From Ordinary AWGN Codes to Optimal MIMO Wiretap Schemes

Anatoly Khina
EE—Systems Dept., TAU
Tel Aviv, Israel
Email: anatolyk@eng.tau.ac.il

Yuval Kochman
School of CSE, HUJI
Jerusalem, Israel
Email: yuvalko@cs.huji.ac.il

Ashish Khisti
ECE Dept., U. of Toronto
Toronto, ON M5S 3G4, Canada
Email: akhisti@comm.utoronto.ca

***Abstract*—The problem of sending a secret message over the Gaussian multiple-input multiple-output wiretap channel is studied. In a recent work, we have proposed a layered coding scheme where a scalar wiretap code is used in each layer, and successive interference cancellation (SIC) is carried at the legitimate receiver. By a proper rate allocation across the layers, we showed that this scheme satisfies the secrecy constraint at the eavesdropper and achieves the secrecy capacity. However, the existence of the scalar codes was based upon a random coding argument. In this work we take a further step and show how the scheme can be based upon any codes that are good for the ordinary (non-secrecy) additive white Gaussian noise channel. As any stage of the SIC process is equivalent to achieving a corner point of a Gaussian multiple-access channel (MAC) capacity region, the class of codes used needs to be good for the MAC under SIC. Since in the secrecy analysis of our layered scheme, it suffices at each stage to consider a genie-aided eavesdropper that performs SIC, the coding task reduces to guaranteeing secrecy for corner points of induced MACs to the eavesdropper. Structured generation of such codes from ordinary ones is discussed.**

I. Introduction

The wiretap channel (WTC), introduced by Wyner [1], comprises a sender ("Alice") who wishes to convey data to a legitimate user ("Bob"), s.t. the eavesdropper ("Eve") can gain no information of this data. The solution to the Gaussian case was given in [2]. Its vector extension to the multiple-input multiple-output (MIMO) Gaussian WTC was given in [3]–[5].

Although capacity is well understood, it is less clear how to construct codes for WTCs. For the scalar Gaussian case, various approaches have been suggested, see, *e.g.*, [6]–[8] and references therein. The recent work of Tyagi and Vardy in [8] is particularly appealing, since it uses a black-box approach: it takes any code that is good for the ordinary (non-secrecy) additive white Gaussian noise (AWGN) channel, and turns it into a good wiretap code using an apropos hashing procedure.

However, assuming such a scalar code exists, how do we extend it to the vector case? Do we need to construct different codes for every channel matrix? In [9] we have presented a scheme based on scalar random-binning wiretap codes, in conjunction with a linear encoder and a successive interference cancellation (SIC) decoder, that approaches the MIMO wiretap capacity. Interestingly, the proof that Eve cannot extract information also hinges on the optimality of the SIC procedure, this time in a "genie-aided" setting: after Eve extracts all possible information from a stream, the content of that stream is revealed to her for the sake of trying to decode the next streams. We note that at any stage of a SIC decoding process, the decoder sees a multiple-access channel (MAC) where the inputs are the streams that are not decoded yet. Thus, the optimality of the scheme is intimately related to that of a scheme for the MAC. Using a random coding argument, we establish the existence of a secrecy-capacity achieving codebook, where in each layer it is optimal for the genie-aided Eve to treat the higher layers as noise. Unfortunately, this guarantees only the *existence* of good scalar codes.

In this work, we use this scheme for the MIMO WTC as a baseline. However, we replace the random scalar codes by an explicit construction based on any ordinary AWGN codes. While the focus in the present paper is on achieving the weak notion of secrecy, as noted in [9], strong secrecy can also be attained by restricting our decompositions to be of a specific form, as will be commented later in the paper. Our framework thereby extends the result of [8] to the vector case. Indeed, the extension to this case is not trivial. The key point is that, as with random-binning codes, when any good set of codes is used, a "genie-aided" Eve cannot do better than follow a SIC process. Hence, we focus on structured codes where SIC is optimal for the MAC channel. However, the construction of such is also not immediate. Not any collection of good AWGN codes is good for any Gaussian MAC (see, *e.g.*, [10]): if the codebooks have structure (as they should, in practice), the signal resulting from one code may not look as noise when decoding the other; this compromises MAC decoding, whose optimality is needed both for the "Bob" and "Eve" parts of the secrecy proofs. This effect can be circumvented by a dithering process, which makes sure that codewords play the part of "independent noise" when decoding a different codebook. We thus define a class of MAC WTC codes that have both good individual secrecy properties, and mutual independence; such codebook sets can be obtained from any set of good AWGN codebooks by a two-stage process of hashing and dithering.

II. Definitions

A. Secrecy

Given a memoryless channel from x to y_B and y_E, a scheme that achieves (ϵ, δ)-weak secrecy is defined as follows. Let $\mathcal{M} = \{1, \ldots, 2^{nR}\}$. The encoder is given by a (possibly random) mapping $x^n = g(m)$, known to Alice, Bob and Eve. The message m is assumed to be chosen uniformly over $\mathcal{M}$.

Then, the scheme must satisfy:

1) There exist decoders from y_B^n s.t. the average error probability in decoding m is at most δ
2) $I(m; y_E^n) \leq n\epsilon$

The secrecy capacity of the channel is the supremum over rates s.t. for any $\epsilon, \delta > 0$ there exists a secrecy scheme.

In this work we shall concentrate on a class of schemes that we call *fully recoverable*. Indeed, all of the coding proofs and techniques for the Gaussian WTC that we are aware of fall into this category. Let $\mathcal{F} = \{1, \ldots, 2^{n\tilde{R}}\}$. A codebook $\mathcal{C}$ of rate $R + \tilde{R}$ is indexed by (m, f); both the codebook and the indexing are known to Alice, Bob and Eve. Given a message m, Alice draws a fictitious message f uniformly over $\mathcal{F}$ and transmits the corresponding codeword. Bob decodes, with low error probability, the pair (m, f), and then discards f.

B. Channels and Capacities

In the scalar Gaussian wiretap problem, the channels from Alice to Bob and Eve are given by

$$y_B = h_B x + z_B \tag{1a}$$
$$y_E = h_E x + z_E\,, \tag{1b}$$

where h_B and h_E are complex scalar gains, z_B and z_E are mutually-independent circularly-symmetric standard AWGNs and the transmission is subject to a unit power constraint. Then, the capacity is given by

$$C_S(h_B, h_E) = \left[\mathrm{C}\left(|h_B|^2\right) - \mathrm{C}\left(|h_E|^2\right)\right]_+\,,$$

where $[x]_+ \triangleq \max\{0, x\}$ and $\mathrm{C}(S) = \log(1+S)$ is the AWGN capacity at SNR S.

The Gaussian MIMO WTC is given by

$$\boldsymbol{y}_B = \mathbf{H}_B \boldsymbol{x} + \boldsymbol{z}_B \tag{2a}$$
$$\boldsymbol{y}_E = \mathbf{H}_E \boldsymbol{x} + \boldsymbol{z}_E, \tag{2b}$$

where $\boldsymbol{x}$, $\boldsymbol{y}_B$ and $\boldsymbol{y}_E$ are complex-valued vectors with dimensions of the number of antennas in the terminals of Alice, Bob and Eve, denoted by N_A, N_B, and N_E, respectively. The channel matrices $\mathbf{H}_B$ and $\mathbf{H}_E$ have the corresponding dimensions. The additive noise vectors $\boldsymbol{z}_B$ and $\boldsymbol{z}_E$ are mutually independent with i.i.d. circularly-symmetric Gaussian elements of unit variance. Finally, the transmission is subject to a total (over all antennas) unit power constraint. The capacity of this channel is given by:

$$C_S(\mathbf{H}_B, \mathbf{H}_E) \triangleq \max_{\mathbf{K}:\ \mathrm{trace}\{\mathbf{K}\} \leq 1} I(\mathbf{H}_B, \mathbf{K}) - I(\mathbf{H}_E, \mathbf{K})\,, \tag{3}$$

where $I(\mathbf{H}, \mathbf{K}) = \log\left|\mathbf{I} + \mathbf{H}\mathbf{K}\mathbf{H}^\dagger\right|$. Thus, capacity is given by the difference of MIs to Bob and Eve, optimized over all Gaussian channel inputs that satisfy the power constraint.

C. Gaussian MAC Model

The N-user Gaussian MAC WTC is given by

$$y_B = \sum_{k=1}^{N} h_{B;k} x_k + z_B \tag{4a}$$
$$y_E = \sum_{k=1}^{N} h_{E;k} x_k + z_E\,, \tag{4b}$$

where x_k is the channel input of user k ($k = 1, \ldots, N$) subject to an average unit power constraint, and z_B and z_E are circularly-symmetric AWGNs of unit power. A scheme with rates $\mathbf{R} \triangleq (R_1, \ldots, R_N)$ is defined by (possibly random) mappings $x_k^n = g_k(m_k)$ where $m_k \in \mathcal{M}_k \triangleq \left\{1, \ldots, 2^{nR_k}\right\}$.

Without secrecy constraints, the MAC capacity region of (4a) is given by the convex hull of the "corner points" [11]:

$$\boldsymbol{S}\left(\{h_{B;k}\}\right) \triangleq \left\{ \mathbf{R} \;\middle|\; \begin{array}{l} R_k = \mathrm{C}\left(\frac{|h_{B;k}|^2}{1+\sum_{\pi(\ell)<\pi(k)}|h_{B;\ell}|^2}\right) \\ k = 1, \ldots, N; \quad \forall \pi \in S_N \end{array} \right\} \tag{5}$$

where S_N is the symmetric group of degree N (all possible orderings of $\{1, \ldots, N\}$). The sum-capacity of this channel,

$$C^{\mathrm{sum}}\left(\{h_{B;k}\}_{k=1}^N\right) = \mathrm{C}\left(\sum_{k=1}^{N} |h_{B;k}|^2\right)\,,$$

is achieved at any corner point in $\boldsymbol{S}(\{h_{B;k}\})$. We further define the corner-points dominated region $\boldsymbol{S}_\epsilon(\{h_{B;k}\})$:

$$\boldsymbol{S}_\epsilon\left(\{h_{B;k}\}\right) \triangleq \left\{\mathbf{R} \;\middle|\; \exists \mathbf{r} \in \boldsymbol{S},\, R_k \leq r_k - \epsilon\,, k \in \{1, \ldots, N\}\right\}$$

An (ϵ, δ)-weak secrecy scheme for the MAC WTC (4) is defined as in the point-to-point case, with the requirements enforced on all the messages. We also define a fully-recoverable scheme as the obvious extension of the single-user case, using fictitious message sets $\mathcal{F}_k \triangleq \left\{1, \ldots, 2^{n\tilde{R}_k}\right\}$. The capacity region is the closure of rate points s.t. there exists a secrecy scheme for any $\epsilon, \delta > 0$. This region is yet to be found; nevertheless, for the Gaussian MAC (4), the superposition secrecy sum-rate is

$$R_S^{\mathrm{sum}}\left(\{(h_{B;k}, h_{E;k})\}\right) = C^{\mathrm{sum}}\left(\{h_{B;k}\}\right) - C^{\mathrm{sum}}\left(\{h_{E;k}\}\right) \tag{6}$$

III. Good Codes for MAC/WTC

In this section we address coding for the Gaussian point-to-point WTC, for the Gaussian MAC, and for the Gaussian MAC WTC. We discuss the additional coding challenges compared to ordinary AWGN, define classes of good codes, and present ways to obtain such codes from ordinary AWGN codes.

A. Point-to-Point Gaussian WTC

We start with the Gaussian SISO WTC (1). Clearly, if we use a fully recoverable scheme, the codebook $\mathcal{C}$ must be good for Bob's channel. It turns out that the additional requirement in the following (non-secrecy) definition is sufficient.

Definition 1 (Two-level AWGN codes): A two-level AWGN code of rates $(R, \tilde{R})$ and error probabilities (δ_1, δ_2) for the channel pair (1) is a mapping $x^n = g(m, f)$, where $m \in \mathcal{M}$, $f \in \mathcal{F}$ and $x^n \in \mathbb{R}^n$, such that there exist decoders of (m, f) from y_B^n, and of f from (m, y_E^n), with error probabilities δ_1 and δ_2, respectively.

Proposition 1: For any Gaussian WTC (1), let $g(\cdot, \cdot)$ be a two-level AWGN code of rates $(R, \tilde{R})$ and error probabilities (δ_1, δ_2) and denote $\tilde{\epsilon} \triangleq \mathrm{C}\left(|h_E|^2\right) - \tilde{R}$. Then, the mapping

can be used as a code for a fully-recoverable secrecy scheme, which achieves (ϵ, δ_1) secrecy, where ϵ can be made arbitrarily small by taking small enough δ_2 and $\tilde{\epsilon}$.

Proof: The secrecy rate R of this code is indeed $1/n \log |\mathcal{M}| = R$. Bob can decode (m, f) with small error probability δ_1, by definition.

The leakage rate can be bounded from below, as follows:

$$\begin{aligned} H\left(m|y_E^n\right) &= I\left(x^n; m|y_E^n\right) + H\left(m|x^n, y_E^n\right) && \text{(7a)} \\ &= I\left(x^n; m, y_E^n\right) - I\left(x^n; y_E^n\right) && \text{(7b)} \\ &= H\left(x^n\right) - H\left(f|m, y_E^n\right) - I\left(x^n; y_E^n\right) && \text{(7c)} \\ &\geq n\left(R + \tilde{R}\right) - n\epsilon_2 - n\mathsf{C}\left(|h_E|^2\right) && \text{(7d)} \\ &\geq nR - n\epsilon_2 - n\tilde{\epsilon} && \text{(7e)} \\ &\geq H\left(m\right) - n\left(\epsilon_2 + \tilde{\epsilon}\right), && \text{(7f)} \end{aligned}$$

where (7c) follows from the invertibility of the mapping g and (7d) is due to Fano's inequality with ϵ_2 vanishing with δ_2. ■

We now describe a randomized procedure to construct two-level good AWGN codes from any good AWGN code. Let the base codebook $\mathcal{C}_0$ be some good AWGN codebook of rate R_0 satisfying $R + \tilde{R} < R_0 < \mathsf{C}\left(|h_E|^2\right)$. Now, for any $(m, f) \in \mathcal{M} \times \mathcal{F}$ draw a random index $\theta(m, f)$ in $1, \ldots, 2^{nR_0}$. The average codebook is a two-level good AWGN code. Thus, there must exist good choices of θ.

A low-complexity structured approach for constructing such maps for discrete channels is given by two-universal hash functions [12], [13]; it has recently been extended to the Gaussian WTC in [8].

B. Gaussian MAC

We now consider the Gaussian MAC (4a). By time-sharing arguments, it is enough to consider coding for the corner points (5). The rate expression immediately gives rise to a SIC procedure: if the yet-undecoded codebooks can be considered as AWGN, then each codebook should be capacity achieving for an AWGN channel. When using a random-coding argument, indeed codebooks are drawn i.i.d. Gaussian. But what if we want to use specific AWGN-good codebooks?

Unfortunately, in that case the process may fail due to codebook alignment. For example, assume that (4a) gives

$$y_B = x_1 + x_2 + z.$$

Now further assume that the two codebooks are nested lattices. In that case (up to shaping), any possible point of $x_1 + x_2$ is also a point of the higher-rate code, thus one codebook cannot be decoded without the other.

The following family of codes allows to approach the corner points. It is a relaxation of the "MAC capacity-achieving codes" [10], since only corner points are considered.

Definition 2 (MAC-SIC codes): A set of codebooks $\mathcal{C} \triangleq (\mathcal{C}_1, \ldots, \mathcal{C}_N)$ of rates $\mathbf{R} \triangleq (R_1, \ldots, R_N)$ is said to be an (ϵ, δ) MAC-SIC code, if there exists a decoder of $\mathcal{C}$ with error probability at most δ, for any MAC s.t. $\mathbf{R} \in \boldsymbol{S}_\epsilon\left(h_{B;1}, \ldots, h_{B;N}\right)$.

Taking such codes with small ϵ and δ allows to approach the MAC capacity region. Intuitively speaking, such good codes are a collection of codes good for the AWGN channel that are sufficiently different, such that no MAC gains can align them. Thus, they can be constructed from any individual AWGN-good codes by introducing proper inter-codebook randomization. For example, using a modulo-lattice operation in conjunction with subtractive random dither, each codebook becomes (for the purpose of SIC) an independent noise, distributed uniformly over the lattice cell; in the high-dimensional limit this noise is close to Gaussian, and the gap at any finite dimension can be quantified. In practice, simpler randomization such as multiplicative phase dithering, or interleaving, suffice.

C. Gaussian MAC WTC

We now turn to the MAC WTC (4). When coding for this channel, we should consider both two-level and alignment issues; thus we define codes that combine the properties of two-level AWGN codes of Definition 1 with the MAC-SIC codes of Definition 2.

Definition 3 (Two-level MAC-SIC codes): Define $\mathcal{M}_k = \{1, \ldots, 2^{nR_k}\}$ and $\mathcal{F}_k = \{1, \ldots, 2^{n\tilde{R}_k}\}$, for $k = 1, \ldots, N$. Two-level MAC-SIC codes, of rate-pairs $\left\{(R_k, \tilde{R}_k) \middle| k = 1, \ldots, N\right\}$, with parameters $(\epsilon, \delta_1, \delta_2)$ are mappings $x_k^n = g_k(m_k, f_k)$, where $m_k \in \mathcal{M}_k$, $f_k \in \mathcal{F}_k$ and $x^n \in \mathbb{R}^n$, such that:

1) MAC-SIC: There exist decoders of $\{(m_k, f_k)\}$ from y_B^n, with error probability at most δ_1, provided that $(R_1 + \tilde{R}_1, \ldots, R_{N_A} + \tilde{R}_N) \in \boldsymbol{S}_\epsilon\left(h_{B;1}, \ldots, h_{B;N}\right)$
2) Two-level: There exist decoders of $\{f_k\}$ from $(\{m_k\}, y_E^n)$, with error probability at most δ_2, provided that $(\tilde{R}_1, \ldots, \tilde{R}_N) \in \boldsymbol{S}_\epsilon\left(h_{E;1}, \ldots, h_{E;N}\right)$

Proposition 2: Two-level MAC-SIC codes with $\mathbf{R}$ and $\tilde{\mathbf{R}}$ approaching (any) corner points in $\boldsymbol{S}\left(\{h_{B;k}\}\right)$ and $\boldsymbol{S}\left(\{h_{E;k}\}\right)$, respectively, with $\delta_1, \delta_2, \epsilon \to 0$, allow to approach the superposition sum-rate (6).

The proof of Proposition 2 is a straightforward adaptation of the proof of Proposition 1.

A key property of these codes that we shall need for MIMO analysis, is the following.

Lemma 1: Let $\{x_k^n\}$ be two-level MAC-SIC codes with parameters $(\epsilon, \delta_1, \delta_2)$. Let y_E^n be the output of the MAC (4b), with coefficients $\{h_{E;k}\}$ s.t.

$$\exists \mathbf{r} \in \boldsymbol{S}\left(\{h_{E;k}\}_{k=1}^N\right) : \left\{\tilde{R}_k \geq r_k - \epsilon,\ \forall\ k = 1, \ldots, N\right\} \quad (8)$$

Then,

$$h\left(y_E^n \middle| \{m_k\}_{k=1}^N\right) \geq n \log\left(\pi e\left[1 + \sum_{k=1}^N |h_{E;k}|^2\right]\right) - n\epsilon_2$$

where ϵ_2 goes to zero for $\epsilon, \delta_2 \to 0$.

This result is an extension to the two-level case of [10, Lemma 1]. This, in turn, is stated for Gaussian codebooks. However, as stated in [10, Theorem 3] the analysis holds for any "MAC-capacity achieving codes". Indeed, our MAC-SIC definition is weaker, but suffices in the case of rate points that satisfy the corner-point condition (8).

Two-level MAC-SIC codes can be generated from two-level point-to-point codes (of Definition 1) by a dithering process, the same way that MAC-SIC codes can be generated

from point-to-point codes without secrecy; see Section III-B. Indeed, it is not hard to see that the dithering process makes the interfering codebooks appear as noise at both code levels simultaneously. Thus, two-level MAC-SIC codes can be generated from ordinary (non-secrecy) point-to-point code via a double-randomization process of mapping and dithering; in practice, as explained in Sections III-A and III-B, these processes can be made efficient.

IV. Scalar Codes for MIMO Channels

In this section we briefly review the connection between matrix decompositions and scalar transmission schemes, without secrecy requirements. For a more thorough account, see [14].

Consider the MIMO channel (2a), with some input covariance matrix $\mathbf{K}$. Construct the augmented matrix[1]

$$\mathbf{G}_B \triangleq \begin{pmatrix} \mathbf{H}_B\mathbf{K}^{1/2} \\ \mathbf{I} \end{pmatrix}, \tag{9}$$

and choose some unitary matrix $\mathbf{V}$ (for considerations for choosing $\mathbf{V}$, see [9]). Apply the QR decomposition to $\mathbf{G}_B\mathbf{V}$:

$$\mathbf{G}_B\mathbf{V} = \mathbf{U}_B\mathbf{T}_B\,,$$

where $\mathbf{U}_B$ is unitary and $\mathbf{T}_B$ is upper-triangular. Now let $\tilde{\boldsymbol{x}}$ be a vector of standard Gaussian variables, and set

$$\boldsymbol{x} = \mathbf{K}^{1/2}\mathbf{V}\tilde{\boldsymbol{x}}\,. \tag{10}$$

Denote by $\tilde{\mathbf{U}}_B$ the sub-matrix consisting of the upper-left $N_B \times N_A$ block of $\mathbf{U}_B$, define $\tilde{\mathbf{T}} = \tilde{\mathbf{U}}_B^\dagger\mathbf{K}^{1/2}\mathbf{V}$, and let

$$\tilde{\boldsymbol{y}}_B = \tilde{\mathbf{U}}_B^\dagger\boldsymbol{y}_B = \tilde{\mathbf{U}}_B^\dagger\mathbf{K}^{1/2}\mathbf{V}\tilde{\boldsymbol{x}} + \tilde{\mathbf{U}}_B^\dagger\boldsymbol{z}_B = \tilde{\mathbf{T}}\tilde{\boldsymbol{x}} + \tilde{\boldsymbol{z}}_B\,. \tag{11}$$

Since $\tilde{\mathbf{U}}_B$ is not unitary, the statistics of $\tilde{\boldsymbol{z}} \triangleq \tilde{\mathbf{U}}_B^\dagger\boldsymbol{z}$ differ from those of $\boldsymbol{z}$, and its covariance matrix is given by $\mathbf{K}_{\tilde{\boldsymbol{z}}} \triangleq \tilde{\mathbf{U}}_B\tilde{\mathbf{U}}_B^\dagger$. Now, for $i = 1, \ldots, N_A$, define

$$\begin{aligned} y'_{B;i} &= \tilde{y}_{B;i} - \sum_{\ell=i+1}^{N_A} \tilde{T}_{i,\ell}\tilde{x}_\ell \\ &= \tilde{T}_{i,i}\tilde{x}_i + \sum_{\ell=1}^{i-1}\tilde{T}_{i,\ell}\tilde{x}_\ell + \tilde{z}_i \triangleq \tilde{T}_{i,i}\tilde{x}_i + z_i^{\text{eff}}\,. \end{aligned} \tag{12}$$

In this scalar channel from $\tilde{x}_i$ to $y'_{B;i}$, we see other $\tilde{x}_\ell$ as "interference", $\tilde{z}_i$ — as "noise", and their sum z_i^{eff} — as "effective noise". The resulting signal-to-interference-and-noise ratio (SINR) is given by:

$$S_i \triangleq \frac{(\tilde{T}_{i,i})^2}{K_{\boldsymbol{z}^{\text{eff}};i,i}} \triangleq \frac{(\tilde{T}_{i,i})^2}{K_{\tilde{\boldsymbol{z}};i,i} + \sum_{\ell=1}^{i-1}(\tilde{T}_{i,\ell})^2}\,,$$

where $K_{\tilde{\boldsymbol{z}};i,j}$ denotes the (i,j) entry of $\mathbf{K}_{\tilde{\boldsymbol{z}}}$. The following key result achieves the MI (see, *e.g.*, [14, Lemma III.3])

$$I\left(\tilde{x}_i; \boldsymbol{y}_B \middle| \tilde{x}_{i+1}^{N_A}\right) = I\left(\tilde{x}_i; y'_{B;i}\right) = \log(b_i^2) \tag{13}$$

where $\{b_i\}$ are the diagonal values of $\mathbf{T}_B$, such that

$$\sum_{i=1}^{N_A}\log\left(b_i^2\right) = \sum_{i=1}^{N_A}\log\left(1+S_i\right) = I(\mathbf{H}_B, \mathbf{K})\,,$$

which equals the channel capacity for the optimal $\mathbf{K}$.

This gives rise to the following scheme, which is, in turn, a variant of the renowned V-BLAST/GDFE scheme.

Scheme 1 (MIMO comm. without secrecy constraint):

Offline: construct N_A scalar codes.

Alice: At each time instance:

- Forms $\tilde{\boldsymbol{x}}$, using one sample from each codebook
- Transmits $\boldsymbol{x}$ according to (10): $\boldsymbol{x} = \mathbf{K}^{1/2}\mathbf{V}\tilde{\boldsymbol{x}}$

Bob:

- At each time instance forms $\tilde{\boldsymbol{y}}_B$ according to (11).
- The codebooks are decoded using SIC, from last ($i = N_A$) to first ($i = 1$). Assuming correct decoding of all codebooks $i+1, \ldots, N_A$, Bob forms $y'_{B;i}$ (12).

For correct decoding with high probability, we must ensure that each stage of the SIC process succeeds with high probability. To that end, we note that at any stage we have a MAC (12). Thus, MAC-SIC codes suffice.

Proposition 3: Scheme 1 allows to approach the MIMO capacity, by employing Gaussian MAC-SIC codes with $\mathbf{R}$ approaching $\boldsymbol{S}(\{\sqrt{b_k^2-1}\})$ with $\delta, \epsilon \to 0$.

V. Coding for the MIMO Wiretap Channel

In this section we present our main result: construction of capacity-achieving schemes for the MIMO WTC using good ordinary AWGN codes. Specifically, Alice and Bob utilize the V-BLAST technique presented in Section IV, where the codes are two-level MAC-SIC codes presented in Section III-C.

Theorem 1: For any $\epsilon, \delta > 0$ and any rate below $C_S(\mathbf{H}_B, \mathbf{H}_E)$ (3), one can construct a fully-recoverable (ϵ, δ)-secrecy scheme using Scheme 1 with the codebooks being two-level MAC-SIC codes as in Definition 3 of adequate rates, with sufficiently small parameters $(\epsilon, \delta_1, \delta_2)$.

The proof hinges on the optimality of a SIC process for a "genie-aided" Eve. That is, for any k, if Eve is given $\tilde{x}_{k+1}^n, \ldots, \tilde{x}_{N_A}^n$, the best she can do for obtaining information about m_k is to perform an optimal linear projection and use the resulting MAC. As in the analysis for the point-to-point case in Proposition 1, the inability to extract information about the true messages is equivalent to the ability to decode the fictitious messages given the true ones. For that we use Lemma 1, applied to the appropriate projection.

As the secrecy proof relies on SIC arguments, we need to define some quantities for Eve, parallel to those used for Bob in the previous section. Denote by $\tilde{\mathbf{T}}_E$ channel matrix of Eve which is the same as $\tilde{\mathbf{T}}$ of (12), when using Eve's channel matrix $\mathbf{H}_E$ in (9). Denote further the columns of $\tilde{\mathbf{T}}_E$ by $\{\boldsymbol{t}_{E;k}\}$. Similarly, define $\{e_k\}$ as in (13) with $\mathbf{H}_B$ replaced by $\mathbf{H}_E$.

Proof: Take two-level MAC-SIC codes of rate-pairs $R_k = \log(b_k^2) - \epsilon$ and $\tilde{R}_k = \log(e_k^2) - \epsilon$ $(k = 1, \ldots, N_A)$. The proof that Bob achieves a rate of $\sum_{k=1}^{N_A} R_k + \tilde{R}_k$ is as in the non-secret case, as the codes are in particular MAC-SIC codes.

In order to satisfy the secrecy constraint, we show that the following condition holds for $\epsilon_T = N_A \cdot \epsilon$ and large enough n

$$H\left(m_1, \ldots, m_{N_A} | \boldsymbol{y}_E\right) \geq H(m_1, \ldots, m_{N_A}) - n\,\epsilon_T\,.$$

It suffices to show that, for large enough n,

[1] $\mathbf{K}^{1/2}$ is any matrix $\mathbf{B}$ satisfying $\mathbf{B}\mathbf{B}^\dagger = \mathbf{K}$.

$$H(m_k|\boldsymbol{y}_E, m_{k+1}, \ldots, m_{N_A}) \geq H(m_k) - n\,\epsilon$$

is satisfied for $k = 1, \ldots, N_A$. Similarly to (7a)-(7b),

$$H\left(m_k|\boldsymbol{y}_E^n, m_{k+1}, \ldots, m_{N_A}\right) \geq H\left(m_k\middle|\boldsymbol{y}_E^n, \tilde{x}_{k+1}^n, \ldots, \tilde{x}_{N_A}^n\right) \tag{14a}$$

$$= I\left(\tilde{x}_k^n; m_k, \boldsymbol{y}_E^n\middle|\tilde{x}_{k+1}^n, \ldots, \tilde{x}_{N_A}^n\right) - I\left(\tilde{x}_k^n; \boldsymbol{y}_E^n\middle|\tilde{x}_{k+1}^n, \ldots, \tilde{x}_{N_A}^n\right) . \tag{14b}$$

Thus, we are left with bounding the two terms in (14b).

Denote by $\hat{\boldsymbol{t}}_{E;k} \triangleq \boldsymbol{t}_{E;K} / \left\|\boldsymbol{t}_{E;K}\right\|$ the unit vector in the direction of $\boldsymbol{t}_{E;K}$, and by $z_k \triangleq \left\langle \hat{\boldsymbol{t}}_{E;k}, \boldsymbol{z}_E \right\rangle$ the noise component in the same direction. Denote also $\tau_{k,\ell} \triangleq \left\langle \hat{\boldsymbol{t}}_{E;k}, \boldsymbol{t}_{E;\ell} \right\rangle$. Then, the first term in (14b) can be bounded from below as

$$I\left(\tilde{x}_k^n; m_k, \boldsymbol{y}_E^n\middle|\tilde{x}_{k+1}^n, \ldots, \tilde{x}_{N_A}^n\right) \geq I\left(\tilde{x}_k^n; m_k, \left\langle \hat{\boldsymbol{t}}_{E;k}, \boldsymbol{y}_E^n \right\rangle\middle|\tilde{x}_{k+1}^n, \ldots, \tilde{x}_{N_A}^n\right) \tag{15a}$$

$$= I\left(\tilde{x}_k^n; m_k, \sum_{\ell=1}^{k} \tau_{k,\ell}\tilde{x}_\ell^n + z_k\right) \tag{15b}$$

$$= I\left(\tilde{x}_k^n; m_k\right) + I\left(\tilde{x}_k^n; \sum_{\ell=1}^{k} \tau_{k,\ell}\tilde{x}_\ell^n + z_k \middle| m_k\right) \tag{15c}$$

$$= H\left(m_k\right) + h\left(\sum_{\ell=1}^{k} \tau_{k,\ell}\tilde{x}_\ell^n + z_k \middle| m_k\right) - h\left(\sum_{\ell=1}^{k} \tau_{k,\ell}\tilde{x}_\ell^n + z_k \middle| m_k, \tilde{x}_k^n\right) \tag{15d}$$

$$\geq n\left[\log\left(\frac{b_k^2}{e_k^2}\right) - \epsilon\right] + h\left(\sum_{\ell=1}^{k} \tau_{k,\ell}\tilde{x}_\ell^n + z_k \middle| \{m_\ell\}_{\ell=1}^k\right) - h\left(\sum_{\ell=1}^{k-1} \tau_{k,\ell}\tilde{x}_\ell^n + z_k\right) . \tag{15e}$$

We now bound the two entropy terms. For this, denote by $\tilde{\chi}_k^n$ tuples of i.i.d. Gaussian random variables with the same average (over n) power as of $\tilde{x}_k^n$.

$$h\left(\sum_{\ell=1}^{k-1} \tau_{k,\ell}\tilde{x}_\ell^n + z_k\right) \leq h\left(\sum_{\ell=1}^{k-1} \tau_{k,\ell}\tilde{\chi}_\ell^n + z_k\right) \tag{16a}$$

$$h\left(\sum_{\ell=1}^{k} \tau_{k,\ell}\tilde{x}_\ell^n + z_k \middle| \{m_\ell\}_{\ell=1}^k\right) \geq h\left(\sum_{\ell=1}^{k} \tau_{k,\ell}\tilde{\chi}_\ell^n + z_k\right) - n\epsilon_2 \tag{16b}$$

where (16a) holds since the Gaussian distribution maximizes entropy; (16b) follows from Lemma 1 by noting that the rates $\{\tilde{R}_\ell\}$ satisfy (8) for coefficients $\{\tau_{\ell,\ell}\}$, and hence (8) is satisfied for $\{\tau_{k,\ell}\}$ which can only be smaller.

Thus, using (15) and (16), we have

$$I\left(\tilde{x}_k^n; m_k, \boldsymbol{y}_E^n\middle|\tilde{x}_{k+1}^n, \ldots, \tilde{x}_{N_A}^n\right) \geq h\left(\sum_{\ell=1}^{k} \tau_{k,\ell}\tilde{\chi}_\ell^n + z_k\right) - h\left(\sum_{\ell=1}^{k-1} \tau_{k,\ell}\tilde{\chi}_\ell^n + z_k\right) + n\left[\log\left(\left(b_k^2/e_k^2\right)\right) - \epsilon\right] - n\epsilon_2 \tag{17a}$$

$$= n\left[\log\left(\frac{b_k^2}{e_k^2}\right) - \epsilon - \epsilon_2\right] + I\left(\tilde{\chi}_k^n; \sum_{\ell=1}^{k} \tau_{k,\ell}\tilde{\chi}_\ell^n + z_k\right) \tag{17b}$$

$$= n\log\left(b_k^2\right) - n\left(\epsilon + \epsilon_2\right) , \tag{17c}$$

where (17c) follows from the definition of e_k.

We are left now with bounding from the above the second term in (14b), which is equal, in turn, to

$$I\left(\tilde{x}_k^n; \boldsymbol{y}_E^n\middle|\tilde{x}_{k+1}^n, \ldots, \tilde{x}_{N_A}^n\right) = I\left(\tilde{x}_k^n; \sum_{\ell=1}^{k} \boldsymbol{t}_{E;\ell}\tilde{x}_\ell^n + \boldsymbol{z}_E\right) .$$

Lemma 2: For $k = 1, \ldots, N_A$:

$$I\left(\tilde{\chi}_k^n; \sum_{\ell=1}^{k} \boldsymbol{t}_{E;\ell}\tilde{\chi}_\ell^n + \boldsymbol{z}_E\right) - n\epsilon \leq I\left(\tilde{x}_k^n; \sum_{\ell=1}^{k} \boldsymbol{t}_{E;\ell}\tilde{x}_\ell^n + \boldsymbol{z}_E\right) \leq I\left(\tilde{\chi}_k^n; \sum_{\ell=1}^{k} \boldsymbol{t}_{E;\ell}\tilde{\chi}_\ell^n + \boldsymbol{z}_E\right) + n\epsilon .$$

The proof of this lemma can be found in [15]. Combining with (14b) and (15), the proof is completed. ■

Remark 1 (Orthogonalizing Eve's channel): If we choose in Scheme 1 the unitary matrix $\mathbf{V}$ according to the SVD of Eve's channel $\mathbf{H}_E\mathbf{K}^{1/2}$, the channel from $\tilde{\boldsymbol{x}}$ to $\tilde{\boldsymbol{y}}_E$ becomes diagonal, see [9, Section III]. In that case, Eve receives independent observations of the codebooks, thus the secrecy proof simplifies considerably. Furthermore, if the individual codebooks yield *strong secrecy*, the MIMO scheme will automatically have the same property. Indeed, strong-secrecy codes for the AWGN can be constructed, *e.g.* by the method of [8].

REFERENCES

[1] A. D. Wyner. The wiretap channel. *IEEE Trans. Info. Theory*, 54:1355–1387, 1975.

[2] S. K. Leung-Yan-Cheong and M. E. Hellman. The Gaussian wiretap channel. *IEEE Trans. Info. Theory*, 24:451–456, 1978.

[3] A. Khisti and G. W. Wornell. Secure transmission with multiple antennas—part II: The MIMOME wiretap channel. *IEEE Trans. Info. Theory*, 56:5515–5532, 2010.

[4] F. Oggier and B. Hassibi. The secrecy capacity of the MIMO wiretap channel. *IEEE Trans. Info. Theory*, 57:4961–4972, 2011.

[5] T. Liu and S. Shamai. A note on the secrecy capacity of the multiple-antenna wiretap channel. *IEEE Trans. Info. Theory*, 55:2547–2553, 2009.

[6] D. Klinc, H. Jeongseok, S. W. McLaughlin, J. Barros, and B.-J Kwak. LDPC codes for the Gaussian wiretap channel. *IEEE Trans. Info. Theory*, 6:532–540, 2011.

[7] F. Oggier, P. Solé, and J.-C. Belfiore. Lattice codes for the wiretap Gaussian channel: Construction and analysis. *IEEE Trans. Info. Theory*, Submitted, Jan. 2013. Available: http://arxiv.org/abs/0708.4219.

[8] H. Tyagi and A. Vardy. Explicit capacity-achieving coding scheme for the Gaussian wiretap channel. In *Proc. IEEE Int. Symp. on Info. Theory (ISIT)*, Honolulu, HI, USA, June/July 2014.

[9] A. Khina, Y. Kochman, and A. Khisti. Decomposing the MIMO wiretap channel. In *Proc. IEEE Int. Symp. on Info. Theory (ISIT)*, Honolulu, HI, USA, June/July 2014.

[10] F. Baccelli, A. El Gamal, and D. N. C. Tse. Interference networks with point-to-point codes. *IEEE Trans. Info. Theory*, 57:2582–2596, 2011.

[11] H. Liao. *Multiple Access Channels*. PhD thesis, Department of Electrical Engineering, University of Hawaii, Honolulu, 1972.

[12] M. Bellare, S. Tessaro, and A. Vardy. Semantic security for the wiretap channel. In *Proc. CRYPTO, LNCS*, volume 7417, pages 294–311, 2012.

[13] M. Hayashi and R. Matsumoto. Construction of wiretap codes from ordinary channel codes. In *Proc. Int. Symp. Info. Theory (ISIT), Austin, TX*, pages 2538–2542, June 2010.

[14] Y. Jiang, W. Hager, and J. Li. Uniform channel decomposition for MIMO communications. *IEEE Trans. Sig. Proc.*, 53:4283–4294, 2005.

[15] A. Khina, Y. Kochman, and A. Khisti. Technical report, May 2014. Available: www.eng.tau.ac.il/∼anatolyk/papers/wiretap_itw2014.pdf.