Enhancing Secrecy in Fading Wiretap Channels with Only Transmitter-Side Channel State Information

Pang-Chang Lan[†], Y.-W. Peter Hong[⋆], and C.-C. Jay Kuo[†]

[†]Ming Hsieh Department of Electrical Engineering, University of Southern California, Los Angeles, CA 90089-2564, USA
[⋆]Institute of Communications Engineering, National Tsing Hua University, Hsinchu, Taiwan 30013
Emails: pangchal@usc.edu; ywhong@ee.nthu.edu.tw; cckuo@sipi.usc.edu

***Abstract*—This work examines the advantages of having only channel state information at the transmitter (CSIT), and not at the receiver and the eavesdropper, when achieving secrecy in fading wiretap channels. The key idea is that, with only CSIT, the transmitter can pre-compensate for the amplitude and phase distortions on the main channel. This allows the receiver to decode coherently even without knowledge of the CSI, while leaving the eavesdropper confused by the unknown variations of its own channel. When the channel is reciprocal, this CSI assumption can be achieved in practice through reverse training, i.e., by having the receiver emit the training signal so that the transmitter can estimate the channel by itself. Two secrecy-enhancing transmission schemes are proposed to exploit the CSIT. The truncated channel inversion scheme is used when the receiver and the eavesdropper have no CSI available, and the truncated phase compensation scheme is adopted when they can practically measure the SNR. The achievable secrecy rates of these schemes are derived for both single-antenna and multi-antenna wireless fading scenarios. Numerical results show significant improvements in secrecy rate compared to the case with full CSI at all terminals.**

I. Introduction

Information-theoretic secrecy has received renewed interest in recent years due to the increasing demand for data confidentiality and the challenges caused by the broadcast nature of the wireless medium. Most of the studies stem from the seminal works by Wyner [1] and by Csiszár and Körner [2]. In their works, the secrecy capacity was examined for the degraded and the more general discrete memoryless wiretap channels, respectively. In particular, secrecy capacity refers to the maximum achievable rate between the transmitter and the receiver subject to vanishing error probability at the receiver and vanishing information rate at the eavesdropper. Their works provided evidence that secure communication is possible in the physical layer solely through coding and signal processing approaches [3].

More recently, studies of the wiretap channel have been extended to single-antenna wireless fading scenarios in, e.g., [4], [5], and to multi-antenna scenarios, e.g., in [6], [7]. These works showed that positive secrecy rates can be achieved by exploiting temporal or spatial dimensions in which the main channel (i.e., the channel between the transmitter and the receiver) is more favorable than the eavesdropper channel. The achievable secrecy rate is known to increase as the channel quality discrepancy among the two channels increases and to depend strongly on the channel state information (CSI) available at the different terminals. The above works examined secrecy capacity for cases with full CSI at all terminals, i.e., at the transmitter, the receiver, and the eavesdropper.

In practice, the CSI at the receiver and the eavesdropper (CSIRE) is typically obtained by performing channel estimation at the respective terminals. And the CSI at the transmitter (CSIT) is obtained through feedback from the receiver and/or the eavesdropper. Based on this conventional procedure, the quality of the CSI at the receiver (and, thus, the transmitter) is improved by increasing the training signal power emitted by the transmitter. However, this benefits the channel estimation at the eavesdropper as well and may not improve the achievable secrecy rate [8]. Motivated by the concept of reverse training [8], we show in this work that the achievable secrecy rate can actually improve by acquiring CSI only at the transmitter but not at the receiver and the eavesdropper. This work is related to studies on wiretap channels with side information in [9] and [10], where noncausal side information was assumed available at the transmitter but not the receiver and the eavesdropper. In particular, [9] examined the Gaussian wiretap channel with concepts similar to dirty paper coding, where the known interference was treated as the side information. The work was extended to discrete memoryless channels in [10].

Our main objective is to propose techniques to exploit the advantages of having causal main-channel CSIT but no (or limited) CSIRE in wireless fading wiretap channels. The key idea is that, with the main-channel CSIT, the transmitter can pre-compensate for the amplitude and phase distortions occurring on the main channel so that the receiver can decode coherently, even when no CSI is available at the receiver. The eavesdropper, on the other hand, can only decode non-coherently, which greatly reduces its ability to overhear the message. When the channel is reciprocal, the assumptions of the main-channel CSIT and no CSIRE can be achieved by the so-called reverse training [8], where the training signal is instead emitted by the receiver and the channel is estimated directly by the transmitter. This work examines both the case with no CSIRE and the case with practical CSIRE. In the latter case, the receiver and the eavesdropper are assumed to be able to practically measure the received SNR. Two transmission schemes are proposed to exploit the CSIT, i.e., the truncated channel inversion scheme for the case with no

978-1-4799-7470-2/14/$31.00 ©2014 IEEE

CSIRE and the truncated phase compensation scheme for the case with practical CSIRE. The achievable secrecy rates are evaluated for systems with single-antenna and with multi-antenna transmitters. We show that the secrecy rate achievable with only transmitter-side CSI can be significantly higher than that with full CSI at all terminals.

II. SISOSE Wiretap Channel with Perfect Main-Channel CSIT but Limited CSIRE

In this section, we examine the achievable secrecy rate of the single-input single-output single-antenna eavesdropper (SISOSE) scenario with causal main-channel CSIT but no or limited CSIRE.

Let X be the channel input with power $E[|X|^2] \leq P$. In this case, the received signals at the receiver and the eavesdropper can be written as

$$Y = HX + W, \tag{1}$$

$$Z = GX + W', \tag{2}$$

where $H \sim \mathcal{CN}(0, \sigma_H^2)$ and $G \sim \mathcal{CN}(0, \sigma_G^2)$ are independent fading coefficients on the main and eavesdropper channels, and W, $W' \sim \mathcal{CN}(0,1)$ are the additive white Gaussian noise (AWGN). The fading coefficients are assumed to remain constant over a sufficient number of channel uses.

Here, we assume that only the receiver emits training signals to enable channel estimation at the transmitter. Therefore, the CSIT considered here includes only the knowledge of H (and not G). This is referred to as the main-channel CSIT. With no training signals emitted by the transmitter, two CSI conditions can be considered at the receiver and the eavesdropper, i.e., the case with no CSIRE and the case with practical CSIRE, where the receiver and the eavesdropper are able to practically measure the received SNR. These cases are examined in the following subsections.

A. SISOSE Wiretap Channel with No CSIRE

In the case with no CSIRE, the transmitter should pre-compensate for both the amplitude and phase distortions if coherent detection is to be allowed at the legitimate receiver. To do this, we first employ a Gaussian wiretap codebook to encode the confidential message and then employ the truncated channel inversion technique [11] to generate the channel input.

Suppose that $S \sim \mathcal{CN}(0, \sigma_S^2)$ is a symbol in the Gaussian codeword. Then, the channel input can be written as

$$X = \frac{1_{\{|H|>\gamma\}}}{H} S \tag{3}$$

where $1_{\{.\}}$ is the indicator function. Under the power constraint $E[|X|^2] \leq P$, the variance of S must be chosen as

$$\sigma_S^2(\gamma) = P / E[1_{\{|H|>\gamma\}}/|H|^2], \tag{4}$$

which depends on γ. By letting $S = \sigma_S(\gamma)\tilde{S}$, where $\tilde{S} \sim \mathcal{CN}(0,1)$, the received signals can be written as

$$Y = 1_{\{|H|>\gamma\}}\sigma_S(\gamma)\tilde{S} + W, \tag{5}$$

$$Z = G' 1_{\{|H|>\gamma\}}\sigma_S(\gamma)\tilde{S} + W', \tag{6}$$

where $G' \triangleq G/H$ is the effective fading coefficient at the eavesdropper. Given the choice of the channel input in (3), we now have an equivalent wiretap channel with Gaussian input $\tilde{S} \sim \mathcal{CN}(0,1)$ and outputs Y and Z. By the results in [2], the achievable secrecy rate can be written as

$$R_{s,\text{NoCSIRE}} = \max_{\gamma \geq 0} I(\tilde{S}; Y) - I(\tilde{S}; Z), \tag{7}$$

To derive the achievable secrecy rate, let $A \triangleq 1_{\{|H|>\gamma\}}$ and

$$p_A(1) \triangleq \Pr(A=1) = \exp(-\gamma^2/\sigma_H^2)$$

$$p_A(0) \triangleq \Pr(A=0) = 1 - p_A(1).$$

Then, for the received signal Y at the receiver, we have

$$f_{Y|A}(y|a) = \frac{1}{\pi(1 + a\sigma_S^2(\gamma))} e^{-\frac{|y|^2}{(1+a\sigma_S^2(\gamma))}} \tag{8}$$

and

$$f_{Y|\tilde{S},A}(y|\tilde{s}, a) = \frac{1}{\pi} e^{-|y - a\sigma_S(\gamma)\tilde{s}|^2}, \tag{9}$$

for $a \in \{0,1\}$. Thus, $f_Y(y) = p_A(0) f_{Y|A}(y|0) + p_A(1) f_{Y|A}(y|1)$ and $f_{Y|\tilde{S}}(y|\tilde{s}) = p_A(0) f_{Y|\tilde{S},A}(y|\tilde{s}, 0) + p_A(1) f_{Y|\tilde{S},A}(y|\tilde{s}, 1)$ are Gaussian mixture distributions. The mutual information $I(\tilde{S}; Y) = h(Y) - h(Y|\tilde{S})$ can then be evaluated numerically using the above distributions.

Moreover, for the signal received at the eavesdropper, we have

$$f_{Z|A}(z|1) = \int f_{Z|G',A}(z|g', 1) f_{G'|A}(g'|1) dg' \tag{10}$$

$$= \int_0^\infty \frac{2r\, f_{G'|A}(r|1)}{\sigma_S^2(\gamma) r^2 + 1} e^{-\frac{|z|^2}{\sigma_S^2(\gamma) r^2 + 1}} dr, \tag{11}$$

where $f_{G'|A}(g'|1) = \frac{1+\gamma^2(\frac{|g'|^2}{\sigma_G^2} + \frac{1}{\sigma_H^2})}{\pi\sigma_G^2\sigma_H^2(\frac{|g'|^2}{\sigma_G^2} + \frac{1}{\sigma_H^2})^2} e^{-\gamma^2|g'|^2/\sigma_G^2}$, and, similarly,

$$f_{Z|\tilde{S},A}(z|\tilde{s}, 1) = \int_\gamma^\infty \frac{2r e^{-\frac{|z|^2}{\sigma_G^2\sigma_S^2(\gamma)\left|\frac{\tilde{s}}{r}\right|^2 + 1} - \frac{r^2}{\sigma_H^2}}}{\pi\sigma_H^2[\sigma_G^2\sigma_S^2(\gamma)\left|\frac{\tilde{s}}{r}\right|^2 + 1] e^{-\frac{\gamma^2}{\sigma_H^2}}} dr. \tag{12}$$

It is also easy to verify that

$$f_{Z|A}(z|0) = f_{Z|\tilde{S},A}(z|\tilde{s}, 0) = \frac{1}{\pi} e^{-|z|^2}. \tag{13}$$

Then, from the above density functions, we can obtain $f_Z(z) = p_A(0) f_{Z|A}(z|0) + p_A(1) f_{Z|A}(z|1)$, $f_{Z|\tilde{S}}(z|\tilde{s}) = p_A(0) f_{Z|\tilde{S},A}(z|\tilde{s}, 0) + p_A(1) f_{Z|\tilde{S},A}(z|\tilde{s}, 1)$, and the mutual information $I(\tilde{S}; Z) = h(Z) - h(Z|\tilde{S})$.

With $I(\tilde{S}; Y)$ and $I(\tilde{S}; Z)$, the achievable secrecy rate can then be evaluated as in (7). The optimal value of γ can be found by line search or by approximation methods to be shown in Section II-C. By choosing γ to be large, the receiver is more likely to experience a better effective channel than the eavesdropper, on the average, but the number of channel uses that are actually used to convey the information is reduced, which limits the achievable secrecy rate. Hence, an appropriate choice of γ is essential to achieve a high secrecy rate.

B. SISOSE Wiretap Channel with Practical CSIRE

In the case with practical CSIRE, we assume that the receivers are able to practically measure their receive SNRs under each channel condition. Specifically, we assume that the receiver and the eavesdropper can obtain the conditional SNRs

$$V \triangleq |H|^2 E[|X|^2|H] \text{ and } L \triangleq |G|^2 E[|X|^2|H]$$

respectively, by measuring their received signal powers. Similar assumptions were made in [12]. In this case, the receiver will be able to infer knowledge of the channel amplitude (if the signal power is known) and, thus, one need only to pre-compensate for the phase at the transmitter.

Let us express the fading coefficients as $H = |H|e^{j\Theta}$ and $G = |G|e^{j\Phi}$, where Θ and Φ are i.i.d. uniform over $[0, 2\pi)$. Then, the proposed channel input can be written as

$$X = 1_{\{|H|>\gamma\}} e^{-j\Theta} S, \tag{14}$$

where $S \sim \mathcal{CN}(0, \sigma_S^2)$. Similarly, under the power constraint $E[|X|^2] \leq P$, the signal variance can be chosen as

$$\sigma_s^2(\gamma) = P/E[1_{\{|H|>\gamma\}}] = Pe^{\gamma^2/\sigma_H^2}. \tag{15}$$

By letting $S = \sigma_S(\gamma)\tilde{S}$, where $\tilde{S} \sim \mathcal{CN}(0, 1)$, the received signals are then given by

$$Y = |H| 1_{\{|H|>\gamma\}} \sigma_S(\gamma)\tilde{S} + W \tag{16}$$

$$Z = |G| e^{j\Theta'} 1_{\{|H|>\gamma\}} \sigma_S(\gamma)\tilde{S} + W' \tag{17}$$

where $\Theta' \triangleq \Phi - \Theta$ is also uniformly distributed over $[0, 2\pi)$. Note that the wiretap channel turns out to be a non-coherent phase-noise channel [13] of which the explicit point-to-point capacity expression for is still unclear [14]. Nevertheless, we are interested in the ergodic achievable secrecy rate

$$\begin{aligned} R_{s,\text{PCSIRE}} = \max_{\gamma \geq 0} E_{G,H}[I(\tilde{S}; Y|V = |H|^2 1_{\{|H|>\gamma\}} \sigma_S^2(\gamma)) \\ - I(\tilde{S}; Z|L = |G|^2 1_{\{|H|>\gamma\}} \sigma_S^2(\gamma))]. \end{aligned} \tag{18}$$

by treating $\tilde{S}$ as the effective channel input.

Notice that, given $H = h$, the main-channel mutual information can be written as

$$I\left(\tilde{S}; Y|V = |h|^2 1_{\{|h|>\gamma\}} \sigma_S^2(\gamma)\right) = 1_{\{|h|>\gamma\}} \log(1 + |h|^2 \sigma_S^2(\gamma)).$$

Therefore, the first term in (18) can be obtained by replacing h by H.

Similarly, given $H = h$ and $G = g$, the eavesdropper's mutual information is

$$\begin{aligned} I(\tilde{S}; Z|L = |g|^2 1_{\{|h|>\gamma\}} \sigma_S^2(\gamma)) = h(Z|L = |g|^2 1_{\{|h|>\gamma\}} \sigma_S^2(\gamma)) \\ - h(Z|\tilde{S}, L = |g|^2 1_{\{|h|>\gamma\}} \sigma_S^2(\gamma)). \end{aligned} \tag{19}$$

More specifically, for $|h| < \gamma$, we have $I(\tilde{S}; Z|L = 0) = 0$ whereas, for $|h| > \gamma$, we have

$$I(\tilde{S}; Z|L = |g|^2 \sigma_S^2(\gamma)) \tag{20}$$

$$= h(Z|L = |g|^2 \sigma_S^2(\gamma)) - h(Z|\tilde{S}, L = |g|^2 \sigma_S^2(\gamma)), \tag{21}$$

whose expression does not depend on h.

For the first term, it is easy to show that $h\left(Z|L = |g|^2 \sigma_S^2(\gamma)\right) = \log \pi e \left(1 + |g|^2 \sigma_S^2(\gamma)\right)$. To obtain an expression for the second term, suppose that $\tilde{S} = \tilde{s}$ and $L = |g|^2 \sigma_S^2(\gamma)$ are given. Let $Z = Re^{j\Psi}$, where $R = |Z|$ and $\Psi = \angle Z$. It can be shown that the random variable $R = |e^{j\Theta'}|g|\sigma_S(\gamma)\tilde{s} + W'|$ is Rician distributed with parameters $(|g\sigma_S(\gamma)\tilde{s}|, \frac{1}{\sqrt{2}})$ (since $\sigma_{W'} = 1$), and Ψ is uniformly distributed over $[0, 2\pi)$ and is independent of R. In this case, we have

$$\begin{aligned} &h(Z|\tilde{S} = \tilde{s}, L = |g|^2 \sigma_S^2(\gamma)) \\ &= \int_0^\infty 2re^{-(r^2 + |k|^2)} I_0(2|k|r) \log(\pi e^{r^2 + |k|^2} I_0^{-1}(2|k|r)) dr \end{aligned}$$

where k is a constant defined as $k \triangleq |g|\sigma_S(\gamma)\tilde{s}$ and $I_0(\cdot)$ is the modified Bessel function of the first kind with order 0. By taking expectation on G and $\tilde{S}$, we can obtain $h(Z|\tilde{S}, L = |G|^2 \sigma_S^2(\gamma))$. Hence, the second term in (18) can be computed as

$$\begin{aligned} &I(\tilde{S}; Z|L = |G|^2 1_{\{|H|>\gamma\}} \sigma_S^2(\gamma)) \\ &= 1_{\{|H|>\gamma\}} [\log(\pi e(1 + |G|^2 \sigma_S^2(\gamma))) - h(Z|\tilde{S}, L = |G|^2 \sigma_S^2(\gamma))]. \end{aligned}$$

C. Asymptotic Secrecy Rate Lower Bounds at High SNR and Search for Asymptotically Optimal γ

Notice that the mutual information expressions in the previous subsections, especially the parts associated with the eavesdropper, requires numerical evaluation of several integrals. This can be cumbersome and may result in high computational complexity when determining the optimal γ. To overcome this issue, we find asymptotic lower bounds for the achievable secrecy rates derived previously that are simpler for evaluation.

Let us first consider the case with no CSIRE. It is interesting to note that, even though CSI is not available a priori at the receiver in this case, the receiver and eavesdropper are still able to perform simple binary hypothesis testing to determine the presence or absence of the transmitted signal, i.e., determine if $A = 1$ or $A = 0$. The detection will be more and more accurate as the SNR increases. That is, at high SNR, we have $I(\tilde{S}; A|Y) \approx 0$ and, thus, $I(\tilde{S}; Y) \approx I(\tilde{S}; Y, A) = I(\tilde{S}; Y|A)$. Similar approximations hold for Z as well. Hence, we can approximate the mutual information as

$$I(\tilde{S}; Y) \approx I(\tilde{S}; Y|A) = e^{-\gamma^2/\sigma_H^2} \log(1 + \sigma_S^2(\gamma))$$

$$I(\tilde{S}; Z) \approx I(\tilde{S}; Z|A) = e^{-\gamma^2/\sigma_H^2} I(\tilde{S}; Z|A = 1).$$

Let $T = |Z|^2$. By the fact that the distribution of Z is determined completely by T and by following the derivations in [13], [15], it can be shown that the term $I(\tilde{S}; Z|A = 1)$ is bounded asymptotically as

$$\begin{aligned} &I(\tilde{S}; Z|A = 1) \leq I(\tilde{S}; Z|A = 1, H = h) \\ &\leq \alpha - \alpha \log \alpha + \log \Gamma(\alpha) + \alpha \log E[T|A = 1, H = h] \\ &\quad + (1 - \alpha) \mathrm{E}[\log T|A = 1, H = h] - h(T|\tilde{S}, A = 1, H = h) \end{aligned}$$

where $\Gamma(\cdot)$ is the Gamma function, and $\alpha > 0$ is an arbitrary constant that can be chosen to minimize the upper bound. At high SNR, we can approximate T as $|\frac{G}{H}1_{\{|H|>\gamma\}}\sigma_S(\gamma)\tilde{S}|^2$ and obtain $E[T|A=1, H=h] = \sigma_G^2\sigma_S^2(\gamma)/|h|^2$, $E[\log T|A=1, H=h] = -C+\log(\sigma_G^2/|h|^2)+E_{\tilde{S}}[\log|S|^2]$, and $h(T|\tilde{S}, A=1, H=h) = 1+\log(\sigma_G^2/|h|^2)+E_{\tilde{S}}[\log|S|^2]$ where C is the Euler constant. By combining the above, we get

$$I(\tilde{S}; Z|A=1) \lesssim \alpha - \alpha\log\alpha + \log\Gamma(\alpha) - (1-2\alpha)C - 1.$$

Note that, by taking derivative of the above bound, the value of α that minimizes the upper bound is approximately 0.54. Hence, by taking $\alpha = \frac{1}{2}$ for simplicity, we obtain an asymptotic lower bound for the achievable secrecy rate in the case with no CSIRE, i.e.,

$$R^{\text{lb}}_{s,\text{NoCSIRE}} = \max_{\gamma>0} e^{-\frac{\gamma^2}{\sigma_H^2}}\left[\log(1+\sigma_S^2(\gamma)) - \frac{1}{2}\log\frac{2\pi}{e}\right]. \quad (22)$$

The simulation results in Section IV show that this bound is asymptotically tight as P increases. Note that the objective in (22) is a quasi-concave function. Thus, the optimal γ can be efficiently determine by employing a bisection search.

For the case with practical CSIRE, we can also show, by following the techniques in [13], [16] and by assuming that P is sufficiently large, that

$$I(S; Z|L = |g|^2\sigma_S^2(\gamma)) \leq \frac{1}{2}\log\left(1+|g|^2\sigma_S^2(\gamma)\right) - \frac{1}{2}\log 2.$$

Hence, the achievable secrecy rate in this case can be asymptotically lower bounded by

$$\begin{aligned} R^{lb}_{s,\text{PCSIRE}} = \max_{\gamma>0} E_H\Bigg[1_{\{|H|>\gamma\}}\Bigg(&\log(1+|H|^2\sigma_S^2(\gamma)) \\ -e^{-\frac{\gamma^2}{\sigma_H^2}}E_G\left[\frac{1}{2}\log\left(1+|G|^2\sigma_S^2(\gamma)\right)\right] &+ \frac{1}{2}\log 2\Bigg)\Bigg]. \quad (23) \end{aligned}$$

The simulation results in Section IV also show that this bound is tight at high SNR. The optimal γ can be found by performing a similar bisection search as mentioned in the case with no CSIRE.

III. MISOSE Wiretap Channel with Perfect Main-Channel CSIT but Limited CSIRE

In this section, we examine the achievable secrecy rate of the multiple-input single-output single-antenna eavesdropper (MISOSE) scenario with the causal main-channel CSIT but no (or limited) CSIRE.

Suppose that the transmitter has M antennas. Let $\mathbf{x} \in \mathbb{C}^{M\times 1}$ be the channel input vector satisfying the average power constraint $\mathrm{E}[\|\mathbf{x}\|^2] \leq P$. The received signals at the receiver and the eavesdropper can be written as

$$Y = \mathbf{h}\mathbf{x} + W \quad (24)$$

$$Z = \mathbf{g}\mathbf{x} + W' \quad (25)$$

where $\mathbf{h} \sim \mathcal{CN}(\mathbf{0}, \sigma_{\mathbf{h}}^2\mathbf{I}_M)$ and $\mathbf{g} \sim \mathcal{CN}(\mathbf{0}, \sigma_{\mathbf{g}}^2\mathbf{I}_M)$ are the independent fading coefficient vectors with dimension $1 \times M$, and W, $W' \sim \mathcal{CN}(0,1)$ are AWGN. Here, we also assume that the transmitter has knowledge of the main-channel vector $\mathbf{h}$ but not $\mathbf{g}$. We also consider both the case with no CSIRE and the case with practical CSIRE as to be discussed in the following subsections.

A. MISOSE Wiretap Channel with No CSIRE

Let $S \in \mathcal{CN}(0, \sigma_S^2(\gamma))$ be a symbol in the Gaussian codebook. By employing the truncated channel inversion scheme, similar to that in Section II-A, the channel input vector can be written as

$$\mathbf{x} = \frac{\mathbf{h}^H}{\|\mathbf{h}\|^2}1_{\{\|\mathbf{h}\|>\gamma\}}S. \quad (26)$$

To satisfy the power constraint $\mathrm{E}[|X|^2] \leq P$, the signal variance can be chosen as $\sigma_S^2(\gamma) = P/\mathrm{E}[\frac{1}{\|\mathbf{h}\|^2}1_{\{\|\mathbf{h}\|>\gamma\}}]$. By letting $S = \sigma_S(\gamma)\tilde{S}$, the corresponding received signals are then given by

$$\begin{aligned} Y &= 1_{\{\|\mathbf{h}\|>\gamma\}}\sigma_S(\gamma)\tilde{S} + W \\ Z &= G'1_{\{\|\mathbf{h}\|>\gamma\}}\sigma_S(\gamma)\tilde{S} + W'. \end{aligned}$$

where $G' \triangleq \frac{\mathbf{g}\mathbf{h}^H}{\|\mathbf{h}\|^2}1_{\{\|\mathbf{h}\|>\gamma\}}$ is the effective fading coefficient of the eavesdropper. In this case, the achievable secrecy rate can still be given as in (7).

To derive the achievable secrecy rate, define the random variables $A \triangleq 1_{\{\|\mathbf{h}\|>\gamma\}}$, and $\tilde{H} = \|\mathbf{h}\|$. Let $p_A(1) \triangleq \Pr(A=1)$ and $p_A(0) \triangleq \Pr(A=0)$. Note that $\tilde{H}$ is a scaled chi random variable with density $f_{\tilde{H}}(\tilde{h}) = \frac{2\tilde{h}^{2M-1}e^{-\frac{\tilde{h}^2}{\sigma_H^2}}}{\sigma_H^{2M}\Gamma(M)}$. The computation of $I(\tilde{S}; Y)$ is almost the same as that in Section III-A except for the different expressions for $p_A(1)$ and $p_A(0)$.

To compute $I(\tilde{S}; Z)$, we first obtain the densities

$$f_{Z|A}(z|1) = \int_{|g'|\geq 0} f_{G'|A}(g'|1)\frac{e^{-\frac{|z|^2}{|g'|^2\sigma_S^2(\gamma)+1}}}{\pi(|g'|^2\sigma_S^2(\gamma)+1)}\mathrm{d}g' \quad (27)$$

where $f_{G'|A}(g'|1) = \frac{M\left[1-\Gamma(M+1,\gamma^2(\frac{1}{\sigma_{\mathbf{h}}^2}+\frac{|g'|^2}{\sigma_{\mathbf{g}}^2}))\right]}{p_A(1)\pi\sigma_{\mathbf{g}}^2\sigma_{\mathbf{h}}^{2M}(\frac{1}{\sigma_{\mathbf{h}}^2}+\frac{|g'|^2}{\sigma_{\mathbf{g}}^2})^{M+1}}$ with $\Gamma(\cdot,\cdot)$ being the regulated Gamma function, and, similarly,

$$f_{Z|\tilde{S},A}(z|\tilde{s},1) = \int_{\gamma}^{\infty}\frac{e^{-\frac{|z|^2}{1+\sigma_{\mathbf{g}}^2\sigma_S^2(\gamma)\frac{|\tilde{s}|^2}{\tilde{h}^2}}}}{\pi(1+\sigma_{\mathbf{g}}^2\sigma_S^2(\gamma)\frac{|\tilde{s}|^2}{\tilde{h}^2})}\frac{2\tilde{h}^{2M-1}e^{-\frac{\tilde{h}^2}{\sigma_{\mathbf{h}}^2}}}{\sigma_{\mathbf{h}}^{2M}\Gamma(M)p_A(1)}\mathrm{d}\tilde{h}.$$

Also, $f_{Z|A}(z|0) = p_{Z|\tilde{S},A}(z|\tilde{s},0) = \frac{1}{\pi}e^{-|z|^2}$. Finally, by substituting the above density functions into $f_Z(z) = f_{z|A}(z|1)p_A(1) + f_{Z|A}(z|0)p_A(0)$ and $f_{Z|\tilde{S}}(z|\tilde{s}) = f_{Z|\tilde{S},A}(z|\tilde{s},1)p_A(1) + f_{Z|\tilde{S},A}(z|\tilde{s},0)p_A(0)$, the mutual information $I(\tilde{S}; Z) = h(Z) - h(Z|\tilde{S})$ can then be computed.

B. MISOSE Wiretap Channel with Practical CSIRE

Here, we assume that the receiver and the eavesdropper can obtain practical CSIRE by measuring the conditional receive SNR. In this case, we consider a transmission scheme where only the phase rotation on the main channel is precompensated at the transmitter. The channel input can be written as

$$\mathbf{x} = \frac{\mathbf{h}^H}{\|\mathbf{h}\|}1\{\|\mathbf{h}\| > \gamma\}S. \quad (28)$$

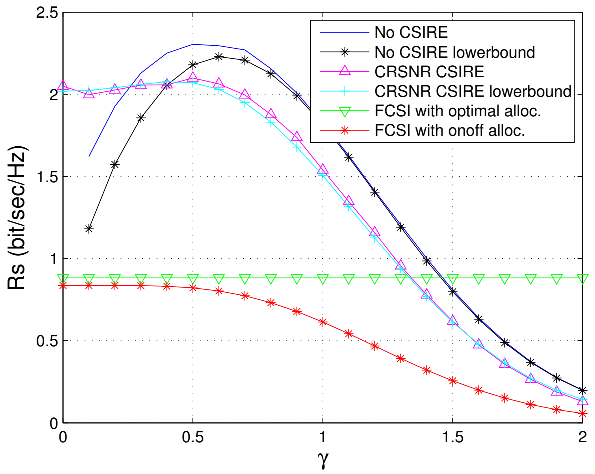

Fig. 1. R_s vs. γ with $P = 10$ dB and $\sigma_G^2 = \sigma_H^2 = 1$

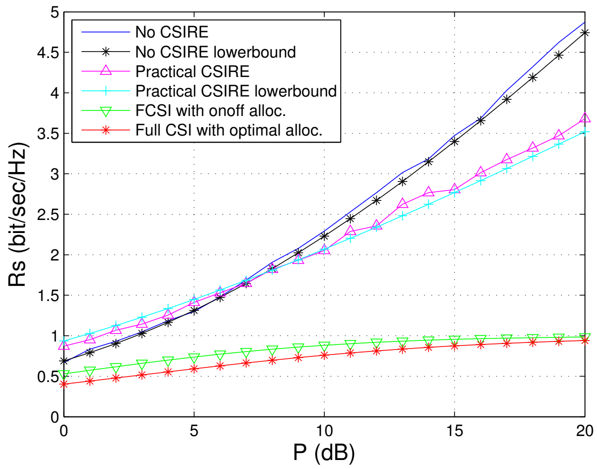

Fig. 2. R_s vs. P with suboptimal γ^* and $\sigma_G^2 = \sigma_H^2 = 1$

Let $S = \sigma_S(\gamma)\tilde{S}$ with $\sigma_S^2(\gamma) = P/\,\mathrm{E}[1_{\{\|\mathbf{h}\|>\gamma\}}]$ so that the average power constraint $E[|\mathbf{x}|^2] \leq P$ is satisfied. The corresponding received signals at the receiver and the eavesdropper are then given by

$$Y = \|\mathbf{h}\| 1\{\|\mathbf{h}\| > \gamma\} S + W \tag{29}$$

$$Z = \frac{\mathbf{g}\mathbf{h}^H}{\|\mathbf{h}\|} 1\{\|\mathbf{h}\| > \gamma\} S + W'. \tag{30}$$

It can be shown that $\tilde{G} \triangleq \mathbf{g}\mathbf{h}^H/\|\mathbf{h}\|$ is $\mathcal{CN}(0, M\sigma_{\mathbf{g}}^2)$ since $E[|\tilde{G}|^2] = M\sigma_{\mathbf{g}}^2$ and $f_{\tilde{G}|\mathbf{h}}(\tilde{g}|\mathbf{h}) = \frac{1}{\pi M \sigma_{\mathbf{g}}^2}\exp(|\tilde{g}|^2/M\sigma_{\mathbf{g}}^2)$. In this case, the wiretap channel is, in fact, a Gaussian channel but with M-fold variance. Therefore, the MISOSE wiretap channel with practical CSIRE is equivalent to that in Section II-B and the achievable secrecy rate is given by (18).

The asymptotic lower bounds can also be derived for these cases following similar approaches as in Section II-C. The results are omitted due to the space limitations.

IV. Numerical Results

In this section, we provide the numerical results to demonstrate the benefits of having only CSIT but no or limited CSIRE. Monte Carlo methods are used to compute the integrals when needed.

First, we examine the achievable secrecy rate in the SISOSE scenario. In Fig. 1, the achievable secrecy rate is shown with respect to the channel truncation threshold γ. Here, we set $P = 10$ dB and $\sigma_G^2 = \sigma_H^2 = 1$. The lines labeled by no CSIRE LB and practical CSIRE LB are the curves corresponding to their asymptotic lower bounds. We also consider two conventional full-CSI schemes for comparison. For the case labeled full CSI (FCSI) with the optimal power allocation, full CSI is available at all terminals. In this case, the transmitter allocates power optimally over time instants for which the main channel is more favorable than the eavesdropper channel. The optimal power allocation strategy was previously derived in [4] and does not depend on γ. For the case labeled full CSI with on-off power allocation, the transmitter is assumed to have only main-channel CSI and employs a scheme similar to ours where transmission with constant power is employed only when $|H| \geq \gamma$. We can see from the figure that, by choosing an appropriate γ, the schemes with only main-channel CSIT (but no or limited CSIRE) can outperform those with full CSI at all terminals. We can also observe that the achievable secrecy rate of the scheme with no CSIRE drops much faster than the case with practical CSIRE as γ decreases. This is due to the fact that, when γ is small, there is higher probability for the channel gain to be small, resulting in significant power amplification in the channel inversion scheme. The asymptotic lower bounds are also shown to be tight, which validates the strategies introduced to find the suboptimal γ^* in Section II-C.

In Fig. 2, we plot the achievable secrecy rate versus the average power constraint. Each point in the curve corresponds to an optimally chosen γ. We can see that the cases with only CSIT and no or limited CSIRE performs significantly better than the case with full CSI at all terminals. This gain increases rapidly as the average power increases. It is also interesting to observe that the secrecy rate for the case with no CSIRE increases much faster with P than the case with practical CSIRE. This is because the channel uncertainty at the eavesdropper lies only in the phase in the practical CSIRE scenario but lies in both the amplitude and the phase in the case with no CSIRE. Hence, the increase of power will cause no additional uncertainty to the eavesdropper in the former case, but may do so in the latter case.

Similar trends can also be observed in the MISOSE case. In Fig. 3, we plot the achievable secrecy rate with respect to the channel truncation threshold γ for the case with $M = 4$ antennas at the transmitter. Here, we set $P = 10$ dB and $\sigma_{\mathbf{g}}^2 = \sigma_{\mathbf{h}}^2 = 1$. We can see that having only CSIT and no or limited CSIRE can have an even greater advantage when the transmitter is equipped with multiple antennas. An optimal γ still exists in each case, but the secrecy rate in the case

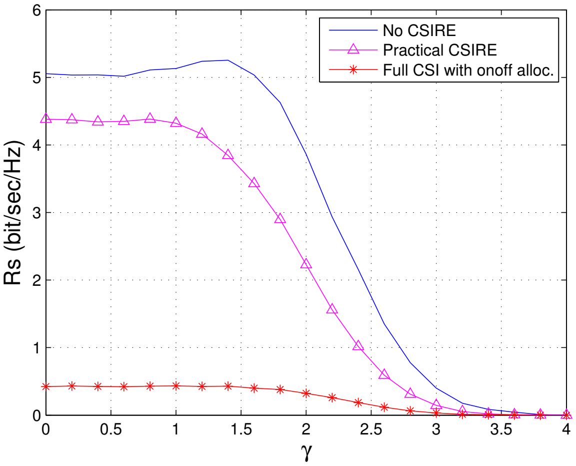

Fig. 3. R_s vs. γ with $P = 10$ dB and $\sigma_{\mathbf{g}}^2 = \sigma_{\mathbf{h}}^2 = 1$

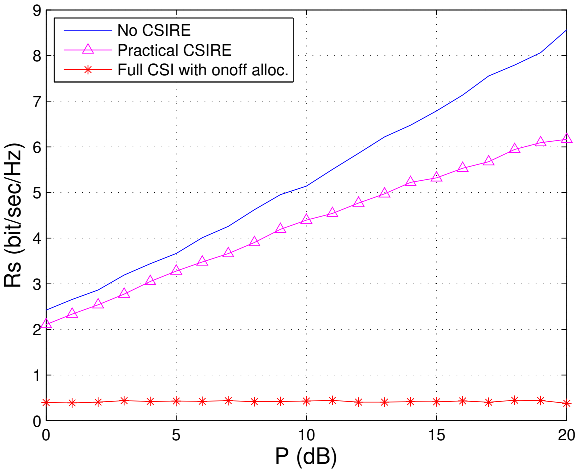

Fig. 4. R_s vs. P with suboptimal γ^* and $\sigma_{\mathbf{g}}^2 = \sigma_{\mathbf{h}}^2 = 1$

with no CSIRE no longer drops dramatically for small γ. This is owing to the fact that multi-antenna diversity reduces the probability of obtaining a small effective channel gain $\|\mathbf{h}\|$, which mitigates the impact of power amplification under channel inversion. In Fig. 4, we plot the achievable secrecy rate with respect to the average power constraint. Note that the optimal γ can also be derived using techniques similar to that in Section II-C. Similar to the SISOSE case, we can see that the achievable secrecy rate in the case with no CSIRE increases much more rapidly with power than that in the case with practical CSIRE.

V. Conclusion

In this paper, we examined the secrecy-rate enhancements that can be achieved by having only CSIT and no (or limited) CSIRE. In wireless fading scenarios, truncated channel inversion and truncated phase compensation methods were proposed as special cases of the translation function. By allowing the transmitter to pre-compensate for the amplitude and phase distortions on the main channel, the receiver is allowed to decode coherently even with no CSI available a priori but the eavesdropper is left confused by its own channel. The secrecy rate was derived for both cases with single-antenna and multi-antenna transmitters. Asymptotic bounds on the secrecy rates were also given to reduce the complexity of the evaluation of the optimal channel truncation threshold γ. With the support of the simulation results, we conclude that having main-channel CSIT but limited or no CSIRE can be more beneficial than having full CSI at all terminals.

References

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

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

[3] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29–40, Sep. 2013.

[4] 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, Sep. 2007.

[5] 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, June 2008.

[6] A. Khisti and G. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[7] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[8] C. Huang, T. Chang., X. Zhou, and Y. P. Hong, "Two-way training for discriminatory channel estimation in wireless MIMO systems," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2724–2738, May 2013.

[9] C. Mitrpant, A. Vink, and Y. Luo, "An achievable region for the Gaussian wiretap channel with side information," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2181 – 2190, May 2006.

[10] Y. Chen and A. Vinck, "Wiretap channel with side information," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 395 – 402, Jan. 2008.

[11] A. J. Goldsmith and P. P. Varaiya, "Capacity of fading channels with side information," *IEEE Trans. Inf. Theory*, vol. 43, no. 6, pp. 1986–1992, Nov. 1997.

[12] G. Caire and S. Shamai, "On the capacity of some channel with channel state information," *IEEE. Trans. Inf. Theory*, vol. 45, no. 6, pp. 2007–2019, Sep. 1999.

[13] A. Lapidoth, "On phase noise channels at high SNR," in *Proceedings of IEEE Information Theory Workshop 2002*, Oct. 2002, pp. 1–4.

[14] G. Durisi, "On the capacity of the block-memoryless phase-noise channel," *IEEE Commun. Lett.*, vol. 16, no. 8, pp. 1157–1160, Aug. 2012.

[15] A. Lapidoth and S. M. Moser, "Capacity bounds via duality with applications to multiple-antenna systems on flat-fading channels," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2426–2467, Oct. 2003.

[16] M. Katz and S. Shamai (Shitz), "On the capacity-achieving distribution of the discrete-time noncoherent and partially coherent AWGN channels," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2257–2270, Oct. 2004.