On Gaussian MIMO Compound Wiretap Channels

Ersen Ekrem Sennur Ulukus
Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742
ersen@umd.edu *ulukus@umd.edu*

***Abstract*— We study the two-user one-eavesdropper discrete memoryless compound wiretap channel, where the transmitter sends a common confidential message to both users, which needs to be kept perfectly secret from the eavesdropper. We provide a new achievable secrecy rate which is shown to be potentially better than the best known lower bound for the secrecy capacity of this compound wiretap channel. We next consider the two-user one-eavesdropper Gaussian multiple-input multiple-output (MIMO) compound wiretap channel. We obtain an achievable secrecy rate for the Gaussian MIMO compound wiretap channel by using dirty-paper coding (DPC) in the achievable scheme we provided for the discrete memoryless case. We show that the corresponding achievable secrecy rate achieves at least half of the secrecy capacity of the two-user one-eavesdropper Gaussian MIMO wiretap channel. We also obtain the secrecy capacity of the two-user one-eavesdropper Gaussian MIMO compound wiretap channel when the eavesdropper is degraded with respect to one of the two users.**

I. Introduction

The compound wiretap channel consists of a user and an eavesdropper, where there are a finite number of channel states determining the channel transition probability distribution. The channel state is assumed to be fixed during the entire transmission and known at the receivers, but not at the transmitter. The goal of the transmitter in the compound wiretap channel is to ensure a perfect secrecy rate irrespective of the channel state realization. In addition to this definition, the compound wiretap channel admits another interpretation. Regarding each channel state as a user and eavesdropper pair, the compound wiretap channel can be viewed as a wiretap channel with a group of users and a group of eavesdroppers, where the transmitter sends a common confidential message to the users while keeping all eavesdroppers ignorant of this message. In this paper, we adopt this interpretation.

The compound wiretap channel is first studied in [1], [2], which consider the parallel wiretap channel with two sub-channels where each sub-channel is wiretapped by a different eavesdropper. Recent works on compound wiretap channels are [3]–[11]. Reference [3] studies the fading wiretap channel with many receivers, [4]–[6] consider the transmission of a common confidential message to many legitimate receivers in the presence of a single eavesdropper, [7] focuses on two-user one-eavesdropper and one-user two-eavesdropper scenarios. Reference [8] considers the general discrete memoryless compound wiretap channel and provides inner and outer bounds for the secrecy capacity. In addition to these inner and outer bounds, [8] also establishes the secrecy capacity of the degraded compound wiretap channel as well as its degraded Gaussian multiple-input multiple-output (MIMO) instance. Another work on the compound wiretap channel is [9] where the secrecy capacity of a class of non-degraded Gaussian parallel compound wiretap channels is established, and an upper bound for the secrecy capacity of the discrete memoryless compound wiretap channel is proposed. Recently, compound multi-receiver wiretap channels, where there are two groups of users and a group of eavesdroppers, and each group of users receives a confidential message, have been studied in [10], [11].

Here, we first consider the two-user one-eavesdropper discrete memoryless compound wiretap channel. Recently, [7] proposed an achievable scheme for this compound wiretap channel. The achievable scheme in [7] uses indirect decoding [12] and Marton's inner bound for discrete memoryless broadcast channels [13]. In [7], it is shown that this achievable scheme provides a strictly better achievable secrecy rate than the one in [8], which corresponds to an extension of the Csiszar-Korner achievable scheme in [14] to a compound setting. To the best of our knowledge, the achievable scheme in [7] constitutes the best known lower bound for the secrecy capacity of the two-user one-eavesdropper discrete memoryless compound wiretap channel. Here, we provide a new achievable scheme which is potentially better than this best known lower bound in [7]. In other words, the secrecy rate our scheme can provide is always as large as the secrecy rate that the achievable scheme in [7] can provide. Our achievable scheme is similar to the achievable scheme in [7] in the sense that it also uses indirect decoding [12] and Marton's inner bound [13]. However, our achievable scheme differs from the one in [7] in the way we compute the equivocation rate. In particular, at a certain step of the equivocation computation in [7], joint conditional entropy of two random variables is upper bounded by conditional individual entropies, and the proof is concluded. Here, we compute the equivocation rate without using this potentially loose outer bound, which is also the reason why the achievable scheme in this paper is potentially better than the achievable scheme in [7].

We next consider the two-user one-eavesdropper Gaussian MIMO compound wiretap channel. We first propose an achievable secrecy rate by using dirty-paper coding (DPC) [15] in the achievable scheme we provided for the discrete memoryless channel. We address the tightness of the resulting achievable

This work was supported by NSF Grants CCF 04-47613, CCF 05-14846, CNS 07-16311 and CCF 07-29127.

secrecy rate, and show that the achievable secrecy rate relying on DPC can achieve at least half of the secrecy capacity. We also consider a special class of two-user one-eavesdropper Gaussian MIMO compound wiretap channels. In channels belonging to this class, the eavesdropper is degraded with respect to one of the two users. We obtain the secrecy capacity of these channels as the minimum of the secrecy capacities of the two underlying wiretap channels in the two-user one-eavesdropper Gaussian MIMO compound wiretap channel.

II. Channel Model and Definitions

We study the two-user one-eavesdropper discrete memoryless compound wiretap channel with a transition probability $p(y_1, y_2, z|x)$ where $x \in \mathcal{X}$ is the channel input, $y_j \in \mathcal{Y}_j$ is the jth user's observation, and $z \in \mathcal{Z}$ is the eavesdropper's observation. We consider the scenario where the transmitter sends a common confidential message to both users, which needs to be kept perfectly secret from the eavesdropper.

An $(n, 2^{nR})$ code for this channel consists of one message set $\mathcal{W} = \{1, \ldots, 2^{nR}\}$, one encoder at the transmitter $f_n : \mathcal{W} \to \mathcal{X}^n$, and one decoder at each user $g_{j,n} : \mathcal{Y}_j^n \to \mathcal{W},\ j = 1, 2$. The probability of error is defined as $P_{e,n} = \max_{j=1,2} \Pr\left[g_{j,n}(f_n(W)) \neq W\right]$, where W is a uniformly distributed random variable in $\mathcal{W}$. We measure the secrecy of the message W by its equivocation rate at the eavesdropper $(1/n)H(W|Z^n)$ [14], [16].

A perfect secrecy rate R is said to be achievable if there exists an $(n, 2^{nR})$ code which has $\lim_{n\to\infty} P_{e,n} = 0$, and

$$\lim_{n\to\infty} \frac{1}{n} I(W; Z^n) = 0 \tag{1}$$

The secrecy capacity C_S is defined to be the supremum of all achievable perfect secrecy rates.

III. An Achievable Secrecy Rate

Here, we revisit the existing achievability results for two-user one-eavesdropper discrete memoryless compound wiretap channels, and provide a potentially higher achievable secrecy rate than the best known achievable secrecy rate given in [7]. The first achievable scheme for discrete memoryless compound wiretap channels is proposed in [8]. This achievable scheme can be viewed as an extension of the Csiszar-Korner achievable scheme for discrete memoryless wiretap channels [14] to compound wiretap channels. The achievable secrecy rate in [8] is stated in the following theorem.

Theorem 1 ([8], Theorem 1) *The secrecy capacity of the two-user one-eavesdropper discrete memoryless compound wiretap channel is lower bounded as follows*

$$C_S \geq \max_{U \to X \to (Y_1, Y_2, Z)} \min_{j=1,2} I(U; Y_j) - I(U; Z) \tag{2}$$

This inner bound is strictly improved in [7], where a new achievable scheme is proposed by using indirect decoding [12] and Marton's achievable scheme for discrete memoryless broadcast channels [13]. This achievable secrecy rate is stated in the following theorem.

Theorem 2 ([7], Theorem 1) *The secrecy capacity of the two-user one-eavesdropper discrete memoryless compound wiretap channel is lower bounded by the maximum of R satisfying*

$$R \leq I(V_0, V_1; Y_1) - I(V_0, V_1; Z) \tag{3}$$
$$R \leq I(V_0, V_2; Y_2) - I(V_0, V_2; Z) \tag{4}$$
$$2R \leq I(V_0, V_1; Y_1) + I(V_0, V_2; Y_2) - 2I(V_0; Z) - I(V_1; V_2|V_0) \tag{5}$$

for some (V_0, V_1, V_2) such that $(V_0, V_1, V_2) \to X \to (Y_1, Y_2, Z)$, and

$$I(V_1, V_2; Z|V_0) + I(V_1; V_2|V_0) \leq I(V_1; Z|V_0) + I(V_2; Z|V_0) \tag{6}$$

We now show that the third bound in (5) is redundant. To see this point, consider the sum of the first two bounds in (3)-(4)

$$I(V_0, V_1; Y_1) - I(V_0, V_1; Z) + I(V_0, V_2; Y_2) - I(V_0, V_2; Z) \tag{7}$$
$$= I(V_0, V_1; Y_1) + I(V_0, V_2; Y_2) - 2I(V_0; Z) - I(V_1; Z|V_0) - I(V_2; Z|V_0) \tag{8}$$
$$\leq I(V_0, V_1; Y_1) + I(V_0, V_2; Y_2) - 2I(V_0; Z) - I(V_1, V_2; Z|V_0) - I(V_1; V_2|V_0) \tag{9}$$
$$\leq I(V_0, V_1; Y_1) + I(V_0, V_2; Y_2) - 2I(V_0; Z) - I(V_1; V_2|V_0) \tag{10}$$

where (9) comes from the constraint in (6). Equation (10) implies the redundancy of the third bound in (5). Thus, Theorem 2 can be equivalently expressed as follows.

Theorem 3 ([7], Theorem 1) *The secrecy capacity of the two-user one-eavesdropper discrete memoryless compound wiretap channel is lower bounded by the maximum of R satisfying*

$$R \leq I(V_0, V_1; Y_1) - I(V_0, V_1; Z) \tag{11}$$
$$R \leq I(V_0, V_2; Y_2) - I(V_0, V_2; Z) \tag{12}$$

for some (V_0, V_1, V_2) such that $(V_0, V_1, V_2) \to X \to (Y_1, Y_2, Z)$, and

$$I(V_1, V_2; Z|V_0) + I(V_1; V_2|V_0) \leq I(V_1; Z|V_0) + I(V_2; Z|V_0) \tag{13}$$

We now provide a new achievable secrecy rate for two-user one-eavesdropper discrete memoryless compound wiretap channels. This new achievable scheme is similar to the achievable scheme given in Theorem 3 in terms of the techniques used. In particular, this new achievable scheme also uses indirect decoding [12] and Marton's inner bound for discrete memoryless broadcast channels [13]. The only new ingredient in the achievable scheme we provide here as compared to the achievable scheme in Theorem 3 is the way we compute the equivocation rate. In particular, while computing the equivocation rate in the proof of Theorem 3, one needs to show the

following

$$\lim_{n\to\infty}\frac{1}{n}H(V_1^n,V_2^n|W,V_0^n,Z^n)=0 \tag{14}$$

To this end, [7] first considers the following bound

$$\frac{1}{n}H(V_1^n,V_2^n|W,V_0^n,Z^n)\leq\frac{1}{n}H(V_1^n|W,V_0^n,Z^n)+\frac{1}{n}H(V_2^n|W,V_0^n,Z^n) \tag{15}$$

and shows that each term on the right hand side of (15) vanishes as $n\to\infty$. The upper bound in (15) might result in potential suboptimality in the achievable secrecy rate given in Theorem 3 as compared to the achievable secrecy rate that can be obtained by directly showing (14) without any recourse to the bound in (15). The corresponding new achievable secrecy rate, obtained by showing (14) without using the bound in (15), is given in the following theorem.

Theorem 4 *The secrecy capacity of the two-user one-eavesdropper discrete memoryless compound wiretap channel is lower bounded by the maximum of R satisfying*

$$R\leq I(V_0,V_1;Y_1)-I(V_0,V_1;Z) \tag{16}$$

$$R\leq I(V_0,V_2;Y_2)-I(V_0,V_2;Z) \tag{17}$$

$$2R\leq I(V_0,V_1;Y_1)+I(V_0,V_2;Y_2)-2I(V_0;Z)-I(V_1,V_2;Z|V_0)-I(V_1;V_2|V_0) \tag{18}$$

for some (V_0,V_1,V_2) such that $(V_0,V_1,V_2)\to X\to(Y_1,Y_2,Z)$.

The proof of this theorem is given in Appendix I. We note that the achievable secrecy rate given in Theorem 4 has one more rate constraint than the achievable secrecy rate given in Theorem 3, while both achievable secrecy rates have two rate constraints (16)-(17) in common. On the other hand, the new achievable secrecy rate in Theorem 4 does not have the constraint in (13) that Theorem 3 has. We next obtain a potentially looser version of the achievable secrecy rate in Theorem 4, which will be useful to compare the achievable secrecy rates in Theorems 3 and 4. This potentially looser version of the achievable secrecy rate given in Theorem 4 is stated in the following corollary.

Corollary 1 *The secrecy capacity of the two-user one-eavesdropper compound wiretap channel is lower bounded as follows*

$$C_S\geq\max\left\{R_S^{12},R_S^{21}\right\} \tag{19}$$

for some (V_0,V_1,V_2) such that $(V_0,V_1,V_2)\to X\to(Y_1,Y_2,Z)$, and R_S^{12},R_S^{21} are given by

$$R_S^{12}=\min\{I(V_0,V_1;Y_1)-I(V_0,V_1;Z),I(V_0,V_2;Y_2)-I(V_0;Z)-I(V_2;Z,V_1|V_0)\} \tag{20}$$

$$R_S^{21}=\min\{I(V_0,V_1;Y_1)-I(V_0;Z)-I(V_1;Z,V_2|V_0),I(V_0,V_2;Y_2)-I(V_0,V_2;Z)\} \tag{21}$$

The proof of Corollary 1 is given in Appendix II. We now compare the potentially looser version of Theorem 4 given in Corollary 1 with Theorem 3 to show that the achievable secrecy rate in Theorem 4 is potentially higher than the one in Theorem 3. We note that the constraint in (13) implies

$$0\leq I(V_1;Z|V_0)+I(V_2;Z|V_0)-I(V_1;V_2|V_0)-I(V_1,V_2;Z|V_0) \tag{22}$$

$$=I(V_2;Z|V_0)-I(V_1;V_2|V_0)-I(V_2;Z|V_0,V_1) \tag{23}$$

$$=I(V_2;Z|V_0)-I(V_2;Z,V_1|V_0) \tag{24}$$

$$=-I(V_2;V_1|V_0,Z) \tag{25}$$

which is equivalent to

$$I(V_2;V_1|V_0,Z)=0 \tag{26}$$

Consider a random variable triple (V_0,V_1,V_2) such that it satisfies $(V_0,V_1,V_2)\to X\to(Y_1,Y_2,Z)$ and (13). Due to (26), we have

$$R_S^{12}=R_S^{21}=\min\{I(V_0,V_1;Y_1)-I(V_0,V_1;Z),I(V_0,V_2;Y_2)-I(V_0,V_2;Z)\} \tag{27}$$

which is the achievable secrecy rate in Theorem 3. Thus, for any random variable triple (V_0,V_1,V_2) satisfying (13), both the new achievable secrecy rate in Corollary 1, hence in Theorem 4, and the achievable secrecy rate in Theorem 3 are equal. However, since the new achievable secrecy rate in Theorem 4 does not have the constraint, i.e., restriction, in (13), it is potentially higher than the achievable secrecy rate in Theorem 3.

IV. Gaussian MIMO Compound Wiretap Channel

We consider the two-user one-eavesdropper Gaussian MIMO compound wiretap channel which is defined by

$$\mathbf{Y}_1=\mathbf{X}+\mathbf{N}_1 \tag{28}$$

$$\mathbf{Y}_2=\mathbf{X}+\mathbf{N}_2 \tag{29}$$

$$\mathbf{Z}=\mathbf{X}+\mathbf{N}_Z \tag{30}$$

where the channel input $\mathbf{X}$, a $t\times 1$ vector, is subject to a covariance constraint as

$$E\left[\mathbf{X}\mathbf{X}^\top\right]\preceq\mathbf{S} \tag{31}$$

and $\mathbf{S}$ is a positive semi-definite matrix, i.e., $\mathbf{S}\succeq\mathbf{0}$. The noise covariance matrices of the Gaussian random vectors $\mathbf{N}_1,\mathbf{N}_2,\mathbf{N}_Z$, $t\times 1$ vectors, are denoted by $\mathbf{\Sigma}_1,\mathbf{\Sigma}_2,\mathbf{\Sigma}_Z$, respectively, where we assume $\mathbf{\Sigma}_1\succ\mathbf{0},\mathbf{\Sigma}_2\succ\mathbf{0},\mathbf{\Sigma}_Z\succ\mathbf{0}$. We remark that the Gaussian MIMO compound wiretap channel defined in (28)-(30) actually corresponds to a special case of the more general form of the Gaussian MIMO compound wiretap channel given by

$$\mathbf{Y}_j=\mathbf{H}_j\mathbf{X}+\mathbf{N}_j,\quad j=1,2 \tag{32}$$

$$\mathbf{Z}=\mathbf{H}_Z\mathbf{X}+\mathbf{N}_Z \tag{33}$$

However, using the rather straightforward analysis given in Section 7.1 of [17], the results we obtain for the channel model in (28)-(30) can be extended to the most general form of the Gaussian MIMO compound wiretap channel in (32)-(33).

Thus, here, we restrict our attention to the channel model in (28)-(30). Another remark about the channel model is the way we impose the power constraint on the channel input $\mathbf{X}$. We note that the covariance constraint in (31) subsumes the more common total power constraint $E\left[\mathbf{X}^\top\mathbf{X}\right] \leq P$, in that both inner and outer bounds proved for the covariance constraint in (31) can be extended to the case where the channel input $\mathbf{X}$ is subject to a total power constraint; see Lemma 1 and Corollary 1 in [18]. Thus, without loss of generality, we consider only the covariance constraint in (31).

We now present an achievable secrecy rate for the two-user one-eavesdropper Gaussian MIMO compound wiretap channel in (28)-(30) given in the following theorem.

Theorem 5 *The secrecy capacity of the two-user one-eavesdropper Gaussian MIMO compound wiretap channel $C_S(\mathbf{S})$ is lower bounded by the maximum of R satisfying*

$$R = \max\left\{R_S^{12}(\mathbf{K}_0,\mathbf{K}_1,\mathbf{K}_2), R_S^{21}(\mathbf{K}_0,\mathbf{K}_1,\mathbf{K}_2)\right\} \tag{34}$$

for some positive semi-definite matrices $\mathbf{K}_0,\mathbf{K}_1,\mathbf{K}_2$ such that $\mathbf{K}_0+\mathbf{K}_1+\mathbf{K}_2 \preceq \mathbf{S}$, and $R_S^{12}(\mathbf{K}_0,\mathbf{K}_1,\mathbf{K}_2)$ is given by

$$\begin{aligned} R_S^{12}(\mathbf{K}_0,\mathbf{K}_1,\mathbf{K}_2) = \min\{&R_{S1}^{12}(\mathbf{K}_0,\mathbf{K}_1,\mathbf{K}_2),\\ &R_{S2}^{12}(\mathbf{K}_0,\mathbf{K}_1,\mathbf{K}_2)\} \end{aligned} \tag{35}$$

where $R_{S1}^{12}(\mathbf{K}_0,\mathbf{K}_1,\mathbf{K}_2), R_{S2}^{12}(\mathbf{K}_0,\mathbf{K}_1,\mathbf{K}_2)$ are

$$\begin{aligned} R_{S1}^{12}(\mathbf{K}_0,\mathbf{K}_1,\mathbf{K}_2) &= \frac{1}{2}\log\frac{|\mathbf{K}_0+\mathbf{K}_1+\mathbf{K}_2+\mathbf{\Sigma}_1|}{|\mathbf{K}_2+\mathbf{\Sigma}_1|}\\ &\quad - \frac{1}{2}\log\frac{|\mathbf{K}_0+\mathbf{K}_1+\mathbf{K}_2+\mathbf{\Sigma}_Z|}{|\mathbf{K}_2+\mathbf{\Sigma}_Z|} \end{aligned} \tag{36}$$

$$\begin{aligned} R_{S2}^{12}(\mathbf{K}_0,\mathbf{K}_1,\mathbf{K}_2) &= \frac{1}{2}\log\frac{|\mathbf{K}_0+\mathbf{K}_1+\mathbf{K}_2+\mathbf{\Sigma}_1|}{|\mathbf{K}_1+\mathbf{K}_2+\mathbf{\Sigma}_2|}\\ &\quad - \frac{1}{2}\log\frac{|\mathbf{K}_0+\mathbf{K}_1+\mathbf{K}_2+\mathbf{\Sigma}_Z|}{|\mathbf{K}_1+\mathbf{K}_2+\mathbf{\Sigma}_Z|}\\ &\quad + \frac{1}{2}\log\frac{|\mathbf{K}_2+\mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} - \frac{1}{2}\log\frac{|\mathbf{K}_2+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \end{aligned} \tag{37}$$

Moreover, $R_S^{21}(\mathbf{K}_0,\mathbf{K}_1,\mathbf{K}_2)$ can be obtained from $R_S^{12}(\mathbf{K}_0,\mathbf{K}_1,\mathbf{K}_2)$ by swapping the indices 1 and 2.

Theorem 5 can be obtained from Corollary 1 by choosing (V_0,V_1,V_2) to be jointly Gaussian with a specific correlation structure. V_0, to which the covariance matrix $\mathbf{K}_0$ is allotted, can be viewed as the common part, and is decoded by both users. V_1 (resp. V_2) can be thought of as a private message that is directed to only the first (resp. second) user, the second (resp. first) user does not bother to decode. V_1, V_2 are encoded using DPC [15]. Thus, depending on the encoding order used in DPC, we get a different achievable secrecy rate. For example, $R_S^{12}(\mathbf{K}_0,\mathbf{K}_1,\mathbf{K}_2)$ comes from encoding V_1 first, then using DPC for V_2. We next note the following special case of Theorem 5.

Corollary 2 *The secrecy capacity of the two-user one-eavesdropper Gaussian MIMO compound wiretap channel $C_S(\mathbf{S})$ is lower bounded by the maximum of R satisfying*

$$R = \max\left\{R_S^{12}(\mathbf{K}_1,\mathbf{K}_2), R_S^{21}(\mathbf{K}_1,\mathbf{K}_2)\right\} \tag{38}$$

for some positive semi-definite matrices $\mathbf{K}_1,\mathbf{K}_2$ such that $\mathbf{K}_1+\mathbf{K}_2 \preceq \mathbf{S}$, and $R_S^{12}(\mathbf{K}_1,\mathbf{K}_2)$ is given by

$$R_S^{12}(\mathbf{K}_1,\mathbf{K}_2) = \min\{R_{S1}^{12}(\mathbf{K}_1,\mathbf{K}_2), R_{S2}^{12}(\mathbf{K}_1,\mathbf{K}_2)\} \tag{39}$$

where $R_{S1}^{12}(\mathbf{K}_1,\mathbf{K}_2), R_{S2}^{12}(\mathbf{K}_1,\mathbf{K}_2)$ are

$$\begin{aligned} R_{S1}^{12}(\mathbf{K}_1,\mathbf{K}_2) &= \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{K}_2+\mathbf{\Sigma}_1|}{|\mathbf{K}_2+\mathbf{\Sigma}_1|}\\ &\quad - \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{K}_2+\mathbf{\Sigma}_Z|}{|\mathbf{K}_2+\mathbf{\Sigma}_Z|} \end{aligned} \tag{40}$$

$$R_{S2}^{12}(\mathbf{K}_1,\mathbf{K}_2) = \frac{1}{2}\log\frac{|\mathbf{K}_2+\mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} - \frac{1}{2}\log\frac{|\mathbf{K}_2+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{41}$$

Moreover, $R_S^{21}(\mathbf{K}_1,\mathbf{K}_2)$ can be obtained from $R_S^{12}(\mathbf{K}_1,\mathbf{K}_2)$ by swapping the indices 1 and 2.

This corollary can be obtained by setting $\mathbf{K}_0 = \phi$ in Theorem 5. We next assess the tightness of the inner bound in Corollary 2. To this end, we introduce the following simple outer bound on the secrecy capacity of the two-user one-eavesdropper Gaussian MIMO compound wiretap channel.

Lemma 1 *The secrecy capacity of the two-user one-eavesdropper Gaussian MIMO compound wiretap channel is upper bounded as follows*

$$C_S(\mathbf{S}) \leq \min\{C_{S1}(\mathbf{S}), C_{S2}(\mathbf{S})\} \tag{42}$$

where $C_{Sj}(\mathbf{S}),\ j=1,2$, is given by

$$C_{Sj}(\mathbf{S}) = \max_{\mathbf{0}\preceq\mathbf{K}\preceq\mathbf{S}} \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_j|}{|\mathbf{\Sigma}_j|} - \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{43}$$

We note that $C_{Sj}(\mathbf{S})$ is the secrecy capacity of the Gaussian MIMO wiretap channel between the jth user and the eavesdropper. If one wants to multicast a common confidential message to both users, one cannot transmit at a higher rate than the secrecy capacity of the wiretap channel between the jth user and the eavesdropper for $j=1,2$. This observation proves Lemma 1. We now provide the following theorem which assesses the tightness of the achievable secrecy rate in Corollary 2 in terms of the outer bound in Lemma 1.

Theorem 6 *The secrecy capacity $C_S(\mathbf{S})$ of the two-user one-eavesdropper Gaussian MIMO compound wiretap channel satisfies*

$$\frac{1}{2}\min\{C_{S1}(\mathbf{S}), C_{S2}(\mathbf{S})\} \leq C_S(\mathbf{S}) \leq \min\{C_{S1}(\mathbf{S}), C_{S2}(\mathbf{S})\} \tag{44}$$

The proof of this theorem is omitted due to space limitations here. In the proof of this theorem, we use the achievable secrecy rate in Corollary 2 and the channel enhancement technique [18]. Hence, Theorem 6 states that using Corollary 2, one can get an achievable secrecy rate R such that

$$\min\{C_{S1}(\mathbf{S}), C_{S2}(\mathbf{S})\} \leq 2R \tag{45}$$

which, in turn, implies that $C_S(\mathbf{S}) \leq 2R$ using Lemma 1. Thus, the achievable secrecy rate given in Corollary 2 achieves

at least half of the secrecy capacity. We note that there are two possible directions that might improve this result. The first one is to consider the more general form of Corollary 2 given in Theorem 5. This might lead to higher achievable secrecy rates. The second possible improvement is to find better outer bounds for the secrecy capacity of the Gaussian MIMO compound wiretap channel. The outer bound in Lemma 1 seems to be loose. In general, we do not expect the secrecy capacity of a Gaussian MIMO compound wiretap channel to be the minimum of the secrecy capacities of the underlying wiretap channels. However, still, there might be cases that the outer bound in Lemma 1 is tight. To give an example, assume that the eavesdropper is degraded with respect to the second user, i.e., we have $\mathbf{X} \rightarrow \mathbf{Y}_2 \rightarrow \mathbf{Z}$, which is equivalent to

$$\mathbf{\Sigma}_2 \preceq \mathbf{\Sigma}_Z \tag{46}$$

The secrecy capacity of a Gaussian MIMO compound wiretap channel satisfying (46) is given by the following theorem.

Theorem 7 *The secrecy capacity region of the two-user one-eavesdropper Gaussian MIMO compound wiretap channel satisfying (46) is given by*

$$C_S(\mathbf{S}) = \min\{C_{S1}(\mathbf{S}), C_{S2}(\mathbf{S})\} \tag{47}$$

The proof of this theorem is also omitted due to space limitations here. Theorem 7 states that if the eavesdropper is degraded with respect to one of the two users, the secrecy capacity of the two-user one-eavesdropper Gaussian MIMO compound wiretap channel is equal to the minimum of the secrecy capacities of the underlying two Gaussian MIMO wiretap channels.

V. Conclusions

We study two-user one-eavesdropper compound wiretap channels. We first propose an achievable secrecy rate for the general two-user one-eavesdropper discrete memoryless compound wiretap channel. We show that this new achievable secrecy rate is potentially better than the best known lower bound in [7]. We next consider the two-user one-eavesdropper Gaussian MIMO compound wiretap channel. We propose an achievable secrecy rate by using DPC in the achievable scheme we provided for the discrete case. We show that the resulting secrecy rate achieves at least half of the secrecy capacity. Finally, we consider a special class of two-user one-eavesdropper Gaussian MIMO compound wiretap channels, where the eavesdropper is degraded with respect to one of the two users. We obtain the secrecy capacity of these Gaussian MIMO wiretap channels.

Appendix I
Proof of Theorem 4

We fix a random variable tuple (V_0, V_1, V_2, X) such that

$$p(v_0, v_1, v_2, x, y_1, y_2, z) = p(v_0, v_1, v_2)p(x|v_0, v_1, v_2)\, p(y_1, y_2, z|x) \tag{48}$$

Codebook generation:

- Generate $2^{n(R+\tilde{R}_0)}$ length-n $\mathbf{v}_0$ sequences through $p(\mathbf{v}_0) = \prod_{i=1}^n p(v_{0,i})$. Index them as $\mathbf{v}_0(w, \tilde{w}_0)$ where $W \in \{1, \ldots, 2^{nR}\}$, and $\tilde{W}_0 \in \{1, \ldots, 2^{n\tilde{R}_0}\}$.
- For each $\mathbf{v}_0$ sequence and $j \in \{1, 2\}$, generate $2^{n(\tilde{R}_j+L_j)}$ length-n $\mathbf{v}_j$ sequences through $p(\mathbf{v}_j|\mathbf{v}_0) = \prod_{i=1}^n p(v_{j,i}|v_{0,i})$. Index them as $\mathbf{v}_j(w, \tilde{w}_0, \tilde{w}_j, l_j)$ where $\tilde{W}_j \in \{1, \ldots, 2^{n\tilde{R}_j}\}, L_j \in \{1, \ldots, 2^{nL_j}\}$.

Encoding:

If $W = w$ is to be transmitted, randomly pick $(\tilde{w}_0, \tilde{w}_1, \tilde{w}_2)$. Then, find an (l_1, l_2) pair such that

$$(V_0^n(w, \tilde{w}_0), V_1^n(w, \tilde{w}_0, \tilde{w}_1, l_1), V_2^n(w, \tilde{w}_0, \tilde{w}_2, l_2)) \tag{49}$$

is jointly typical. Finally, generate the channel input X^n through $\prod_{i=1}^n p(x_i|v_{1,i}, v_{2,i})$.

Selection of $\tilde{R}_0, \tilde{R}_1, \tilde{R}_2, L_1, L_2$:

We select the rates $\tilde{R}_0, \tilde{R}_1, \tilde{R}_2, L_2$ as follows

$$\tilde{R}_0 = I(V_0; Z) - \epsilon \tag{50}$$

$$\tilde{R}_1 + \tilde{R}_2 = I(V_1, V_2; Z|V_0) - 2\epsilon \tag{51}$$

$$L_1 + L_2 = I(V_1; V_2|V_0) + \epsilon \tag{52}$$

$$\tilde{R}_1 + L_1 \leq I(V_1; Z, V_2|V_0) \tag{53}$$

$$\tilde{R}_2 + L_2 \leq I(V_2; Z, V_1|V_0) \tag{54}$$

Probability of error analysis:

- Since we have $L_1 + L_2 > I(V_1; V_2|V_0)$, encoding, i.e., to find an (l_1, l_2) pair such that (49) is jointly typical, can be accomplished with vanishingly small probability of error.
- The jth user decodes W through (V_0^n, V_j^n), which can be accomplished with vanishingly small probability of error if we have

$$R + \tilde{R}_0 + \tilde{R}_j + L_j < I(V_0, V_j; Y_j),\ j = 1, 2 \tag{55}$$

Equivocation computation:

We now show that this coding scheme satisfies the perfect secrecy requirement in (1). To this end, consider the following

$$\begin{aligned} H(W|Z^n) &= H(W, \tilde{W}_0, \tilde{W}_1, \tilde{W}_2|Z^n) \\ &\quad - H(\tilde{W}_0, \tilde{W}_1, \tilde{W}_2|Z^n, W) \qquad (56) \\ &= H(W, \tilde{W}_0, \tilde{W}_1, \tilde{W}_2) - I(W, \tilde{W}_0, \tilde{W}_1, \tilde{W}_2; Z^n) \\ &\quad - H(\tilde{W}_0, \tilde{W}_1, \tilde{W}_2|Z^n, W) \qquad (57) \end{aligned}$$

The first term in (57) is

$$H(W, \tilde{W}_0, \tilde{W}_1, \tilde{W}_2) = n(R + \tilde{R}_0 + \tilde{R}_1 + \tilde{R}_2) \tag{58}$$

where we used the fact that $(W, \tilde{W}_0, \tilde{W}_1, \tilde{W}_2)$ are independent and uniformly distributed random variables. The second term in (57) is

$$\begin{aligned} I(W, \tilde{W}_0, \tilde{W}_1, \tilde{W}_2; Z^n) &\leq I(V_0^n, V_1^n, V_2^n; Z^n) \qquad (59) \\ &\leq nI(V_0, V_1, V_2; Z) + n\gamma_{1n} \qquad (60) \end{aligned}$$

where $\gamma_{1n} \to 0$ as $n \to \infty$. Equation (59) is due to the Markov chain $(W, \tilde{W}_0, \tilde{W}_1, \tilde{W}_2) \to (V_0^n, V_1^n, V_2^n) \to Z^n$, and (60) can be proved by following Lemma 8 [16]. We next consider the third term in (57)

$$\begin{aligned} &H(\tilde{W}_0, \tilde{W}_1, \tilde{W}_2 | Z^n, W) \\ &= H(\tilde{W}_0 | Z^n, W) + H(\tilde{W}_1, \tilde{W}_2 | Z^n, W, \tilde{W}_0) \quad (61) \\ &= H(\tilde{W}_0 | Z^n, W) + H(\tilde{W}_1, \tilde{W}_2 | Z^n, W, \tilde{W}_0, V_0^n) \quad (62) \end{aligned}$$

Since $\tilde{R}_0 < I(V_0; Z)$, given $W = w$, the eavesdropper can decode $\tilde{W}_0$ through V_0^n. Thus, for the first term in (62), we have

$$H(\tilde{W}_0 | Z^n, W) \leq n\gamma_{2n} \quad (63)$$

due to Fano's lemma, where $\gamma_{2n} \to 0$ as $n \to \infty$. Since $\tilde{R}_1, \tilde{R}_2, L_1, L_2$ are selected to satisfy (see (51)-(54))

$$\tilde{R}_1 + L_1 \leq I(V_1; Z, V_2 | V_0) \quad (64)$$

$$\tilde{R}_2 + L_2 \leq I(V_2; Z, V_1 | V_0) \quad (65)$$

$$\tilde{R}_1 + \tilde{R}_2 + L_1 + L_2 \leq I(V_1, V_2; Z | V_0) + I(V_1; V_2 | V_0) \quad (66)$$

the eavesdropper can decode $(\tilde{W}_1, \tilde{W}_2)$ by looking for the unique jointly typical tuple

$$(V_0^n(w_0, \tilde{w}_0), V_1^n(w_0, \tilde{w}_0, \tilde{w}_1, l_1), V_2^n(w_0, \tilde{w}_0, \tilde{w}_2, l_2), Z^n) \quad (67)$$

Thus, for the second term in (62), we have

$$H(\tilde{W}_1, \tilde{W}_2 | Z^n, W, \tilde{W}_0, V_0^n) \leq n\gamma_{3n} \quad (68)$$

due to Fano's lemma, where $\gamma_{3n} \to 0$ as $n \to \infty$. Using (58), (60), (62)-(68) in (57), we get

$$\begin{aligned} H(W|Z^n) &\geq nR + n(\tilde{R}_0 + \tilde{R}_1 + \tilde{R}_2) - nI(V_0, V_1, V_2; Z) \\ &\quad - n(\gamma_{1n} + \gamma_{2n} + \gamma_{3n}) \quad (69) \\ &= nR - n3\epsilon - n(\gamma_{1n} + \gamma_{2n} + \gamma_{3n}) \quad (70) \end{aligned}$$

where (70) follows from (50)-(51). Hence, taking $\epsilon \to 0$, and $n \to \infty$ yields

$$\lim_{n\to\infty} \frac{1}{n} I(W; Z^n) = 0 \quad (71)$$

which completes the equivocation computation.

Thus, we have shown that for a given (V_0, V_1, V_2, X) such that the Markov chain $(V_0, V_1, V_2) \to X \to (Y_1, Y_2, Z)$ holds, the perfect secrecy rate R is achievable if the conditions in (50)-(55) are satisfied for some $\tilde{R}_1, \tilde{R}_2, L_1, L_2$. Finally, Fourier-Motzkin elimination can be used to remove the terms $\tilde{R}_1, \tilde{R}_2, L_1, L_2$ from the inequalities in (50)-(55), which results in the inequalities given in Theorem 4.

APPENDIX II
PROOF OF COROLLARY 1

We first show the achivability of R_S^{12} for a given random variable triple (V_0, V_1, V_2) satisfying $(V_0, V_1, V_2) \to X \to (Y_1, Y_2, Z)$. Let us define a, b as follows

$$a = I(V_0, V_1; Y_1) - I(V_0, V_1; Z) \quad (72)$$

$$b = I(V_0, V_2; Y_2) - I(V_0, V_2; Z) \quad (73)$$

Using (72)-(73) in (16)-(18), we have that

$$R = \min\left\{a, b, \frac{a + b - I(V_1; V_2 | V_0, Z)}{2}\right\} \quad (74)$$

is an achievable secrecy rate. Since we have

$$R \geq \min\{a, b - I(V_1; V_2 | V_0, Z)\} \quad (75)$$

and

$$\begin{aligned} b - I(V_1; V_2 | V_0, Z) &= I(V_0, V_2; Z) - I(V_0; Z) \\ &\quad - I(V_2; Z, V_1 | V_0) \quad (76) \end{aligned}$$

the achievability of R_S^{12} follows. Using the symmetry, the achievability of R_S^{21} for the same given random variable triple (V_0, V_1, V_2) can be shown as well; completing the proof.

REFERENCES

[1] H. Yamamoto. Coding theorem for secret sharing communication systems with two noisy channels. *IEEE Trans. Inf. Theory*, 35(3):572–578, May 1989.

[2] H. Yamamoto. A coding theorem for secret sharing communication systems with two Gaussian wiretap channels. *IEEE Trans. Inf. Theory*, 37(3):634–638, May 1991.

[3] P. Wang, G. Yu, and Z. Zhang. On the secrecy capacity of fading wireless channel with multiple eavesdroppers. In *IEEE Intnl. Symp. Inf. Theory*, pages 1301–1305, Jun. 2007.

[4] A. Khisti, A. Tchamkerten, and G. W. Wornell. Secure broadcasting over fading channels. *IEEE Trans. Inf. Theory*, 54(6):2453–2469, Jun. 2008.

[5] E. Ekrem and S. Ulukus. On secure broadcasting. In *42th Asilomar Conf. Signals, Syst. and Comp.*, Oct. 2008.

[6] E. Ekrem and S. Ulukus. Secrecy capacity of a class of broadcast channels with an eavesdropper. *EURASIP Journal on Wireless Communications and Networking, Special Issue on Wireless Physical Layer Security*, 2009(824235), Oct. 2009.

[7] Y-K. Chia and A. El Gamal. 3-receiver broadcast channels with common and confidential messages. Submitted to *IEEE Trans. Inf. Theory*, Oct. 2009. Also available at [arXiv:0910.1407].

[8] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz). Compound wire-tap channels. *EURASIP Journal on Wireless Communications and Networking, Special Issue on Wireless Physical Layer Security*, 2009(142374), 2009.

[9] T. Liu, V. Prabhakaran, and S. Viswanath. The secrecy capacity of a class of parallel Gaussian compound wiretap channels. In *IEEE Intnl. Symp. Inf. Theory*, pages 116–120, Jul. 2008.

[10] E. Ekrem and S. Ulukus. Secrecy capacity region of the degraded compound multi-receiver wiretap channel. In *47th Annual Allerton Conf. Commun., Contr. and Comput.*, Oct. 2009.

[11] E. Ekrem and S. Ulukus. Degraded compound multi-receiver wiretap channels. Submitted to *IEEE Trans. Inf. Theory*, Oct. 2009. Also available at [arXiv:0910.3033].

[12] C. Nair and A. El Gamal. The capacity region of a class of 3-receiver broadcast channels with degraded message sets. *IEEE Trans. Inf. Theory*, 55(10):4479–4493, Oct. 2009.

[13] K. Marton. A coding theorem for the discrete memoryless channels. *IEEE Trans. Inf. Theory*, 25(1):306–311, May 1979.

[14] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, IT-24(3):339–348, May 1978.

[15] W. Yu and J. Cioffi. Sum capacity of Gaussian vector broadcast channels. *IEEE Trans. Inf. Theory*, 50(9):1875–1892, Sep. 2004.

[16] A. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54(8):1355–1387, Jan. 1975.

[17] E. Ekrem and S. Ulukus. The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel. Submitted to *IEEE Trans. Inf. Theory*, Mar. 2009. Also available at [arXiv:0903.3096].

[18] H. Weingarten, Y. Steinberg, and S. Shamai (Shitz). The capacity region of the Gaussian multiple-input multiple-output broadcast channel. *IEEE Trans. Inf. Theory*, 52(9):3936–3964, Sep. 2006.