A Statistical Physics Approach to the Wiretap Channel

Iñaki Esnaola
Dept. of Electrical Engineering
Princeton University
Princeton, NJ 08544, USA
Email: jesnaola@princeton.edu

Antonia M. Tulino
Bell Laboratories, Alcatel-Lucent
Wireless Communication Theory Research
Holmdel, NJ 07733, USA
Email: a.tulino@alcatel-lucent.com

H. Vincent Poor
Dept. of Electrical Engineering
Princeton University
Princeton, NJ 08544, USA
Email: poor@princeton.edu

***Abstract*—The secrecy rate of Wyner wiretap channels is analyzed for general classes of sources, sensing schemes, and channel distributions. Using the replica method, heuristic closed form expressions are obtained for the asymptotic secrecy rate as a function of the statistics of the system model. This result is then applied in practically oriented scenarios, leading to expressions that expose the existing trade-offs between system parameters and security requirements, including the region in which perfect secrecy is feasible. As a particular example of the broad class of sources that are considered in the main contribution, source distributions giving rise to sparse signals are studied. In that setting, the secrecy rate linked to the disclosure of information about the support of the signals is investigated.**

I. Introduction

With the introduction of information theoretic secrecy [1], Shannon provided a mathematical framework to measure confidentiality in communications. A classical example for which secrecy is investigated from an information theoretic perspective is the Wyner wiretap channel [2], in which an eavesdropper has access to a degraded version of a message transmitted to a legitimate receiver.

A main challenge when using information theoretic measures resides in the difficulty of evaluating them. In our approach, we overcome this problem by using statistical physics methods in the evaluation of the mutual information. Specifically, we use the replica method [3], and therefore, due to its heuristic nature we state our results as claims. That being said, the replica method has proven to be successful in several areas before. For instance, in the analysis of code-division multiple-access (CDMA) systems [4], [5] or characterizing the performance of compressed sensing with independent and identically distributed (i.i.d.) sensing matrices [6], [7]. Our results build upon the generalization to non i.i.d. sensing matrices in [8] which successfully extends the framework in which the replica method can be applied.

Secrecy via compressed sensing has received attention recently. The work in [9] investigates the privacy provided by compressed sensing measurements under LP decoding. In [10], Rachlin and Baron show that using the sensing matrix as a key does not provide secrecy in an information theoretic sense. However, they do point out the possibility of developing strong cryptographic schemes that are not breakable in polynomial time. A more interesting scenario arises when the sensing matrix is known to both the eavesdropper and the legitimate receiver. In [11] Reeves et al. show that, for binary sparse sources, secrecy can be achieved provided the channel of the eavesdropper is strictly worse than the channel of the legitimate receiver. The idea is to operate close to the phase transition regime, which allows the legitimate receiver to estimate correctly with high probability while the eavesdropper does not have enough measurements to reconstruct the signal. The extension to multiple-input multiple-output (MIMO) channels is considered in [12] by Agrawal and Vishwanath.

In this paper, we characterize the source, the sensing matrix, and the channel as random processes. By doing so, we obtain closed form expressions for the asymptotic secrecy rate that depend on the statistics of the system. Specifically, we consider i.i.d. sources whose entries follow an arbitrary distribution. This model allows us to consider the compressed sensing setting as a particular case simply by choosing distributions with low probability of producing a non-zero output. For this case, we also study the secrecy rate when the goal is to estimate the support. Additionally, combining the replica method with random matrix theory tools, we investigate several statistical structures that appear in practical scenarios. Although not present in this paper due to space limitations, the importance of these results is not limited to information theoretic measures. Indeed, the results presented below can be extended for evaluating the performance of specific estimation techniques, such as the Minimum Mean Square Error (MMSE) estimator or the Maximum A Posteriori Probability (MAP) estimator.

The rest of the paper is organized as follows. The next section describes the system model. Section III presents the secrecy results for the case in which the signal is estimated at both the receiver and the eavesdropper. In Section IV the source model is particularized to generate sparse signals and secrecy results are presented for the case in which the goal is the estimation of the support. We conclude in Section V with numerical evaluations of the secrecy regions described by the expressions obtained in the previous sections. Because of space limitations we omit the proofs, but it is worth mentioning that our results are obtained by combining the results in [8] with random matrix theory tools.

The research was supported in part by the Air Force Office of Scientific Research under MURI Grant FA9550-09-1-0643, in part by the National Science Foundation under Grant DMS-1118605, and in part by the Office of Naval Research under Grant N00014-12-1-0767.

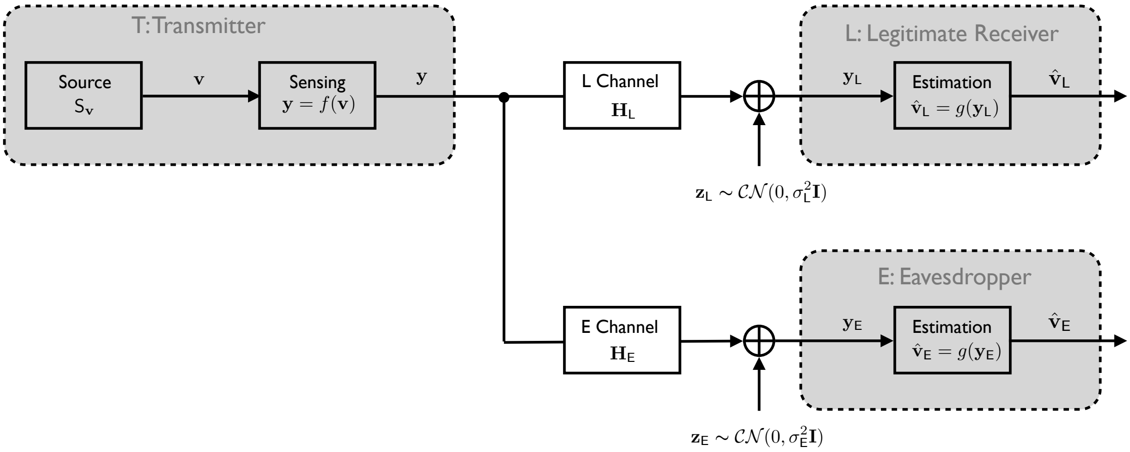
T: Transmitter
Source
S_v
$\mathbf{v}$
Sensing
$\mathbf{y} = f(\mathbf{v})$
$\mathbf{y}$
L Channel
$\mathbf{H}_{\mathsf{L}}$
$\mathbf{z}_{\mathsf{L}} \sim \mathcal{CN}(0, \sigma_{\mathsf{L}}^2\mathbf{I})$
L: Legitimate Receiver
$\mathbf{y}_{\mathsf{L}}$
Estimation
$\hat{\mathbf{v}}_{\mathsf{L}} = g(\mathbf{y}_{\mathsf{L}})$
$\hat{\mathbf{v}}_{\mathsf{L}}$
E Channel
$\mathbf{H}_{\mathsf{E}}$
$\mathbf{z}_{\mathsf{E}} \sim \mathcal{CN}(0, \sigma_{\mathsf{E}}^2\mathbf{I})$
E: Eavesdropper
$\mathbf{y}_{\mathsf{E}}$
Estimation
$\hat{\mathbf{v}}_{\mathsf{E}} = g(\mathbf{y}_{\mathsf{E}})$
$\hat{\mathbf{v}}_{\mathsf{E}}$

Fig. 1. Block diagram of the Wyner wiretap channel.

II. System Model

A. Signal Model

We consider a stationary source, $\mathsf{S}_{\mathbf{v}}$, producing realizations $\mathbf{v} \in \mathbb{C}^n$, such that $\mathbf{v} = (\mathsf{V}_1, \ldots, \mathsf{V}_n)$ is a vector whose elements are i.i.d. with distribution $\mathsf{V}_i \sim f_V$. Note that, this structure models signals arising from memoryless random processes but does not limit the distribution of the entries.

B. Wiretap Channel

Figure 1 depicts a block diagram of the wiretap channel under consideration. The transmitter, T, acquires a source realization, $\mathbf{v}$, using sensing function f. The resulting sequence, $\mathbf{y}$, is transmitted to the legitimate receiver, L, through channel $\mathbf{H}_{\mathsf{L}} \in \mathbb{R}^{n \times k_{\mathsf{L}}}$ which incorporates an Additive White Gaussian Noise (AWGN) component with variance σ_{L}^2. Simultaneously, an eavesdropper, E, observes the sequence $\mathbf{y}_{\mathsf{E}}$ at the output of its corresponding channel $\mathbf{H}_{\mathsf{E}} \in \mathbb{R}^{n \times k_{\mathsf{E}}}$ which also incorporates an AWGN component with variance σ_{E}^2. With received signals $\mathbf{y}_{\mathsf{L}}$ and $\mathbf{y}_{\mathsf{E}}$, the legitimate receiver and the eavesdropper produce estimates $\hat{\mathbf{v}}_{\mathsf{L}}$ and $\hat{\mathbf{v}}_{\mathsf{E}}$, respectively.

C. Linear Observation Model

In the following, we limit our analysis to the case in which the sensing function, f, is linear. Specifically, the signal is observed in a domain determined by matrix $\mathbf{U}$ and with a sensing pattern defined by a matrix $\mathbf{A}$. The observations at the legitimate receiver, $\mathbf{y}_{\mathsf{L}}$, and the eavesdropper, $\mathbf{y}_{\mathsf{E}}$, are given by

$$\mathbf{y}_{\mathsf{L}} = \mathbf{H}_{\mathsf{L}}\mathbf{A}\mathbf{U}\mathbf{v} + \mathbf{z}_{\mathsf{L}}, \tag{1}$$

$$\mathbf{y}_{\mathsf{E}} = \mathbf{H}_{\mathsf{E}}\mathbf{A}\mathbf{U}\mathbf{v} + \mathbf{z}_{\mathsf{E}} \tag{2}$$

where $\mathbf{A} \in \mathbb{C}^{n \times n}$ is a diagonal matrix whose elements are i.i.d. Bernoulli distributed, i.e., $\mathsf{P}[\mathsf{A}_{ii} = 1] = p = 1 - \mathsf{P}[\mathsf{A}_{ii} = 0]$, $\mathbf{U} \in \mathbb{C}^{n \times n}$ is a random matrix that is free [13] from any deterministic Hermitian matrix, and $\mathbf{z}_{\mathsf{L}} \in \mathbb{C}^n$ and $\mathbf{z}_{\mathsf{E}} \in \mathbb{C}^n$ are i.i.d. noise terms whose entries are $\mathcal{CN}(0, \sigma_{\mathsf{L}}^2)$ and $\mathcal{CN}(0, \sigma_{\mathsf{E}}^2)$, respectively. For simplicity and without loss of generality we assume $\sigma_{\mathsf{L}} = 1$ for the remainder of the paper.

III. Signal Estimation

To guarantee secrecy in the communication with the legitimate user, the encoding function needs to take into account the information that the eavesdropper can retrieve from its observation. The amount of information that leaks to the eavesdropper can be quantified using information theoretic measures, specifically, mutual information. Unfortunately, computing the mutual information is complex, in general, for arbitrary finite length sources. A more manageable task is to tackle the problem in the asymptotic regime. We start by defining the *asymptotic secrecy rate* as

$$\mathcal{I}_S \triangleq \lim_{n \to \infty} \frac{1}{n} \left(I(\mathbf{v}; \mathbf{y}_{\mathsf{L}} | \mathbf{A}, \mathbf{U}, \mathbf{H}_{\mathsf{L}}) - I(\mathbf{v}; \mathbf{y}_{\mathsf{E}} | \mathbf{A}, \mathbf{U}, \mathbf{H}_{\mathsf{E}}) \right)^+ \tag{3}$$

where $(\cdot)^+$ is the positive part operator. Recall that in this paper we assume that both the legitimate receiver and the eavesdropper perform coherent detection, and that the sensing function, f, is known to both. For that reason, the estimates of the legitimate receiver and the eavesdropper are produced with knowledge of $\{\mathbf{H}_{\mathsf{L}}, \mathbf{A}, \mathbf{U}\}$ and $\{\mathbf{H}_{\mathsf{E}}, \mathbf{A}, \mathbf{U}\}$, respectively. For ease of notation we define $\mathbf{\Phi} = \mathbf{A}\mathbf{U}$.

A straightforward numerical evaluation of (3) is computationally unfeasible for most signal distributions of interest. However, this limitation can be overcome by using the replica method. Specifically, the approach developed in [8] provides the necessary tools to describe the asymptotic secrecy rate. In order to set our problem within the framework in [8], we split (3) into two terms given by

$$\mathcal{I}_{\mathsf{L}} \triangleq \lim_{n \to \infty} \frac{1}{n} I(\mathbf{v}; \mathbf{y}_{\mathsf{L}} | \mathbf{A}, \mathbf{U}, \mathbf{H}_{\mathsf{L}}) \tag{4}$$

$$\mathcal{I}_{\mathsf{E}} \triangleq \lim_{n \to \infty} \frac{1}{n} I(\mathbf{v}; \mathbf{y}_{\mathsf{E}} | \mathbf{A}, \mathbf{U}, \mathbf{H}_{\mathsf{E}}) \tag{5}$$

from which the asymptotic secrecy rate can be obtained by noticing that

$$\mathcal{I}_S \triangleq \left(\mathcal{I}_{\mathsf{L}} - \mathcal{I}_{\mathsf{E}} \right)^+ . \tag{6}$$

Based on the above definitions and the result in [8], the asymptotic secrecy rate as defined in (3) can be obtained in closed form. The following claim states the result.

Claim 1 *Let* V *and* Z *be independent random variables with* $\mathsf{V} \sim \mathsf{F}_{\mathsf{V}}$ *and* $\mathsf{Z} \sim \mathcal{CN}(0,1)$*. Let* $\mathcal{R}_{\mathbf{R}_{\mathsf{E}}}(\cdot)$ *and* $\mathcal{R}_{\mathbf{R}_{\mathsf{L}}}(\cdot)$ *denote the R-transforms [13] of random matrices* $\mathbf{R}_{\mathsf{L}} = \mathbf{\Phi}^{\dagger}\mathbf{H}_{\mathsf{L}}^{\dagger}\mathbf{H}_{\mathsf{L}}\mathbf{\Phi}$ *and* $\mathbf{R}_{\mathsf{E}} = \mathbf{\Phi}^{\dagger}\mathbf{H}_{\mathsf{E}}^{\dagger}\mathbf{H}_{\mathsf{E}}\mathbf{\Phi}$*, respectively. Then,*

$$\mathcal{I}_S = \Bigg(I_s(\mathsf{V}, \eta_{\mathsf{L}}, \eta_{\mathsf{E}}) - \log e\,(\eta_{\mathsf{L}}\chi_{\mathsf{L}} - \eta_{\mathsf{E}}\chi_{\mathsf{E}}) + \log e \left(\int_0^{\chi_{\mathsf{L}}} \mathcal{R}_{\mathbf{R}_{\mathsf{L}}}(-u)du - \int_0^{\chi_{\mathsf{E}}} \mathcal{R}_{\mathbf{R}_{\mathsf{E}}}(-u)du \right) \Bigg)^{+} \quad (7)$$

where

$$I_s(\mathsf{V}, \eta_{\mathsf{L}}, \eta_{\mathsf{E}}) \triangleq I\left(\mathsf{V}; \mathsf{V} + \frac{1}{\sqrt{\eta_{\mathsf{L}}}}\mathsf{Z}\right) - I\left(\mathsf{V}; \mathsf{V} + \frac{\sigma_{\mathsf{E}}}{\sqrt{\eta_{\mathsf{E}}}}\mathsf{Z}\right) \quad (8)$$

and η_{L}*,* η_{E}*,* χ_{L}*,* χ_{E} *are the non-negative solutions to the system of fixed point equations given by*

$$\eta_{\mathsf{L}} = \mathcal{R}_{\mathbf{R}_{\mathsf{L}}}(-\chi_{\mathsf{L}}) \quad (9)$$

$$\chi_{\mathsf{L}} = \mathsf{mmse}(\eta_{\mathsf{L}}) \quad (10)$$

$$\eta_{\mathsf{E}} = \mathcal{R}_{\mathbf{R}_{\mathsf{E}}}(-\chi_{\mathsf{E}}) \quad (11)$$

$$\chi_{\mathsf{E}} = \mathsf{mmse}(\eta_{\mathsf{E}}) \quad (12)$$

where we define

$$\mathsf{mmse}(\eta) \triangleq \mathbb{E}\left[|\mathsf{V} - \mathbb{E}(\mathsf{V}|\mathsf{V} + \eta^{-\frac{1}{2}}\mathsf{Z})|^2 \right]. \quad (13)$$

With this expression the evaluation of mutual information terms (4) and (5) is greatly simplified. Indeed, the evaluation of the mutual information between multidimensional variables is reduced to evaluating the mutual information of equivalent scalar variables. Note, that the noise statistics of the equivalent scalar channel are determined by the solution to the set of fixed point equations.

In some special cases, the expression for the secrecy rate can be further adapted. In the following, we particularize the result from claim 1 to specific scenarios of practical interest. The procedure involves incorporating the statistical characteristics of each specific setting to the expression of the secrecy rate.

A. MIMO Gaussian Wiretap I.i.d. Channels

When $\mathbf{H}_{\mathsf{L}}$ and $\mathbf{H}_{\mathsf{E}}$ are random matrices with i.i.d. entries and $\mathbf{\Phi} = \mathbf{I}$, the setting corresponds to a MIMO Gaussian wiretap channel. This channel has been considered in [14] and [15]. The following result characterizes the asymptotic secrecy rate when arbitrary input distributions are considered.

Claim 2 *Let* V *and* Z *be independent random variables with* $\mathsf{V} \sim \mathsf{F}_{\mathsf{V}}$ *and* $\mathsf{Z} \sim \mathcal{CN}(0,1)$*. Let random matrices* $\mathbf{H}$ *and* $\mathbf{H}_{\mathsf{L}}$ *have i.i.d zero mean entries with variance* $\frac{1}{n}$*. Then*

$$\mathcal{I}_S = \Bigg(I_s(\mathsf{V}, \eta_{\mathsf{L}}, \eta_{\mathsf{E}}) + \frac{1}{\beta_{\mathsf{L}}}\log\eta_{\mathsf{L}} - \frac{1}{\beta_{\mathsf{E}}}\log\eta_{\mathsf{E}} - \left(\frac{1-\eta_{\mathsf{L}}}{\beta_{\mathsf{L}}}\right) + \left(\frac{1-\eta_{\mathsf{E}}}{\beta_{\mathsf{E}}}\right) \Bigg)^{+} \quad (14)$$

where $\beta_{\mathsf{L}} = \frac{n}{k_{\mathsf{L}}}$*,* $\beta_{\mathsf{E}} = \frac{n}{k_{\mathsf{E}}}$ *and* η_{L} *and* η_{E} *are given by*

$$\frac{1}{\eta_{\mathsf{L}}} = 1 + \beta_{\mathsf{L}}\mathsf{mmse}(\eta_{\mathsf{L}}) \quad (15)$$

$$\frac{1}{\eta_{\mathsf{E}}} = 1 + \beta_{\mathsf{E}}\mathsf{mmse}(\eta_{\mathsf{E}}). \quad (16)$$

When random matrices $\mathbf{H}_{\mathsf{L}}$ and $\mathbf{H}_{\mathsf{E}}$ have circularly symmetric complex Gaussian entries, the setting reduces to a wireless MIMO wiretap channel with Rayleigh fading. However, in wireless communications the case in which the channels are correlated is also of interest. The next result incorporates the effect of correlation at the receiver.

B. MIMO Gaussian Wiretap with Correlated Channels

The proximity between antennas might result in correlation between received signals. The separable correlation model [16] is a widely used model for modeling the dependence between antennas. Due to the physical limitations within which an eavesdropper usually operates, considering that the channel it observes is correlated seems a reasonable assumption. Accordingly, the secrecy rate will increase as the correlation at the eavesdropper's side increases. The following claim quantifies the impact of the receiver side correlation over the asymptotic secrecy rate.

Claim 3 *Let* V *and* Z *be independent random variables with* $\mathsf{V} \sim \mathsf{F}_{\mathsf{V}}$ *and* $\mathsf{Z} \sim \mathcal{CN}(0,1)$*. Let the channels be given by* $\mathbf{H}_{\mathsf{E}} = \mathbf{\Theta}_{\mathsf{E}}^{1/2}\mathbf{W}$ *and* $\mathbf{H}_{\mathsf{L}} = \mathbf{\Theta}_{\mathsf{L}}^{1/2}\mathbf{W}$ *where* $\mathbf{W}$ *has i.i.d. zero mean entries with variance* $\frac{1}{n}$*, and full-rank correlation defining matrices* $\mathbf{\Theta}_{\mathsf{L}}$ *and* $\mathbf{\Theta}_{\mathsf{E}}$*. Then*

$$\mathcal{I}_S = \Big(I_s(\mathsf{V}, \eta_{\mathsf{L}}, \eta_{\mathsf{E}}) + \beta_{\mathsf{L}}\mathbb{E}\left[\log(1 + \Lambda_{\mathsf{L}}\mathsf{mmse}(\eta_{\mathsf{L}}))\right] - \beta_{\mathsf{E}}\mathbb{E}\left[\log(1 + \Lambda_{\mathsf{E}}\mathsf{mmse}(\eta_{\mathsf{E}}))\right] - (\eta_{\mathsf{L}}\mathsf{mmse}(\eta_{\mathsf{L}}) - \eta_{\mathsf{E}}\mathsf{mmse}(\eta_{\mathsf{E}})) \Big)^{+} \quad (17)$$

where $\beta_{\mathsf{L}} = \frac{n}{k_{\mathsf{L}}}$*,* $\beta_{\mathsf{E}} = \frac{n}{k_{\mathsf{E}}}$ *and* η_{L} *and* η_{E} *are given by*

$$\eta_{\mathsf{L}} = \beta_{\mathsf{L}}\mathbb{E}\left[\frac{\Lambda_{\mathsf{L}}}{1 + \Lambda_{\mathsf{L}}\mathsf{mmse}(\eta_{\mathsf{L}})}\right] \quad (18)$$

$$\eta_{\mathsf{E}} = \beta_{\mathsf{E}}\mathbb{E}\left[\frac{\Lambda_{\mathsf{E}}}{1 + \Lambda_{\mathsf{E}}\mathsf{mmse}(\eta_{\mathsf{E}})}\right], \quad (19)$$

with Λ_{L} *and* Λ_{E} *being independent random variables whose distributions are the asymptotic spectra of* $\mathbf{\Theta}_{\mathsf{L}}$ *and* $\mathbf{\Theta}_{\mathsf{E}}$ *respectively.*

C. MIMO Gaussian Wiretap with Asymptotically Free Channels

Many asymptotic results in random matrix theory have been obtained using a free probability framework [17]. For that reason, it is interesting to identify under which freeness conditions our results hold. In the following, it is shown that the asymptotic secrecy rate can be obtained via the replica method under mild freeness conditions. Specifically, the statistical structures arising from the sensing process and the channel are asymptotically free. A more precise description of the conditions follows.

Claim 4 *Let* V *and* Z *be independent random variables with* $\mathsf{V} \sim \mathsf{F}_{\mathsf{V}}$ *and* $\mathsf{Z} \sim \mathcal{CN}(0,1)$*, and let* $\mathbf{\Sigma}_{\mathbf{\Phi}\mathbf{\Phi}^{\dagger}}(\cdot)$ *and* $\eta_{\mathbf{H}^{\dagger}\mathbf{H}}(\cdot)$ *denote the S-transform and* η*-transform [13] of* $\mathbf{\Phi}\mathbf{\Phi}^{\dagger}$ *and* $\mathbf{H}^{\dagger}\mathbf{H}$*, respectively. If* $\mathbf{\Phi}\mathbf{\Phi}^{\dagger}$ *and* $\left\{\mathbf{H}_{\mathsf{L}}^{\dagger}\mathbf{H}_{\mathsf{L}}, \mathbf{H}_{\mathsf{E}}^{\dagger}\mathbf{H}_{\mathsf{E}}\right\}$

are asymptotically free, then

$$\mathcal{I}_S{=}\Big(I_S(\mathsf{V},\eta_{\mathsf{L}},\eta_{\mathsf{E}}) - \log e\,(\eta_{\mathsf{L}}\mathsf{mmse}(\eta_{\mathsf{L}}) - \eta_{\mathsf{E}}\mathsf{mmse}(\eta_{\mathsf{E}}))$$
$$+\int_0^{\mathsf{mmse}(\eta_{\mathsf{L}})} \mathcal{R}_{\mathbf{R}_{\mathsf{L}}}(-u)du\,\log e - \int_0^{\mathsf{mmse}(\eta_{\mathsf{E}})} \mathcal{R}_{\mathbf{R}_{\mathsf{E}}}(-u)du\,\log e\Big)^+$$

where η_{L}, η_{E}, γ_{L}, γ_{E}, δ_{L}, and δ_{E} are the non-negative solutions to the system of fixed point equations

$$\eta_{\mathsf{L}}{=}\frac{1-\delta_{\mathsf{L}}}{\mathsf{mmse}(\eta_{\mathsf{L}})} \tag{20}$$
$$\delta_{\mathsf{L}}\gamma_{\mathsf{L}}{=}\mathsf{mmse}(\eta_{\mathsf{L}}) \tag{21}$$
$$\delta_{\mathsf{L}}{=}\bar{\eta}_{\mathbf{H}_{\mathsf{L}}^\dagger\mathbf{H}_{\mathsf{L}}}\left(\frac{\gamma_{\mathsf{L}}}{\Sigma_{\mathbf{\Phi}\mathbf{\Phi}^\dagger}(\delta_{\mathsf{L}}-1)}\right) \tag{22}$$
$$\eta_{\mathsf{E}}{=}\frac{1-\delta_{\mathsf{E}}}{\mathsf{mmse}(\eta_{\mathsf{E}})} \tag{23}$$
$$\delta_{\mathsf{E}}\gamma_{\mathsf{E}}{=}\mathsf{mmse}(\eta_{\mathsf{E}}) \tag{24}$$
$$\delta_{\mathsf{E}}{=}\bar{\eta}_{\mathbf{H}_{\mathsf{E}}^\dagger\mathbf{H}_{\mathsf{E}}}\left(\frac{\gamma_{\mathsf{E}}}{\Sigma_{\mathbf{\Phi}\mathbf{\Phi}^\dagger}(\delta_{\mathsf{E}}-1)}\right). \tag{25}$$

In (20)-(25), δ_{L} and δ_{E} denote the η-transform of $\mathbf{R}_{\mathsf{L}}$ and $\mathbf{R}_{\mathsf{E}}$, respectively. The pairs (20)-(21), and (23)-(24) follow from the relationship between the η-transform and the R-transform given in [13, Section 2.2.5]. Finally, (22) and (25) are obtained using [13, Theorem 2.68] to calculate δ_{L} and δ_{E} as η-transforms of the product of asymptotically free matrices.

IV. Support estimation results

We now focus on source distributions describing sparse signals in order to pose the problem in a compressed sensing framework. Consider a sparse random vector $\mathbf{v} \in \mathbb{C}^n$ such that

$$\mathbf{v} = \mathbf{B}\mathbf{x} \tag{26}$$

where $\mathbf{B} = \text{diag}\{\mathsf{B}_{11}, \ldots, \mathsf{B}_{nn}\} \in \mathbb{C}^{n\times n}$ is a diagonal matrix whose elements, $\mathsf{B}_{ii} \sim q_B(\cdot)$, are i.i.d. Bernoulli distributed, i.e., $\mathsf{P}[\mathsf{B}_{ii} = 1] = q = 1 - \mathsf{P}[\mathsf{B}_{ii} = 0]$ and $\mathbf{x} \in \mathbb{C}^n$ is an i.i.d. circularly symmetric complex Gaussian vector with entries $x_i \sim \mathcal{CN}(0, \sigma_x^2)$. This signal structure allows modeling of the random processes governing the signal support and the amplitude of the non-zero elements independently. The average sparsity of the signal is nq.

At the receiver, the goal is to produce an estimate of the support, $\hat{\mathbf{B}}_{\mathsf{L}} = \text{diag}\{\hat{\mathsf{B}}_{11}, \ldots, \hat{\mathsf{B}}_{nn}\} \in \mathbb{C}^{n\times n}$. In order to obtain the mutual information with respect to the support, in addition to (4) and (5) we need to define the following two quantities:

$$\mathcal{I}_{\mathsf{L}}^*{=}\lim_{n\to\infty}\frac{1}{n}I(\mathbf{x};\mathbf{y}_{\mathsf{L}}|\mathbf{A},\mathbf{U},\mathbf{B},\mathbf{H}_{\mathsf{L}}) \tag{27}$$
$$\mathcal{I}_{\mathsf{E}}^*{=}\lim_{n\to\infty}\frac{1}{n}I(\mathbf{x};\mathbf{y}_{\mathsf{E}}|\mathbf{A},\mathbf{U},\mathbf{B},\mathbf{H}_{\mathsf{E}}). \tag{28}$$

Noting that [8] we can write

$$I(\mathbf{B};\mathbf{y}|\mathbf{\Phi}) = I(\mathbf{v};\mathbf{y}|\mathbf{A},\mathbf{U},\mathbf{H}) - I(\mathbf{x};\mathbf{y}|\mathbf{A},\mathbf{U},\mathbf{B},\mathbf{H}), \tag{29}$$

it is straightforward to see that the *asymptotic support secrecy rate* is given by

$$\widehat{\mathcal{I}}_S{\overset{\Delta}{=}}\lim_{n\to\infty}\frac{1}{n}\Big(I(\mathbf{B};\mathbf{y}_{\mathsf{L}}|\mathbf{A},\mathbf{U},\mathbf{H}_{\mathsf{L}}){-}I(\mathbf{B};\mathbf{y}_{\mathsf{L}}|\mathbf{A},\mathbf{U},\mathbf{H}_{\mathsf{E}})\Big)^+ \tag{30}$$
$$={(\mathcal{I}_{\mathsf{L}} - \mathcal{I}_{\mathsf{E}} - (\mathcal{I}_{\mathsf{L}}^* - \mathcal{I}_{\mathsf{E}}^*))^+}. \tag{31}$$

In order to compute (30), we need to evaluate (27) and (28). These quantities were obtained in [8] using random matrix theory tools.

Theorem 1 *Let $\mathcal{V}_{\mathbf{R}}(\cdot)$ denote the Shannon transform of $\mathbf{R} = \mathbf{\Phi}^\dagger\mathbf{H}^\dagger\mathbf{H}\mathbf{\Phi}$. Then,*

$$\mathcal{I}^* = \mathcal{V}_{\mathbf{R}}(\alpha\,\sigma_X^2) + q\log\left(1+\nu\sigma_X^2\right) - \log(1+\alpha\,\nu\sigma_X^2) \tag{32}$$

where α and ν are the unique non-negative solutions of the system of equations

$$\bar{\eta}_{\mathbf{R}}(\alpha\,\sigma_X^2) = \frac{1}{1+\alpha\,\nu\sigma_X^2} = \frac{q}{1+\nu\sigma_X^2} + (1-q). \tag{33}$$

Putting together (27) and (28) with Theorem 1 we can state the following result for the asymptotic support secrecy rate.

Claim 5 *Let V and Z be independent random variables with $\mathsf{V} \sim \mathsf{F}_{\mathsf{V}}$ and $\mathsf{Z} \sim \mathcal{CN}(0,1)$. Then*

$$\widehat{\mathcal{I}}_S{=}\Bigg(I_S(\mathsf{V},\eta_{\mathsf{L}},\eta_{\mathsf{E}}) - \log(e)\,(\eta_{\mathsf{L}}\chi_{\mathsf{L}} - \eta_{\mathsf{E}}\chi_{\mathsf{E}})$$
$$+\int_0^{\chi_{\mathsf{L}}}\mathcal{R}_{\mathbf{R}_{\mathsf{L}}}(-u)du\,\log e - \int_0^{\chi_{\mathsf{E}}}\mathcal{R}_{\mathbf{R}_{\mathsf{E}}}(-u)du\,\log e$$
$$-\mathcal{V}_{\mathbf{R}_{\mathsf{L}}}(\alpha_{\mathsf{L}}\sigma_x^2) + \mathcal{V}_{\mathbf{R}_{\mathsf{E}}}(\alpha_{\mathsf{E}}\sigma_x^2) - q\log\left(\frac{1+\nu_{\mathsf{L}}\sigma_X^2}{1+\nu_{\mathsf{E}}\sigma_X^2}\right)$$
$$+\log\left(\frac{1+\alpha_{\mathsf{L}}\,\nu_{\mathsf{L}}\sigma_X^2}{1+\alpha_{\mathsf{E}}\,\nu_{\mathsf{E}}\sigma_X^2}\right)\Bigg)^+ \tag{34}$$

where η_{L}, η_{E}, χ_{L}, $\chi_{\mathsf{E}}, \alpha_{\mathsf{L}}, \alpha_{\mathsf{E}}$, and ν_{L} are the non-negative solutions of

$$\eta_{\mathsf{L}}{=}\mathcal{R}_{\mathbf{R}_{\mathsf{L}}}(-\chi_{\mathsf{L}}) \tag{35}$$
$$\chi_{\mathsf{L}}{=}\mathsf{mmse}(\eta_{\mathsf{L}}) \tag{36}$$
$$\eta_{\mathsf{E}}{=}\mathcal{R}_{\mathbf{R}_{\mathsf{E}}}(-\chi_{\mathsf{E}}) \tag{37}$$
$$\chi_{\mathsf{E}}{=}\mathsf{mmse}(\eta_{\mathsf{E}}) \tag{38}$$
$$\bar{\eta}_{\mathbf{R}_{\mathsf{L}}}(\alpha_{\mathsf{L}}\,\sigma_X^2){=}\frac{1}{1+\alpha_{\mathsf{L}}\,\nu_{\mathsf{L}}\sigma_X^2} = \frac{q}{1+\nu_{\mathsf{L}}\sigma_X^2} + (1-q) \tag{39}$$
$$\bar{\eta}_{\mathbf{R}_{\mathsf{E}}}(\alpha_{\mathsf{E}}\,\sigma_X^2){=}\frac{1}{1+\alpha_{\mathsf{E}}\,\nu_{\mathsf{E}}\sigma_X^2} = \frac{q}{1+\nu_{\mathsf{E}}\sigma_X^2} + (1-q). \tag{40}$$

V. Numerical results

In this section, we numerically evaluate the asymptotic secrecy rate for both the estimation and the support pattern recovery settings. We consider the case in which the source produces sparse random vectors as given in (26) with $q = 0.1$, the sensing scheme is $\mathbf{\Phi} = \mathbf{I}$, and channel matrices have i.i.d. zero mean entries with variance $\frac{1}{n}$. We define the signal to noise ratio for the legitimate receiver as $\mathsf{SNR}_{\mathsf{L}} = 10\log\left(q\sigma_x^2\right)$ and the signal to noise ratio for the eavesdropper as $\mathsf{SNR}_{\mathsf{E}} = 10\log\left(\frac{q\sigma_x^2}{\sigma_{\mathsf{E}}^2}\right)$. In order to compute the secrecy rates, we fix $\mathsf{SNR}_{\mathsf{L}} = 10$ dB and $\beta_{\mathsf{L}} = 1$ for the legitimate receiver while

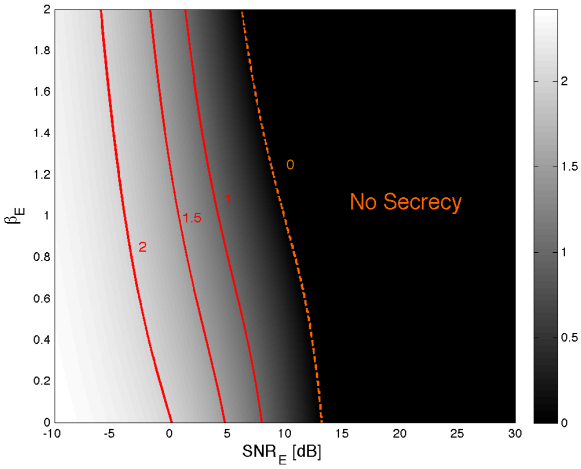

Fig. 2. Asymptotic secrecy rate in signal estimation for different values of SNR_E and β_E when $\text{SNR}_\text{L} = 10$ dB and $\beta_\text{L} = 1$. The dashed level curve delimits the region in which perfect secrecy is not feasible.

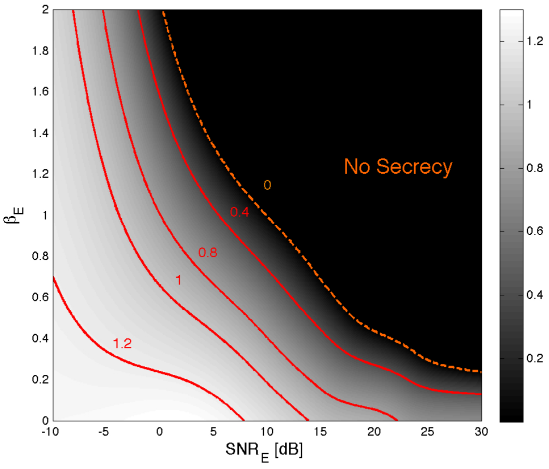

Fig. 3. Asymptotic support secrecy rate in sparsity pattern recovery for different values of SNR_E and β_E when $\text{SNR}_\text{L} = 10$ dB and $\beta_\text{L} = 1$. The dashed level curve delimits the region in which perfect secrecy is not feasible.

varying the parameters corresponding to the eavesdropper. Recall that β_L is the ratio between the number of transmit and receive dimensions (for a wireless channels it would be equivalent to the ratio between transmitter to receiver antennas).

Figure 2 depicts the asymptotic secrecy rate for each $\{\text{SNR}_\text{E}, \beta_E\}$ pair when $\text{SNR}_\text{L} = 10$ dB and $\beta_\text{L} = 1$. The intensity describes the secrecy rate, i.e., the darker the point the lower the asymptotic secrecy rate. The dashed level curve delineates the secrecy region. Interestingly, for SNR_E values higher than 13 dB, the dimensions of the channel stop playing a role and perfect secrecy becomes unattainable regardless of the value of β_E. On the other hand, for SNR_E values below 8 dB, the legitimate user can always obtain private information regardless of the dimensionality ratio.

The support pattern recovery case is shown in Figure 3 when $\text{SNR}_\text{L} = 10$ dB and $\beta_\text{L} = 1$. Interestingly, contrary to what happens in the estimation case, for every SNR_E value there exists a value of β_E that guarantees that $\widehat{\mathcal{I}}_S$ is strictly positive. However, the minimum value SNR_E for which secrecy can always be attained for some value of β_E, has also moved to 0 dB. This forces the legitimate user to operate in higher signal to noise ratio regimes if it wants to guarantee secrecy and does not know the dimensions of the eavesdroppers channels. Remarkably, in this scenario, the impact of the dimensionality of the channel is significantly higher than in the signal estimation one.

VI. Conclusion

We have characterized the secrecy rate for a broad class of sources, sensing procedures and wiretap channel statistics. Combining random matrix theory results with the replica method, closed form expressions for the secrecy rates for practical scenarios of interest have been obtained. Exploiting the generality of the results, the link to compressed sensing secrecy has also been presented.

References

[1] C. E. Shannon, “Communication theory of secrecy systems,” *Bell System Technical Journal*, vol. 28, pp. 656-715, 1949.

[2] A. Wyner, “The wiretap channel,” *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, 1975.

[3] S. F. Edwards and P. W. Anderson, “Theory of spin glasses,” *J. Phys. F: Metal Physics*, vol. 5, pp. 965 974, 1975.

[4] T. Tanaka, “A statistical-mechanics approach to large-system analysis of CDMA multiuser detectors,” *IEEE Trans. Inf. Theory,* vol. 48, no. 11, pp. 2888-2910, Nov. 2002.

[5] D. Guo and S. Verdú, “Randomly spread CDMA: asymptotics via statistical physics,” *IEEE Trans. Inf. Theory,* vol. 51, no. 6, pp. 1983-2010, June 2005.

[6] D. Guo, D. Baron and S. Shamai (Shitz), “A single-letter characterization of optimal noisy compressed sensing,” in *Proc. Annual Allerton Conference in Communication, Control, and Computing*, Oct. 2008.

[7] S. Rangan, A. K. Fletcher, and V. K. Goyal, “Asymptotic analysis of MAP estimation via the replica method and applications to compressed sensing,” *IEEE Trans. Inf. Theory,* vol. 58, no. 3, pp. 1902-1923, March 2012.

[8] A. M. Tulino, G. Caire, S. Shamai and S. Verdú, “Support recovery with sparsely sampled free random matrices,” To appear in *IEEE Trans. Inf. Theory*.

[9] C. Dwork, F. McSherry, and K. Talwar, “The price of privacy and the limits of LP decoding,” in *Proc. Annual ACM Symposium on Theory of Computing,* vol. 39, pp. 85-94, 2007.

[10] Y. Rachlin and D. Baron, “The secrecy of compressed sensing measurements,” in *Proc. Annual Allerton Conference in Communication, Control, and Computing*, Oct. 2009.

[11] G. Reeves, N. Goela, N. Milosavljevic, and M. Gastpar, “A compressed sensing wire-tap channel,” in *Proc. IEEE Information Theory Workshop,* Oct. 2011.

[12] S. Agrawal and S. Vishwanath, “Secrecy using compressive sensing,” in *Proc. IEEE Information Theory Workshop*, Oct. 2011.

[13] A. M. Tulino and S. Verdú, “Random Matrix Theory and Wireless Communications,” *Foundations and Trends In Communications and Information Theory*, vol. 1, no. 1, pp. 1–184, 2004.

[14] A. Khisti and G. Wornell, “The MIMOME channel,” in *Proc. Annual Allerton Conference on Communication, Control and Computing*, Sep. 2007.

[15] F. Oggier and B. Hassibi, “The secrecy capacity of the MIMO wiretap channel,” in *Proc. Annual Allerton Conference on Communication, Control and Computing*, Sep. 2007.

[16] A.M. Tulino, A. Lozano, and S. Verdú, “Impact of antenna correlation on the capacity of multiantenna channels,” *IEEE Trans. Inf. Theory*, vol. 51, no. 7, pp. 2491-2509, Jul. 2005.

[17] D. Voiculescu, “Asymptotically commuting finite rank unitary operators without commuting approximants,” *Acta Sci. Math.*, vol. 45, pp. 429-431, 1983.