryption. In Section IV, we look at the problem from a different perspective, and formulate an optimization problem to minimize the transmitted power to achieve a target secured transmission rate at the presence of encryption. Section V presents some numerical results to illustrate the advantages of the proposed framework in enhancing the security in wiretap channels. Finally, Section VI concludes the paper.

II. Encryption-Aware Physical Layer Security: Preliminaries and Fundamental Limits

In this section, we first present the two fundamental concepts in PHY security: the traditional rate equivocation region and the corresponding secrecy capacity. Then, by further considering the effect of error-prone ciphertexts, we show that one can benefit from the concept of rate-equivocation region to expand the region of secure communication. As a result, a key secrecy rate optimization problem is established to demonstrate the feasibility of going beyond the secrecy capacity with encryption.

A. PHY Security: Rate-Equivocation Region and Secrecy Capacity

Consider a wiretap channel as shown in Fig. 1 that includes a transmitter (Alice) and a receiver (Bob) in the presence of a passive eavesdropper (Eve). Alice attempts to send plain message M_p to Bob by encrypting it with a shared key K to the cipher message M_c before encoding it to a codeword X^n using a $(2^{nR}, n)$ code $\mathcal{C}_n$ and the encoding function $\mathscr{E}$: $M_c \times \mathcal{R} \rightarrow X^n$, where $\mathcal{R}$ is a source of local randomness [39]. At the receiving side, Bob maps the channel observation Y^n to a message $\hat{M}_c \in \mathcal{M}$ using a decoding function $\mathscr{D} : \mathcal{Y} \rightarrow \mathcal{M} \cup ?$. Here, $\mathcal{M}$ denotes the set of 2^{nR} codewords. For a given code $\mathcal{C}_n$, the average error probability, denoted as $\mathbf{P}_e(\mathcal{C}_n)$, can be calculated as the probability that $\hat{M}_c$ is different from

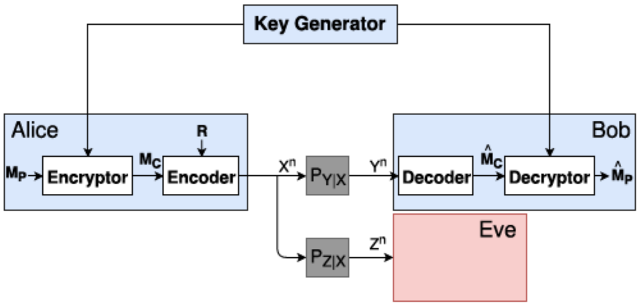

Fig. 1. A simple 3-node wiretap system model.

M_c [39], which is:

$$\mathbf{P}_e(\mathcal{C}_n) \triangleq P_r\left[\hat{M}_c \neq M_c \,|\mathcal{C}_n\right]. \quad (1)$$

Furthermore, the equivocation $\mathbf{E}(\mathcal{C}_n)$ and the leakage information $\mathbf{L}(\mathcal{C}_n)$ are, respectively, given as

$$\mathbf{E}(\mathcal{C}_n) \triangleq H\left(M_c\,|Z^n, \mathcal{C}_n\right), \quad (2)$$

and

$$\mathbf{L}(\mathcal{C}_n) \triangleq I\left(M_c; Z^n\,|\mathcal{C}_n\right). \quad (3)$$

Here, $H(\cdot)$ is the entropy of a random variable (RV), while $I(\cdot;\cdot)$ denotes the mutual information (MI) between two RVs. It should be noted that, in this work, we consider the equivocation and the leakage information in terms of ciphertext. By doing so, we can make a direct connection between our proposed joint security framework and traditional PHY security concepts. Using this approach, we are able to exploit the equivocation-rate region of the ciphertext to quantify the amount of leakage that can be protected by encryption. It is also of great interest to consider the rate-equivocation of the plaintext. This consideration, however, requires an explicit derivation of the plaintext-based equivocation, which depends on a specific cipher being used and the nature of encryption mechanisms. In addition, the secrecy rate of the plaintext also depends on two different equivocating factors: encryption and wiretap coding. Such an important study is, therefore, beyond the scope of this work, and it deserves further investigations. Given that, an achievable rate-equivocation pair (R, R_e) is defined as follows [39].

Definition 1: A strong rate-equivocation pair (R, R_e) is said to be achievable if there exists a sequence of $(2^{nR}, n)$ codes $\{\mathcal{C}_n\}_{n\geq 1}$, such that

$$\lim_{n\to\infty} \mathbf{P}_e(\mathcal{C}_n) = 0, \quad (4)$$

$$\text{and} \quad \lim_{n\to\infty} (\mathbf{E}(\mathcal{C}_n) - nR_e) \geq 0. \quad (5)$$

Note that inherently $R_e \leq R$. Then, the secrecy capacity, which is denoted as R_S, can be obtained by solving the following optimization problem

$$R_S \triangleq \sup_{R} \left\{R : (R, R) \in \bar{\mathcal{R}}^{WTC}\right\}. \quad (6)$$

Here, $\bar{\mathcal{R}}^{WTC}$ is referred to as the strong rate-equivocation region, which is the closure of all achievable pairs of (R, R_e). The secrecy capacity R_S is always less than the capacity of the main channel between Alice and Bob, R_B. From a physical layer perspective, security is guaranteed even when Eve has full access to the shared key K as long as the transmission rate is less than R_S. On the other hand, transmitting beyond R_S leads to a non-zero leakage, and hence, jeopardizes the secrecy. In many cases, it turns out that R_S can be found without the need of obtaining the detailed characteristics of the rate-equivocation region [20]–[29]. For example, for many Gaussian-based wiretap channels, the secrecy capacity can be obtained by exploiting the characteristics of the physical channels, such as power and fading, to maximize the difference between the two rates of Alice-Bob and Alice-Eve channels [38].

Assuming achievable rate-equivocation pair of (R, R_e), for the leakage information we have

$$\begin{aligned} \mathbf{L}(\mathcal{C}_n) &= H\left(M_c\,|\mathcal{C}_n\right) - \mathbf{E}(\mathcal{C}_n) \\ &= nR - \mathbf{E}(\mathcal{C}_n) \leq n(R - R_e). \end{aligned} \quad (7)$$

Tolerating leakage, by transmitting with a rate higher than R_e, increases Eve's chance for a correct detection. In this case, encryption can become useful to secure the part of information that is leaked. Using Fano's inequality [40], the message error probability at the eavesdropper satisfies the following condition

$$P_{Eve} \geq \frac{H\left(M_c\,|Z^n\mathcal{C}_n\right) - h(P_{Eve})}{\log_2(2^{nR}-1)} \geq \frac{nR_e - h(P_{Eve})}{\log_2(2^{nR}-1)}. \quad (8)$$

For a sufficiently large n, we have

$$P_{Eve} \geq \frac{R_e}{R}, \quad n \gg 1. \quad (9)$$

Not surprisingly, when the rate R is very close to R_e, the message error probability approaches one indicating that eavesdropper always decodes the wrong message. Equation (9) also indicates that the eavesdropper at best can detect the message with probability $\frac{R-R_e}{R}$, which equals to the normalized leakage information. Note that although the use of the Fano's inequality may not be suitable for all system models, it provides a secure region that is generic, reasonably tight in many scenarios [41]–[43], simple enough to be specified in the two-dimensional rate-equivocation region, and also intuitively justified.

B. Encryption-Aware Rate Maximization With Noisy Ciphertext

The above results on the secrecy capacity R_S still hold true with encryption under the extreme assumption that Eve can completely recover the entire ciphertext without error. However, with error-prone ciphertexts, it is more difficult for Eve to intercept the ciphertext. As we have discussed earlier, the effect of error-prone ciphertexts imposed by physical layer at Eve has been studied in [6]–[13] to demonstrate that Eve needs to be computationally stronger or equipped with more sophisticated attacks in order to successfully break a ciphertext when it is noisy. In addition, it was demonstrated that the effective error rate at Eve is an important factor that determines how much computation is needed by Eve for a successful attack. As an alternative, we shall demonstrate, in the following, the mutual impact between physical layer and encryption via a connection between noisy ciphertext and the transmission rates for beyond-capacity performances.

1) Error Threshold P_{cipher} and Encryption Strength λ: Because there is a certain computational strength possessed by Eve, noisy ciphertext makes it more difficult for Eve to break the cipher. As a result, there is a minimum level of ciphertext error that causes Eve to fail in breaking the cipher [6]. We define this minimum error probability threshold as P_{cipher}. For any cryptographic algorithm and a computationally limited Eve, P_{cipher} can be equivalently understood as the minimum error probability needed at Eve to prevent the eavesdropper from extracting the confidential message. In such a paradigm, secrecy is achieved as long as the probability of error at Eve is greater than or equal to P_{cipher}; i.e., $P_{Eve} \geq P_{cipher}$. P_{cipher} is therefore an indicating factor to reflect how strong the encryption is under a certain Eve's computational strength. For example, if Eve has an unlimited computational power, the maximum message error probability, i.e., $P_{cipher} = 1$, is required, and relying on encryption does not help (weak encryption). On the other hand, if Eve is incapable of performing any sort of computation, no message error is required; i.e. $P_{cipher} = 0$, and we can completely rely on encryption (strong encryption). Given P_{cipher}, we can now define an encryption factor λ that can be used to reflect the strength of encryption. It is clear that a stronger encryption dictates a larger value for λ, or equivalently, a smaller threshold P_{cipher}. From this inverse relationship, λ can be simply defined as

$$\lambda = \frac{1}{P_{cipher}}. \tag{10}$$

It should be noted that the minimum value of λ is 1, which corresponds to the case of no encryption. On the other hand, a very strong or unbreakable encryption corresponds to a large λ.

To demonstrate the meaningfulness of the above definition of encryption strength, let us consider a simple example of LFSR-based stream ciphers. Authors in [6] investigated the impact of an error-prone LFSR-based stream ciphertext on fast-correlation attacks [44]. In particular, they showed that the number of iterations needed to break the cipher is governed by how the LFSR output is correlated with the generated key sequence. As a result, for a fixed correlation probability, they derived the relationship between the number of required trials and the bit error rate at the eavesdopper (p_e^b). On the other hand, to consider a robust encryption, we assume the cipher satisfies the strict avalanche criterion [45], which indicates that the bit error rate (p_e^b) is almost half of the message error rate P_{Eve}. Based on this and the findings in [6], one can find the minimum required error probability P_{cipher} (or, equivalently, encryption strength λ) for LFSR-based stream ciphertext as a function of the number of trials available at Eve to perform the fast-correlation attack. Fig. 2 shows the relationship between the number of iterations required to break the cipher for different P_{Eve}. It can be observed from the figure that for error-free cipher, the attacker needs about 1.8×10^3 iterations to break the cipher. With the noisy ciphertext, P_{Eve} is bounded away from zero (noisier ciphertext), and significantly more number of iterations are needed to have a successful attack. In practice, Eve has a limited computational capability that constrains her to perform only certain number of iterations. This amount of trials fails to break the cipher when P_{Eve} becomes relatively larger. As an illustrative example, let us assume a scenario where the eavesdropper can only afford a maximum of $A = 10^9$ iterations, which corresponds to $P_{Eve} = 0.44$. If more errors happen, the adversary cannot break the cipher, and perfect secrecy is still ensured; i.e. $P_{cipher} = 0.44$.

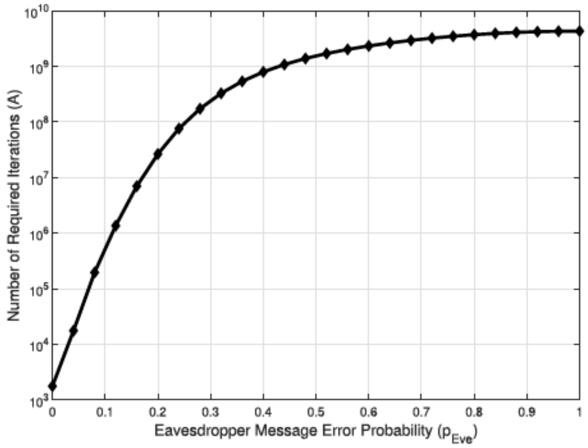

Fig. 2. The number of iterations required to break the cipher for different eavesdropper message error probabilities P_{cipher}.

2) Encryption-Aware Rate Maximization: We can now use the defined encryption strength λ to establish a connection between PHY security and encryption. From (9), and setting the ratio $\frac{R_e}{R}$ as an upper bound for P_{cipher} will ensure that $P_{eve} \geq P_{cipher}$. This means that in this case the system is secure. Therefore, from (10), we have

$$\frac{R_e}{R} \geq \frac{1}{\lambda}. \tag{11}$$

The rate maximization problem at the physical layer can now be modified by taking into account an additional constraint imposed by the encryption; i.e., $R \leq \lambda R_e$. Of course, stronger encryption means a smaller P_{cipher}, and consequently, a larger λ. This new security condition applied at the physical layer can therefore lead to a larger security region. The new encryption-aware secrecy rate is the solution to the following optimization problem

$$\bar{R}_S \triangleq \sup_R \left\{ R : \left(R, \frac{R}{\lambda} \right) \in \bar{\mathcal{R}}^{WTC} \right\}. \tag{12}$$

Different from (6), the solution of (12) requires a complete characterization of the rate-equivocation region and its boundary region, which makes the problem non-trivial. As we demonstrate shortly, to overcome this difficulty, our approach is to examine different cases of the channel state information (CSI) to shed light on the detailed properties of the secrecy rates as a function of the transmit power. While the results in some cases are rather simple, this approach allows us to explicitly establish the boundary region of the

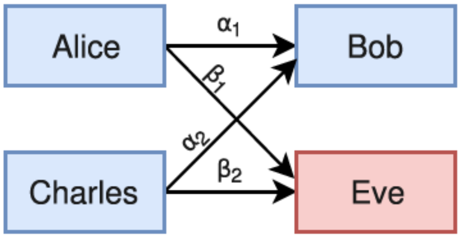

Fig. 3. 4-node wiretap system model, where Charles is a jamming transmitter.

rate-equivocation region, and eventually, to determine the encryption-aware secrecy rate.

III. Encryption-Aware Rate Maximization for Gaussian Wiretap Channel

In this section, we focus on a common 4-node Gaussian wiretap channel [46] to demonstrate the strength and usefulness of the proposed joint security design. In this model, besides Alice, Bob, and Eve, it is assumed that there is a cooperating transmitter (Charles) that sends only a parasite signal to facilitate secure communication between Alice and Bob. For convenience, let α_1 and β_1 be Alice-Bob and Alice-Eve channel power gains, respectively. Similarly, assume α_2 and β_2 are, respectively, Charles-Bob and Charles-Eve channel power gains. Note that if $\alpha_2 = \beta_2 = 0$, the 4-node model reduces to a simpler 3-node model consisting of Alice, Bob, and Eve only as in Fig. 1. The channels are assumed to be static, and full channel state information (CSI) is available at Alice and Charles.

In this work, we consider a joint power constraint $\rho = \rho_1 + \rho_2$ on the two transmitting nodes, where ρ_1 and ρ_2 are the powers to be allocated to Alice and Charles, respectively. The joint power assumption is feasible in current and future wireless networks, and it has been considered extensively in the literature. It is because Alice and Charles are managed by the same control center. By using Gaussian codebooks as in [38], the achievable rate and secrecy rate of the Alice-Bob channel as functions of ρ_2 can be obtained as

$$R_b(\rho_2) = \log_2\left(1 + \alpha_1 \frac{\rho - \rho_2}{1 + \alpha_2\rho_2}\right), \tag{13}$$

$$R_s(\rho_2) = \left[R_b(\rho_2) - \log_2\left(1 + \beta_1 \frac{\rho - \rho_2}{1 + \beta_2\rho_2}\right)\right]^+, \tag{14}$$

where $[x]^+ = max\{0, x\}$. It is evident from (13) that $R_b(\rho_2)$ is a decreasing function of the jammer power ρ_2. Therefore, the capacity is achieved when no power is allocated for jamming, i.e., $R_B = \log_2(1 + \alpha_1\rho)$. Also, it is clear from (14) that the jammer works in favor of secrecy only when $\beta_2 > \alpha_2$. Furthermore, the region $\bar{\mathcal{R}}^{WTC}(\rho_2)$, within which the rate-equivocation pair (R, R_e) is achievable, can be defined as follows

$$\bar{\mathcal{R}}^{WTC}(\rho_2) = \left\{ (R, R_e) : \begin{array}{c} 0 \leq R \leq R_b(\rho_2) \\ 0 \leq R_e \leq R_s(\rho_2) \\ R_e \leq R \end{array} \right\}. \tag{15}$$

As a result, the rate-equivocation region can be expressed as $\bar{\mathcal{R}}^{WTC} = \bigcup_{\rho_2} \bar{\mathcal{R}}^{WTC}(\rho_2)$. To shed further light on the rate-equivocation region $\bar{\mathcal{R}}^{WTC}$, and eventually, to find the encryption-aware secrecy capacity $\bar{R}_S$, we first study the detailed characteristics of $R_s(\rho_2)$, so that the relationship between R and R_e in the boundary region can be determined. It should also be emphasized that encryption awareness is beneficial only in the case of a positive $R_s(\rho_2)$. Therefore, hereafter, we only need to focus on the case of positive $R_s(\rho_2)$ and the notation $[x]^+$ in (14) can be dropped.

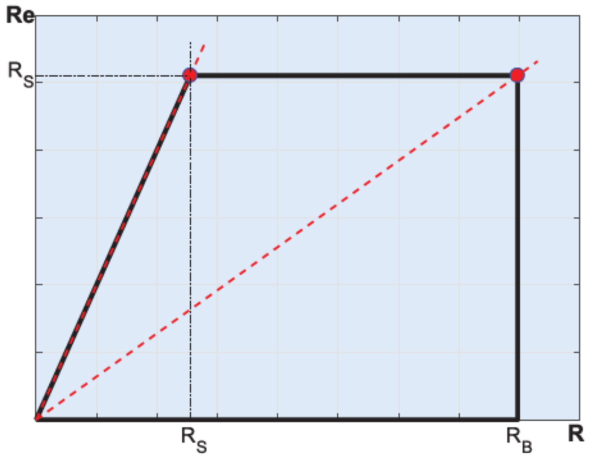

Fig. 4. Rate-equivocation region $\bar{\mathcal{R}}^{WTC}(\rho_2)$ as a sharp trapezoid.

A. Secrecy Rate $R_s(\rho_2)$

It is clear that $R_s(\rho_2)$ is positive if and only if $\alpha_1 \frac{\rho - \rho_2}{1+\alpha_2\rho_2} > \beta_1 \frac{\rho-\rho_2}{1+\beta_2\rho_2}$. Equivalently, we need $(\alpha_1 - \beta_1)\left(1 - \frac{\rho_2}{\rho_T}\right) > 0$, where

$$\rho_T = \frac{\alpha_1 - \beta_1}{\alpha_2\beta_1 - \alpha_1\beta_2}. \tag{16}$$

Therefore, depending on the channel conditions, there are four possibilities for the channel gains as follows

1) If $\alpha_1 > \beta_1$ and $\alpha_1/\alpha_2 \geq \beta_1/\beta_2$: ρ_T is negative and the secrecy function is always positive, regardless of the value of ρ_2.
2) If $\alpha_1 > \beta_1$ and $\alpha_1/\alpha_2 < \beta_1/\beta_2$: ρ_T is positive. The secrecy function is only positive when $\rho_2 < \rho_T$.
3) If $\alpha_1 < \beta_1$ and $\alpha_1/\alpha_2 > \beta_1/\beta_2$: ρ_T is positive. The secrecy function is only positive when $\rho_2 > \rho_T$.
4) If $\alpha_1 \leq \beta_1$ and $\alpha_1/\alpha_2 \leq \beta_1/\beta_2$: ρ_T is negative and the secrecy function is never positive.

Note that α_1/α_2 and β_1/β_2 can, respectively, be considered as Bob's and Eve's normalized channel gains.

As the next step, we shall investigate the detailed characteristics of the secrecy function in each case in order to establish the rate-equivocation region. It should be noted that for a given power allocation ρ_2 that results in a positive secrecy rate, the corresponding rate-equivocation region $\bar{\mathcal{R}}^{WTC}(\rho_2)$ is a sharp trapezoid as shown in Fig. 4. As such, the shape of the boundary of $\bar{\mathcal{R}}^{WTC}$ is determined by $\tilde{R}_s$ as a function of R_b, denoted as $\tilde{R}_s(R_b)$, that sweeps over all possible corner points. To further characterize this function, from (13), we first

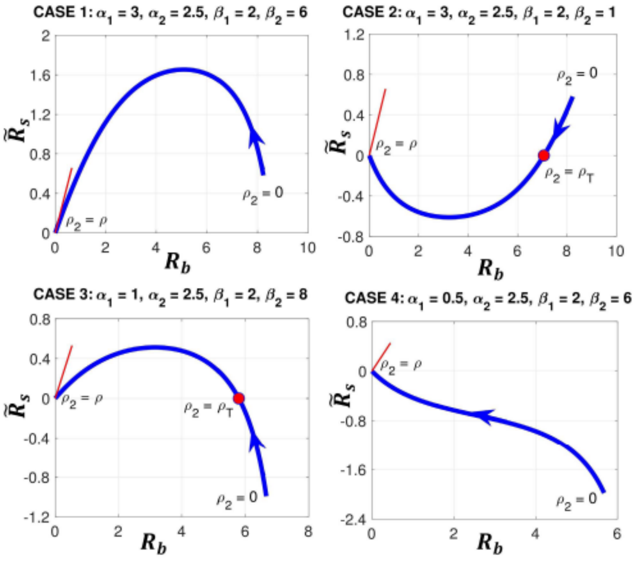

Fig. 5. Typical sweeping functions for four different cases (ρ = 20 dB). Note that arrow is in direction of increasing ρ_2.

write ρ_2 as a function of R_b as follows

$$\rho_2 = \frac{\alpha_1\rho - (2^{R_b} - 1)}{\alpha_1 + \alpha_2(2^{R_b} - 1)}, \tag{17}$$

Substituting (17) into (14), the sweeping function $\tilde{R}_s(R_b)$ is given as

$$\tilde{R}_s(R_b) = R_b - \log_2 \times \left[1 + \frac{\beta_1(1+\alpha_2\rho)(2^{R_b} - 1)}{\alpha_1(1+\beta_2\rho) + (\alpha_2 - \beta_2)(2^{R_b} - 1)}\right]. \tag{18}$$

Now, for convenience, and with a slight abuse of notation, let R_b be represented by a variable x; so, we can write the sweeping function $\tilde{R}_s(R_b)$ as a function of x, i.e.,

$$f(x) = x - \log_2 \times \left[1 + \frac{\beta_1(1+\alpha_2\rho)(2^x - 1)}{\alpha_1(1+\beta_2\rho) + (\alpha_2 - \beta_2)(2^x - 1)}\right]. \tag{19}$$

After some simple manipulations, $f(x)$ can be written as:

$$f(x) = x - \log_2(u(x)), \text{ for all } x : 0 \le 2^x - 1 \le \alpha_1\rho, \tag{20}$$

where

$$u(x) = (1 + a) - \frac{a}{1 + b(2^x - 1)}, \tag{21}$$

with

$$a = \frac{\beta_1(1 + \alpha_2\rho)}{\alpha_2 - \beta_2} \quad \text{and} \quad b = \frac{\alpha_2 - \beta_2}{\alpha_1(1 + \beta_2\rho)}. \tag{22}$$

As an example, in Fig. 5, this sweeping curve is illustrated for four cases of the channel gains as discussed earlier by varying ρ_2 and finding the corresponding rate R_b and the sweep function $f(x)$, or equivalently, $\tilde{R}_s(R_b)$. We now state the following lemma regarding the properties of parameters a and b.

Lemma 1: [Properties of terms a and b]

$$\text{(a) } 1 - ab = \frac{\alpha_1 - \beta_1}{\alpha_1(1 + \beta_2\rho)}\left(1 - \frac{\rho}{\rho_T}\right). \tag{23}$$

(b) If $\alpha_2 < \beta_2$, then $1 + bz > 0$ for all $0 \le z \le \alpha_1\rho$. (24)

(c) If $\alpha_2 < \beta_2$ and $(\alpha_1 - \beta_1)\rho_T < 0$, then

$$1 - b(a + 1) > 0 \text{ for all } \rho > \rho_T. \tag{25}$$

Proof: The proof is provided in Appendix A. ■

Given the above results, we are now ready to obtain important properties of the sweeping function $f(x)$ in (20). In particular, we have the following propositions regarding $f(x)$ that are helpful in characterizing the rate-equivocation region.

Proposition 1: If $\alpha_2 \ge \beta_2$, $f(x)$ in (20) is a convex function in the region of interest $0 \le 2^x - 1 \le \alpha_1\rho$. Furthermore, $f(x)$ is maximized at $x^* \in \{0, \log_2(\alpha_1\rho + 1)\}$.

Proof: Since $-\log(\cdot)$ is a non-increasing convex function, based on [47], it is sufficient to show that $u(x)$ in (21) is concave. Specifically, it can be verified that $u'(x) = \frac{ab\ln 2}{[1+b(2^x-1)]^2}$ and $u''(x) = \frac{-2ab^2(\ln 2)^2}{[1+b(2^x-1)]^3}$. Since a and b are both positive, $u''(x) \le 0$ and, as a result, $u(x)$ is concave. Therefore, $f(x)$ is convex, and the maximum is attained on the boundary. ■

Proposition 2: If $\alpha_2 < \beta_2$, $(\alpha_1 - \beta_1)\rho_T < 0$ and $\rho \ge \rho_T$, $f(x)$ is a concave function in the region of interest. Furthermore, $f(x)$ is maximized at

$$x^* = \begin{cases} \min\{\log_2\left(\frac{b-1}{2b}\right), \log_2(\alpha_1\rho + 1)\}, & a = -1 \\ \min\{\log_2\left(\frac{-1+\sqrt{\Delta}}{b(1+a)} + 1\right), \log_2(\alpha_1\rho + 1)\}, & a \ne -1 \end{cases}$$

where

$$\Delta = 1 - (a + 1)(1 - ab) = a\left(-(1 - ab) + b\right). \tag{26}$$

Proof: The proof is given in Appendix B. ■

B. Rate-Equivocation Region

Given the obtained properties of $f(x)$, we are now ready to establish the rate-equivocation region. In Fig. 6, three different scenarios for rate-equivocation region are illustrated. Specifically, No Jamming (NJ) scenario, when the channel gains are such that allocating power to jamming does not improve the secrecy rate, the rate-equivocation region of Fig. 6.a is achievable. On the other hand, in Beneficial Jamming (BJ) scenario, where the secrecy rate without applying jamming is positive, yet power allocation to jamming further improves the secrecy rate, the typical rate-equivocation region is illustrated in Fig. 6.b. There is also the Essential Jamming (EJ) scenario, where a non-zero secrecy rate can only be achieved by applying jamming. The rate-equivocation region for such a scenario is shown in Fig. 6.c. In the following, based on the properties derived for the secrecy function in the previous subsection, we investigate each of these cases. We first have the following proposition.

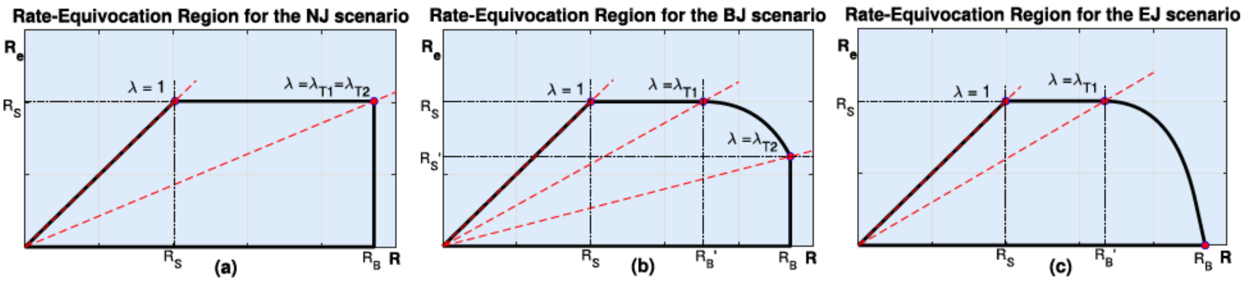

Fig. 6. Typical rate-equivocation regions for: (a) NJ scenario, (b) BJ scenario and (c) EJ scenario. Note that the dashed red lines specify the thresholds for encryption strength.

Proposition 3: When $\alpha_1 \geq \beta_1$ and $\alpha_2 < \beta_2$, the maximum total power resulting in the optimal jamming power to be zero, i.e., $\rho_2^* = 0$, is

$$\rho_C = \frac{-q + \sqrt{q^2 + 4pr}}{2p}, \tag{27}$$

where $p = \beta_1\alpha_1(\beta_2 - \alpha_2)$, $q = \beta_1\beta_2 - \alpha_1\alpha_2$, and $r = \alpha_1 - \beta_1$.

Proof: The proof is straightforward and can be obtained by setting the optimal ρ_2 to zero. ∎

The next theorem then characterizes the detailed properties of the rate-equivocation region for the 4-node Gaussian channel.

Theorem 1: Depending on the channel conditions, the rate-equivocation region for the 4-node Gaussian channel can be described as follows:

(a) The rate-equivocation region of $\bar{\mathcal{R}}_1^{WTC}$ in Fig. 6.a is achievable iff $\alpha_1 > \beta_1$, and one of the following conditions are satisfied:
- $\alpha_2 \geq \beta_2$.
- $\alpha_2 < \beta_2$ and $0 < \rho \leq \rho_C$.

(b) The rate-equivocation region of $\bar{\mathcal{R}}_2^{WTC}$ in Fig. 6.b is achievable iff $\alpha_1 > \beta_1$, $\alpha_2 < \beta_2$ and $\rho > \rho_C$.

(c) The rate-equivocation region of $\bar{\mathcal{R}}_3^{WTC}$ in Fig. 6.c is achievable iff $\alpha_1 \leq \beta_1$, $\alpha_1/\alpha_2 > \beta_1/\beta_2$ and $\rho > \rho_T$.

(d) No positive equivocation rate is achievable iff $\alpha_1 \leq \beta_1$ and one of the following conditions are satisfied:
- $\alpha_1/\alpha_2 \leq \beta_1/\beta_2$.
- $\alpha_1/\alpha_2 > \beta_1/\beta_2$ and $0 < \rho \leq \rho_T$.

Proof: The proof is in Appendix C. ∎

Corollary 1: When the rate-equivocation region $\bar{\mathcal{R}}_2^{WTC}$ or $\bar{\mathcal{R}}_3^{WTC}$ is achieved, the maximum achievable transmission rate that results in maximum equivocation rate of R_S is

$$R_B' = f^{-1}(R_S) = \begin{cases} \log_2\left(1 + \dfrac{\sqrt{\Delta} - 1}{b(1+a)}\right), & a \neq -1 \\ \log_2\left(\dfrac{b-1}{2b}\right), & a = -1. \end{cases} \tag{28}$$

Proof: Based on the proof of Theorem 1 in Appendix C, for each case, the secrecy function is maximized at x^*. ∎

Corollary 2: Assuming fixed channel gains for Bob, α_1 and β_1, and the available power ρ, different rate-equivocation regions are achievable depending on Eve's channel gains, α_2 and β_2. This is shown in Fig. 7 where

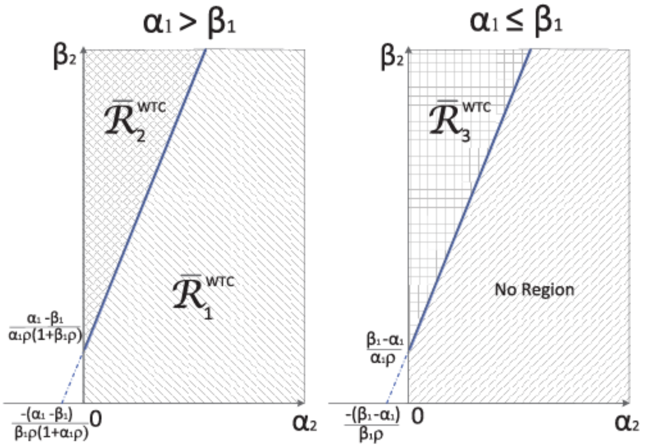
$\alpha_1 > \beta_1$
$\alpha_1 \leq \beta_1$
β_2
$\bar{\mathcal{R}}_2^{WTC}$
$\bar{\mathcal{R}}_1^{WTC}$
$\bar{\mathcal{R}}_3^{WTC}$
No Region
$\frac{\alpha_1 - \beta_1}{\alpha_1\rho(1+\beta_1\rho)}$
$\frac{-(\alpha_1 - \beta_1)}{\beta_1\rho(1+\alpha_1\rho)}$
$\frac{\beta_1 - \alpha_1}{\alpha_1\rho}$
$\frac{-(\beta_1 - \alpha_1)}{\beta_1\rho}$
0
α_2

Fig. 7. The conditions for different rate-equivocation region shapes.

(a) The left figure is for the case of $\alpha_1 > \beta_1$, where $\bar{\mathcal{R}}_1^{WTC}$ is achievable when the point (α_2, β_2) is located below the line $[\beta_1\rho(1+\alpha_1\rho)]\ \beta_2 - [\alpha_1\rho(1+\beta_1\rho)]\ \alpha_2 = \alpha_1 - \beta_1$. On the contrary, $\bar{\mathcal{R}}_2^{WTC}$ in achievable when the point is above the line.

(b) The right figure is for the case of $\alpha_1 \leq \beta_1$, where $\bar{\mathcal{R}}_3^{WTC}$ is achievable when the point (α_2, β_2) is located above the line $(\alpha_1\rho)\ \beta_2 - (\beta_1\rho)\ \alpha_2 = \beta_1 - \alpha_1$. On the contrary, no rate-equivocation is achievable when the point is below the line.

Proof: For each case, the threshold line can be easily obtained by combining different conditions in Theorem 1. ∎

C. Rate Maximization

Given that the rate-equivocation has been fully characterized, we are now ready to analyze the effect of encryption on the maximum achievable rate. As can be seen from Fig. 6, the boundary of the rate-equivocation region $\bar{\mathcal{R}}^{WTC}$, in general, can be divided into four segments, connecting five corner points $(R, R_e) = (0, 0)$, $(R, R_e) = (R_S, R_S)$, $(R, R_e) = (R_{B'}, R_S)$, $(R, R_e) = (R_{S'}, R_B)$, and $(R, R_e) = (R_B, 0)$. Here, R_B' is the maximum transmission rate that $R_e = R_S$ is achievable; i.e., $R_B' = f^{-1}(R_S)$, and R_S' is the maximum achievable equivocation rate for $R = R_B$; i.e., $R_S' = f(R_B)$. It should be noted that for the NJ and EJ scenarios, the boundary regions are simplified to three segments. To conveniently examine the intersection between the line segment $R = \lambda R_e$ for a given λ and the boundary of $\bar{\mathcal{R}}^{WTC}$ so that a maximum secrecy rate can be found, we can define two threshold values for encryption factor as $\lambda_{T1} = R'_B/R_S$ and $\lambda_{T2} = R_B/R'_S$. It is clear from Fig. 6 that the two line segments $R = \lambda_{T1} R_e$ and $R = \lambda_{T2} R_e$ intersect the boundary of $\bar{\mathcal{R}}^{WTC}$ at $(R, R_e) = (R_{B'}, R_S)$ and $(R, R_e) = (R_{S'}, R_B)$, respectively. Therefore, to evaluate the maximum rate in different scenarios, we can consider three different regions for λ as $1 \le \lambda \le \lambda_{T1}$, $\lambda_{T1} < \lambda < \lambda_{T2}$ and $\lambda \ge \lambda_{T2}$. The following corollary states a main result.

Corollary 3: The maximum secrecy rate can be obtained as

$$\begin{cases} \bar{R}_S = \lambda R_S & 1 \le \lambda \le \lambda_{T1} \\ \bar{R}_S = \lambda f(R_{max}) & \lambda_{T1} < \lambda < \lambda_{T2} \\ \bar{R}_S = R_B & \lambda \ge \lambda_{T2}, \end{cases} \tag{29}$$

Proof: The proof comes straightforwardly from Theorem 1, and it is omitted here. ■

Before closing this section, it should be noted that for a 3-node wiretap channel with $\lambda_{T1} = \lambda_{T2} = \lambda_T$, the maximum achievable rate can be obtained as

$$\begin{cases} \bar{R}_S = \lambda R_S & 1 \le \lambda \le \lambda_T \\ \bar{R}_S = R_B & \lambda \ge \lambda_T. \end{cases} \tag{30}$$

IV. Power Allocation for 4-Node Gaussian Wiretap Model

In this section, by considering the same 4-node Gaussian wiretap channel as in Section III, we investigate the power allocation problem. The goal is to minimize the total transmit power ρ given an encryption level λ to achieve a certain transmission rate $R = R^*$. It should be noted that the design for transmit power minimization can also be formulated via a power optimization problem, which might give important insights on power allocation strategies. However, for consistency, our focus is on the encryption-aware secrecy rate. This optimization problem can be formulated as

$$\begin{aligned} &\underset{R_e}{\text{minimize}}\ \rho \\ &\text{subject to } R_B(\rho) \ge R^*, \\ &\qquad R_S(\rho) \ge R_e, \\ &\qquad \frac{R^*}{\lambda} \le R_e \le R^*. \end{aligned} \tag{31}$$

The shape of the rate-equivocation region is a key factor in solving the optimization problem in (31). In the following, we shall provide the solutions to each of the region types in Fig. 6 using a graphical method.

A. No Jamming

This is the case where having the jammer node does not have any added benefit. This case, as shown in Fig. 6.a, has a trapezoid rate-equivocation region, and we know from Theorem 1 that the best secrecy performance is experienced when the jammer is silent. So, the 4-node system can be treated as if there are three nodes in the system. Considering the rate-equivocation of a Gaussian wiretap channel for a certain transmit power illustrated in Fig. 6.a, the main channel capacity $R_B(\rho)$ and secrecy capacity $R_S(\rho)$ can be found from (13) and (14), respectively, with $\rho_2 = 0$.

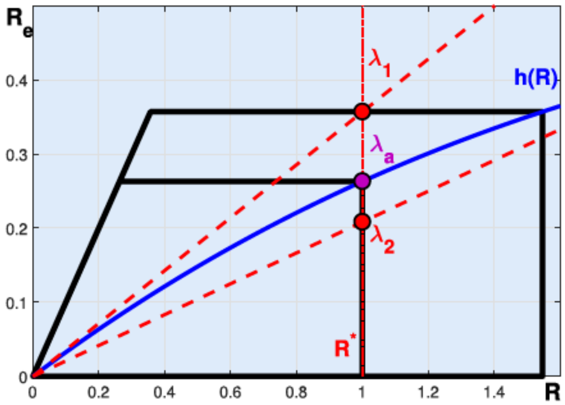

Fig. 8. Optimal power allocation for the NJ scenario. Two cases of $\lambda = \lambda_1$ and $\lambda = \lambda_2$ are illustrated, where ($\lambda_1 \ge \lambda_a$ and $\lambda_2 < \lambda_a$); Both cases satisfy the target rate of $R^* = 1$ bit/channel use.

To solve this optimization problem, we define a curve in $R_e - R$ plane that sweeps the boundaries of the rate-equivocation regions with different powers. This curve can be obtained by solving the following equations

$$\begin{cases} R = R_B(\rho) \\ R_e = R_S(\rho). \end{cases} \tag{32}$$

From (13), we have

$$\rho = R_B^{-1}(x) = \frac{2^x - 1}{\alpha_1}. \tag{33}$$

As a result, the curve can be expressed as $R_e = h(R)$, where

$$h(x) = R_s(R_B^{-1}(x)) = x - \log_2\left[1 + \frac{\beta_1}{\alpha_1}(2^x - 1)\right], \quad \text{for all } x: 0 \le 2^x - 1 \le \alpha_1 \rho. \tag{34}$$

By calculating the first and second derivatives of $h(x)$, it is not difficult to show that $h(x)$ is an increasing concave function of x, since $h'(x) > 0$ and $h''(x) < 0$ for all $x: 0 \le 2^x - 1 \le \alpha_1 \rho$.

For a given target rate R^*, let us define a threshold encryption strength λ_a above which the power budget achieving the desired rate cannot be further reduced. Therefore, we have

$$\lambda_a = \frac{R^*}{h(R^*)} \tag{35}$$

In other words, ρ_{min} can be reduced by increasing the encryption strength, but it saturates at λ_a. Also, note that since $R_S(\rho)$ from (14) is bounded by $\log_2(\frac{\alpha_1}{\beta_1})$, the target rate is restricted to be always less than or equal to $\lambda \log_2(\frac{\alpha_1}{\beta_1})$. The following proposition summarizes the solution to this case.

Proposition 4: For the rate-equivocation region of $\bar{\mathcal{R}}_1^{WTC}$, the minimum power satisfying security condition and rate at $R^* \le \lambda \log_2(\frac{\alpha_1}{\beta_1})$ can be obtained by

$$\rho_{min} = \begin{cases} R_S^{-1}(\frac{R^*}{\lambda}) = \frac{2^{R^*/\lambda} - 1}{\alpha_1 - \beta_1 2^{R^*/\lambda}}, & \lambda < \lambda_a \\ R_B^{-1}(R^*) = \frac{2^{R^*} - 1}{\alpha_1}, & \lambda \ge \lambda_a \end{cases} \tag{36}$$

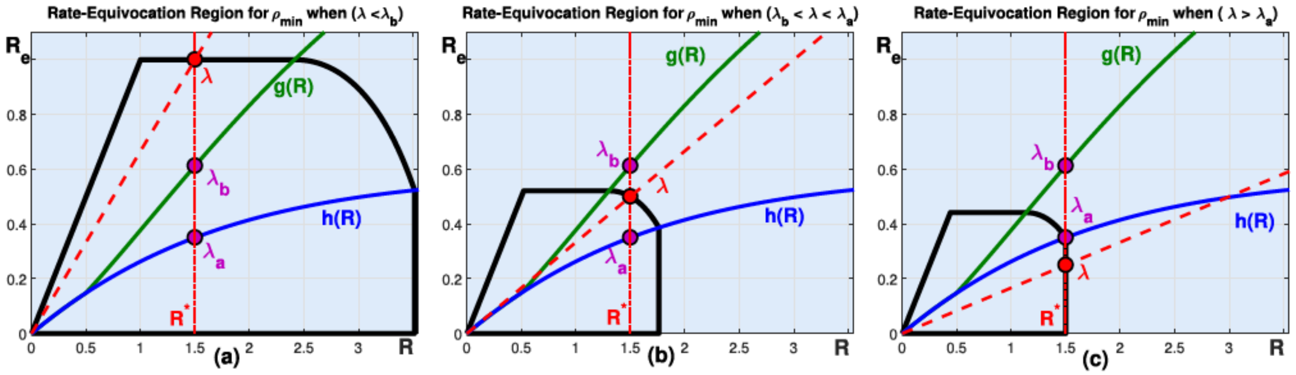

Fig. 9. Optimal power allocation for the BJ scenario. Three cases are illustrated: (a) $\lambda \leq \lambda_b$, (b)$\lambda_b < \lambda < \lambda_a$ and (c) $\lambda \geq \lambda_a$; all the cases satisfy the target rate $R^* = 1.5$ bits/channel use.

Proof: The proof is straightforwardly obtained from Fig. 8. ■

B. Beneficial Jamming

In this case, the rate-equivocation region shown in Fig. 6.b, is achievable for any ρ. Also, note that there is always a nonzero secrecy rate R'_S corresponding to the maximum main channel capacity R_B, which occurs at $\rho_2 = 0$ (see (13)). A 4-node system with no power allocated for the jammer is equivalent to a 3-node system. Therefore, the same curve $h(x)$ from (34) can be effectively used to sweep the point (R_B, R'_S). Similarly, in this case, at some point, increasing the encryption strength is no longer useful in terms of power minimization. The same threshold λ_a from (35) is used for a given target rate R^* (see Fig. 9). This threshold determines whether the solution point is on the vertical line of the rate-equivocation region or not.

In order to solve the optimization problem, it is required to locate the solution point on the non-vertical part of the rate-equivocation region when $\lambda < \lambda_a$. Thus, for a given ρ, we define another curve that sweeps the point at which the boundary of rate region transitions from being a horizontal line into a curve by $R_e = f(R)$ from (20) for $R : R'_B \leq R \leq \log_2(1 + \alpha_1\rho)$, as seen in Fig. 6.b. However, the curve sweeping the rate pair (R'_B, R_S) can be obtained by solving the following equation

$$\begin{cases} R = R'_B(\rho) \\ R_e = R_S(\rho), \end{cases} \tag{37}$$

where $R'_B(\rho)$ is obtained from (28). Then, the curve can be expressed as $R_e = g(R)$, where

$$g(x) = R_S((R'_B)^{-1}(x)), \text{ for all } x : 0 \leq 2^x - 1 \leq \alpha_1\rho. \tag{38}$$

Again, for a given target rate R^*, let us define another threshold λ_b, such that any encryption with less strength will have a unique solution point that lies on the horizontal boundary of the rate-equivocation region. This threshold is obtained by

$$\lambda_b = \frac{R^*}{g(R^*)}. \tag{39}$$

Therefore, the following proposition states the solution of the optimization problem in this case.

Proposition 5: For the rate-equivocation region of $\bar{\mathcal{R}}_2^{WTC}$, by using the two thresholds λ_a and λ_b, the minimum power satisfying security condition and rate at R^* with a strength λ can be obtained by

$$\rho_{min} = \begin{cases} R_B^{-1}(R^*) = \dfrac{2^{R^*} - 1}{\alpha_1}, & \lambda \geq \lambda_a \\ \rho : R^*/\lambda = f(R^*), & \lambda_b < \lambda < \lambda_a \\ \rho : R^*/\lambda = R_S(\rho), & \lambda \leq \lambda_b, \end{cases} \tag{40}$$

where $R^*/\lambda = f(R^*)$ and $R^*/\lambda = R_S(\rho)$ are nonlinear and can be simply solved by using the bisection method.

Proof: The proof can readily be seen from Fig. (9). ■

The corresponding optimal jamming power is given by

$$\rho_2 = \begin{cases} 0, & \lambda \geq \lambda_a \\ \dfrac{\alpha_1\rho_{min} - (2^{R^*} - 1)}{\alpha_1 + \alpha_2(2^{R^*} - 1)}, & \lambda_b < \lambda < \lambda_a \\ \dfrac{\alpha_1\rho_{min} - (2^{R'_B} - 1)}{\alpha_1 + \alpha_2(2^{R'_B} - 1)}, & \lambda \leq \lambda_b, \end{cases} \tag{41}$$

where R'_B is evaluated using (28), at $\rho = \rho_{min}$. Three different rate regions in Fig. 9 graphically represent each case.

C. Essential Jamming

In this case, the rate-equivocation region shown in Fig. 6.c, is achievable only for $\rho > \rho_T$. Different from the first case, when the main channel capacity is maximized at $\rho_2 = 0$, PHY security is not achievable without encryption. To solve the optimization problem in (31), we only need to use the same curve $g(x)$ from (38) that sweeps the point (R'_B, R_S) for all $\rho > \rho_T$; and then, evaluate λ_b using (39) for a given target rate R^*. The solution is given in the following proposition.

Proposition 6: For the rate-equivocation of $\bar{\mathcal{R}}_3^{WTC}$, using the threshold (λ_b), the minimum power satisfying security condition and rate at R^* with a strength λ can be obtained as

$$\rho_{min} = \begin{cases} \rho : R^*/\lambda = f(R^*), & \lambda > \lambda_b \\ \rho : R^*/\lambda = R_S(\rho), & \lambda \leq \lambda_b, \end{cases} \tag{42}$$

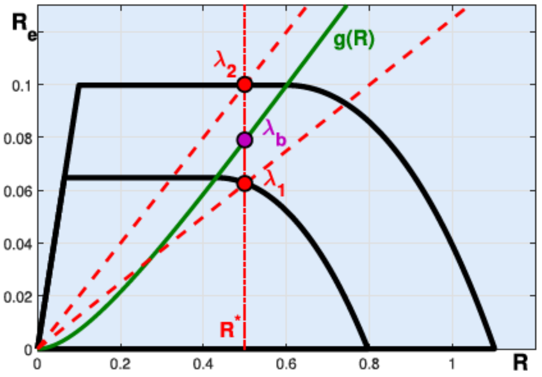

Fig. 10. Optimal power allocation for the EJ scenario: two cases of $\lambda = \lambda_1$ and $\lambda = \lambda_2$ are illustrated, where $\lambda_1 > \lambda_b$ and $\lambda_2 \leq \lambda_b$; Both cases satisfy the target rate $R^* = 0.5$ bits/channel use.

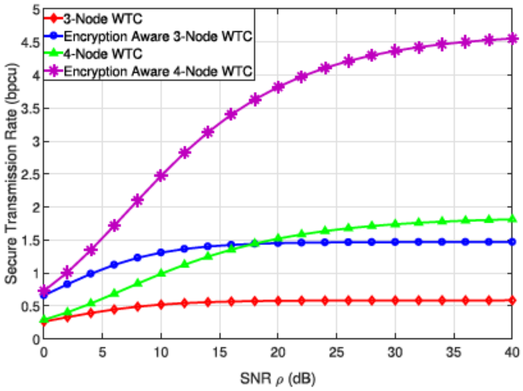

Fig. 11. Secure transmission rate versus SNR for three- and 4-node WTCs with and without encryption awareness in the BJ scenario with $\alpha_1 = 1, \alpha_2 = 0.83, \beta_1 = 0.67, \beta_2 = 2$, and $\lambda = 4$ dB.

where $R^*/\lambda = f(R^*)$ and $R^*/\lambda = R_S(\rho)$ are nonlinear equations. Similar to the previous case, these equations can be solved by applying the bisection method. The corresponding optimal jamming power is given by

$$\rho_2 = \begin{cases} \dfrac{\alpha_1 \rho_{min} - (2^{R^*} - 1)}{\alpha_1 + \alpha_2(2^{R^*} - 1)}, & \lambda > \lambda_b \\ \dfrac{\alpha_1 \rho_{min} - (2^{R'_B} - 1)}{\alpha_1 + \alpha_2(2^{R'_B} - 1)}, & \lambda \leq \lambda_b \end{cases} \tag{43}$$

Fig. 10 shows two different rate-equivocation regions that graphically represent each of these cases.

V. Numerical Results

In this section, we present insightful results to show the significance of the proposed encryption aware scheme over traditional PHY security. Specifically, we first demonstrate that with encryption, secrecy rate can be significantly increased, and beyond traditional secrecy capacity performances can be achieved. In addition, compared to traditional PHY security, the same secrecy rate can be achieved with a smaller power budget.

A. Enhanced Secrecy Performance

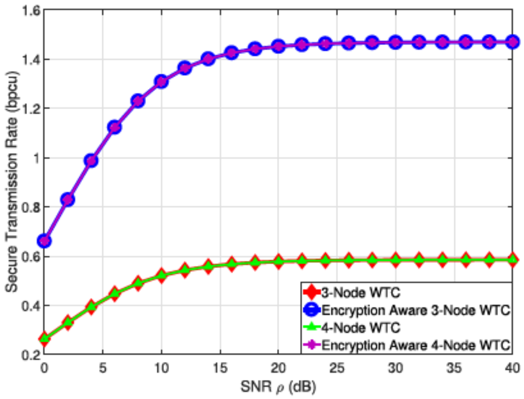

Fig. 12. Secure transmission rate versus SNR for three- and 4-node WTCs with and without encryption awareness in the NJ scenario with $\alpha_1 = 1, \alpha_2 = 0.83, \beta_1 = 0.67, \beta_2 = 0.33$, and $\lambda = 4$ dB.

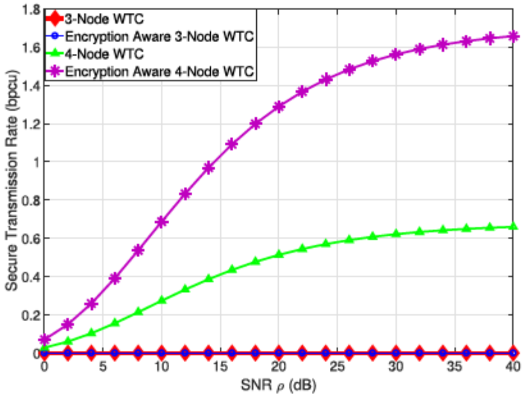

Fig. 13. Secure transmission rate versus SNR for 3- and 4-node WTCs with and without encryption awareness in the EJ scenario with $\alpha_1 = 1, \alpha_2 = 2.5, \beta_1 = 2, \beta_2 = 8$, and $\lambda = 4$ dB.

Fig. 11 first compares the achievable secrecy rate of encryption-aware systems with that of conventional systems for 3- and 4-node WTCs with $\lambda = 4$ dB. Here, it is assumed $\alpha_1 = 1, \alpha_2 = 0.83, \beta_1 = 0.67, \beta_2 = 2$, which results in the BJ scenario. The advantage of encryption awareness can be clearly observed, and we can achieve a significantly higher secrecy rate. It is interesting to note that at low SNRs, encryption aided 3-node WTC even outperforms the conventional 4-node WTC. It means that encryption knowledge can significantly reduce the complexity by relinquishing the jammer, while enjoying a higher transmission rate.

Fig. 12 presents the secrecy performance in the NJ scenario with $\lambda = 4$ dB, where the channel gains are chosen as $\alpha_1 = 1, \alpha_2 = 0.83, \beta_1 = 0.67, \beta_2 = 0.33$. It is clear from Fig. 12 that encryption awareness also significantly enhances the secrecy rate in this case. Furthermore, it can be seen that the 4-node system achieves the same performance as that of the 3-node system. It is because under this scenario, the jammer channel conditions are not in favor of adding secrecy.

The advantage of the proposed encryption-aware scheme for the EJ scenario is shown in Fig. 13, where we use $\alpha_1 = 1, \alpha_2 = 2.5, \beta_1 = 2, \beta_2 = 8$, and $\lambda = 4$dB. Note that, in this case, the secrecy rate is always zero for the 3-node system whether or not encryption is exploited. However, with the

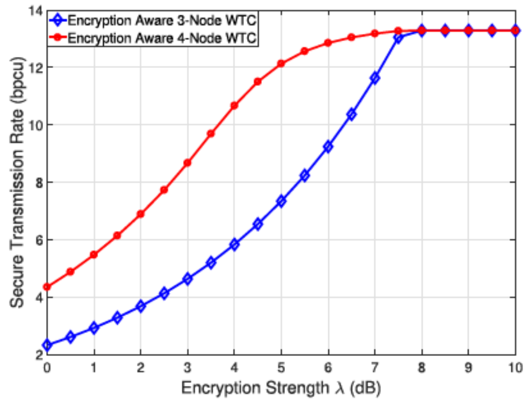

Fig. 14. Secure transmission rate versus encryption strength for 3- and 4-node WTCs in the BJ scenario with $\alpha_1 = 1, \alpha_2 = 0.25, \beta_1 = 0.2, \beta_2 = 1.1$, and SNR $= 40$ dB.

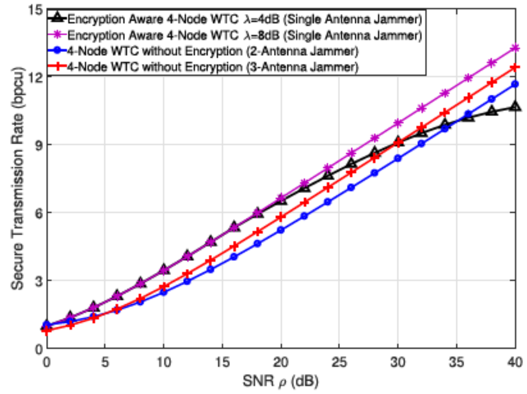

Fig. 15. Secure transmission rate comparison: Encryption-aware versus cooperative jamming [30], [31] in the BJ scenario with $\alpha_1 = 1, \alpha_2 = 0.25, \beta_1 = 0.2, \beta_2 = 1.1$.

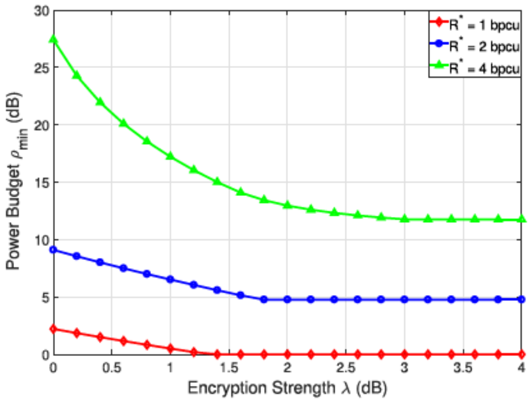

Fig. 16. Optimal power allocation versus encryption strength for the BJ scenario with $\alpha_1 = 1, \alpha_2 = 0.25, \beta_1 = 0.2, \beta_2 = 1.1$, and different target rate R^* values.

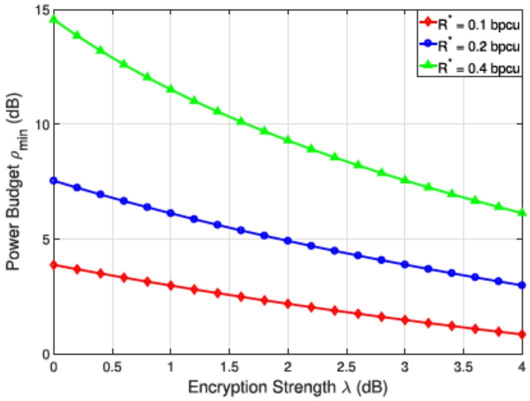

Fig. 17. Optimal power allocation versus encryption strength for the EJ scenario with $\alpha_1 = 1, \alpha_2 = 2.5, \beta_1 = 2, \beta_2 = 8$, and different target rate R^* values.

presence of the jammer, the secrecy rate increases significantly with encryption, especially at higher SNR regions.

It is also interesting to see the effect of λ to the secrecy performance. Let us consider the BJ scenario with $\alpha_1 = 1, \alpha_2 = 0.25, \beta_1 = 0.2, \beta_2 = 1.1$. Fig. 14 shows the secrecy rates achieved by the 4-node and 3-node networks, respectively, for a wide range of λ, with SNR being fixed at 40dB. It can be seen from Fig. 14 when λ is small enough, i.e., $\lambda < \lambda_{T2}$, the 4-node networks achieve a higher secrecy rate. However, when $\lambda \geq \lambda_{T2}$, the two rates are almost the same. It is because we achieve the maximum secrecy rate that cannot be exceeded neither by using a helping interferer nor by making the encryption stronger.

Finally, to demonstrate the significance of the proposed appraoch over traditional physical layer approaches, Fig. 15 compares the secrecy rates achieved by the encryption-aware 4-node systems with $\lambda = 4$dB and $\lambda = 8$dB under the same BJ scenario with $\alpha_1 = 1, \alpha_2 = 0.25, \beta_1 = 0.2, \beta_2 = 1.1$, and those of traditional cooperative jamming schemes using multiple antennas in [30], [31]. Specifically, we consider the scheme in [30] in which Alice communicates with Bob with the help of a jammer being equipped with 2 and 3 antennas, respectively. In this cooperative jamming system, the secrecy rate is maximized by jointly optimizing the antenna weights and transmit power of the source and the jammer [30]. For a fair comparison, it is assumed that Alice-Bob and Alice-Eve channel gains are the same. Furthermore, as in [30], the amplitudes of the channel gains from each of the antennas at the jammers to Bob and to Eve are the same, which are 0.2 and 1.1, respectively, while their phases are uniformly distributed. With $\lambda = 8$dB, the proposed 4-node system with only a single-antenna jammer outperforms the schemes in [30] using multiple antennas. When the encryption is slighly weaker, i.e., $\lambda = 4$dB, the proposed 4-node system still performs better than the multiple-antenna schemes in [30] over a wide range of SNRs.

B. Reduced Power Consumption

With the aid of encryption, we can also reduce the transmission power while still achieving the same targeted secrecy rate with the no-encrypted system. This advantage is shown in Fig. 16 and Fig. 17 for the BJ and EJ scenarios, respectively, where the consumed power is plotted versus λ for different target secrecy rates. Note that $\lambda = 0$ corresponds to the case of no encryption. It can also be observed for the EJ scenario, having a stronger encryption is always beneficial. However, in the BJ case, when the encryption strength is sufficiently

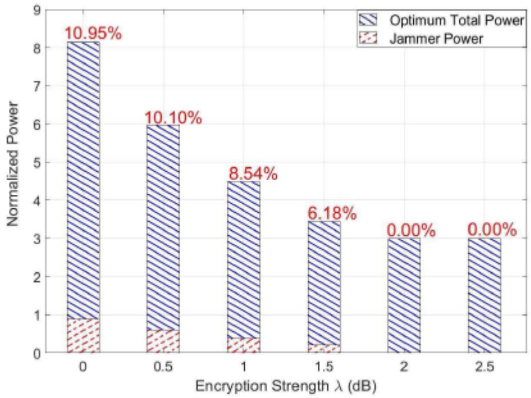

Fig. 18. Minimum required power to achieve a target rate of 2 bpcu, and the corresponding jammer power for different encryption strength values. Channel gains satisfy the BJ scenario with $\alpha_1 = 1, \alpha_2 = 0.25, \beta_1 = 0.2, \beta_2 = 1.1$, and $\lambda_a = 1.8$ dB.

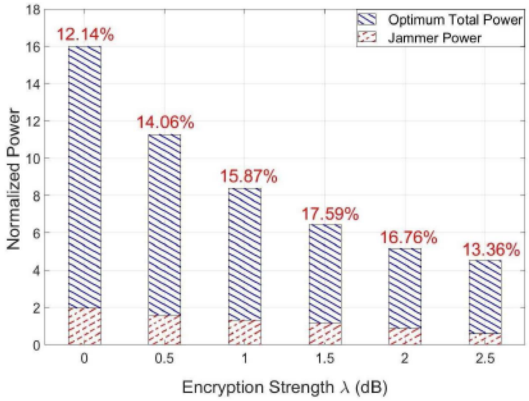

Fig. 19. Minimum required power to achieve a target rate of 2 bpcu, and the corresponding jammer power for different encryption strength values. Channel gains satisfy the EJ scenario with $\alpha_1 = 1, \alpha_2 = 0.5, \beta_1 = 0.2, \beta_2 = 1.5$, and $\lambda_b = 1.8$ dB.

large enough, i.e., $\lambda > \lambda_a$, the consumed power cannot be further reduced.

Using the results in Theorems 5 and 6, the power allocation between the source and the jammer to achieve a given secrecy rate can also be obtained for different values of λ. The results are shown in Fig. 18 and Fig. 19 for the BJ and EJ scenarios, respectively, with the target rate of 2 bpcu. In both scenarios, it can be seen that the power allocated to the jammer decreases as the encryption strength increases. In the BJ scenario, when the encryption is strong enough, e.g., $\lambda > \lambda_a$, the jammer can be kept silent, and the total power is allocated to the source only.

VI. Conclusion

In this article, we proposed a novel encryption-aided physical layer security scheme for Gaussian channels. We introduced an approach that can directly link encryption strength with the amount of leakage at the eavesdropper. Furthermore, we have shown that the encryption awareness enables us to improve the secure transmission rate beyond what is achievable in traditional physical layer security; i.e. the secrecy rate. An encryption-aware secrecy capacity was derived by fully characterizing the rate-equivocation regions for a 4-node systems with different conditions on channel gains. Finally, an optimization problem was formulated and solved to minimize the total transmission power for a predetermined encryption strength.

Finally, it is worth mentioning that the extension of this work to multi-antenna wiretap channels is very interesting, and it is currently under investigation. In addition, while we have defined the encryption strength λ as an inverse of the threshold P_{cipher}, more meaningful measurements for λ can also be investigated. Such an important topic deserves further studies.

Appendix A
Proof of Lemma 1

To prove Property (a), we use (16) and

$$\begin{aligned} 1 - ab &= 1 - \frac{\beta_1(1+\alpha_2\rho)}{\alpha_1(1+\beta_2\rho)} \\ &= \frac{(\alpha_1-\beta_1)+(\alpha_1\beta_2-\alpha_2\beta_1)\rho}{\alpha_1(1+\beta_2\rho).} \\ &= \frac{\alpha_1-\beta_1}{\alpha_1(1+\beta_2\rho)}\left(1-\frac{\rho}{\rho_T}\right). \end{aligned} \tag{44}$$

Now, we prove Properties (b) and (c) with the assumption of $\alpha_2 < \beta_2$ as follows

$$\begin{aligned} 1 + bz &= \frac{\alpha_1(1+\beta_2\rho)+(\alpha_2-\beta_2)z}{\alpha_1(1+\beta_2\rho)} \\ &\geq \frac{\alpha_1(1+\beta_2\rho)+(\alpha_2-\beta_2)\alpha_1\rho}{\alpha_1(1+\beta_2\rho)} \\ &= \frac{1+\alpha_2\rho}{1+\beta_2\rho} > 0, \end{aligned} \tag{45}$$

$$\begin{aligned} 1 - b(a+1) &= \frac{(\alpha_1-\beta_1)+(\alpha_1\beta_2-\alpha_2\beta_1)\rho+(\beta_2-\alpha_2)}{\alpha_1(1+\beta_2\rho)} \\ &= \frac{(\alpha_1-\beta_1)(1-\frac{\rho}{\rho_T})+(\beta_2-\alpha_2)}{\alpha_1(1+\beta_2\rho)} \\ &> \frac{(\alpha_1-\beta_1)(1-\frac{\rho}{\rho_T})}{\alpha_1(1+\beta_2\rho).} \end{aligned} \tag{46}$$

Since $(\alpha_1 - \beta_1)\rho_T < 0$, if $\alpha_1 > \beta_1$, then ρ_T is negative. Also, if $\alpha_1 < \beta_1$, then ρ_T is positive. Therefore, for both cases, the last term in (46) is positive for $\rho > \rho_T$.

Appendix B
Proof of Proposition 2

Let us start with the concavity. We first have

$$f'(x) = 1 - \frac{ab\, 2^x}{p_1(2^x-1)} = \frac{p_2(2^x-1)}{p_1(2^x-1)}, \tag{47}$$

$$f''(x) = \frac{ab \ln 2 \times 2^x \times p_3(2^x-1)}{[p_1(2^x-1)]^2}, \tag{48}$$

where

$$\begin{aligned} p_1(z) &= b^2(1+a)z^2 + b(2+a)z + 1 \\ &= b^2(1+a)\left(z+\frac{1}{b}\right)\left(z+\frac{1}{b(1+a)}\right), \end{aligned} \tag{49}$$

$$p_2(z) = b^2(1+a)z^2 + 2bz + 1 - ab, \tag{50}$$

$$p_3(z) = b^2(1+a)z^2 + 2b^2(1+a)z + b(2+a) - 1. \tag{51}$$

Now, consider the case $a \geq -1$: Let $v(z) = -\log_2\left((1+a) - \frac{a}{1+bz}\right)$ for $0 \leq z \leq \alpha_1\rho$. Since $z = 2^x - 1$ is convex, it is sufficient to show that $v(z)$ is a non-increasing concave function of z. The first and second derivatives of $v(z)$ are calculated as follows

$$\begin{aligned} v'(z) &= \frac{-ab}{\ln 2} \times \frac{1}{[1+bz][1+bz+abz]} \\ v''(z) &= \frac{ab^2}{\ln 2} \times \frac{2(a+1)+2(1+a)bz-a}{[1+bz]^2[1+(a+1)bz]^2}. \end{aligned} \tag{52}$$

From property (b) in Lemma 1, we have $1+bz > 0$. Moreover, because $\alpha_2 < \beta_2$, $a < 0$ and $b < 0$, $v'(z) < 0$ and $v''(z) < 0$. As a result, $f(x)$ is a concave function when $a \geq -1$.

For the case $a < -1$: Using property (c) in Lemma 1, we have $p_3(z) = b^2(1+a)(z+1)^2 - \left(b^2(1+a) - b(2+a) + 1\right) < -(1-b(1+a))(1-b) < 0$. Thus, $f''(x) < 0$, and $f(x)$ is concave.

Given its concavity, it is clear that $f(x)$ is maximized at a stationary point, which can be found by solving $p_2(z) = 0$. For the special case of $a = -1$, from (50), $p_2(z)$ has one root $z^* = \frac{-b-1}{2b}$, and $p_1(z^*) \neq 0$. Therefore, we have $x^* = \log_2\left(\frac{b-1}{2b}\right)$. In the case that $a \neq -1$, $p_2(z)$ has a quadratic form with the following roots

$$z_{\pm} = \frac{-1 \pm \sqrt{\Delta}}{b(1+a)}, \tag{53}$$

where Δ is given in (26). From property (a) in Lemma 1, we have $(1-ab) > 0$ for all $\rho > \rho_T$. Since a and b are negative, Δ is always positive. Given that, we examine the two roots in (53). For z_-, If $a > -1$, we have $z_- > \alpha_1\rho$. On the other hand, when $a < -1$, we have $z_- < 0$. Thus, in any case, $z_- \notin [0, \alpha_1\rho]$, which means z_- is not a valid solution. For z_+, if $a > -1$, we have $\Delta \leq 1$, and therefore, $z_+ \geq 0$. If, on the other hand, $a < -1$, we have $\Delta > 1$, and $z_+ > 0$. This means that z_+ is a valid solution. As a result, when $a \neq -1$, $z^* = \frac{-1+\sqrt{\Delta}}{b(1+a)}$ and $p_1(z^*) \neq 0$. Therefore, $f(x)$ is maximized at $x^* = \log_2\left(\frac{-1+\sqrt{\Delta}}{b(1+a)} + 1\right)$.

Appendix C
Proof of Theorem 1

(a) $\alpha_1 > \beta_1$ and $\alpha_2 \geq \beta_2$ imply that the secrecy function is convex and is maximized at $x^* = \log_2(\alpha_1\rho + 1)$ (see Propositions 1). On the other hand, when $\alpha_1 > \beta_1$ and $\alpha_2 < \beta_2$, the secrecy function is concave, but since $\rho \leq \rho_C$, the function is maximized at $x^* = \log_2(\alpha_1\rho_1 + 1)$ (it decreases as ρ_2 increases), (see Proposition 2 and 3).

(b) $\alpha_1 > \beta_1$ and $\alpha_2 < \beta_1$ imply $\rho_T < 0$. As a result, $\rho > \rho_T$ and $(\alpha_1 - \beta_1)\rho_T < 0$. Therefore, the secrecy function is a concave. If $\rho > \rho_C$, then $x^* = \log_2\left(\frac{-1+\sqrt{\Delta}}{b(1+a)} + 1\right)$ if $a \neq -1$, and $x^* = \log_2\left(\frac{b-1}{2b}\right)$ if $a = -1$, (see Propositions 2 and 3).

(c) $\alpha_1 \leq \beta_1$ and $\alpha_1/\alpha_2 > \beta_1/\beta_2$ imply that $\rho_T \geq 0$ and $\alpha_2 < \beta_2$. Therefore, for $\rho > \rho_T$, the function is concave (see Proposition 2). On the other hand, since the function is zero at $\rho_2 = 0$ and $\rho_2 = \rho_T$, $x^* = \log_2\left(\frac{-1+\sqrt{\Delta}}{b(1+a)} + 1\right)$ if $a \neq -1$, and $x^* = \log_2\left(\frac{b-1}{2b}\right)$ if $a = -1$.

(d) $\alpha_1 \leq \beta_1$ and $\alpha_1/\alpha_2 > \beta_1/\beta_2$ imply that the secrecy function is not positive. On the other hand, $\alpha_1 \leq \beta_1$ and $\alpha_1/\alpha_2 > \beta_1/\beta_2$ imply that $\rho_T \geq 0$ and $\alpha_2 < \beta_2$. However, the available power is not sufficient to make the secrecy function positive.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

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

[3] D.-S. Lee, "Substitution deciphering based on HMMs with applications to compressed document processing," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 24, no. 12, pp. 1661–1666, Dec. 2002.

[4] T. Siegenthaler, "Decrypting a class of stream ciphers using ciphertext only," *IEEE Trans. Comput.*, vol. C-34, no. 1, pp. 81–85, Jan. 1985.

[5] T. Johansson and F. Jonsson, "Theoretical analysis of a correlation attack based on convolutional codes," *IEEE Trans. Inf. Theory*, vol. 48, no. 8, pp. 2173–2181, Aug. 2002.

[6] W. K. Harrison and S. W. McLaughlin, "Physical-layer security: Combining error control coding and cryptography," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2009, pp. 1–5.

[7] W. K. Harrison and S. W. McLaughlin, "Tandem coding and cryptography on wiretap channels: EXIT chart analysis," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2009, pp. 1939–1943.

[8] W. K. Harrison and S. W. McLaughlin, "EXIT charts applied to tandem coding and cryptography in a wiretap scenario," in *Proc. IEEE Inf. Theory Workshop*, Oct. 2009, pp. 173–177.

[9] W. K. Harrison, J. Almeida, D. Klinc, S. W. McLaughlin, and J. Barros, "Stopping sets for physical-layer security," in *Proc. IEEE Inf. Theory Workshop*, Aug. 2010, pp. 1–5.

[10] W. K. Harrison, J. Almeida, S. W. McLaughlin, and J. Barros, "Coding for cryptographic security enhancement using stopping sets," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 575–584, Sep. 2011.

[11] W. K. Harrison, J. Almeida, S. W. McLaughlin, and J. Barros, "Physical-layer security over correlated erasure channels," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2012, pp. 888–892.

[12] W. K. Harrison and S. W. McLaughlin, "Equivocations for the simple substitution cipher with erasure-prone ciphertext," in *Proc. IEEE Inf. Theory Workshop*, Sep. 2012, pp. 622–626.

[13] N. L. Gross and W. K. Harrison, "An analysis of an HMM-based attack on the substitution cipher with error-prone ciphertext," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 749–754.

[14] H. Feistel, "Cryptography and computer privacy," *Sci. Amer.*, vol. 228, no. 5, pp. 15–23, May 1973.

[15] M. A. Haleem, C. N. Mathur, R. Chandramouli, and K. P. Subbalakshmi, "Opportunistic encryption: A trade-off between security and throughput in wireless networks," *IEEE Trans. Dependable Secure Comput.*, vol. 4, no. 4, pp. 313–324, Oct. 2007.

[16] J. Wang, J. Mu, S. Wei, C. Jiang, and N. C. Beaulieu, "Statistical characterization of decryption errors in block-ciphered systems," *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4363–4376, Nov. 2015.

[17] S. Wei, J. Wang, R. Yin, and J. Yuan, "Trade-off between security and performance in block ciphered systems with erroneous ciphertexts," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 4, pp. 636–645, Apr. 2013.

[18] Y. Xiao, H.-H. Chen, X. Du, and M. Guizani, "Stream-based cipher feedback mode in wireless error channel," *IEEE Trans. Wireless Commun.*, vol. 8, no. 2, pp. 622–626, Feb. 2009.

[19] O. Cepheli, G. Dartmann, G. K. Kurt, and G. Ascheid, "An encryption aware physical layer security system," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2017, pp. 1277–1281.

[20] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.

[21] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "On the application of cooperative transmission to secrecy communications," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 359–368, Feb. 2012.

[22] H.-M. Wang, Q. Yin, and X.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3532–3545, Jul. 2012.

[23] C. Dang, L. J. Rodriguez, N. H. Tran, S. Shelly, and S. Sastry, "Secrecy capacity of the full-duplex AF relay wire-tap channel under residual self-interference," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2015, pp. 1–3.

[24] M. Zhang, M. Ding, G. Lin, H. Luo, and M. Bennis, "Sum secrecy rate maximization for relay-aided multiple-source multiple-destination networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 4098–4109, May 2016.

[25] X. Gong, H. Yin, F. Dong, H. Li, and H. Long, "Robust beamforming design for secrecy in multiuser peer-to-peer wireless relay networks," *IEEE Syst. J.*, vol. 12, no. 1, pp. 682–690, Mar. 2018.

[26] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[27] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.

[28] J. Yang, I.-M. Kim, and D. I. Kim, "Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2840–2852, Jun. 2013.

[29] J. Hu, Y. Cai, N. Yang, X. Zhou, and W. Yang, "Artificial-noise-aided secure transmission scheme with limited training and feedback overhead," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 193–205, Jan. 2017.

[30] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Cooperative jamming for wireless physical layer security," in *Proc. IEEE/SP 15th Workshop Stat. Signal Process.*, Aug. 2009, pp. 417–420.

[31] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[32] H. Guo, Z. Yang, L. Zhang, J. Zhu, and Y. Zou, "Joint cooperative beamforming and jamming for physical-layer security of decode-and-forward relay networks," *IEEE Access*, vol. 5, pp. 19620–19630, Sep. 2017.

[33] H.-M. Wang, F. Liu, and M. Yang, "Joint cooperative beamforming, jamming, and power allocation to secure AF relay systems," *IEEE Trans. Veh. Technol.*, vol. 64, no. 10, pp. 4893–4898, Oct. 2015.

[34] J. Kim, A. Ikhlef, and R. Schober, "Combined relay selection and cooperative beamforming for physical layer security," *J. Commun. Netw.*, vol. 14, no. 4, pp. 364–373, Aug. 2012.

[35] H. Fang, L. Xu, Y. Zou, X. Wang, and K. R. Choo, "Three-stage stackelberg game for defending against full-duplex active eavesdropping attacks in cooperative communication," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 10788–10799, Sep. 2018.

[36] A. Garnaev and W. Trappe, "A power control game involving jamming and eavesdropping defense," in *Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS)*, Dec. 2019, pp. 1–6.

[37] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[38] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[39] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[40] R. M. Fano and D. Hawkins, "Transmission of information: A statistical theory of communications," *Amer. J. Phys.*, vol. 29, no. 11, pp. 793–794, Nov. 1961.

[41] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York, NY, USA: Wiley, 1991.

[42] X.-B. Liang, "A note on Fano's inequality," in *Proc. 45th Annu. Conf. Inf. Sci. Syst.*, 2011, pp. 1–3.

[43] S.-W. Ho and S. Verdu, "On the interplay between conditional entropy and error probability," *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 5930–5942, Dec. 2010.

[44] W. Meier and O. Staffelbach, "Fast correlation attacks on certain stream ciphers," *J. Cryptol.*, vol. 1, no. 3, pp. 159–176, Oct. 1989.

[45] A. F. Webster and S. E. Tavares, *On the Design of S-Boxes* (Lecture Notes in Computer Science). Cham, Switzerland: Springer, 1986, pp. 523–534.

[46] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[47] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

Tarig Sadig (Student Member, IEEE) received the B.Sc. degree in electrical and electronic engineering from the University of Khartoum, Khartoum, Sudan, in 2014, and the M.Sc. degree in engineering from The University of Akron, Akron, OH, USA, in 2019. He has been a Research Assistant with the Department of Electrical and Computer Engineering, The University of Akron, since 2016. His research interest includes security in wireless communication and encryption with a focus on physical-layer security.

Mehdi Maleki (Member, IEEE) received the B.Sc. and M.Sc. degrees in electrical engineering from the Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran, in 2006 and 2009, respectively, and the Ph.D. degree from The University of Akron, Akron, OH, USA, in 2015. Since 2017, he has been a Faculty Member of the Electrical and Computer Engineering Department, The University of Akron. His research interests include digital communications, digital signal processing, multiuser communications, multiple-input–multiple-output wireless systems, cognitive radio networks, and secure communications.

Nghi H. Tran (Senior Member, IEEE) received the B.Eng. degree from the Hanoi University of Technology, Vietnam, in 2002, and the M.Sc. and Ph.D. degrees from the University of Saskatchewan, Canada, in 2004 and 2008, respectively, all in electrical and computer engineering. From May 2008 to July 2010, he was a Post-Doctoral Scholar with McGill University under the prestigious Natural Sciences and Engineering Research Council of Canada (NSERC) Postdoctoral Fellowship. From August 2010 to July 2011, he was a Research Associate with McGill University. Since August 2011, he has been with the Department of Electrical and Computer Engineering, The University of Akron, OH, USA, where he is currently an Associate Professor. His research interests include signal processing and communication and information theories for wireless systems and networks and network security. His work has been supported by the U.S. National Science Foundation and the Office of Naval Research/Department of Defense. He received the Graduate Thesis Award for his M.Sc. degree. He is an Editor of IEEE TRANSACTIONS ON COMMUNICATIONS and *Physical Communication* (Elsevier) and a Senior Editor of IEEE COMMUNICATIONS LETTERS.

Hamid Reza Bahrami (Senior Member, IEEE) received the B.Sc. degree from the Sharif University of Technology, the M.Sc. degree from the University of Tehran, Iran, and the Ph.D. degree from McGill University, Montreal, QC, Canada, in 2008, all in electrical engineering. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, The University of Akron, OH, USA. From 2007 to 2009 and prior to joining The University of Akron, he was a Scientist with Wavesat Inc. (now Cavium Inc.) Montreal, where he was working with the Research and Development Team to develop receiver algorithms for WiMAX and LTE radios. His main research interests include wireless communications, information theory, and applications of signal processing in communications. He is a member of the IEEE Communications Society and the IEEE Vehicular Technology Society. He has served as an Editor for IEEE TRANSACTIONS ON COMMUNICATIONS and *Transactions on Emerging Telecommunications Technologies* (formerly *European Transactions on Telecommunications*), a Guest Editor for *The Scientific World Journal* and *Electronics* Journal, and a Technical Program Committee Member of numerous IEEE conferences, including IEEE GLOBECOM, International Conference on Communications (ICC), and Vehicular Technology Conference (VTC).