# On Secrecy Metrics for Physical Layer Security Over Quasi-Static Fading Channels

Biao He, *Member, IEEE*, Xiangyun Zhou, *Member, IEEE*, and A. Lee Swindlehurst, *Fellow, IEEE*

***Abstract*— Theoretical studies on physical layer security often adopt the secrecy outage probability as the performance metric for wireless communications over quasi-static fading channels. The secrecy outage probability has two limitations from a practical point of view: 1) it does not give any insight into the eavesdropper's decodability of confidential messages and 2) it cannot characterize the amount of information leakage to the eavesdropper when an outage occurs. Motivated by the limitations of the secrecy outage probability, we propose three new secrecy metrics for secure transmissions over quasi-static fading channels. The first metric establishes a link between the concept of secrecy outage and the decodability of messages at the eavesdropper. The second metric provides an error-probability-based secrecy metric which is typically used for the practical implementation of secure wireless systems. The third metric characterizes how much or how fast the confidential information is leaked to the eavesdropper. We show that the proposed secrecy metrics collectively give a more comprehensive understanding of physical layer security over fading channels and enable one to appropriately design secure communication systems with different views on how secrecy is measured.**

***Index Terms*— Physical layer security, secrecy outage probability, secure transmission design, quasi-static fading channel.**

## I. Introduction

### A. Background and Motivation

AN UNPRECEDENTED amount of private and sensitive information is transmitted over wireless channels as a result of the ubiquitous wireless devices adopted in modern life. Security issues associated with wireless communications consequently have become critical due to the unchangeable open nature of the wireless medium. As a complement to traditional cryptographic techniques, physical layer security has been proposed for ensuring secure wireless communications by exploiting the characteristics of wireless channels [2], [3]. Shannon [4] introduced the notion of information-theoretic secrecy, which does not rely on assumptions about the computational abilities of the eavesdropper. Classical information-theoretic secrecy[1] requires that the amount of information leakage to the eavesdropper vanishes. It guarantees that the eavesdropper's optimal attack is to guess the message at random, and hence the eavesdropper's decoding error probability, $P_e$, asymptotically goes to 1. In his seminal work [5], Wyner introduced the wiretap channel, and addressed the tradeoff between the information rate achieved by the intended receiver and the level of ignorance at the eavesdropper. This result was later extended to the broadcast channel with confidential messages [6] and the Gaussian wiretap channel [7].

More recently, physical layer security over wireless fading channels has been extensively studied, e.g., [8]–[12]. In particular, practical scenarios involving imperfect or no knowledge about the eavesdropper's instantaneous channel state information (CSI) has drawn an increasing amount of attention, e.g., see [13] and references therein. The secrecy performance in such scenarios is often characterized by either ergodic secrecy capacity [8] or secrecy outage probability [11], [12]. For a system in which the encoded messages can span sufficient channel realizations to capture the ergodic features of the fading channel, the ergodic secrecy capacity characterizes the capacity limit subject to the constraint of classical information-theoretic secrecy. For transmission over quasi-static fading channels where classical information-theoretic secrecy is not always achievable, the (classical) secrecy outage probability measures the probability of failing to achieve classical information-theoretic secrecy. With either the ergodic secrecy capacity or the secrecy outage probability as the secrecy metric, many researchers have studied secure transmission designs and/or secrecy enhancements, e.g., [14]–[18].

Classical secrecy outage probability has two major limitations in evaluating the secrecy performance of wireless systems.

a) Classical secrecy outage probability does not give any insight into the eavesdropper's ability to decode the confidential messages. The eavesdropper's decodability is an intuitive measure of security in real-world communication systems when classical information-theoretic secrecy is not always achievable, and error-probability-based secrecy metrics are often adopted to quantify secrecy performance in the literature, e.g., [19]–[21] focusing on infinite-length code design, [22]–[24] investigating finite-length

Manuscript received January 14, 2016; revised May 3, 2016; accepted July 6, 2016. Date of publication July 20, 2016; date of current version October 7, 2016. This work was supported by the Australian Research Council through the Discovery Project under Grant DP150103905. This work was presented at the 2014 IEEE Global Communications Conference [1]. The associate editor coordinating the review of this paper and approving it for publication was A. Wyglinski.

B. He is with the Department of Electronic and Computer Engineering, The Hong Kong University of Science and Technology, Hong Kong (e-mail: eebiaohe@ust.hk).

X. Zhou is with the Research School of Engineering, The Australian National University, Canberra, ACT 2601, Australia (e-mail: xiangyun.zhou@anu.edu.au).

A. L. Swindlehurst is with the Center for Pervasive Communications and Computing, Department of Electrical Engineering and Computer Science, University of California at Irvine, Irvine, CA 92697 USA (e-mail: swindle@uci.edu).

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

Digital Object Identifier 10.1109/TWC.2016.2593445

[1] In this paper, we use the term "classical information-theoretic secrecy" to refer to Shannon's perfect secrecy, strong secrecy, and weak secrecy, which will be described in Section II-A.

coding schemes, [25] utilizing probabilistic ciphering, [26] investigating secure network coding, and [27] studying secrecy with compressive sensing. A general secrecy requirement for the eavesdropper's decoding error probability can be given as $P_e \geq \epsilon$, where $0 < \epsilon \leq 1$ denotes the minimum acceptable value of $P_e$. In contrast, classical secrecy outage probability reflects only an extremely stringent requirement on $P_e$ for $\epsilon \to 1$, i.e., requiring $\epsilon \to 1$, since classical information-theoretic secrecy guarantees $P_e \to 1$.

b) The amount of information leakage to the eavesdropper cannot be characterized. When classical information-theoretic secrecy is not achievable, some information will be leaked to the eavesdropper. Different secure transmission designs that lead to the same secrecy outage probability may actually result in very different amounts of information leakage. Consequently, it is important to know how much or how fast the confidential information is leaked to the eavesdropper to obtain a finer view of the secrecy performance. However, the classical outage-based approach is not able to evaluate the amount of information leakage when a secrecy outage occurs.

It is worth mentioning that, apart from the two above mentioned limitations, the classical secrecy outage probability also has a severe limitation in evaluating the secrecy performance of systems with finite-length coding schemes. Since classical information-theoretic secrecy cannot be achieved by any coding scheme with a finite-length codeword, the classical secrecy outage probability based on the classical information-theoretic secrecy cannot be adopted in the studies focusing on finite-length coding schemes. Thus, it is of significant importance to examine secrecy metrics specifically for wireless systems with finite-length codes, although such a study is beyond the scope of this paper.

### *B. Our Approach and Contribution*

As previously discussed, the classical information-theoretic secrecy is not always achievable for transmissions over quasi-static fading channels, and we cannot ensure that the eavesdropper's decoding error probability always goes to 1. The classical secrecy outage probability, which is the secrecy metric for quasi-static fading channels, in fact has limitations in evaluating the secrecy performance of wireless systems. This motivates us to propose new secrecy metrics for wireless transmissions focusing on quasi-static fading channels in this paper. The classical secrecy outage probability is based on the concept of classical information-theoretic secrecy. On the other hand, our proposed secrecy metrics are based on another regime of interest in physical layer security, namely the *partial* secrecy regime. The partial secrecy of a system is often evaluated using the equivocation, which reflects the level at which the eavesdropper is confused. The study of equivocation for secrecy can be found as early as Wyner's pioneering work for the wiretap channel [5]. Similarly, Csiszár and Körner [6] used the normalized equivocation to quantify partial secrecy for the broadcast channel with confidential information. Importantly, the equivocation is closely related to the decoding error probability [5], [28], [29]. Therefore, evaluating the secrecy performance on the basis of equivocation can reflect the decodability of confidential messages at the eavesdropper.

Specifically, we propose three new secrecy metrics:

1) Extended from the classical definition of secrecy outage, a generalized formulation of secrecy outage probability is proposed. The generalized secrecy outage probability takes into account the level of secrecy measured by equivocation, and hence establishes a link between the concept of secrecy outage and the decodability of messages at the eavesdropper.
2) An asymptotic lower bound on the eavesdropper's decoding error probability is proposed. This proposed metric provides a *direct* link to error-probability-based secrecy metrics that are often used for the practical implementation of security in wireless systems operating over fading channels.
3) A metric evaluating the average information leakage rate is proposed. This proposed secrecy metric gives an answer to the important question of how much or how fast the confidential information is leaked to the eavesdropper when classical information-theoretic secrecy is not achieved.

We note that both the generalized secrecy outage probability and the asymptotic lower bound on the eavesdropper's decoding error probability give insights into the eavesdropper's ability to decode the confidential messages. In comparing these two metrics, we highlight that the asymptotic lower bound on the eavesdropper's decoding error probability provides a more direct bridge to the error-probability-based secrecy metrics. Although the eavesdropper's decoding error probability cannot be exactly characterized, the asymptotic lower bound gives a worst-case estimation of the eavesdropper's decodability. On the other hand, the generalized secrecy outage probability is extended from the classical secrecy outage probability. Hence, existing studies on secrecy outage probability can be easily extended to the generalized secrecy outage probability.

To illustrate the use of the newly proposed secrecy metrics, we evaluate the secrecy performance of an example wireless system with fixed-rate wiretap codes. We show that the proposed secrecy metrics can provide a more comprehensive and in-depth understanding of the secrecy performance over fading channels. Moreover, we investigate the impact of the new secrecy metrics on the transmission design. We find that the newly proposed secrecy metrics lead to very different optimal design parameters that optimize the secrecy performance of the system, compared with the optimal design minimizing the classical secrecy outage probability. We also find that applying the optimal design that minimizes the secrecy outage probability can result in a large secrecy loss, if the actual system requires a low decodability at the eavesdropper and/or a low information leakage rate.

It is worth mentioning that this work is solely motivated by the limitations of the classical secrecy outage probability from a more practical point of view. Our proposed new secrecy metrics based on the concept of partial secrecy do not imply that the secrecy metrics based on classical information-theoretic secrecy are inappropriate from the

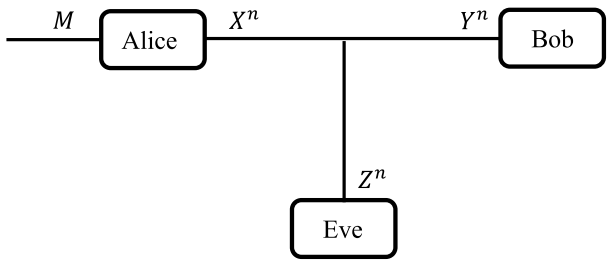



Fig. 1. Basic wiretap channel.

information-theoretic perspective. We acknowledge the importance of requiring classical information-theoretic secrecy for research on information-theoretic security. Meanwhile, we notice the large gap between the requirement of information-theoretic security and the condition of practical secrecy. We hope that the newly proposed secrecy metrics can enable contributions that bridge the gap between theory and practice in physical layer security.

The remainder of the paper is organized as follows. Section II provides background information on classical information-theoretic secrecy and partial secrecy. Section III introduces the three new secrecy metrics for wireless transmissions over fading channels. Section IV illustrates the use of the newly proposed metrics by evaluating the secrecy performance of an example wireless system with fixed-rate wiretap codes. Section V demonstrates the impact of the new secrecy metrics on system design, and finally Section VI concludes the paper.

## II. Preliminaries

Consider the basic wiretap-channel system shown in Fig. 1. A transmitter, Alice, sends confidential information, $M$, to an intended receiver, Bob, in the presence of an eavesdropper, Eve. The source is stationary and ergodic. The confidential information, $M$, is encoded into a $n$-vector $X^n$. The received vectors at Bob and Eve are denoted by $Y^n$ and $Z^n$, respectively. The entropy of the source information and the residual uncertainty for the message at the eavesdropper are denoted by $H(M)$ and $H(M \mid Z^n)$, respectively.

### A. Classical Information-Theoretic Secrecy

As mentioned before, classical information-theoretic secrecy implies that the amount of information leakage to the eavesdropper vanishes, and guarantees that the eavesdropper's optimal attack is to guess the message at random. From Shannon's definition, perfect secrecy requires statistical independence between the original message and Eve's observation, which is given by

$$H(M \mid Z^n) = H(M) \text{ or, equivalently, } \quad I(M; Z^n) = 0. \quad (1)$$

Since Shannon's definition of perfect secrecy is not convenient to be used for further analysis, current research often investigates strong secrecy or weak secrecy. Strong secrecy requires asymptotic statistical independence of the message and Eve's observation as the codeword length goes to infinity, i.e., $\lim_{n\to\infty} I(M; Z^n) = 0$. Weak secrecy requires that the rate of information leaked to the eavesdropper vanishes, i.e., $\lim_{n\to\infty} \frac{1}{n} I(M; Z^n) = 0$. Since strong secrecy, weak secrecy and Shannon's perfect secrecy all belong to the classical information-theoretic secrecy regime, for simplicity we use the term "classical information-theoretic secrecy" to refer to such a regime in this paper. For simplicity, we also do not explicitly denote the assumption of $n \to \infty$ for the discussions in the rest of this paper.

The requirement of no information leakage to Eve in fact guarantees the highest possible decoding error probability at Eve. As explained in [2, Remark 3.1], consider that messages are uniformly taken from a size $K$ set $[1, 2, \cdots, K]$, and Eve minimizes her decoding error probability $P_e$ by performing maximum-likelihood decoding. The condition of no information leakage ensures that Eve can only guess the original message, and the probability of error under maximum-likelihood decoding is $P_e = \frac{K-1}{K}$. Therefore, from the decodability point of view, classical information-theoretic secrecy guarantees $P_e \geq \frac{K-1}{K}$. Furthermore, when the entropy of the message is very large so that $K \to \infty$, classical information-theoretic secrecy actually guarantees that $P_e$ asymptotically goes to 1,

$$\lim_{K\to\infty} P_e \geq \lim_{K\to\infty} \frac{K-1}{K} = 1. \quad (2)$$

In practice, the secrecy requirement on the decodability of messages at Eve can be generally written as $P_e \geq \epsilon$ for some $\epsilon$. Depending on the application, the value of $\epsilon$ ranges from 0 to 1, which falls outside the classical information-theoretic secrecy regime.

### B. Partial Secrecy

Partial secrecy is often quantified by the equivocation, which indicates the level at which Eve is confused. In this paper, we specifically consider the fractional equivocation, which is defined as [7]

$$\Delta = \frac{H(M \mid Z^n)}{H(M)}. \quad (3)$$

Note that evaluating security on the basis of equivocation is related to the conventional requirement on the decodability of messages at Eve [5]. Although there is no one-to-one relation between the equivocation and the error probability, tight lower and upper bounds of the decoding error probability can be derived from the equivocation [28], [29].

When studying secrecy, we particularly want to ensure that the decoding error probability at the eavesdropper is larger than a certain level. Thus, it is desirable to have the decoding error probability at Eve lower bounded by the equivocation. Still consider the general case where messages are uniformly taken from a size $K$ set $[1, 2, \cdots, K]$, which achieves the maximal entropy over an alphabet of size $K$. Then, the entropy of the message is given by $H(M) = \log_2(K)$. From Fano's inequality [28, Ch. 2.10], we have

$$H(M \mid Z^n) \leq h(P_e) + P_e \log_2(K), \quad (4)$$

where $h(x) = -x\log_2(x) - (1-x)\log_2(1-x),\ 0 \le x \le 1$. This inequality can be weakened to

$$P_e \ge \frac{H(M \mid Z^n) - 1}{\log_2(K)} = \Delta - \frac{1}{\log_2(K)}. \tag{5}$$

When the entropy of the message is very large such that $K \to \infty$, we can further derive (5) as

$$\lim_{K\to\infty} P_e \ge \Delta - \lim_{K\to\infty} \frac{1}{\log_2(K)} = \Delta. \tag{6}$$

Thus, $P_e$ is asymptotically lower bounded by $\Delta$.

## III. New Secrecy Metrics for Wireless Transmissions

Consider the basic wiretap-channel system as introduced in the previous section. We now assume that the messages are transmitted over quasi-static fading channels. Bob and Eve perfectly know their own CSI, but Eve's instantaneous CSI is not available at the legitimate side. For wireless transmissions in such a system, classical information-theoretic secrecy is not always achievable, and the secrecy outage probability is commonly used to measure the secrecy performance. From the classical information-theoretic secrecy perspective, the classical definition of secrecy outage probability treats the failure of achieving *classical information-theoretic secrecy* as a secrecy outage. Thus, the classical secrecy outage probability is applicable only for the system which has an extremely stringent requirement on Eve's decoding error probability, $\epsilon \to 1$, but cannot handle the general requirement on Eve's decoding error probability, $0 < \epsilon \le 1$. In addition, the outage-based secrecy metric cannot evaluate how much or how fast the confidential information is leaked to Eve.

Unlike classcial secrecy outage probability, we study the secrecy performance of wireless communications from the partial secrecy perspective. For wireless transmissions over fading channels, the fractional equivocation, $\Delta$, is a random quantity due to the fading properties of the channel. Thus, we start from the derivation of $\Delta$ for a given fading realization. The distribution of $\Delta$ can be obtained according to the distribution of the channel gains. After that, three new secrecy metrics are proposed based on the distribution of $\Delta$.

### A. Fractional Equivocation for a Given Fading Realization

A given fading realization of the wireless channel is equivalent to the (non-degraded) Gaussian wiretap channel [9]. The value of the fractional equivocation for the Gaussian wiretap channel actually depends on the coding and transmission strategies, and there is no general expression applicable for all scenarios. However, an upper bound on $\Delta$ can be easily derived following closely from [7, Th. 1] and [9, Corollary 2]. The maximum achievable fractional equivocation for a given fading realization of the wireless channel is given by

$$\Delta = \begin{cases} 1, & \text{if } C_e \le C_b - R \\ (C_b - C_e)/R, & \text{if } C_b - R < C_e < C_b \\ 0, & \text{if } C_b \le C_e, \end{cases} \tag{7}$$

where $C_b$ and $C_e$ denote Bob and Eve's channel capacities, respectively, and $R = \frac{H(M)}{n}$ denotes the secrecy rate for transmission.

### B. New Secrecy Metrics

From (7), we note that $\Delta$ is a random quantity determined by the instantaneous channel gains and the transmission rate. Since the instantaneous knowledge of Eve's channel is unknown, we cannot directly characterize the instantaneous secrecy performance of the transmissions. Consequently, a meaningful system characterization relies on studying the distribution of $\Delta$, which measures the long-term performance of the system with time-varying channel realizations. In the following, we investigate the distribution of $\Delta$ from three aspects to propose three secrecy metrics.

*1) Generalized Secrecy Outage Probability:* Extending the classical definition of secrecy outage probability, we propose a generalized definition of secrecy outage probability, given by

$$p_{\text{out}} = \mathbb{P}\left(\Delta < \theta\right), \tag{8}$$

where $\mathbb{P}(\cdot)$ denotes the probability measure and $0 < \theta \le 1$ denotes the minimum acceptable value of the fractional equivocation.

Since the fractional equivocation is related to the decoding error probability, the generalized secrecy outage probability is applicable for systems with different levels of secrecy requirements measured in terms of Eve's ability to decode the confidential messages (by choosing different values of $\theta$). The classical secrecy outage probability is defined as $\mathbb{P}(\Delta < 1)$, and hence is a special case of the new secrecy outage metric. Apart from the discussion above, another way to understand the generalized secrecy outage probability can be described as follows. From (3), the information leakage ratio to Eve can be written as $\frac{I(M;Z^n)}{H(M)} = 1 - \Delta$. The information leakage ratio quantifies the percentage of transmitted confidential information leaked to the eavesdropper. As such, the generalized secrecy outage probability, $p_{\text{out}} = \mathbb{P}(\Delta < \theta) = \mathbb{P}(1 - \Delta > 1 - \theta)$, actually characterizes the probability that the information leakage ratio is larger than a certain value, $1 - \theta$.

In fact, we can also explain the generalized secrecy outage probability as an extension of partial secrecy in the Gaussian channel to the fading channel. Partial secrecy was originally proposed and investigated in the Gaussian channel in some of the pioneering studies of physical layer security, e.g., [5]–[7]. It has also been adopted in evaluating the secrecy performance of finite-length codes in the Gaussian channel, e.g., [22], [30], [31]. It is worth mentioning that a secrecy metric similar to the generalized secrecy outage probability was adopted in [32], which focused on analyzing the performance of finite-length codes in the fading channel. In [32], a secrecy metric was adopted that quantifies the probability of Eve's decoding error being less than a given threshold, a result that was motivated by the fact that finite-length codes cannot guarantee Eve's decoding error rate will approach 1. The secrecy metric in [32] is based on the partial secrecy metric adopted in [31] for finite-length codes in the Gaussian channel. The fact that [32] also adopts a partial secrecy metric further shows that classical secrecy outage probability has a severe limitation in evaluating the secrecy performance of wireless systems with finite-length codes.

*2) Average Fractional Equivocation—Asymptotic Lower Bound on Eavesdropper's Decoding Error Probability:* Taking the average of the fractional equivocation, we can derive the (long-term) average value of the fractional equivocation, given by

$$\bar{\Delta} = \mathbb{E}\{\Delta\}, \tag{9}$$

where $\mathbb{E}\{\cdot\}$ denotes the expectation operation. Note that the average fractional equivocation takes the average of the values of fractional equivocation over all fading realizations. Since the fading varies slowly compared with one symbol time in quasi-static fading channels, it takes a relatively long time to experience a sufficient number of fading realizations during the transmissions. Thus, to be rigorous, we define $\bar{\Delta}$ as the (*long-term*) average fractional equivocation. As discussed earlier in (6), Eve's decoding error probability for a given fading realization is asymptotically lower bounded by the fractional equivocation. Thus, the average fractional equivocation, $\bar{\Delta}$, actually gives an asymptotic lower bound on the overall decoding error probability at Eve, i.e, $P_e \geq \bar{\Delta}$.

*3) Average Information Leakage Rate:* With knowledge of message transmission rate $R = \frac{H(M)}{n}$, we can further derive the average information leakage rate, given by

$$R_L = \mathbb{E}\left\{\frac{I(M; Z^n)}{n}\right\} = \mathbb{E}\left\{(1-\Delta)R\right\}. \tag{10}$$

The average information leakage rate tells how fast the information is leaked to the eavesdropper. Note that the transmission rate $R$ cannot be simply taken out of the expectation in (10), since $R$ can be a variable parameter (e.g., adaptive-rate transmission) and its distribution may be correlated with the distribution of $\Delta$. However, when a fixed-rate transmission scheme is adopted, (10) can be simplified as

$$R_L = \mathbb{E}\left\{(1-\Delta)R\right\} = (1-\bar{\Delta})R. \tag{11}$$

*Remark 1:* The proposed secrecy metrics in this section, i.e., (8), (9) and (10), are general and can be applied to evaluate the performance of any coding and transmission strategy under any system model (e.g., signal-antenna or multi-antenna systems). A specific scenario is studied as an example in the next section, wherein the expressions for the proposed secrecy metrics are further derived in terms of transmission rates and channel statistics.

## IV. Wireless Transmissions With Fixed-Rate Wiretap Codes: An Example

### A. System Model

We consider the system where a transmitter, Alice, wants to send confidential information to an intended receiver, Bob, in the present of an eavesdropper, Eve, over a quasi-static Rayleigh fading channel. Alice, Bob and Eve are assumed to have a single antenna each. The instantaneous channel capacities at Bob and Eve are given by

$$C_b = \log_2(1+\gamma_b) \tag{12}$$

and

$$C_e = \log_2(1+\gamma_e), \tag{13}$$

respectively, where $\gamma_b$ and $\gamma_e$ denote the instantaneous received signal-to-noise ratios (SNRs) at Bob and Eve, respectively. The instantaneous received SNRs at Bob and Eve have exponential distributions, given by

$$f_{\gamma_b}(\gamma_b) = \frac{1}{\bar{\gamma_b}} \exp\left(-\frac{\gamma_b}{\bar{\gamma_b}}\right) \tag{14}$$

and

$$f_{\gamma_e}(\gamma_e) = \frac{1}{\bar{\gamma_e}} \exp\left(-\frac{\gamma_e}{\bar{\gamma_e}}\right), \tag{15}$$

respectively, where $\bar{\gamma_e}$ and $\bar{\gamma_e}$ denote the average received SNRs at Bob and Eve, respectively.

We consider the widely-adopted wiretap code [5] for message transmissions. There are two rate parameters, namely, the codeword transmission rate, $R_b = \frac{H(X^n)}{n}$, and the confidential information rate, $R_s = \frac{H(M)}{n}$. A length $n$ wiretap code is constructed by generating $2^{nR_b}$ codewords $x^n(w, v)$, where $w = 1, 2, \cdots, 2^{nR_s}$ and $v = 1, 2, \cdots, 2^{n(R_b - R_s)}$. For each message index $w$, we randomly select $v$ from $\left\{1, 2, \cdots, 2^{n(R_b-R_s)}\right\}$ with uniform probability and transmit the codeword $x^n(w, v)$. In addition, we consider fixed-rate transmission,[2] where the transmission rates, i.e., $R_b$ and $R_s$, are fixed over time.

Bob and Eve are assumed to perfectly know their own channels. Hence, $C_b$ and $C_e$ are known at Bob and Eve, respectively. Alice has statistical knowledge of Bob and Eve's channels, but does not know either Bob or Eve's instantaneous CSI. We further assume that Bob provides a one-bit feedback about his channel quality to Alice in order to avoid unnecessary transmissions [12], [16]. The one-bit feedback enables an on-off transmission scheme to guarantee that the transmission takes place only when $R_b \leq C_b$. In addition, the on-off transmission scheme incurs a probability of transmission, given by

$$p_{\text{tx}} = \mathbb{P}\left(R_b \leq C_b\right) = \exp\left(-\frac{2^{R_b}-1}{\bar{\gamma_b}}\right). \tag{16}$$

### B. Secrecy Performance Evaluation

To characterize the secrecy performance of wireless transmissions over the fading channel, we start from the investigation on a given fading realization of the channel.

*Proposition 1:* For a given fading realization of the wireless channel, the maximum achievable fractional equivocation for the wiretap code with $R_b \leq C_b$ and $R_s \leq R_b$ is given by

$$\Delta = \begin{cases} 1, & \text{if } C_e \leq R_b - R_s \\ (R_b - C_e)/R_s, & \text{if } R_b - R_s < C_e < R_b \\ 0, & \text{if } R_b \leq C_e. \end{cases} \tag{17}$$

*Proof:* The proof follows closely from [9, Corollary 2] and the steps in [7, Sec. III] with $\frac{H(X^n)}{n} = R_b$. ■

Note that $\Delta$ in (17) actually gives an upper bound on the achievable fractional equivocation for the wiretap code, which is achieved by an ideal coding scheme with infinite

[2]Fixed-rate transmissions are often adopted to reduce system complexity. In practice, applications like video streaming in multimedia applications often require fixed-rate transmission.

codeword length. It is worth mentioning that it is also of significant importance to obtain the lower bound of the fractional equivocation when investigating the performance of a specific code, e.g., [22], [30] which study finite-length LDPC codes. The secrecy performance guaranteed by a given code can be characterized by the lower bound on the fractional equivocation.

From (13), we can further derive (17) as

$$\Delta = \begin{cases} 1, & \text{if } \gamma_e \le 2^{R_b-R_s}-1 \\ \frac{R_b-\log_2(1+\gamma_e)}{R_s}, & \text{if } 2^{R_b-R_s}-1 < \gamma_e < 2^{R_b}-1 \\ 0, & \text{if } 2^{R_b}-1 \le \gamma_e. \end{cases} \quad (18)$$

Now, we are ready to evaluate the secrecy performance of wireless transmissions over fading channels from the distribution of $\Delta$, which can be derived according to the distribution of $\gamma_e$ given in (15).

*1) Generalized Secrecy Outage Probability:* The generalized secrecy outage probability is given by

$$\begin{aligned} p_{\text{out}} &= \mathbb{P}(\Delta < \theta) \\ &= \mathbb{P}\left(2^{R_b}-1 \le \gamma_e\right) + \mathbb{P}\left(2^{R_b-R_s}-1 < \gamma_e < 2^{R_b}-1\right) \\ &\quad \cdot \mathbb{P}\left(\frac{R_b-\log_2(1+\gamma_e)}{R_s} < \theta \,\middle|\, 2^{R_b-R_s}-1 < \gamma_e < 2^{R_b}-1\right) \\ &= \exp\left(-\frac{2^{R_b-\theta R_s}-1}{\bar{\gamma_e}}\right), \end{aligned} \quad (19)$$

where $0 < \theta \le 1$.

For the extreme case of $\theta = 1$, we have

$$p_{\text{out}}(\theta = 1) = \exp\left(-\frac{2^{R_b-R_s}-1}{\bar{\gamma_e}}\right). \quad (20)$$

We note that (20) is exactly the same as [12, Eq. (8)], which gives the classical secrecy outage probability of wireless transmissions with fixed-rate wiretap codes.

*2) Average Fractional Equivocation—Asymptotic Lower Bound on Eavesdropper's Decoding Error Probability:* The average fractional equivocation is given by

$$\begin{aligned} \bar{\Delta} &= \mathbb{E}\{\Delta\} \\ &= \int_0^{2^{R_b-R_s}-1} f_{\gamma_e}(\gamma_e)\mathrm{d}\gamma_e \\ &\quad + \int_{2^{R_b-R_s}-1}^{2^{R_b}-1} \left(\frac{R_b-\log_2(1+\gamma_e)}{R_s}\right) f_{\gamma_e}(\gamma_e)\mathrm{d}\gamma_e \\ &= 1 - \frac{1}{R_s \ln 2} \exp\left(\frac{1}{\bar{\gamma_e}}\right)\left(\mathrm{Ei}\left(-\frac{2^{R_b}}{\bar{\gamma_e}}\right) - \mathrm{Ei}\left(-\frac{2^{R_b-R_s}}{\bar{\gamma_e}}\right)\right), \end{aligned} \quad (21)$$

where $\mathrm{Ei}(x) = \int_{-\infty}^{x} e^t/t \ \mathrm{d}t$ denotes the exponential integral function. As mentioned before, the average fractional equivocation actually gives an asymptotic lower bound on the eavesdropper's decoding error probability.

*3) Average Information Leakage Rate:* Since a fixed-rate transmission scheme is adopted, the average information leakage rate can be derived from (11), given by

$$\begin{aligned} R_L &= (1-\bar{\Delta})R_s \\ &= \frac{1}{\ln 2} \exp\left(\frac{1}{\bar{\gamma_e}}\right)\left(\mathrm{Ei}\left(-\frac{2^{R_b}}{\bar{\gamma_e}}\right) - \mathrm{Ei}\left(-\frac{2^{R_b-R_s}}{\bar{\gamma_e}}\right)\right), \end{aligned} \quad (22)$$

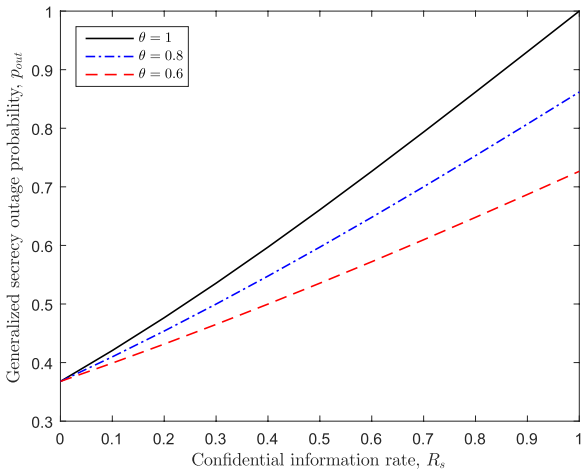



Fig. 2. Generalized secrecy outage probability versus confidential information rate. Results are shown for networks with different requirements on the fractional equivocation, $\theta = 1, 0.8, 0.6$. The other parameters are $R_b = 1$ and $\bar{\gamma_e} = 1$.

which captures how fast on average information is leaked to Eve. Note that the derivation of $R_L$ in (22) does not depend on the probability of transmission $p_{\text{tx}}$, which indicates that $R_L$ actually characterizes how fast on average the information is leaked to the eavesdropper when a message transmission occurs.

### C. Numerical Results

We first compare the generalized secrecy outage probabilities subject to different requirements on the fractional equivocation. Fig. 2 plots $p_{\text{out}}$ versus $R_s$ with different values of $\theta$. Note that the case of $\theta = 1$ represents classical secrecy outage probability. As shown in the figure, for different levels of secrecy requirements measured in terms of the fractional equivocation or the decodability of messages at Eve, the transmission has different secrecy outage performance. We find that the difference in the generalized secrecy outage probabilities increases as the confidential information rate increases.

We then present the secrecy performance measured by the average fractional equivocation, which gives an asymptotic lower bound on Eve's decoding error probability. Fig. 3 plots $\bar{\Delta}$ versus $R_s$. As shown in the figure, the average fractional equivocation decreases as the confidential information rate increases and/or the average received SNR at Eve increases. We note that the average fractional equivocation at Eve is not extremely high even when the confidential information rate is very small. We also note that the average fractional equivocation is non-zero even when the confidential information rate approaches the total transmission rate ($R_b = R_s$). These observations indicate that the quality of the wireless channel itself plays an important role in determining the secrecy performance of the wireless system.

Next, we illustrate the secrecy performance measured by the average information leakage rate. Fig. 4 plots $R_L$ versus $R_s$. As the figure shows, the average information leakage rate

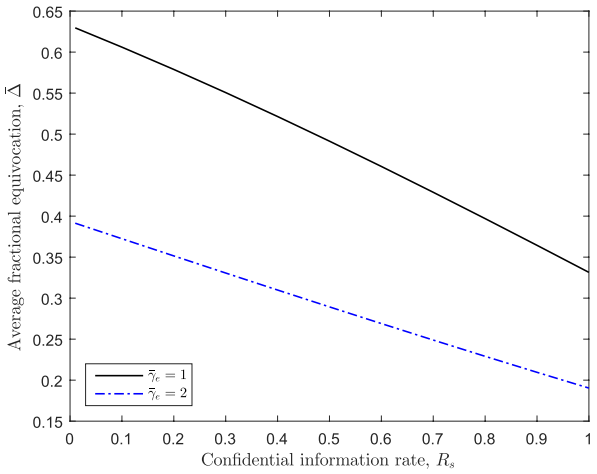



Fig. 3. Average fractional equivocation (asymptotic lower bound on the decoding error probability at Eve) versus confidential information rate. Results are shown for networks with different average received SNRs at Eve, $\bar{\gamma_e} = 1, 2$. The other parameter is $R_b = 1$.

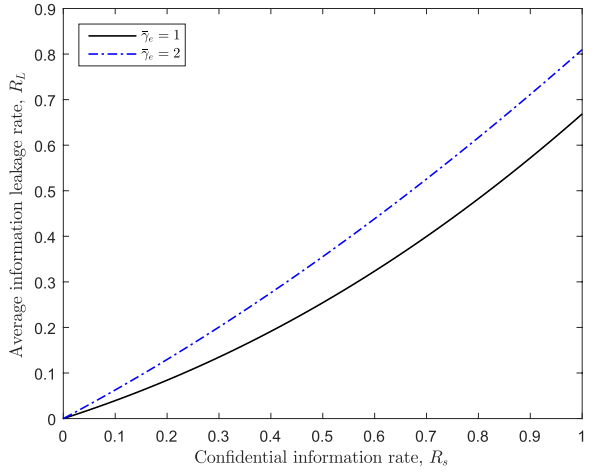



Fig. 4. Average information leakage rate versus confidential information rate. Results are shown for networks with different average received SNRs at Eve, $\bar{\gamma_e} = 1, 2$. The other parameter is $R_b = 1$.

increases as the confidential information rate increases and/or the average received SNR at Eve increases. We note that $R_L$ does not reach $R_s$ even when $R_s$ goes to $R_b = 1$. This implies that the information is not all leaked to the eavesdropper even when we use an ordinary code instead of the wiretap code for transmission. This observation once again confirms that the wireless channel itself can provide a certain level of secrecy for the transmission.

Finally, we show that the secrecy performance of wireless systems sometimes cannot be appropriately characterized by the classical secrecy outage probability, while on the other hand can be quantified by the newly purposed secrecy metrics. In Fig. 5, we evaluate the secrecy performance using classical secrecy outage probability and the newly proposed secrecy metrics for systems with different channel quality for Eve. We consider an extreme case where the confidential information rate is the same as the total codeword rate, $R_b = R_s$. This is equivalent to using an ordinary code instead of the wiretap code for transmission. As shown in Fig. 5(a), the secrecy performance measured by the classical secrecy outage probability ($\theta = 1$) is not related to Eve's channel condition, since it is always equal to 1. However, we know that the decodability of messages at the receiver is related to the channel condition. Intuitively, with an improvement in Eve's channel quality, the probability of error at Eve should decrease, and the secrecy performance should become worse. Therefore, we see that the secrecy performance cannot be properly characterized by the classical secrecy outage probability. In contrast, we find that the change of the secrecy performance with Eve's channel quality can be appropriately quantified by all three of the newly proposed secrecy metrics. In Fig. 5(a), the generalized secrecy outage probability ($\theta = 0.8$) increases as the average SNR at Eve increases. In Fig. 5(b), the average fractional equivocation decreases as the average SNR at Eve increases. In Fig. 5(c), the average information leakage rate increases as the average SNR at Eve increases. This simple example of transmission with an ordinary code shows that the newly proposed secrecy metrics are able to reveal information about the secrecy performance that cannot be captured by the classical secrecy outage probability.

## V. Impact on System Designs

In this section, we examine the significance of the newly proposed secrecy metrics from the perspective of a system designer, by answering the following questions:

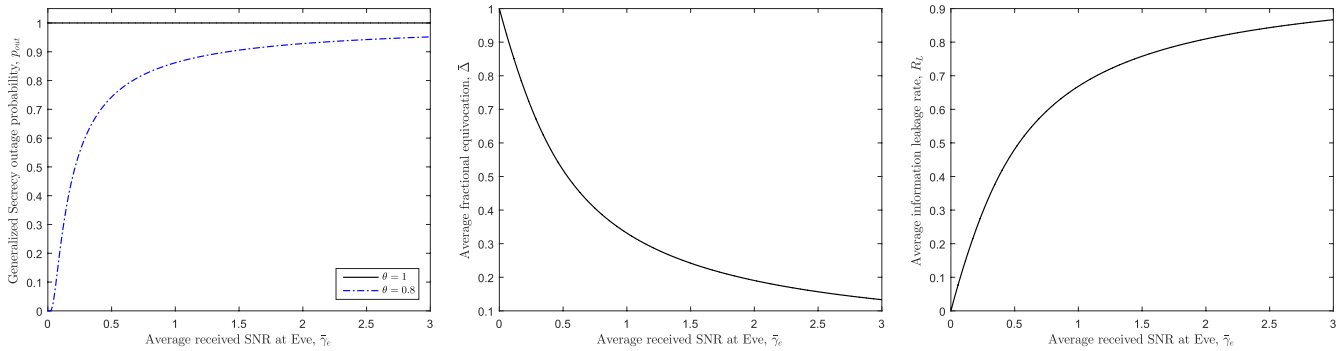
Q1) Do the newly proposed secrecy metrics lead to different system designs that optimize the secrecy performance, compared with the optimal design parameters minimizing the classical secrecy outage probability?

Q2) Does applying the optimal transmission design based on the classical secrecy outage probability result in a large secrecy loss, if the actual system requires a low decodability at the eavesdropper or a low information leakage rate?

As illustrated by the numerical results later in Section V-D, the answers to both Q1 and Q2 are yes, which shows that the newly proposed secrecy metrics have impact on the system design, and the impact is significant. The fact that the answer to Q1 is yes implies that system designers cannot adopt the optimal design based on the classical secrecy outage probability to optimize the secrecy performance measured by the newly proposed secrecy metrics. The fact that the answer to Q2 is yes indicates that adopting the optimal design based on the classical secrecy outage probability would lead to a large secrecy loss when the secrecy performance is measured by the newly proposed secrecy metrics.

### A. Problem Formulation

We still consider the system with fixed-rate wiretap codes described in the previous section. We optimize the secrecy performance of the wireless system subject to a throughput constraint $\eta > \Gamma$, where $\eta$ denotes the throughput of confidential message transmission and $\Gamma$ denotes its minimum required value. The controllable parameters to design are the wiretap




(a) (b) (c)

Fig. 5. Secrecy performance versus Eve's channel quality. Results are shown for the transmission with $R_b = R_s = 1$. (a) Generalized secrecy outage probability versus average received SNR at Eve. (b) Average fractional equivocation versus average received SNR at Eve. (c) Average information leakage rate versus average received SNR at Eve.

code rates $R_b$ and $R_s$. Taking into account the probability of transmission given in (16), the throughput of the confidential message transmission is given by

$$\eta = p_{\text{tx}} R_s = \exp\left(-\frac{2^{R_b}-1}{\bar{\gamma_b}}\right) R_s. \tag{23}$$

We specifically formulate three problems for the systems with different secrecy metrics as follows.

*Problem 1:* Minimize the generalized secrecy outage probability

$$\min_{R_b,R_s} \; p_{\text{out}} = \exp\left(-\frac{2^{R_b-\theta R_s}-1}{\bar{\gamma_e}}\right), \tag{24}$$

$$\text{s.t. } \eta \geq \Gamma, \quad R_b \geq R_s > 0. \tag{25}$$

*Problem 2:* Maximize the average fractional equivocation

$$\max_{R_b,R_s} \; \bar{\Delta} = 1 - \frac{1}{R_s \ln 2} \exp\left(\frac{1}{\bar{\gamma_e}}\right) \cdot \left(\text{Ei}\left(-\frac{2^{R_b}}{\bar{\gamma_e}}\right) - \text{Ei}\left(-\frac{2^{R_b-R_s}}{\bar{\gamma_e}}\right)\right), \tag{26}$$

$$\text{s.t. } \eta \geq \Gamma, \quad R_b \geq R_s > 0. \tag{27}$$

*Problem 3:* Minimize the average information leakage rate

$$\min_{R_b,R_s} \; R_L = \frac{1}{\ln 2} \exp\left(\frac{1}{\bar{\gamma_e}}\right) \cdot \left(\text{Ei}\left(-\frac{2^{R_b}}{\bar{\gamma_e}}\right) - \text{Ei}\left(-\frac{2^{R_b-R_s}}{\bar{\gamma_e}}\right)\right), \tag{28}$$

$$\text{s.t. } \eta \geq \Gamma, \quad R_b \geq R_s > 0. \tag{29}$$

### B. Feasibility of Constraint

The required throughput constraint is not feasible when $\Gamma$ is larger than the maximum achievable throughput for $R_b \geq R_s > 0$. We find that the three problems have the same feasible constraint region, which is given by the following proposition.

*Proposition 2:* The feasible range of the throughput constraint is given by

$$0 \leq \Gamma \leq \frac{W_0(\bar{\gamma_b})}{\ln 2} \exp\left(-\frac{2^{\frac{W_0(\bar{\gamma_b})}{\ln 2}}-1}{\bar{\gamma_b}}\right), \tag{30}$$

where $W_0(\cdot)$ denotes the principal branch of the Lambert W function.

*Proof:* See Appendix A. ■

### C. Optimal Rate Parameters

We denote $R_{s,\min}$ and $R_{s,\max}$ as the solutions of $x$ to $\exp\left(-\frac{2^x-1}{\bar{\gamma_b}}\right) x = \Gamma$ with $R_{s,\min} < R_{s,\max}$. The optimal solutions to Problems 1, 2 and 3 are summarized in Propositions 3, 4 and 5, respectively, as follows.

*Proposition 3:* The optimal rate parameters minimizing the generalized secrecy outage probability are given as follows:

$$R_{b1}^* = \log_2\left(1 - \bar{\gamma_b} \ln \frac{\Gamma}{R_{s1}^*}\right) \tag{31}$$

and

$$R_{s1}^* = \begin{cases} R_{s,\min}, & \text{if } R_{s,\min} > R_{so} \\ R_{so}, & \text{if } R_{s,\min} \leq R_{so} \leq R_{s,\max} \\ R_{s,\max}, & \text{if } R_{s,\max} < R_{so}, \end{cases} \tag{32}$$

where $R_{so}$ is the solution of $x$ to

$$\theta = \frac{\bar{\gamma_b}}{x \ln(2) \left(1 - \bar{\gamma_b} \ln\left(\frac{\Gamma}{x}\right)\right)}. \tag{33}$$

*Proof:* See Appendix B. ■

*Proposition 4:* The optimal rate parameters maximizing the average fractional equivocation are given as follows:

$$R_{b2}^* = \log_2\left(1 - \bar{\gamma_b} \ln \frac{\Gamma}{R_{s2}^*}\right) \tag{34}$$

and $R_{s2}^*$ is obtained by numerically solving the following problem:

$$\min_{x} \; \frac{1}{x}\left(\text{Ei}\left(-\frac{1-\bar{\gamma_b}\ln\frac{\Gamma}{x}}{\bar{\gamma_e}}\right) - \text{Ei}\left(-\frac{1-\bar{\gamma_b}\ln\frac{\Gamma}{x}}{\bar{\gamma_e} 2^x}\right)\right), \tag{35}$$

$$\text{s.t. } R_{s,\min} \leq x \leq R_{s,\max}. \tag{36}$$

*Proof:* See Appendix C. ■

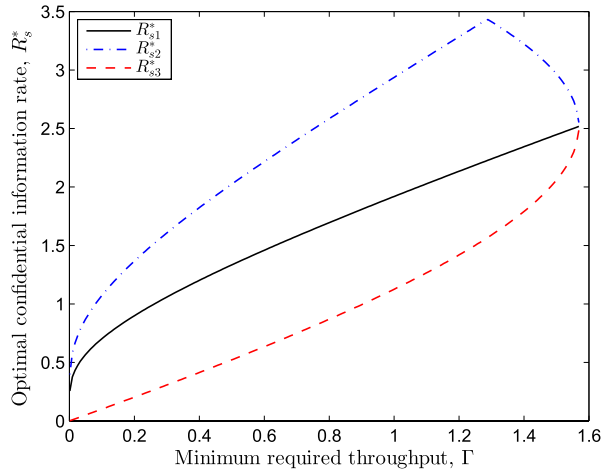



Fig. 6. For different secrecy metrics: optimal confidential information rate versus minimum required throughput. The other parameters are $\theta = 1$, $\bar{\gamma_b} = 10$ dB and $\bar{\gamma_e} = 10$ dB.

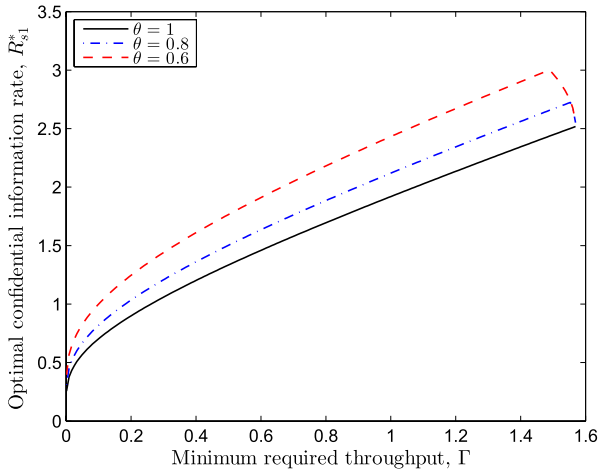



Fig. 7. For generalized secrecy outage probability: optimal confidential information rate versus minimum required throughput. Results are shown for networks with different requirements on the fractional equivocation, $\theta = 1, 0.8, 0.6$. The other parameters are $\bar{\gamma_b} = 10$ dB and $\bar{\gamma_e} = 10$ dB.

*Proposition 5:* The optimal rate parameters minimizing the average information leakage rate are given as follows:

$$R_{b3}^* = \log_2\left(1 - \bar{\gamma_b} \ln \frac{\Gamma}{R_{s3}^*}\right) \tag{37}$$

and $R_{s3}^*$ is obtained by numerically solving the following problem:

$$\min_x \ \mathrm{Ei}\left(-\frac{1-\bar{\gamma_b}\ln\frac{\Gamma}{x}}{\bar{\gamma_e}}\right) - \mathrm{Ei}\left(-\frac{1-\bar{\gamma_b}\ln\frac{\Gamma}{x}}{\bar{\gamma_e} 2^x}\right), \tag{38}$$

$$\text{s.t. } R_{s,\min} \le x \le R_{s,\max}. \tag{39}$$

*Proof:* The proof follows closely from the proof of Proposition 4 in Appendix C. ■

*Remark 2:* The numerical optimization problems for obtaining $R_{s2}^*$ and $R_{s3}^*$ in Propositions 4 and 5 can be easily solved by either a simple brute-force search or techniques like the golden section search [33].

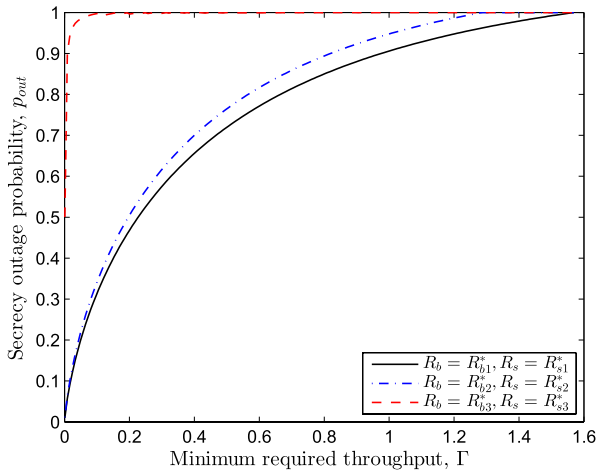



Fig. 8. Secrecy outage probability versus minimum required throughput. The other parameters are $\theta = 1$, $\bar{\gamma_b} = 10$ dB and $\bar{\gamma_e} = 10$ dB.

### *D. Numerical Results*

In this subsection, we present numerical results for a wireless system with $\bar{\gamma_b} = 10$ dB and $\bar{\gamma_e} = 10$ dB to demonstrate the impact of the new secrecy metrics on system designs. The feasible range of the throughput constraint is $0 \le \Gamma \le 1.569$, which is obtained by Proposition 2. Specifically, we can find the answer to Q1 by examining Figs. 6 and 7 and we can find the answer to Q2 by examining Figures 8–10.

We first compare the transmission rates that optimize the secrecy performance of the system measured by different secrecy metrics. Figure 6 plots the optimal confidential information rate $R_s^*$ versus the throughput constraint $\Gamma$. The values of $R_{s1}^*$, $R_{s2}^*$ and $R_{s3}^*$ are obtained by Propositions 3, 4 and 5, respectively. The optimal codeword transmission rate $R_b^*$ is not shown in the figure, since the optimal codeword transmission rate is equal to $R_b^* = \log_2\left(1 - \bar{\gamma_b} \ln \frac{\Gamma}{R_s^*}\right)$ for all three problems, and the differences between $R_{b1}^*$, $R_{b2}^*$ and $R_{b3}^*$ are determined by the differences between $R_{s1}^*$, $R_{s2}^*$ and $R_{s3}^*$. As depicted in the figure, the values of $R_{s1}^*$, $R_{s2}^*$ and $R_{s3}^*$ are clearly different from each other. We note that $R_{s1}^* = R_{s2}^* = R_{s3}^*$ if and only if the throughput constraint is very stringent, in which case the transmission rates are totally determined by the throughput constraint. The observations above illustrate that the optimal transmission designs are very different when we use different secrecy metrics to evaluate secrecy performance.

Next, we focus on the optimal transmission rates that minimize the generalized secrecy outage probabilities subject to different requirements on the fractional equivocation. Figure 7 plots $R_{s1}^*$ versus $\Gamma$ for different values of $\theta$. As shown in the figure, the optimal transmission rates minimizing the secrecy outage probability are different if the required values of $\theta$ are different. We find that the optimal confidential information rate $R_{s1}^*$ increases as the level of required fractional equivocation $\theta$ decreases. The observations

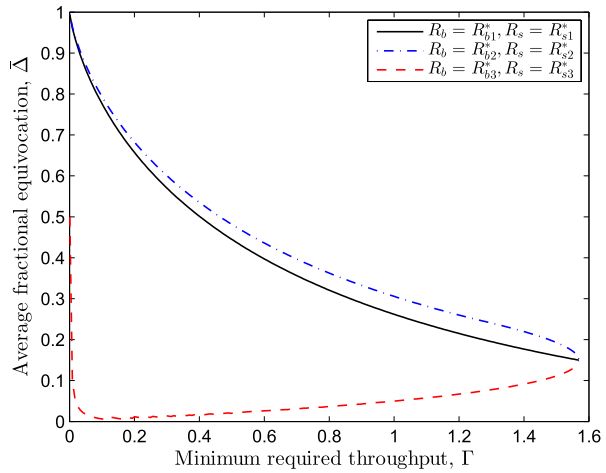



Fig. 9. Average fractional equivocation (asymptotic lower bound on the decoding error probability at Eve) versus minimum required throughput. The other parameters are $\theta = 1$, $\bar{\gamma_b} = 10$ dB and $\bar{\gamma_e} = 10$ dB.

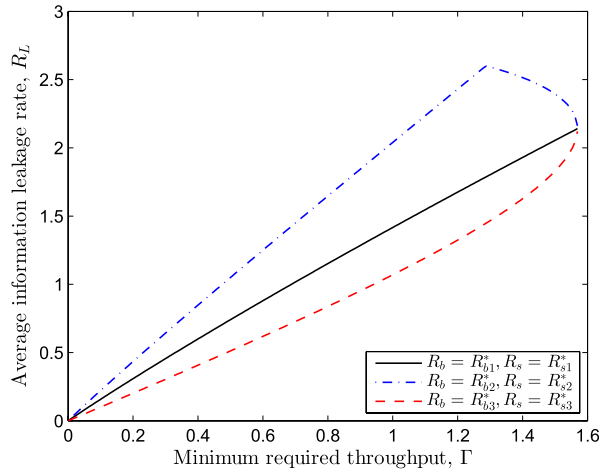



Fig. 10. Average information leakage rate versus minimum required throughput. The other parameters are $\theta = 1$, $\bar{\gamma_b} = 10$ dB and $\bar{\gamma_e} = 10$ dB.

from Figs. 6 and 7 confirm that the answer to Q1 is yes: the newly proposed secrecy metrics lead to very different system design choices that optimize the secrecy performance.

In the following, we answer the second question listed at the beginning of this section using Figs. 8–10. From the analytical results, we have obtained three different solutions of the optimal design parameters: $\left(R^*_{b1}, R^*_{s1}\right)$ is optimal for minimizing the generalized secrecy outage probability; $\left(R^*_{b2}, R^*_{s2}\right)$ is optimal for maximizing the average fractional equivocation; $\left(R^*_{b3}, R^*_{s3}\right)$ is optimal for minimizing the average information leakage rate. We collectively consider all three design solutions and study their performance for all three secrecy metrics. Specifically, Fig. 8 plots $p_{\text{out}}$, Fig. 9 plots $\bar{\Delta}$, and Fig. 10 plots $R_L$ achieved by the different design strategies. As shown in the figures, transmission with $R^*_{b1}$ and $R^*_{s1}$ minimizes the secrecy outage probability, but leads to a considerable loss if the practical secrecy requirement is to ensure a high fractional equivocation (decoding error probability at Eve) or a low information leakage rate. Similarly, transmission with $R^*_{b2}$ and $R^*_{s2}$ maximizes the average fractional equivocation, but incurs a considerable loss if the practical secrecy requirement is to have a low secrecy outage probability or a low information leakage rate. Finally, transmission with $R^*_{b3}$ and $R^*_{s3}$ minimizes the average information leakage rate, but incurs a large loss if the practical secrecy requirement is to maintain a low secrecy outage probability or a high fractional equivocation. The observations from Figs. 8–10 show that it is important to design the system with the appropriate secrecy metric. It is also confirmed that the answer to Q2 is yes: applying the transmission design based on the classical secrecy outage probability can result in a large secrecy loss if the actual system requires a low decodability at the eavesdropper or a low information leakage rate.

## VI. Conclusion and Future Work

To address the practical limitations of using classical secrecy outage probability as a metric for secrecy, we proposed three new metrics for physical layer security over quasi-static fading channels. Specifically, the generalized secrecy outage probability establishes a link between the concept of secrecy outage and the decodability of messages at the eavesdropper. The asymptotic lower bound on the eavesdropper's decoding error probability provides a direct error-probability-based secrecy metric. The average information leakage rate characterizes how fast the confidential information is leaked to the eavesdropper when classical information-theoretic secrecy is not achieved. We evaluated the performance of an example wireless system with fixed-rate wiretap codes using the proposed secrecy metrics. We showed that the new secrecy metrics provide a more comprehensive understanding of physical layer security over fading channels. We also found that the new secrecy metrics can give insights on the secrecy performance of wireless transmissions that sometimes cannot be captured by classical secrecy outage probability. Furthermore, we examined the significance of the newly proposed secrecy metrics from the perspective of a system designer. We found that applying the optimal transmission design minimizing the classical secrecy outage probability can result in a large secrecy loss, if the actual system requires a low decodability at the eavesdropper or a low information leakage rate. The new secrecy metrics enable appropriate transmission designs for systems with different secrecy requirements. We hope that this work can help bridge the gap between theory and practice in physical layer security by inspiring more future studies adopting and building on the newly proposed secrecy metrics. Besides, as mentioned previously in Section I-A, it is of importance to investigate secrecy metrics for wireless systems with finite-length coding schemes, since the classical information-theoretic secrecy cannot be achieved by finite-length codes. While the secrecy metrics proposed in this work did not focus on the finite-length coding schemes, it is also a very interesting future research direction to investigate appropriate secrecy metrics specifically for wireless systems with finite-length codes.

## Appendix A
## Proof of Proposition 2

To determine the maximum achievable secrecy throughput, we first obtain the optimal rate parameters that maximize the

secrecy throughput. The problem is formulated as

$$\max_{R_b,R_s} \ \eta = \exp\left(-\frac{2^{R_b}-1}{\bar{\gamma_b}}\right) R_s, \tag{40}$$

$$\text{s.t. } R_b \geq R_s > 0. \tag{41}$$

Given any $R_s$, we find that $\partial\eta/\partial R_b$ is always less than 0. Hence given any $R_s$, it is wise to have the minimum $R_b$, i.e., $R_b = R_s$, for maximizing $\eta$. Then, the problem changes to

$$\max_{R_s} \ \eta\left(R_b = R_s\right) = \exp\left(-\frac{2^{R_s}-1}{\bar{\gamma_b}}\right) R_s, \tag{42}$$

$$\text{s.t. } R_s > 0. \tag{43}$$

Taking the first order derivative of $\eta\left(R_b = R_s\right)$ with respect to $R_s$, we have

$$\frac{\partial \eta\left(R_b = R_s\right)}{\partial R_s} = \exp\left(-\frac{2^{R_s}-1}{\bar{\gamma_b}}\right)\left(1 - \frac{2^{R_s} R_s \ln 2}{\bar{\gamma_b}}\right). \tag{44}$$

By solving for $R_s$ in $\frac{\partial \eta(R_b=R_s)}{\partial R_s} = 0$, we obtain the optimal value of $R_s$ that maximizes $\eta$, which is given by

$$R_s^{\diamond} = \frac{W_0(\bar{\gamma_b})}{\ln 2}. \tag{45}$$

Finally, substituting $R_s = R_s^{\diamond}$ into (42) completes the proof.

## Appendix B
## Proof of Proposition 3

As analyzed in Appendix A, given any $R_s$, it is wise to have the minimum $R_b$, i.e., $R_b = R_s$, for maximizing $\eta$. Hence, we can obtain the feasible range of $R_s$ for satisfying the throughput constraint by solving $R_s$ in the equation $\eta\left(R_b = R_s\right) = \Gamma$. The feasible range is given by $R_{s,\min} \leq R_s \leq R_{s,\max}$.

From $p_{\text{out}} = \exp\left(-\frac{2^{R_b-\theta R_s}-1}{\bar{\gamma_e}}\right)$, we find that minimizing $p_{\text{out}}$ is equivalent to maximizing

$$O_1 = R_b - \theta R_s. \tag{46}$$

To minimize $O_1$ in (46), it is wise to have the maximum $R_b$ while satisfying the throughput constraint, for any given $R_s$. From $\eta = \exp\left(-\frac{2^{R_b}-1}{\bar{\gamma_b}}\right) R_s \geq \Gamma$, we have

$$R_b \leq \log_2\left(1 - \bar{\gamma_b} \ln \frac{\Gamma}{R_s}\right). \tag{47}$$

Hence, we obtain $R_{b1}^*$ as in (31). Then, we can rewrite the optimization problem as

$$\max_{R_s} \ \log_2\left(1 - \bar{\gamma_b} \ln \frac{\Gamma}{R_s}\right) - \theta R_s, \tag{48}$$

$$\text{s.t. } R_{s,\min} \leq R_s \leq R_{s,\max}. \tag{49}$$

Finally, by solving for $R_s$ in the equation $\frac{\partial O_1}{\partial R_s} = 0$ and considering the feasible range of $R_s$, we obtain $R_{s1}^*$ as in (32). This completes the proof.

## Appendix C
## Proof of Proposition 4

The feasible range of $R_s$ for satisfying the throughput constraint is given by $R_{s,\min} \leq R_s \leq R_{s,\max}$. From $\bar{\Delta} = 1 - \frac{1}{R_s \ln 2} \exp\left(\frac{1}{\bar{\gamma_e}}\right)\left(\text{Ei}\left(-\frac{2^{R_b}}{\bar{\gamma_e}}\right) - \text{Ei}\left(-\frac{2^{R_b-R_s}}{\bar{\gamma_e}}\right)\right)$, we find that maximizing $\bar{\Delta}$ is equivalent to minimizing

$$O_2 = \frac{1}{R_s}\left(\text{Ei}\left(-\frac{2^{R_b}}{\bar{\gamma_e}}\right) - \text{Ei}\left(-\frac{2^{R_b-R_s}}{\bar{\gamma_e}}\right)\right). \tag{50}$$

Given any $R_s$, we have

$$\frac{\partial O_2}{\partial R_b} = \frac{\ln(2)}{R_s}\left(\exp\left(-\frac{2^{R_b}}{\bar{\gamma_e}}\right) - \exp\left(-\frac{2^{R_b-R_s}}{\bar{\gamma_e}}\right)\right) < 0. \tag{51}$$

Hence given any $R_s$, it is wise to have the maximum $R_b$ while satisfying the throughput constraint to minimize $O_2$ in (50). Hence, we obtain $R_{b2}^*$ as in (34). Then, we rewrite the optimization problem as (35). We find that the closed-form solution of $R_{s2}^*$ is mathematically intractable. We can obtain $R_{s2}^*$ by numerically solving the problem. This completes the proof.

## References


[1] B. He and X. Zhou, "New physical layer security measures for wireless transmissions over fading channels," in *Proc. IEEE GLOBECOM*, Dec. 2014, pp. 722–727.

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

[3] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. Boca Raton, FL, USA: CRC Press, 2013.

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

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

[6] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

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

[8] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[9] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[10] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453–2469, Jun. 2008.

[11] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[12] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.

[13] B. He, X. Zhou, and T. D. Abhayapala, "Wireless physical layer security with imperfect channel state information: A survey," *ZTE Commun.*, vol. 11, no. 3, pp. 11–19, Sep. 2013.

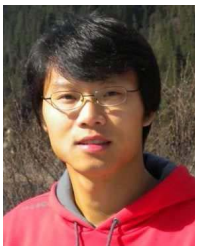
[14] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[15] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.

[16] B. He and X. Zhou, "Secure on-off transmission design with channel estimation errors," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 1923–1936, Dec. 2013.

[17] J. Chen, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure decode-and-forward two-way relay communications," in *Proc. IEEE GLOBECOM*, Dec. 2011, pp. 1–5.
[18] J. Wang, J. Lee, F. Wang, and T. Q. S. Quek, "Secure communication via jamming in massive MIMO Rician channels," in *Proc. IEEE GLOBECOM Workshops*, Dec. 2014, pp. 340–345.
[19] J.-C. Belfiore and F. Oggier, "An error probability approach to MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3396–3403, Aug. 2013.
[20] D. Karpuk, A.-M. Ernvall-Hytönen, C. Hollanti, and E. Viterbo, "Probability estimates for fading and wiretap channels from ideal class zeta functions," *Adv. Math. Commun.*, vol. 9, no. 4, pp. 391–413, Nov. 2015.
[21] J.-C. Belfiore and F. Oggier, "Secrecy gain: A wiretap lattice code design," in *Proc. ISITA*, Oct. 2010, pp. 174–178.
[22] M. Baldi, G. Ricciutelli, N. Maturo, and F. Chiaraluce, "Performance assessment and design of finite length LDPC codes for the Gaussian wiretap channel," in *Proc. IEEE ICC Workshops*, Jun. 2015, pp. 435–440.
[23] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channel," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 532–540, Sep. 2011.
[24] M. Baldi, M. Bianchi, and F. Chiaraluce, "Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: A security gap analysis," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 883–894, Jun. 2012.
[25] R. Soosahabi and M. Naraghi-Pour, "Scalable PHY-layer security for distributed detection in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1118–1126, Aug. 2012.
[26] A. S. Khan, A. Tassi, and I. Chatzigeorgiou, "Rethinking the intercept probability of random linear network coding," *IEEE Commun. Lett.*, vol. 19, no. 10, pp. 1762–1765, Oct. 2015.
[27] J. E. Barcelo-Llado, A. Morell, and G. Seco-Granados, "Amplify-and-forward compressed sensing as a physical-layer secrecy solution in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 5, pp. 839–850, May 2014.
[28] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. New York, NY, USA: Wiley, 2006.
[29] M. Feder and N. Merhav, "Relations between entropy and error probability," *IEEE Trans. Inf. Theory*, vol. 40, no. 1, pp. 259–266, Jan. 1994.
[30] C. W. Wong, T. F. Wong, and J. M. Shea, "LDPC code design for the BPSK-constrained Gaussian wiretap channel," in *Proc. IEEE GLOBECOM Workshops*, Dec. 2011, pp. 898–902.
[31] C. W. Wong, T. F. Wong, and J. M. Shea, "Secret-sharing LDPC codes for the BPSK-constrained Gaussian wiretap channel," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 551–564, Sep. 2011.
[32] M. Baldi, F. Chiaraluce, N. Laurenti, S. Tomasin, and F. Renna, "Secrecy transmission on parallel channels: Theoretical limits and performance of practical codes," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 11, pp. 1765–1779, Nov. 2014.
[33] J. Kiefer, "Sequential minimax search for a maximum," *Proc. Amer. Math. Soc.*, vol. 4, no. 3, pp. 502–506, 1953.

**Biao He** (M'16) received the B.E. (Hons.) degree from The Australian National University (ANU) and the Beijing Institute of Technology in 2012, and the Ph.D. degree from ANU in 2016. He is currently a Post-Doctoral Fellow with the Department of Electronic and Computer Engineering, The Hong Kong University of Science and Technology. His research interests include physical layer security and wireless communications.



**Xiangyun Zhou** (M'11) received the Ph.D. degree in telecommunications engineering from The Australian National University (ANU) in 2010. From 2010 to 2011, he was a Post-Doctoral Fellow with the University Graduate Center, University of Oslo, Norway. He returned to ANU in 2011, where he is currently a Senior Lecturer. His research interests are in the fields of communication theory and wireless networks. He currently serves on the Editorial Board of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and the IEEE COMMUNICATIONS LETTERS. He also served as a Guest Editor of the *IEEE Communications Magazine* of the Special Issue on wireless Physical Layer Security in 2015 and the *EURASIP Journal on Wireless Communications and Networking* of the Special Issue on Energy Harvesting Wireless Communications in 2014. He has also served as a Symposium/Track/Workshop Co-Chair for major IEEE conferences. He was the Chair of the ACT Chapter of the IEEE Communications Society and the Signal Processing Society from 2013 to 2014. He was a recipient of the best paper award at ICC'11.

**A. Lee Swindlehurst** (M'84–SM'99–F'04) received the B.S. (*summa cum laude*) and M.S. degrees from Brigham Young University, Provo, UT, USA, in 1985 and 1986, respectively, and the Ph.D. degree from Stanford University in 1991, all electrical engineering. From 1986 to 1990, he was with ESL, Inc., Sunnyvale, CA, USA, where he was involved in the design of algorithms and architectures for several radar and sonar signal processing systems. He was with the Department of Electrical and Computer Engineering, Brigham Young University, from 1990 to 2007, where he was a Full Professor and served as the Department Chair from 2003 to 2006. From 1996 to 1997, he held a joint appointment as a Visiting Scholar with Uppsala University, Uppsala, Sweden, and the Royal Institute of Technology, Stockholm, Sweden. From 2006 to 2007, he was on leave working as a Vice President of Research with ArrayComm LLC, San Jose, CA, USA. He is currently the Associate Dean for Research and Graduate Studies with the Henry Samueli School of Engineering, University of California at Irvine (UCI), a Professor with the Electrical Engineering and Computer Science Department, UCI, and a Hans Fischer Senior Fellow with the Institute for Advanced Studies, Technical University of Munich. His research interests include sensor array signal processing for radar and wireless communications, detection and estimation theory, and system identification. He has over 275 publications in these areas.

Dr. Swindlehurst was a Secretary of the IEEE Signal Processing Society, the Editor-in-Chief of the IEEE JOURNAL OF SELECTED TOPICS IN SIGNAL PROCESSING, and a member of the Editorial Boards of the *EURASIP Journal on Wireless Communications and Networking*, the *IEEE Signal Processing Magazine*, and the IEEE TRANSACTIONS ON SIGNAL PROCESSING. He was a recipient of several paper awards, such as the 2000 IEEE W. R. G. Baker Prize Paper Award, the 2006 and 2010 IEEE Signal Processing Society's Best Paper Awards, and the 2006 IEEE Communications Society Stephen O. Rice Prize in the Field of Communication Theory. He was a co-author of a paper that received the IEEE Signal Processing Society Young Author Best Paper Award in 2001.