Gaussian wiretap channels with correlated sources: 
approaching capacity region within a constant gap

Yanling Chen, Hendrik Vogt, Aydin Sezgin
Ruhr-Universität Bochum, Germany
\{yanling.chen-q5g, hendrik.vogt, aydin.sezgin\}@rub.de

Abstract—This paper studies the Gaussian wiretap channel with correlated sources available not only at the transmitter and legitimate receiver, but also the eavesdropper. In particular, we are interested in the open problem of finding the optimal auxiliary random variable, which provides a closed-form solution to the secret-message and secret-key capacity region. To do that, we first take a deterministic approach and give a precise characterization of its secrecy capacity region. Then we translate the insights gained to the Gaussian case. As a result, we provide a sub-optimal solution by employing a specified Gaussian choice of the auxiliary random variable. This suggested choice is a compromise of keeping most source information subject to the constraint imposed by the channel capability of conducting source coding. Nevertheless, it is shown to be able to approach the secrecy capacity region within half a bit as the signal-noise-ratio of the main channel is no less than 1.

I. Introduction

There has been a body of literature [1]–[4] studying the problem of either secrecy-message transmission or secret-key generation in different settings and extensions of wiretap channels and source models. Remarkably, a combined approach is taken by Prabhakaran et al. in [5], which aimed to characterize the fundamental trade-off between the secret-message and secret-key rates, by exploring the advantages of both channel and sources to its great extend. In general, they provided an achievable solution and the secrecy capacity region still remains open.

A class of channels and a class of sources that have drawn much attention are Gaussian channels and Gaussian sources. As is well-known, they are practically relevant for applications in wireless and sensor networks. Note that for the Gaussian wiretap channel with correlated Gaussian sources, especially when the eavesdropper also has a source observation, a single-letter characterization of the secret-message and secret-key capacity region is available [5]. However, a closed-form solution is still missing. In fact, it remains open even for the secret-key capacity region under jointly Gaussian sources. This stems from the fact that a single-letter characterization often involves some auxiliary random variables, and the optimal choice in general is difficult to obtain.

This work is inspired by [6], where a linear deterministic approach introduced in [7] was successfully applied to the secured dirty-paper channel, achieving the secrecy capacity of the degraded Gaussian model with side information within half a bit. So, instead of targeting an optimal closed-form solution, in this paper, we are interested in obtaining a sub-optimal solution which approaches the secrecy capacity region within a constant gap.

We proceed as follows. First, we look into the linear deterministic model of the wiretap channel with correlated sources, where we derive a precise characterization of the secrecy capacity. Then, we translate the insights gained to the Gaussian case. As a result, we provide an inner bound and an outer bound on the secrecy capacity region, which are shown to be within a constant gap less than half a bit. Therefore, the achievability scheme for our inner bound actually serves as a sub-optimal option by approaching the secrecy capacity region within half a bit under the assumption that the signal-noise-ratio of the main channel is no less than 1. This is done by employing a Gaussian choice of the auxiliary random variable, simply a degraded version of the Gaussian source available at the transmitter. The specific choice is taken to keep the source information available at the transmitter at most, subject to the constraint imposed by the channel capability of conducting source coding. Interestingly, such a choice serves as an optimal option to achieve the secret-message and secret-key capacities, as the eavesdropper has no access to the sources.

The rest of the paper is organized as follows: In Section II, we introduce the system model. In Section III, we give a precise characterization of the secrecy capacity of the linear deterministic model. A constant-gap result for the Gaussian case is present in Section IV. Finally, we conclude in Section V.

II. System Model

We consider the situation as given in Fig. 1. Alice, Bob and Eve, respectively, observe the dependent memoryless sources \(S_A, S_B, S_E\). Independent of these sources, there is a memoryless broadcast channel from Alice to Bob and Eve given by \(p_{Y,Z|X}\). In order to send a message \(M\) (uniformly distributed over \(\mathcal{M}\)) and share a key \(K\) (over \(\mathcal{K}\)). Alice sends a codeword \(X^n\) to the channel, whilst Bob and Eve observe the channel output \(Y^n\) and \(Z^n\), respectively. Upon receipt of \(Y^n\) and source observation...
from Eve. Define That is, both the message $M$ and key $K$ are made secret from Eve. Define

$$R_{SM, \epsilon_n} = \frac{1}{n} \log |M|;$$

$$R_{SK, \epsilon_n} = \frac{1}{n} \log |K|.$$ We say that $(R_{SM}, R_{SK})$ is a achievable rate pair if there exist a sequence of encoding-decoding schemes with rate pair $(R_{SM, \epsilon_n}, R_{SK, \epsilon_n})$ such that the conditions (1)-(3) are fulfilled, for $\epsilon_n$ such that $\epsilon_n \to 0$ as $n \to \infty$. The capacity region $C$ is defined to be the set of all achievable rate pairs. In this case, the capacity region is the set of non-negative pairs of $(R_{SM}, R_{SK})$ satisfying

$$R_{SM} \leq I(X_F; Y_F) + I(X_R; Y_R) - (I(U_F; S_A, F) - I(U_F; S_B, F));$$

$$R_{SM} + R_{SK} \leq I(X_F; Y_F | V_F) - I(X_F; Z_F | V_F) + I(U_F; S_B, F) - I(U_F; S_E, F),$$

where $U_F, V_F$ are such that $U_F \to S_A, F \to S_B, F \to S_E, F$ and $V_F \to X_F \to Y_F \to Z_F$ are Markov chains.

It is noted in [5] that Theorem 1 also holds for the strong secrecy condition, where the factor of $n$ is dropped in (2); and when the sub-channels and source components are only stochastically degraded.

### III. A Deterministic Approach

Let us first take a look at the deterministic wiretap channel with correlated sources.

Suppose that there are correlated sources $S_A, S_B$ and $S_E$ available at Alice, Bob and Eve, respectively. In particular,

$$S_A = D_{c}^{n_m} S_B;$$

$$S_E = D_{c}^{n_2},$$

where $S_B$ is a binary vector of length $r$ with $r \geq \max\{m_1, n_2\}$, whose elements are i.i.d. Bern($\frac{1}{2}$); $D_c$ is the $r \times r$ down-shift matrix; $m_1, n_2$ are the most significant bits of $S_A$ available at the Bob and Eve, respectively. We note that $S_A \to S_B \to S_E$ forms a Markov chain.

In this model, the received signals at the legitimate receiver and the eavesdropper are given by

$$Y = D_{c}^{n_1} X;$$

$$Z = D_{c}^{n_2} X,$$

where $X$ is the binary input vector of length $q = \max\{n_1, n_2\}$, whose elements are i.i.d. Bern($\frac{1}{2}$); $D_c$ is the $q \times q$ down-shift matrix; and $n_1, n_2$ are the integer channel gains of the channels from Alice to Bob and Eve, respectively. Note that

1) as $n_1 > n_2$, the channel is forwardly degraded in favor of Bob. That is, the channel has only components indexed by $F$, i.e., $X_F = X, Y_F = Y$ and $Z_F = Z$. In this case, the reversely degraded sub-channel is absent, i.e., $X_R = Y_R = Z_R = \emptyset$;

2) as $n_1 \leq n_2$, the channel is reversely degraded in favor of Eve. That is, the channel has only components indexed by $R$, i.e., $X_R = X, Y_R = Y$ and $Z_R = Z$. In this case, the forwardly degraded sub-channel is absent, i.e., $X_F = Y_F = Z_F = \emptyset$.

In both cases, we have

$$I(X_F; Y_F) + I(X_R; Y_R) \leq n_1;$$

$$I(X_F; Y_F | V_F) - I(X_F; Z_F | V_F) \leq n_1.$$ The bounds are simultaneously achieved as $V_F$ is a constant and components of $X$ are Bernoulli-$\frac{1}{2}$ distributed. Note that for this specific wiretap channel, a Bernoulli-1/2 input achieves not only the capacity of the channel to the
legitimate receiver; but also the secrecy capacity of the channel to the legitimate receiver in the presence of an eavesdropper [1], [2].

Applying Theorem 1, we have

\[
R_{SM} \leq n_1 - (I(U_F; S_{A,F}) - I(U_F; S_{B,F}));
\]

\[
R_{SM} + R_{SK} \leq |n_1 - n_2| + I(U; S_{B,F}) - I(U; S_{E,F});
\]

where (a) is due to the Markov chain model is the set of the rate pairs \((R; SM, R_{SK})\) satisfying

\[
I(U; S_{B}) - I(U; S_{E}) \leq I(S_A; S_{B}) - I(S_A; S_{E}).
\]

**Lemma 1.** For any \(U\) such that \(U \rightarrow S_A \rightarrow S_B \rightarrow S_E\) is a Markov chain, we have

\[
I(U; S_{B}) - I(U; S_{E}) \leq I(S_A; S_{B}) - I(S_A; S_{E}).
\]

**Proof:** See the detailed proof in Appendix VI.

**Proposition 1.** The capacity region for the secret-message and secret-key rate pair of the above deterministic model is the set of the rate pairs \((R_{SM}, R_{SK})\) satisfying

\[
R_{SM} \leq n_1;
\]

\[
R_{SM} + R_{SK} \leq |n_1 - n_2| + |m_1 - m_2|.
\]

**Proof:** We bound \((R_{SM}, R_{SK})\) as follows:

\[
R_{SM} \leq n_1 - (I(U; S_A) - I(U; S_B)) \leq n_1;
\]

\[
R_{SM} + R_{SK} \leq |n_1 - n_2| + I(U; S_B) - I(U; S_E)
\]

\[
\leq |n_1 - n_2| + |m_1 - m_2|.
\]

where (a) is due to (8); (b) is due to \(I(U; S_A) = I(U; S_B)\) by the fact that 1); the Markov chain \(U \rightarrow S_A \rightarrow S_B\) gives \(I(U; S_A) \geq I(U; S_B)\) and 2); \(S_A = D_{m_1}^* S_B\) results in \(I(U; S_A) \leq I(U; S_B)\); (c) is due to (9); (d) is due to the Markov chain \(U \rightarrow S_A \rightarrow S_B \rightarrow S_E\) and (10) in Lemma 1; The equality follows by taking \(U = S_A\); (e) is due to the fact that \(S_A = D_{m_1}^* S_B\) and \(S_E = D_{m_2}^* S_B\); thus, \(I(S_A; S_B) - I(S_A; S_E) = I(S_A; S_B|S_E) = H(S_B|S_E) - H(S_B|S_A, S_E) = (r - m_2) - (r - \max\{m_1, m_2\}) = |m_1 - m_2|\) by applying [6, Lemma 1].

As a conclusion, for the model described in this section, i.e., the channel and sources are both linear deterministic, one can achieve the capacity region of \((R_{SM}, R_{SK})\) by taking components of \(X\) to be Bernoulli distributed and the auxiliary random variable \(U = S_A\). Note that the choice of \(X\) provides the maximum gain on secrecy-message transmission by taking the advantage of the channel itself; whilst the choice of \(U = S_A\) maximizes the extra gain on secrecy-key generation.

Fig. 2: Gaussian wiretap channel with correlated Gaussian sources.

**IV. GAUSSIAN MODEL WITH CORRELATED SOURCES**

Let us consider the scalar Gaussian wiretap channel with correlated Gaussian sources, which are channel-independent and available at Alice, Bob and Eve, respectively, as shown in Fig. 2. We are particularly interested in the scenario where both Alice and Eve have noisy observations of the source available at Bob. That is, their correlations are defined as follows:

\[
S_A = S_B + N_1;
\]

\[
S_E = S_B + N_2,
\]

where \(S_B, N_1\) and \(N_2\) are independent zero-mean Gaussian, and of variances \(\sigma_B^2, \sigma_{N_1}^2, \sigma_{N_2}^2\), respectively. This model is motivated by the assumption that user(s) have access to a different orthogonal random source (e.g., OFDM sub-carrier channel estimate) which they back feed to the base station (Alice). At the same time, the feedback is eavesdropped by Eve. Now, let \(\text{SNR}_{A,src} = \sigma_B^2/\sigma_{N_1}^2\) and \(\text{SNR}_{E,src} = \sigma_B^2/\sigma_{N_2}^2\). Then we can write the variances of \(N_1, N_2, S_A, S_E; \sigma_{N_1}^2, \sigma_{N_2}^2, \sigma_B^2\) as follows:

\[
\sigma_{N_1}^2 = \sigma_B^2/\text{SNR}_{A,src};
\]

\[
\sigma_{N_2}^2 = \sigma_B^2/\text{SNR}_{E,src};
\]

\[
\sigma_B^2 = \sigma_B^2(1 + 1/\text{SNR}_{A,src});
\]

\[
\sigma_B^2 = \sigma_B^2(1 + 1/\text{SNR}_{E,src}).
\]

Note that \(S_A \rightarrow S_B \rightarrow S_E\) forms a Markov chain.

Suppose \(X\) is the channel input with a power constraint on it and the signals received by Bob and Eve are

\[
Y = X + N_B;
\]

\[
Z = X + N_E,
\]

where \(N_B\) and \(N_E\) are Gaussian noise independent of \(X\). Let \(\text{SNR}_B\) and \(\text{SNR}_E\) be the signal-to-noise ratios of the channels to Bob and Eve, respectively. We note that

1) as \(\text{SNR}_B > \text{SNR}_E\), the channel is forwardly (stochastically) degraded in favor of Bob. That is, the channel has only components indexed by \(F\), i.e., \(X_F = X, Y_F = Y\) and \(Z_F = Z\). In this case, the reversely degraded sub-channel is absent, i.e., \(X_R = Y_R = Z_R = 0\).
2) as $\text{SNR}_B \leq \text{SNR}_E$, the channel is reversibly (stochastically) degraded in favor of Eve. That is, the channel has only components indexed by $R$, i.e., $X_R = X$, $Y_R = Y$ and $Z_R = Z$. In this case, the forwardly degraded sub-channel is absent, i.e., $X_F = Y_F = Z_F = \emptyset$.

In both cases, we have
\[
I(X_F; Y_F) + I(X_R; Y_R) \leq C(\text{SNR}_B);
\]
\[
I(X_F; Y_F| V_F) - I(X_F; Z_F| V_F) \leq C(\text{SNR}_B) - C(\text{SNR}_E),
\]
where $C(\text{SNR}_B) = \frac{1}{2} \log(1 + \text{SNR}_B)$.

The bounds are simultaneously achieved as $V_F$ is a constant and $X$ is Gaussian of variance $\sigma^2_{X_n} \cdot \text{SNR}_B$, where $\sigma^2_{X_n}$ is the variance of the Gaussian noise $N_B$. Note that for a Gaussian wiretap channel, a Gaussian input achieves not only the capacity of the channel to the legitimate receiver; but also the secrecy capacity in the presence of an eavesdropper [8].

We further apply Theorem 1 and obtain
\[
\begin{align*}
R_{SM} & \leq C(\text{SNR}_B) - (I(U_F; S_{A,F}) - I(U_F; S_{B,F})), \\
R_{SM} + R_{SK} & \leq C(\text{SNR}_B) - C(\text{SNR}_E) + C \left( \frac{\text{SNR}_{A,\text{src}}}{1 + \text{SNR}_{E,\text{src}}} \right),
\end{align*}
\]
where (a) is due to (13); (b) is due to the Markov chain $U \rightarrow S_A \rightarrow S_B$; and the fact $I(U; S_A) \geq I(U; S_B)$ by data processing inequality; (c) is due to (14); (d) is due to the Markov chain $U \rightarrow S_A \rightarrow S_B \rightarrow S_E$ and (10) in Lemma 1. Note that the equality holds by taking $U = S_A$; (e) follows by the following calculations:
\[
I(S_A; S_B) - I(S_A; S_E) = \frac{1}{2} \log \frac{1 - \rho^2_{AE}}{1 - \rho^2_{AB}}
\]
\[
= \frac{1}{2} \log \frac{1 + \text{SNR}_{A,\text{src}} + \text{SNR}_{E,\text{src}}}{1 + \text{SNR}_{E,\text{src}}},
\]
where $\rho_{AB}, \rho_{AE}$ are the correlation coefficients of $S_A$ and $S_B$, $S_A$ and $S_E$, respectively; (f) is due to the fact that
\[
\begin{align*}
\rho^2_{AB} &= \left( \frac{\text{E} \{(S_A \cdot S_B)\}}{\sigma^2_A \cdot \sigma^2_B} \right) = \frac{\text{SNR}_{A,\text{src}}}{1 + \text{SNR}_{A,\text{src}}},
\end{align*}
\]
Recall that the choice of $U = S_A$ is optimal for the linear deterministic model as shown in Section III. And, for the Gaussian model considered in this section, we note that the choice of $U = S_A$ may provide the maximum sum rate $R_{SM} + R_{SK}$, as shown in Proposition 3, if it is doable.

However, unlike for the linear deterministic case, $U = S_A$ does not serve as a feasible choice for the Gaussian case. The reason is that, if $U = S_A$ is taken, then the calculation of $R_{SM}$ (upper bounded by (13)), involves of calculating $I(S_A; S_A)$ which results in $+\infty$ (under the assumption that $S_A$ is Gaussian). By (13), this gives a negative $R_{SM}$ which is contradictory to the non-negativity of the rate.

More specifically, the underlying coding scheme for Theorem 1 needs $I(U; S_A) - I(U; S_B)$ bits from the channel to convey sufficient source information to Bob. Thus a choice of $U = S_A$ implies that one needs $+\infty$ bits to describe $S_A$ accurately; and consumes $(+\infty - C(\text{SNR}_{A,\text{src}}))$ bits from the channel (which capacity is $C(\text{SNR}_B)$). This is impossible for a Gaussian channel with a bounded capacity!

However, as we will show in Proposition 3, one does not have to waste so much bits from the channel to convey source information. As a compromise, we take $U$ to be a degraded version of $S_A$ such that it is feasible for the channel to provide $I(U; S_A) - I(U; S_B)$ bits for the source coding. Surprisingly, we show it is actually a quite effective option especially in case of $\text{SNR}_B \geq 1$, for being able to approach the capacity region within half a bit.

B. An inner bound

We consider $U = S_A + N_0$, where $N_0$ is a zero-mean Gaussian random variable, which is of variance $\sigma^2_{N_0}$, and independent of $S_A, S_B, N_1$ and $N_2$. Note that we can rewrite $U = S_B + N_0 + N_1$. Let $\text{SNR}_{U,\text{src}} = \sigma^2_U / (\sigma^2_{N_0} + \sigma^2_{N_1}) = \theta \cdot \text{SNR}_{A,\text{src}}$; and $\sigma^2_U$ be the variance of $U$. Then we have:
\[
\sigma^2_U = \sigma^2_{N_0} \left( 1 + \frac{1}{\theta} \cdot \text{SNR}_{A,\text{src}} \right).
\]
Proposition 3. An inner bound of the capacity region of the secret-message and secret-key rate pair is given by the set of the rate pairs \((R_{SM}, R_{SK})\) satisfying
\[
R_{SM} \leq C(SNR_B) + \frac{1}{2} \log(1 - \theta);
\]
\[
R_{SM} + R_{SK} \leq [C(SNR_B) - C(SNR_E)]^+ + C\left(\theta \cdot \frac{\text{SNR}_{A,src}}{1 + \text{SNR}_{E,src}}\right),
\]
where \(0 \leq \theta \leq \frac{\text{SNR}_B}{1 + \text{SNR}_E} \).

Proof: One can derive an inner bound of \((R_{SM}, R_{SK})\) by applying Theorem 1 with specified choices of \(X\) and \(U\). In addition to (11)-(12) where a Gaussian choice of \(X\) is taken, we use a Gaussian choice of \(U\) in form of \(S_A + N_0\) to obtain an inner bound as follows.

\[
R_{SM} \overset{(a)}{\leq} C(SNR_B) - I(U; S_A) - I(U; S_B)) \overset{(b)}{\leq} C(SNR_B) + \frac{1}{2} \log(1 - \theta),
\]
where (a) is due to (11) by a Gaussian choice of \(X\); and (b) is due to the following calculations.

\[
I(U; S_A) - I(U; S_B) = \frac{1}{2} \log \frac{1 - \rho_{UB}^2}{1 - \rho_{UA}^2} \overset{(b)}{=} \frac{1}{2} \log \frac{1 - \theta}{1 - \theta},
\]
where \(\rho_{UA}, \rho_{UB}\) are the correlation coefficients of \(U\) and \(S_A, U\) and \(S_B\), respectively.

Similarly, we have

\[
R_{SM} + R_{SK} \overset{(c)}{\leq} [C(SNR_B) - C(SNR_E)]^+ + I(U; S_B) - I(U; S_E) \overset{(d)}{=} [C(SNR_B) - C(SNR_E)]^+ + C\left(\theta \cdot \frac{\text{SNR}_{A,src}}{1 + \text{SNR}_{E,src}}\right),
\]
where (c) is due to (12) by a Gaussian choice of \(X\); (d) is due to the following calculations.

\[
I(U; S_B) - I(U; S_E) = \frac{1}{2} \log \frac{1 - \rho_{UE}^2}{1 - \rho_{UB}^2} = \frac{1}{2} \log \frac{1 + \theta \cdot \text{SNR}_{A,src} + \text{SNR}_{E,src}}{1 + \theta \cdot \text{SNR}_{A,src} + \text{SNR}_{E,src}}.
\]

In particular, due to the non-negativity of the rate \(R_{SM}\), the following condition must be fulfilled in order to have a non-negative rate \(R_{SM}\):

\[
\frac{1}{2} \log \frac{1 - \theta}{1 - \theta} \leq C(SNR_B).
\]

Easy calculation gives us \(0 \leq \theta \leq \frac{\text{SNR}_B}{1 + \text{SNR}_E} \).

C. A constant gap

Proposition 4. By taking a Gaussian choice of the auxiliary random variable \(U\), one can approach the capacity region of the secret-message and secret-key rate pair within a gap that is

\[
C\left(\frac{\text{SNR}_{A,src}}{1 + \text{SNR}_{E,src}}\right) \leq \text{SNR}_E \geq \text{SNR}_{A,src}/(1 + \text{SNR}_{A,src} + \text{SNR}_{E,src})\;
\]

and

\[
C\left(\frac{\text{SNR}_{A,src}}{1 + \text{SNR}_{E,src}}\right) \leq \text{SNR}_B \geq \text{SNR}_{A,src}/(1 + \text{SNR}_{A,src} + \text{SNR}_{E,src}).
\]

Proof: By taking \(U = S_A + N_0\), one can obtain an inner bound on the rate region of \((R_{SM}, R_{SK})\) as described in Proposition 3. Further comparing it with the outer bound given in Proposition 2, we see that for a fixed choice of \(U\) with a specified \(\theta\), a gap between them is bounded by \(\max\{f_1(\theta), f_2(\theta)\}\), where

\[
f_1(\theta) = \frac{1}{2} \log \frac{1 - \theta}{1 - \theta}, \quad f_2(\theta) = C\left(\frac{\text{SNR}_{A,src}}{1 + \text{SNR}_{E,src}}\right) - C\left(\theta \cdot \frac{\text{SNR}_{A,src}}{1 + \text{SNR}_{E,src}}\right)
\]

Optimizing \(U\) over all possible \(0 \leq \theta \leq \frac{\text{SNR}_B}{1 + \text{SNR}_E}\), we could derive a gap to be min \(f_1(\theta), f_2(\theta)\).

Note that for \(0 \leq \theta \leq \frac{\text{SNR}_B}{1 + \text{SNR}_E}\), \(f_1(\theta)\) is increasing with respect to \(\theta\); whilst \(f_2(\theta)\) is decreasing. In particular, we have \(f_1(0) < f_2(0)\) at \(\theta = 0\). Therefore,

- if there exists a \(\theta_0\), such that \(0 \leq \theta_0 \leq \frac{\text{SNR}_B}{1 + \text{SNR}_E}\) and \(f_1(\theta_0) = f_2(\theta_0)\), i.e.,

\[
\frac{1}{2} \log \frac{1 - \theta_0}{1 - \theta_0} = \frac{1}{2} \log \frac{1 + \text{SNR}_{A,src} + \text{SNR}_{E,src}}{1 + \theta_0 \cdot \text{SNR}_{A,src} + \text{SNR}_{E,src}} - \frac{\text{SNR}_{A,src}}{1 + 2\text{SNR}_{A,src} + \text{SNR}_{E,src}}
\]

then we have

\[
\min_\theta \max\{f_1(\theta), f_2(\theta)\} = f_1(\theta_0) = C\left(\frac{\text{SNR}_{A,src}}{1 + \text{SNR}_{A,src} + \text{SNR}_{E,src}}\right) < 0.5.
\]

Note that \(\theta_0 \leq \frac{\text{SNR}_B}{1 + \text{SNR}_E}\) implies that \(\text{SNR}_E \geq \frac{\text{SNR}_A}{1 + \text{SNR}_E}\).

- However, in case that \(\theta_0 > \frac{\text{SNR}_B}{1 + \text{SNR}_E}\), i.e., \(\text{SNR}_E < \frac{\text{SNR}_A}{1 + \text{SNR}_E}\), we have

\[
\min_\theta \max\{f_1(\theta), f_2(\theta)\} = f_2(1 + \frac{\text{SNR}_B}{\text{SNR}_E}) = C\left(\frac{\text{SNR}_{A,src}}{1 + \text{SNR}_{E,src} + \text{SNR}_B(1 + \text{SNR}_B)}\right).
\]

This concludes our proof.
D. Discussions

First, note that as SNR_B \geq 1, the gap can be bounded by a constant: 0.5 bit, since \( C \left( \frac{\text{SNR}_A + \text{SNR}_E}{1+\text{SNR}_A,\text{src} + \text{SNR}_E,\text{src}} \right) < 0.5 \) holds for any SNR_A,src, SNR_E,src \geq 0. One can find a visual interpretation in Fig. 3.

As SNR_A,src = 0, it is easy to see that the gap becomes 0. In this case, the lower bound coincides with the upper bound, and thus is the capacity region. This is consistent with the results in [1], [3], [8].

As SNR_E,src = 0, it corresponds to the scenario that only Alice and Bob have correlated source observations but not Eve. Note that this scenario is similar to the one as described in [5, Proposition 4] wherein Bob has a degraded version of the source observation at Alice. Although the difference in the source model, the capacity region of the secret-message and secret-key rates is the same due to Lemma 2. As demonstrated in [5], a Gaussian choice of U is optimal to achieve the capacity region of the secret-message and secret-key rates. More specifically, one can easily verify that a Gaussian choice of U in form of \( U = S_A + N_0 \) serves as one of the optimal candidates to achieve the secret-message capacity

\[
\frac{1}{2} \log \left( \frac{(1 + \text{SNR}_B)(1 + \text{SNR}_A,\text{src})}{1 + \text{SNR}_A,\text{src} + \min\{\text{SNR}_B,\text{SNR}_E\}} \right) \tag{15}
\]

by taking \( \theta = \frac{\text{SNR}_B}{1 + \text{SNR}_A,\text{src} + \min\{\text{SNR}_B,\text{SNR}_E\}} \); and by taking

\[
\theta = \frac{\text{SNR}_B}{1 + \text{SNR}_A,\text{src}} \quad \text{the secret-key capacity}
\]

\[
\frac{1}{2} \log \left( \frac{(1 + \text{SNR}_B)(1 + \text{SNR}_A,\text{src}) - \text{SNR}_A,\text{src}}{1 + \min\{\text{SNR}_B,\text{SNR}_E\}} \right). \tag{16}
\]

V. Conclusion

We partially answer the open problem of finding the optimal auxiliary random variable for the secrecy capacity region of the Gaussian wiretap channel with correlated Gaussian sources, by suggesting a specific Gaussian choice which is shown to be able to approach the secrecy capacity region within half a bit especially as SNR_B \geq 1.

VI. Appendix

Lemma 1. For any U such that \( U \rightarrow S_A \rightarrow S_B \rightarrow S_E \) is a Markov chain, we have

\[
I(U;S_B) - I(U;S_E) \leq I(S_A;S_B) - I(S_A;S_E).
\]

Proof: Consider

\[
I(U,S_A;S_B) - I(U,S_A;S_E) = I(S_A;S_B) - I(S_A;S_E) + I(U;S_B|S_A) - I(U;S_E|S_A)
\]

\[\leq I(S_A;S_B) - I(S_A;S_E),\]

where (a) is since \( I(U;S_B|S_A) = I(U;S_E|S_A) = 0 \) due to the Markov chain \( U \rightarrow S_A \rightarrow S_B \rightarrow S_E \). In addition,

\[
I(U,S_A;S_B) - I(U,S_A;S_E) = I(U;S_B) - I(U;S_E) + I(S_A;S_B|U) - I(S_A;S_E|U)
\]

\[\geq I(U;S_B) - I(U;S_E).\]

Note that (b) is due to the fact that

\[
I(S_A;S_B|U) = I(S_A;S_B;S_E|U) - I(S_A;S_E|S_B,U)
\]

\[\geq I(S_A;S_B|U) \geq I(S_A;S_B;S_E|U) \geq I(S_A;S_E)|U
\]

\[\geq I(U;S_B) - I(U;S_E).
\]

This concludes the proof.

Lemma 2. Let \( S_A, S_B \) be jointly Gaussian, then for any U such that \( U \rightarrow S_A \rightarrow S_B \) forms a Markov chain, there exists V such that \( S_A \rightarrow V \rightarrow S_B \) forms a Markov chain; and I(V;S_B) = I(U;S_A) and I(V;S_A) = I(U;S_B).

Proof: Since mutual information is invariant to scaling/translate, assume w.l.o.g. that \( p_{S_A, S_B} \) is symmetric in \( S_A, S_B \). The lemma follows by taking \( p_V|S_B = p_V|S_A \).

(Many thanks to Dr. Thomas Courtade for the proof.)

References