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 was funded by the Federal Ministry of Education and Research (BMBF) of the Federal Republic of Germany (Förderkennzeichen 16 KIS 0030, Prophylaxe). The authors alone are responsible for the content of the paper.

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^n, S_B^n and S_E^n. 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

S_B^n, Bob makes an estimate $(\hat{M}, \hat{K})$ of the message-key pair (M, K) such that it satisfies the *reliability condition*:

$$P_e = \Pr\{(\hat{M}, \hat{K}) \neq (M, K)\} \leq \epsilon_n; \tag{1}$$

whilst the information leakage to Eve shall satisfy the *(weak) secrecy condition*

$$I(M, K; Z^n, S_E^n) \leq n\epsilon_n. \tag{2}$$

Moreover, the key generated should satisfy the *uniformity condition*:

$$H(K) \geq \log |\mathcal{K}| - n\epsilon_n. \tag{3}$$

That is, both the message M and key K are made secret from Eve. Define

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

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 ϵ_n such that $\epsilon_n \to 0$ as $n \to \infty$. The *capacity region* $\mathcal{C}$ is defined to be the set of all achievable rate pairs.

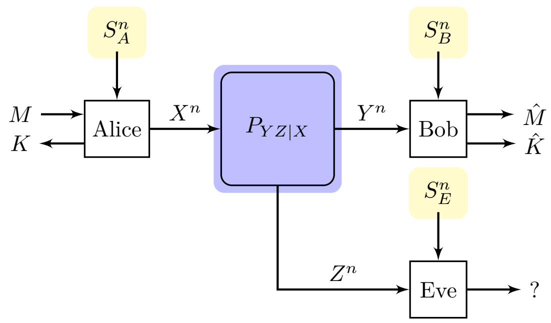

Fig. 1: Wiretap channel with correlated sources at the transmitter (Alice), the legitimate receiver (Bob) and the eavesdropper (Eve).

Prabhakaran *et al.* in [5, Theorem 1] provides a general lower bound on the trade-off of the secret-message and secret-key rate pair. It turns out to be the capacity region for special cases of parallel channels and sources where each sub-channel and source component satisfies a degradation order (either in favor of the legitimate receiver or in favor of the eavesdropper), as shown in Theorem 1.

Theorem 1. [5, Theorem 3] Consider the following:

- The channel has two independent components indexed by F and R : $X = (X_F, X_R)$, $Y = (Y_F, Y_R)$ and $Z = (Z_F, Z_R)$ such that $X_F \to Y_F \to Z_F$ and $X_R \to Z_R \to Y_R$ are Markov chains;
- The sources also have two independent components, again indexed by F and R : $S_A = (S_{A,F}, S_{A,R})$, $S_B = (S_{B,F}, S_{B,R})$ and $S_E = (S_{E,F}, S_{E,R})$ such that $S_{A,F} \to S_{B,F} \to S_{E,F}$ and $S_{A,R} \to S_{E,R} \to S_{B,R}$ are Markov chains.

In this case, the capacity region is the set of non-negative pairs of (R_{SM}, R_{SK}) satisfying

$$\begin{aligned} R_{SM} \leq & I(X_F; Y_F) + I(X_R; Y_R) \\ & - (I(U_F; S_{A,F}) - I(U_F; S_{B,F})); \\ R_{SM} + R_{SK} \leq & I(X_F; Y_F|V_F) - I(X_F; Z_F|V_F) \\ & + I(U_F; S_{B,F}) - I(U_F; S_{E,F}), \end{aligned}$$

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,

$$S_A = D_s^{r-m_1} S_B; \tag{4}$$
$$S_E = D_s^{r-m_2} S_B, \tag{5}$$

where S_B is a binary vector of length r with $r \geq \max\{m_1, m_2\}$, whose elements are i.i.d. Bern$(\frac{1}{2})$; D_s is the $r \times r$ down-shift matrix; m_1, m_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

$$Y = D_c^{q-n_1} X; \tag{6}$$
$$Z = D_c^{q-n_2} X, \tag{7}$$

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

$$I(X_F; Y_F) + I(X_R; Y_R) \leq n_1;$$
$$I(X_F; Y_F|V_F) - I(X_F; Z_F|V_F) \leq |n_1 - n_2|^+.$$

The bounds are simultaneously achieved as V_F is a constant and components of X are Bern$(\frac{1}{2})$ 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

$$\begin{aligned} R_{SM} &\leq n_1 - (I(U_F; S_{A,F}) - I(U_F; S_{B,F})) \\ &\overset{(a)}{\leq} n_1 - (I(U; S_A) - I(U; S_B)); \quad (8) \\ R_{SM} + R_{SK} &\leq |n_1 - n_2|^+ + I(U_F; S_{B,F}) - I(U_F; S_{E,F}) \\ &\overset{(a)}{=} |n_1 - n_2|^+ + I(U; S_B) - I(U; S_E). \quad (9) \end{aligned}$$

where (a) is due to the Markov chain $S_A \to S_B \to S_E$, the sources have only components indexed by F, i.e., $S_{A,F} = S_A$, $S_{B,F} = S_B$, $S_{E,F} = S_E$ and $U_F = U$.

Lemma 1. For any U such that $U \to S_A \to S_B \to S_E$ is a Markov chain, we have

$$I(U; S_B) - I(U; S_E) \leq I(S_A; S_B) - I(S_A; S_E). \quad (10)$$

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

$$\begin{aligned} R_{SM} &\leq n_1; \\ R_{SM} + R_{SK} &\leq |n_1 - n_2|^+ + |m_1 - m_2|^+. \end{aligned}$$

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

$$\begin{aligned} R_{SM} &\overset{(a)}{\leq} n_1 - (I(U; S_A) - I(U; S_B)) \overset{(b)}{=} n_1; \\ R_{SM} + R_{SK} &\overset{(c)}{\leq} |n_1 - n_2|^+ + I(U; S_B) - I(U; S_E) \\ &\overset{(d)}{\leq} |n_1 - n_2|^+ + I(S_A; S_B) - I(S_A; S_E) \\ &\overset{(e)}{=} |n_1 - n_2|^+ + |m_1 - m_2|^+. \end{aligned}$$

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 $U \to S_A \to S_B$ gives $I(U; S_A) \geq I(U; S_B)$) and 2): $S_A = D_s^{r-m_1} S_B$ results in $I(U; S_A) \leq I(U; S_B)$; (c) is due to (9); (d) is due to the Markov chain $U \to S_A \to S_B \to S_E$ and (10) in Lemma 1; The equality follows by taking $U = S_A$; (e) is due to the fact that $S_A = D_s^{r-m_1} S_B$ and $S_E = D_s^{r-m_2} S_B$; 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 Bern($\frac{1}{2}$) 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.

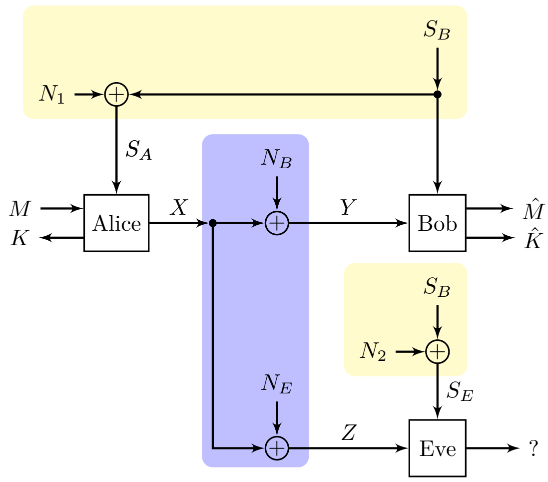

Fig. 2: Gaussian wiretap channel with correlated Gaussian sources.

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:

$$\begin{aligned} S_A &= S_B + N_1; \\ S_E &= S_B + N_2, \end{aligned}$$

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 feed back to the base station (Alice). At the same time, the feedback is eavesdropped by Eve. Now, let $\mathrm{SNR}_{A,src} = \sigma_B^2/\sigma_{N_1}^2$ and $\mathrm{SNR}_{E,src} = \sigma_B^2/\sigma_{N_2}^2$. Then we can write the variances of $N_1, N_2, S_A, S_E : \sigma_{N_1}^2, \sigma_{N_2}^2, \sigma_A^2, \sigma_E^2$ as follows:

$$\begin{aligned} \sigma_{N_1}^2 &= \sigma_B^2/\mathrm{SNR}_{A,src}; \quad \sigma_A^2 = \sigma_B^2(1 + 1/\mathrm{SNR}_{A,src}); \\ \sigma_{N_2}^2 &= \sigma_B^2/\mathrm{SNR}_{E,src}; \quad \sigma_E^2 = \sigma_B^2(1 + 1/\mathrm{SNR}_{E,src}). \end{aligned}$$

Note that $S_A \to S_B \to S_E$ 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

$$\begin{aligned} Y &= X + N_B; \\ Z &= X + N_E, \end{aligned}$$

where N_B and N_E are Gaussian noise independent of X. Let SNR_B and SNR_E be the signal-to-noise ratios of the channels to Bob and Eve, respectively. We note that

1) as $\mathrm{SNR}_B > \mathrm{SNR}_E$, 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., $X_R = Y_R = Z_R = \emptyset$;

2) as $\mathrm{SNR}_B \leq \mathrm{SNR}_E$, the channel is reversely (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

$$I(X_F;Y_F) + I(X_R;Y_R) \leq C(\mathrm{SNR}_B); \tag{11}$$

$$I(X_F;Y_F|V_F) - I(X_F;Z_F|V_F) \leq |C(\mathrm{SNR}_B) - C(\mathrm{SNR}_E)|^+, \tag{12}$$

where $C(\mathrm{SNR}) = \frac{1}{2}\log(1+\mathrm{SNR})$. The bounds are simultaneously achieved as V_F is a constant and X is Gaussian of variance $\sigma^2_{N_B} \cdot \mathrm{SNR}_B$, where $\sigma^2_{N_B}$ 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

$$\begin{aligned} R_{SM} &\leq C(\mathrm{SNR}_B) - (I(U_F;S_{A,F}) - I(U_F;S_{B,F})) \\ &\overset{(a)}{=} C(\mathrm{SNR}_B) - (I(U;S_A) - I(U;S_B)); \end{aligned} \tag{13}$$

$$\begin{aligned} R_{SM} + R_{SK} &\leq |C(\mathrm{SNR}_B) - C(\mathrm{SNR}_E)|^+ \\ &\quad + I(U_F;S_{B,F}) - I(U_F;S_{E,F}) \\ &\overset{(a)}{=} |C(\mathrm{SNR}_B) - C(\mathrm{SNR}_E)|^+ \\ &\quad + I(U;S_B) - I(U;S_E)., \end{aligned} \tag{14}$$

where (a) is due to the Markov chain $S_A \to S_B \to S_E$, the sources have only components indexed by F, i.e., $S_{A,F} = S_A$, $S_{B,F} = S_B$, $S_{E,F} = S_E$ and $U_F = U$.

A. An outer bound

Proposition 2. An outer bound of the capacity region for the secret-message and secret-key rate pair is given by the set of the rate pairs (R_{SM}, R_{SK}) satisfying

$$\begin{aligned} R_{SM} \leq& C(\mathrm{SNR}_B); \\ R_{SM} + R_{SK} \leq& |C(\mathrm{SNR}_B) - C(\mathrm{SNR}_E)|^+ \\ &+ C\left(\frac{\mathrm{SNR}_{A,src}}{1+\mathrm{SNR}_{E,src}}\right). \end{aligned}$$

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

$$R_{SM} \overset{(a)}{\leq} C(\mathrm{SNR}_B) - (I(U;S_A) - I(U;S_B)) \overset{(b)}{\leq} C(\mathrm{SNR}_B);$$

$$\begin{aligned} R_{SM} + R_{SK} &\overset{(c)}{\leq} |C(\mathrm{SNR}_B) - C(\mathrm{SNR}_E)|^+ \\ &\quad + I(U;S_B) - I(U;S_E) \\ &\overset{(d)}{\leq} |C(\mathrm{SNR}_B) - C(\mathrm{SNR}_E)|^+ + I(S_A;S_B) - I(S_A;S_E) \\ &\overset{(e)}{=} |C(\mathrm{SNR}_B) - C(\mathrm{SNR}_E)|^+ + C\left(\frac{\mathrm{SNR}_{A,src}}{1+\mathrm{SNR}_{E,src}}\right), \end{aligned}$$

where (a) is due to (13); (b) is due to the Markov chain $U \to S_A \to S_B$ and thus 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 $U \to S_A \to S_B \to S_E$ and (10) in Lemma 1. Note that the equality holds by taking $U = S_A$; (e) follows by the following calculations:

$$\begin{aligned} I(S_A;S_B) - I(S_A;S_E) &= \frac{1}{2}\log\frac{1-\rho^2_{AE}}{1-\rho^2_{AB}} \\ &\overset{(f)}{=} \frac{1}{2}\log\frac{1+\mathrm{SNR}_{A,src}+\mathrm{SNR}_{E,src}}{1+\mathrm{SNR}_{E,src}} \\ &= C\left(\frac{\mathrm{SNR}_{A,src}}{1+\mathrm{SNR}_{E,src}}\right), \end{aligned}$$

where ρ_{AB}, ρ_{AE} are the correlation coefficients of S_A and S_B, S_A and S_E, respectively; (f) is due to the fact that

$$\begin{aligned} \rho^2_{AB} &= \left(\frac{E\{S_A \cdot S_B\}}{\sigma_A \cdot \sigma_B}\right)^2 = \frac{\sigma^2_B}{\sigma^2_A} = \frac{\mathrm{SNR}_{A,src}}{1+\mathrm{SNR}_{A,src}}; \\ \rho^2_{AE} &= \left(\frac{E\{S_A \cdot S_E\}}{\sigma_A \cdot \sigma_E}\right)^2 = \frac{\sigma^2_B \cdot \sigma^2_B}{\sigma^2_A \cdot \sigma^2_E} \\ &= \frac{\mathrm{SNR}_{A,src}}{1+\mathrm{SNR}_{A,src}} \cdot \frac{\mathrm{SNR}_{E,src}}{1+\mathrm{SNR}_{E,src}}. \end{aligned}$$

■

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 contradict 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 $(+\infty - C(\mathrm{SNR}_{A,src}))$ bits from the channel (which capacity is $C(\mathrm{SNR}_B)$). 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 $\mathrm{SNR}_B \geq 1$, 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 $\mathrm{SNR}_{U,src} = \sigma^2_B/(\sigma^2_{N_0} + \sigma^2_{N_1}) = \theta \cdot \mathrm{SNR}_{A,src}$; and σ^2_U be the variance of U. Then we have:

$$\sigma^2_U = \sigma^2_B\left(1 + \frac{1}{\theta \cdot \mathrm{SNR}_{A,src}}\right).$$

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

$$\begin{aligned} R_{SM} \leq& C(\mathrm{SNR}_B) + \frac{1}{2}\log(1-\theta); \\ R_{SM} + R_{SK} \leq& |C(\mathrm{SNR}_B) - C(\mathrm{SNR}_E)|^+ \\ &+ C\left(\frac{\theta \cdot \mathrm{SNR}_{A,src}}{1+\mathrm{SNR}_{E,src}}\right), \end{aligned}$$

where $0 \leq \theta \leq \frac{\mathrm{SNR}_B}{1+\mathrm{SNR}_B}$.

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.

$$\begin{aligned} R_{SM} &\overset{(a)}{\leq} C(\mathrm{SNR}_B) - (I(U;S_A) - I(U;S_B)) \\ &\overset{(b)}{=} C(\mathrm{SNR}_B) + \frac{1}{2}\log(1-\theta), \end{aligned}$$

where (a) is due to (11) by a Gaussian choice of X; and (b) is due to the following calculations.

$$I(U;S_A) - I(U;S_B) = \frac{1}{2}\log\frac{1-\rho_{UB}^2}{1-\rho_{UA}^2} \overset{(b)}{=} \frac{1}{2}\log\frac{1}{1-\theta},$$

where ρ_{UA}, ρ_{UB} are the correlation coefficients of U and S_A, U and S_B, respectively; (b) is due to the fact that

$$\begin{aligned} \rho_{UB}^2 &= \left(\frac{E\{U \cdot S_B\}}{\sigma_U \cdot \sigma_B}\right)^2 = \frac{\sigma_B^2}{\sigma_U^2} = \frac{\theta \cdot \mathrm{SNR}_{A,src}}{1+\theta \cdot \mathrm{SNR}_{A,src}}; \\ \rho_{UA}^2 &= \left(\frac{E\{U \cdot S_A\}}{\sigma_U \cdot \sigma_A}\right)^2 = \frac{\sigma_A^2}{\sigma_U^2} \\ &= \frac{1+1/\mathrm{SNR}_{A,src}}{1+1/(\theta \cdot \mathrm{SNR}_{A,src})} = \frac{\theta \cdot (1+\mathrm{SNR}_{A,src})}{1+\theta \cdot \mathrm{SNR}_{A,src}}. \end{aligned}$$

Similarly, we have

$$\begin{aligned} R_{SM} + R_{SK} &\overset{(c)}{\leq} |C(\mathrm{SNR}_B) - C(\mathrm{SNR}_E)|^+ \\ &\quad + I(U;S_B) - I(U;S_E) \\ &\overset{(d)}{=} |C(\mathrm{SNR}_B) - C(\mathrm{SNR}_E)|^+ + C\left(\frac{\theta \cdot \mathrm{SNR}_{A,src}}{1+\mathrm{SNR}_{E,src}}\right), \end{aligned}$$

where (c) is due to (12) by a Gaussian choice of X; (d) is due to the following calculations.

$$\begin{aligned} I(U;S_B) - I(U;S_E) &= \frac{1}{2}\log\frac{1-\rho_{UE}^2}{1-\rho_{UB}^2} \\ &\overset{(e)}{=} \frac{1}{2}\log\frac{1+\theta \cdot \mathrm{SNR}_{A,src} + \mathrm{SNR}_{E,src}}{1+\mathrm{SNR}_{E,src}} \\ &= C\left(\frac{\theta \cdot \mathrm{SNR}_{A,src}}{1+\mathrm{SNR}_{E,src}}\right), \end{aligned}$$

where ρ_{UE} is the correlation coefficient of U and S_E; and (e) is due to the calculation of ρ_{UB}^2 in (b), and

$$\begin{aligned} \rho_{UE}^2 &= \left(\frac{E\{U \cdot S_E\}}{\sigma_U \cdot \sigma_E}\right)^2 = \frac{\sigma_B^2 \cdot \sigma_B^2}{\sigma_U^2 \cdot \sigma_E^2} \\ &= \frac{\theta \cdot \mathrm{SNR}_{A,src}}{1+\theta \cdot \mathrm{SNR}_{A,src}} \cdot \frac{\mathrm{SNR}_{E,src}}{1+\mathrm{SNR}_{E,src}}. \end{aligned}$$

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} :

$$\frac{1}{2}\log\frac{1}{1-\theta} \leq C(\mathrm{SNR}_B).$$

Easy calculation gives us $0 \leq \theta \leq \frac{\mathrm{SNR}_B}{1+\mathrm{SNR}_B}$. ■

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 $C\left(\frac{\mathrm{SNR}_{A,src}}{1+\mathrm{SNR}_{A,src}+\mathrm{SNR}_{E,src}}\right)$ bit as $\mathrm{SNR}_B \geq \mathrm{SNR}_{A,src}/(1+\mathrm{SNR}_{A,src}+\mathrm{SNR}_{E,src})$; and $C\left(\frac{\mathrm{SNR}_{A,src}}{1+\mathrm{SNR}_{E,src}+\mathrm{SNR}_B(1+\mathrm{SNR}_{A,src}+\mathrm{SNR}_{E,src})}\right)$ bit otherwise.

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 θ, a gap between them is bounded by $\max\{f_1(\theta), f_2(\theta)\}$, where

$$\begin{aligned} f_1(\theta) &= \frac{1}{2}\log\frac{1}{1-\theta}, \\ f_2(\theta) &= C\left(\frac{\mathrm{SNR}_{A,src}}{1+\mathrm{SNR}_{E,src}}\right) - C\left(\frac{\theta \cdot \mathrm{SNR}_{A,src}}{1+\mathrm{SNR}_{E,src}}\right) \\ &= \frac{1}{2}\log\frac{1+\mathrm{SNR}_{A,src}+\mathrm{SNR}_{E,src}}{1+\theta \cdot \mathrm{SNR}_{A,src}+\mathrm{SNR}_{E,src}}. \end{aligned}$$

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

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

- if there exists a θ_0, such that $0 \leq \theta_0 \leq \frac{\mathrm{SNR}_B}{1+\mathrm{SNR}_B}$ and $f_1(\theta_0) = f_2(\theta_0)$, i.e.,
$$\begin{aligned} \frac{1}{2}\log\frac{1}{1-\theta_0} &= \frac{1}{2}\log\frac{1+\mathrm{SNR}_{A,src}+\mathrm{SNR}_{E,src}}{1+\theta_0 \cdot \mathrm{SNR}_{A,src}+\mathrm{SNR}_{E,src}} \\ \theta_0 &= \frac{\mathrm{SNR}_{A,src}}{1+2\mathrm{SNR}_{A,src}+\mathrm{SNR}_{E,src}}, \end{aligned}$$
then we have
$$\begin{aligned} &\min_\theta \max\{f_1(\theta), f_2(\theta)\} = f_1(\theta_0) \\ =&C\left(\frac{\mathrm{SNR}_{A,src}}{1+\mathrm{SNR}_{A,src}+\mathrm{SNR}_{E,src}}\right) < 0.5. \end{aligned}$$
Note that $\theta_0 \leq \frac{\mathrm{SNR}_B}{1+\mathrm{SNR}_B}$ implies that $\mathrm{SNR}_B \geq \frac{\mathrm{SNR}_{A,src}}{1+\mathrm{SNR}_{A,src}+\mathrm{SNR}_{E,src}}$.
- However, in case that $\theta_0 > \frac{\mathrm{SNR}_B}{1+\mathrm{SNR}_B}$, i.e., $\mathrm{SNR}_B < \frac{\mathrm{SNR}_{A,src}}{1+\mathrm{SNR}_{A,src}+\mathrm{SNR}_{E,src}}$, we have
$$\begin{aligned} &\min_\theta \max\{f_1(\theta), f_2(\theta)\} = f_2(\frac{\mathrm{SNR}_B}{1+\mathrm{SNR}_B}) \\ =&C\left(\frac{\mathrm{SNR}_{A,src}}{1+\mathrm{SNR}_{E,src}+\mathrm{SNR}_B(1+\mathrm{SNR}_{A,src}+\mathrm{SNR}_{E,src})}\right). \end{aligned}$$

This concludes our proof. ■

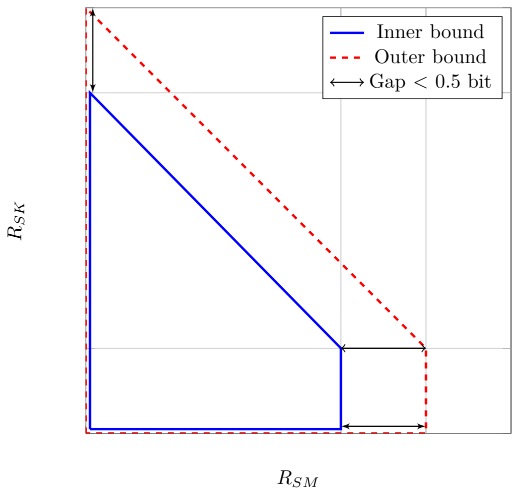

Fig. 3: A constant gap between inner and outer bounds as $\text{SNR}_B \geq 1$.

D. Discussions

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

As $\text{SNR}_{A,src} = 0$, 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 $\text{SNR}_{E,src} = 0$, 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

$$\frac{1}{2}\log\frac{(1+\text{SNR}_B)(1+\text{SNR}_{A,src})}{1+\text{SNR}_{A,src}+\min\{\text{SNR}_B,\text{SNR}_E\}} \tag{15}$$

by taking $\theta = \frac{\min\{\text{SNR}_B,\text{SNR}_E\}}{1+\text{SNR}_{A,src}+\min\{\text{SNR}_B,\text{SNR}_E\}}$; and by taking $\theta = \frac{\text{SNR}_B}{1+\text{SNR}_B}$ the secret-key capacity

$$\frac{1}{2}\log\frac{(1+\text{SNR}_B)(1+\text{SNR}_{A,src})-\text{SNR}_{A,src}}{1+\min\{\text{SNR}_B,\text{SNR}_E\}}. \tag{16}$$

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 Gaussion 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 $\text{SNR}_B \geq 1$.

VI. Appendix

Lemma 1. For any U such that $U \to S_A \to S_B \to S_E$ 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

$$\begin{aligned}&I(U,S_A;S_B) - I(U,S_A;S_E)\\ =&I(S_A;S_B) - I(S_A;S_E) + I(U;S_B|S_A) - I(U;S_E|S_A)\\ \overset{(a)}{=}&I(S_A;S_B) - I(S_A;S_E),\end{aligned}$$

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

$$\begin{aligned}&I(U,S_A;S_B) - I(U,S_A;S_E)\\ =&I(U;S_B) - I(U;S_E) + I(S_A;S_B|U) - I(S_A;S_E|U)\\ \overset{(b)}{\geq}&I(U;S_B) - I(U;S_E).\end{aligned}$$

Note that (b) is due to the fact that

$$\begin{aligned}I(S_A;S_B|U) =&I(S_A;S_B,S_E|U) - I(S_A;S_E|S_B,U)\\ \overset{(c)}{=}&I(S_A;S_B,S_E|U) \geq I(S_A;S_E|U),\end{aligned}$$

where (c) is by $I(S_A;S_E|S_B,U) = 0$ since the Markov chain $S_A \to S_B \to S_E$ holds for any realizations of U. Therefore, we have

$$\begin{aligned}I(U,S_A;S_B) - I(U,S_A;S_E) &= I(S_A;S_B) - I(S_A;S_E)\\ &\geq I(U;S_B) - I(U;S_E).\end{aligned}$$

This concludes the proof. ■

Lemma 2. Let S_A, S_B be jointly Gaussian, then for any U such that $U \to S_A \to S_B$ forms a Markov chain, there exists V such that $S_A \to S_B \to V$ 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/translating, assume w.l.o.g. that $p_{S_A S_B}$ is symmetric in S_A, S_B. The lemma follows by taking $p_{V|S_B} = p_{U|S_A}$. (Many thanks to Dr. Thomas Courtade for the proof.) ■

References

[1] A. D. Wyner, "The Wire-tap Channel," *Bell Systems Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

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

[3] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. i. secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.

[4] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, 1993.

[5] V. M. Prabhakaran, K. Eswaran, and K. Ramchandran, "Secrecy via sources and channels," *IEEE transactions on information theory*, vol. 58, no. 11, pp. 6747–6765, 2012.

[6] M. El-Halabi, T. Liu, C. N. Georghiades, and S. Shamai, "Secret writing on dirty paper: A deterministic view," *IEEE Transactions on Information Theory*, vol. 58, no. 6, pp. 3419–3429, 2012.

[7] A. S. Avestimehr, S. N. Diggavi, and D. N. Tse, "Wireless network information flow: A deterministic approach," *IEEE Transactions on Information Theory*, vol. 57, no. 4, pp. 1872–1905, 2011.

[8] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.