Secret Key Generation From Vector Gaussian Sources With Public and Private Communications

Yinfei Xu
School of Information Science and Engineering
Southeast University, Nanjing 210096, China
Email: yinefeixu@seu.edu.cn

Daming Cao
Department of Computer Science
National University of Singapore, Singapore
Email: dcscad@nus.edu.sg

Abstract—In this paper, we consider the problem of secret key generation with one-way communication through both a rate-limited public channel and a rate-limited secure channels where the public channel is from Alice to Bob and Eve and the secure channel is from Alice to Bob. In this model, we do not pose any constraints on the sources, i.e. Bob is not degraded to or less noisy than Eve. We obtain the optimal secret key rate in this problem, for the vector Gaussian sources setting. The characterization is derived by suitably applying the enhancement argument, and Proving a new extremal inequality. The extremal inequality can be seen as coupling of two extremal inequalities, which are related to the degraded compound MIMO Gaussian broadcast channel, and the vector generalization of Costa’s entropy power inequality, accordingly.

I. INTRODUCTION

The information foundations of secret key generation problem was first laid by Maurer [1], and then by Ahlswede and Csiszár [2]. In their papers, there are two separate terminals, named Alice and Bob, observe the outcomes of a pair of correlated sources separately and want to generate a common secret key, which is concealed from an eavesdropper Eve, given that the terminals can communicate through a noiseless public channel where the eavesdropper has complete access to. In [2], the secret key capacity of correlated sources was characterized when Alice and Bob are allowed to communicate once over a channel with unlimited capacity. The secrecy key capacity was found by Csiszár and Narayan [3] when there is a constraint on the rate of the public channel.

We consider the problem of secret key generation with one-way communication. In addition to the rate limited public link observed by both Bob and Eve, the secure link which only connects Alice and Bob, is also considered in our model. For the vector Gaussian sources setting, one of difficulties to show the fundamental tradeoff between the key capacity and the communication constraints is that vector Gaussian sources are not in general degraded. This difficulty frequently appears in several vector Gaussian multi-terminal problem [4]–[8]. In [9], Watanabe and Oohama circumvent this difficulty by suitably applying the enhancement argument. Further invoking the so-called Costa’s type extremal inequality [7], they showed that one Gaussian auxiliary random variable suffices to characterise the rate region when there is only rate constraint on the public channel. For the private and public communication available in our setting, we show that two auxiliary random variables should be considered, instead of one in the only public communication setting in [9]. The corresponding extremal inequality should be decoupled into two enhanced extremal inequalities, in which one is related to the degraded compound MIMO Gaussian broadcast channel in [10], [11], and the other one is the vector generalization of Costa’s entropy power inequality in [7], [9].

The rest of this paper is organized as follows. The problem setup is given in Section II, we first revisit the optimal achievable rate region for the case of discrete memoryless sources case in [12], and then we show the rate region characterization for the case of vector Gaussian sources considered in this paper. The converse proof for the vector Gaussian sources are shown in Section III. The major ingredients are our new extremal inequality, and we show the Gaussian auxiliary random variables suffice to achieve the optimal rate region. In Section IV, we conclude with a summary of our results.

II. PROBLEM STATEMENT AND MAIN RESULT

A. Discrete Memoryless Sources

Consider a network with three nodes, including a transmitter Alice, a receiver Bob and an eavesdropper Eve. We assume three discrete memoryless sources indicated by random variables \((X, Y, Z)\), defined in the alphabets \((\mathcal{X}, \mathcal{Y}, \mathcal{Z})\), respectively. We assume that Alice and Bob observe the \(n\)-length source sequences \(X^n\) and \(Y^n\), respectively, and Eve observes \(n\)-length source sequence \(Z^n\). In order to generate a secret key \(K\), which is shared by Alice and Bob and concealed from Eve, Alice can send two messages \(M_1\) and \(M_2\), where \(M_1\) is through a noiseless public channel, which can be observed by...
Eve, and $M_2$ is through a noiseless secure channel, to which Eve has no access.

A $(2nR_1, 2nR_2, n)$ code consists of

- a public encoding function $\phi_1 : X^n \mapsto M^n_1 = [1 : 2nR_1]$ that finds a codeword $m_1(x^n)$ to each $n$-length source sequence $x^n$, and sends it to both Bob and Eve,
- a private encoding function $\phi_2 : X^n \mapsto M^n_2 = [1 : 2nR_2]$ that finds a codeword $m_2(x^n)$ to each $n$-length source sequence $x^n$, and sends it to both Bob only,
- a key generation function $\psi_1 : X^n \mapsto K^n = [1 : 2nR_K]$ that assigns a random mapping $k_1(x^n)$ by giving Alice’s $n$-length source sequence $x^n$.
- a key generation function $\psi_2 : Y^n \times M^n_1 \times M^n_2 \mapsto K^n = [1 : 2nR_K]$ that assigns a random mapping $k_2(y^n, m_1, m_2)$ by giving Bob’s $n$-length source sequence $y^n$ and all received indices $m_1$ and $m_2$.

Then the secret key is generated by Alice and Bob from the functions $\psi_1$ and $\psi_2$, respectively, which should agree with probability 1 and be concealed from Eve. The probability of error for the key generation code is defined as

$$P_e(n) = \Pr \{ K_1 \neq K_2 \}.$$  \hspace{1cm} (1)

The key leakage rate at Eve is defined as

$$R_L(n) = \max_{j \in \{1, 2\}} \frac{1}{n} \sum_{i \in M_i} I(K_j; Z^n, M_i).$$  \hspace{1cm} (2)

**Definition 1:** A secret key rate $R_K$ with constraint communication rate pair $(R_1, R_2)$ is achievable if there exists a sequence of $(2nR_1, 2nR_2, n)$ code such that

$$\lim_{n \to \infty} P_e(n) = 0,$$

$$\lim_{n \to \infty} R_L(n) = 0.$$  \hspace{1cm} (3)

For the discrete memoryless source setting, we have the following single-letter expression on the largest achievable secret key rate $R_K$ with public and private communication constraints $R_1$ and $R_2$.

**Theorem 1 (12, Theorem 1):** For the discrete memoryless secret key generation problem with public and private communication constraints, the rate tuple $(R_K, R_1, R_2)$ is achievable if and only if

$$R_K - R_2 \leq I(U; Y|V) - I(U; Z|V),$$

$$R_1 + R_2 \geq I(U; X) + I(V; X),$$

$$R_1 \geq I(V; Y).$$  \hspace{1cm} (5)

(6) (7)

where random variables $(V, U, X, Y, Z)$ satisfy the following Markov chain

$$V \rightarrow U \rightarrow X \rightarrow (Y, Z).$$  \hspace{1cm} (8)

**B. Vector Gaussian Sources**

Now we study the same communication constrained secret key generation problem, for the vector Gaussian sources setting (see Fig.1). Let $\{X(t), Y(t), Z(t)\}_{t=1}^n$ be i.i.d. vector-valued discrete time Gaussian sources, where across the time index $t$, each tuple is drawn from the same jointly vector Gaussian distribution. The encoder, the legitimate decoder and the eavesdropper decoder observe $X(t)$, $Y(t)$ and $Z(t)$, respectively. The vector Gaussian source $(X(t), Y(t), Z(t))_t^n$ can be written as

$$Y(t) = X(t) + N_Y(t),$$

$$Z(t) = X(t) + N_Z(t).$$  \hspace{1cm} (9)

(10)

where each $X(t)$ is a $p \times 1$-dimensional Gaussian random vector with mean zero and covariance $\mathbf{K}_X > 0$, each $N_Y(t)$ is a $p \times 1$-dimensional Gaussian random vector with mean zero and covariance $\mathbf{K}_Y > 0$, and $N_Z(t)$ is a $p \times 1$-dimensional Gaussian random vector with mean zero and covariance $\mathbf{K}_Z > 0$. Respectively. We shall point out that $(N_Y(t), N_Z(t))$ and $X(t)$ are independent from expressions (9) and (10). However, no additional independence relationship is imposed between $N_Y(t)$ and $N_Z(t)$.

In [9], the authors showed that a single layer code suffices, and characterize the optimal trade-off on $R_K$ and $R_1$ for the vector Gaussian sources setting. Their converse method is motivated by the enhancement argument [4], [5] for vector Gaussian wiretap channel in [6]. In this paper, we show a similar enhancement on two-layer superposition codes can be applied to establish the converse proof on the optimal $(R_K, R_1, R_2)$ trade-off problem.

According to Theorem 1 for discrete memoryless sources, a single-letter description of the optimal $(R_K, R_1, R_2)$ trade-off for the vector Gaussian secret key generation problem can be given as follows.

**Theorem 2:** For the vector Gaussian secret key generation problem with public and private communication constraints, the rate tuple $(R_K, R_1, R_2)$ is achievable if and only if

$$R_K - R_2 \leq \frac{1}{2} \log \frac{||\mathbf{K} + \mathbf{K}_Y - \mathbf{B}_1||}{||\mathbf{K} + \mathbf{K}_Y - \mathbf{B}_1 - \mathbf{B}_2||} - \frac{1}{2} \log \frac{||\mathbf{K} + \mathbf{K}_Z - \mathbf{B}_1||}{||\mathbf{K} + \mathbf{K}_Z - \mathbf{B}_1 - \mathbf{B}_2||},$$  \hspace{1cm} (11)

$$R_1 + R_2 \geq \frac{1}{2} \log \frac{||\mathbf{K} - \mathbf{B}_1 - \mathbf{B}_2||}{||\mathbf{K}||} - \frac{1}{2} \log \frac{||\mathbf{K} + \mathbf{K}_Y - \mathbf{B}_1 - \mathbf{B}_2||}{||\mathbf{K} + \mathbf{K}_Y||},$$  \hspace{1cm} (12)

$$R_1 \geq \frac{1}{2} \log \frac{||\mathbf{K}||}{||\mathbf{K} - \mathbf{B}_1||} - \frac{1}{2} \log \frac{||\mathbf{K} + \mathbf{K}_Y||}{||\mathbf{K} + \mathbf{K}_Y - \mathbf{B}_1||}.$$  \hspace{1cm} (13)

for some positive semi-definite matrices $\mathbf{B}_1, \mathbf{B}_2 \succeq 0$.

**Proof:** The achievable part is based on constructing Gaussian test channels to preserve the Markov chain $V \rightarrow U \rightarrow X \rightarrow (Y, Z)$, and the details can be found in [13, Appendix A]. The converse part is presented in Section III.

**III. THE CONVERSE OF THEOREM 2**

**A. The Extremal Inequality**

As in [9], the achievable rate region of $(R_K, R_1, R_2)$ for vector Gaussian sources is defined as

$$\mathcal{R}(\{X, Y, Z\}) \triangleq \{(R_K, R_1, R_2) : (R_K, R_1, R_2) \text{ is achievable}\}.$$  \hspace{1cm} (14)
Due to the convexity of $R(X, Y, Z)$, to characterize the optimal trade-off of $(R_K, R_1, R_2)$ for the vector Gaussian model, we can write the following $\mu$-sum problem, alternatively,

$$\inf_{(R_K, R_1, R_2) \in \mathcal{R}(X, Y, Z)} \mu_1(R_2 - R_K) + \mu_2(R_1 + R_2) + \mu_3R_1$$

(15) = \inf_{(R_K, R_1, R_2) \in \mathcal{R}(X, Y, Z)} (\mu_2 + \mu_3)R_1 + (\mu_1 + \mu_2)R_2 - \mu_1R_K,

(16)

for any $\mu_1, \mu_2, \mu_3 \geq 0$. To prove the converse part of Theorem 2, it is equivalent to show the following inequality holds for any $(R_K, R_1, R_2) \in \mathcal{R}(X, Y, Z),$

$$(\mu_2 + \mu_3)R_1 + (\mu_1 + \mu_2)R_2 - \mu_1R_K \geq \mathfrak{R}^*(\mu_1, \mu_2, \mu_3),$$

(17)

where $\mathfrak{R}^*(\mu_1, \mu_2, \mu_3)$ is a Gaussian optimization problem shown as follows

$$\mathfrak{R}^*(\mu_1, \mu_2, \mu_3) \triangleq \min_{B_1, B_2} \frac{\mu_1 + \mu_2}{2} \log |K + K_Y - B_1 - B_2|$$

$$- \frac{\mu_2}{2} \log |K + K_Z - B_1 - B_2|$$

$$- \frac{\mu_2}{2} \log |K - B_1 - B_2| + \frac{\mu_1}{2} \log |K + K_Z - B_1|$$

$$+ \frac{\mu_3 - \mu_1}{2} \log |K + K_Y - B_1| - \frac{\mu_3}{2} \log |K - B_1|$$

$$+ \frac{\mu_2 + \mu_3}{2} \log |K| - \frac{\mu_2 + \mu_3}{2} \log |K + K_Y|$$

subject to $B_1 \succeq 0, B_2 \succeq 0.$ (18)

Let $(B_1^*, B_2^*)$ be one (non-unique) minimizer of the optimization problem $\mathfrak{R}^*(\mu_1, \mu_2, \mu_3)$. The necessary Karush-Kuhn-Tucker (KKT) conditions are given in the following lemma.

**Lemma 1:** The minimizer $(B_1^*, B_2^*)$ of $\mathfrak{R}^*(\mu_1, \mu_2, \mu_3)$ need to satisfy

$$\frac{\mu_1}{2} (K + K_Z - B_1^* - B_2^*)^{-1} + \frac{\mu_2}{2} (K - B_1^* - B_2^*)^{-1}$$

$$= \frac{\mu_1 + \mu_2}{2} (K + K_Y - B_1^* - B_2^*)^{-1} + M_2, \quad (19)$$

$$\frac{\mu_3}{2} (K - B_1^*)^{-1} + \frac{\mu_3 - \mu_1}{2} (K + K_Y - B_1^*)^{-1} + M_2$$

$$= \frac{\mu_1}{2} (K + K_Z - B_1^*)^{-1} + M_1, \quad (20)$$

for some positive semi-definite matrices $B_1^*, B_2^*, M_1, M_2 \succeq 0$ such that

$$B_1^*M_1 = M_1B_1^* = 0, \quad (21)$$

$$B_2^*M_2 = M_2B_2^* = 0. \quad (22)$$

Now starting from the single-letter expressions in Theorem 1, the $\mu$-sum problem for any rate tuple in $\mathcal{R}(X, Y, Z)$ should be lower bounded by

$$\mu_1[I(U; Z|V) - I(U; Y|V)] + \mu_2I(U; X|Y)$$

(23) + $\mu_3I(V; X|Y)$

(25)

$$= \mu_1[I(U; Z|V) - I(U; Y|V)] + \mu_2[I(U; X) - I(U; Y)]$$

(26) + $\mu_3[I(V; X) - I(V; Y)]$

(27)

$$= \mu_1h(Z|V) + (\mu_3 - \mu_1)h(Y|V) - \mu_3h(X|V)$$

$$+ (\mu_1 + \mu_2)h(Y|U) - \mu_2h(X|U) - \mu_1h(Z|U)$$

$$+ (\mu_1 + \mu_3)h(X) - (\mu_2 + \mu_3)h(Y)$$

$$= (\mu_1 + \mu_2)h(Y|U) - \mu_1h(Z|U) - \mu_2h(X|U)$$

$$+ \mu_1h(Z|V) + (\mu_3 - \mu_1)h(Y|V) - \mu_3h(X|V)$$

$$+ \frac{\mu_2 + \mu_3}{2} \log |K| - \frac{\mu_2 + \mu_3}{2} \log |K + K_Y|,$$

(28)

where

(a) follows from Makov Chain $(U, V) \rightarrow X \rightarrow Y$, (b) follows from Makov Chain $V \rightarrow U \rightarrow X \rightarrow (Y, Z)$.

By comparing (28) with optimization problem $\mathfrak{R}^*(\mu_1, \mu_2, \mu_3)$ in (18), it can be shown that to prove Theorem 2, it is sufficient to prove the following extremal inequality

**Theorem 3:** There exist two positive semi-definite matrices $B_1^*$ and $B_2^*$ which satisfy KKT conditions (19)-(22) in Lemma 1 to minimize optimization problem $\mathfrak{R}^*(\mu_1, \mu_2, \mu_3)$, then for some real numbers $\mu_1, \mu_2, \mu_3 \geq 0$, we have

$$\mu_1h(Z|V) + (\mu_3 - \mu_1)h(Y|V) - \mu_3h(X|V)$$

$$- \frac{\mu_1}{2} \log |K + K_Y - B_1^* - B_2^*|$$

$$- \frac{\mu_2}{2} \log |K + K_Z - B_1^* - B_2^*|$$

$$= \frac{\mu_1}{2} \log |K + K_Z - B_1^* - B_2^*|$$

$$+ \frac{\mu_1 + \mu_2}{2} \log |K + K_Y - B_1^* - B_2^*|$$

$$+ \frac{\mu_3 - \mu_1}{2} \log |K + K_Y - B_1^* - B_2^*|$$

$$+ \frac{\mu_3}{2} \log |K + K_Y - B_1^* - B_2^*|$$

(29)

for any $(U, V)$ such that $V \rightarrow U \rightarrow X \rightarrow (Y, Z)$ forms a Markov chain.

The proof of (29) depends on the enhancement argument introduced in [4], [5], which can be divided into two steps. In the first step, we enhance the source $Y$ to $\tilde{Y}$ such that the Markov chain $X \rightarrow \tilde{Y} \rightarrow (Y, Z)$ holds. In the second step, we decouple to extremal inequality (28) to two new ones, associated with enhanced sources $\tilde{Y}$, respectively. The proof of extremal inequality (28) in provided by involving the two enhanced extremal inequalities, which is related to the degraded compound MIMO Gaussian broadcast channel in [10], [11], and the vector generalization of Costa’s entropy power inequality in [7], [9].

**B. Some Lemmas**

In order to reduce the non-degraded sources to the degraded case, we introduce a new covariance matrix such that

$$\frac{\mu_1 + \mu_2}{2} (K + K_Y - B_1^* - B_2^*)^{-1}$$

$$= \frac{\mu_1 + \mu_2}{2} (K + K_Y - B_1^* - B_2^*)^{-1} + M_2 \succ 0. \quad (30)$$
Then $\tilde{K}_Y$ has useful properties listed in the following lemma.

**Lemma 2**: $\tilde{K}_Y$ has the following properties:
1) $0 \prec \tilde{K}_Y \preceq K_Y$;
2) $K_Y \preceq \tilde{K}_Z$;
3) $\frac{\mu_1 + \mu_2}{2} \left( K + \tilde{K}_Y - B_1^* \right)^{-1} = \frac{\mu_1 + \mu_2}{2} \left( K + K_Y - B_1^* \right)^{-1} + M_2$; \hspace{1cm} (31)
4) \(\left( K + \tilde{K}_Y - B_1^* - B_2^* \right)^{-1} \left( K + \tilde{K}_Y - B_1^* \right) = \left( K + K_Y - B_1^* - B_2^* \right)^{-1} \left( K + K_Y - B_1^* \right)\). \hspace{1cm} (32)

Proof: The proof of Lemma 2 is omitted due to space limitation.

Moreover, to decouple our extremal inequality (29), we need the vector generalization of Costa’s entropy power inequality [7], and the generalized extremal inequality related the degraded compound MIMO Gaussian broadcast channel in [10], [11], as two auxiliary lemmas.

**Lemma 3** ([7, Corollary 2]): Let $Z_1$, $Z_2$ and $Z_3$ be Gaussian random vectors with positive definite covariance matrices $N_1$, $N_2$ and $N_3$, respectively. Furthermore, $N_1$, $N_2$ satisfy $N_1 \preceq N_2$. If there exists a positive semi-definite covariance $B^*$ such that $\left( B^* + N_1 \right)^{-1} + \lambda \left( B^* + N_2 \right)^{-1} = \left( \lambda + 1 \right) \left( B^* + N_3 \right)^{-1}$, \hspace{1cm} (33)
where $\lambda \geq 0$, then $h(X + Z_1|U) + \mu h(X + Z_2|U) - (\mu + 1) h(X + Z_3|U) \leq \frac{1}{2} \log |B^* + N_1| + \frac{\mu}{2} \log |B^* + N_2| - \frac{\mu + 1}{2} \log |B^* + N_3|$, \hspace{1cm} (34)
for any $(X, U)$ independent of $(Z_1, Z_2, Z_3)$.

**Lemma 4** ([10, Corollary 4]): Let $\{Z_j\}_{j=1}^{L_1}$ and $\{Z_j\}_{j=1}^{L_2}$ be real Gaussian random vectors with positive definite covariance matrices $\{N_i\}_{i=1}^{L_1}$ and $\{N_i\}_{i=1}^{L_2}$, respectively. We assume that there exits a covariance matrix $N^*$ such that $\{N_i\}_{i=1}^{L_1} \preceq N^* \preceq \{N_i\}_{i=1}^{L_2}$. \hspace{1cm} (35)
Furthermore, let $B^*$ be a positive semi-definite covariance matrix such that $\sum_{i=1}^{L_1} \lambda_i (B^* + N_i)^{-1} = \sum_{j=1}^{L_2} \lambda_j (B^* + N_j)^{-1} + \Psi$, \hspace{1cm} (36)
where $\lambda_i, \lambda_j \geq 0$, $1 \leq i \leq L_1$, $1 \leq j \leq L_2$, $\Psi \preceq 0$ and $\left( K - B^* \right) \Psi = \Psi \left( K - B^* \right) = 0$. \hspace{1cm} (37)
The for any distribution $(X, U)$ independent of $(Z_j)_{j=1}^{L_1}$ and $(Z_j)_{j=1}^{L_2}$, such that $\text{cov} \{X|U\} \preceq K$, we have $\sum_{i=1}^{L_1} \lambda_i h(X + Z_i|U) - \sum_{j=1}^{L_2} \lambda_j h(X + Z_j|U) \leq \sum_{i=1}^{L_1} \frac{\lambda_i}{2} \log |B^* + N_i| - \sum_{j=1}^{L_2} \frac{\lambda_j}{2} \log |B^* + N_j|$. \hspace{1cm} (38)

**C. Proof of Theorem 3**

We proceed to proof the extremal inequality (29). At the beginning, we rewrite the l.h.s. of (29) by involving the enhanced source $\tilde{Y}$.

$\left( \mu_1 + \mu_2 \right) h(Y|U) - \mu_1 h(Z|U) - \mu_2 h(X|U)$
\[ + \mu_1 h(Z|V) + (\mu_2 - \mu_3) h(Y|V) - \mu_3 h(X|V) \]
\[ = \left( \mu_1 + \mu_2 \right) h(\tilde{Y}|U) - \mu_1 h(Z|U) - \mu_2 h(X|U) \] \hspace{1cm} (39a)
\[ + \mu_1 h(Z|V) + (\mu_2 + \mu_3) h(Y|V) \]
\[ - \mu_1 h(\tilde{Y}|V) - \mu_3 h(X|V) \] \hspace{1cm} (39b)
\[ + (\mu_1 + \mu_2) \left[ h(Y|U) - h(\tilde{Y}|U) \right] - (\mu_1 + \mu_2) [h(Y|V) - h(\tilde{Y}|V)]. \] \hspace{1cm} (39c)

1) **The lower bound of** (39a): Notice that from the definition of $Y$ in (30), and the KKT conditions of (19), we get $\frac{\mu_1 + \mu_2}{2} \left( K + K_Y - B_1^* - B_2^* \right)^{-1} + \frac{\mu_2}{2} \left( K - B_1^* - B_2^* \right)^{-1}$
\[ = \frac{\mu_1 + \mu_2}{2} \left( K + \tilde{K}_Y - B_1^* - B_2^* \right)^{-1}. \] \hspace{1cm} (40)
Furthermore, from the first and second statement of Lemma 2,
\[ 0 \prec \tilde{K}_Y \preceq K_Z. \] \hspace{1cm} (41)

Using which in conjecture with Lemma 3, we have the following lower bound of (39a):

$\left( \mu_1 + \mu_2 \right) h(Z|U) - \mu_1 h(Z|U) - \mu_2 h(X|U)$
\[ \geq \frac{\mu_1 + \mu_2}{2} \log |K + \tilde{K}_Y - B_1^* - B_2^*| \]
\[ - \frac{\mu_1}{2} \log |K + K_Z - B_1^* - B_2^*| \]
\[ - \frac{\mu_2}{2} \log |K - B_1^* - B_2^*|. \] \hspace{1cm} (42)

2) **The lower bound of** (39b): Notice that from the third statement of Lemma 2, and the KKT conditions of (20), we get $\frac{\mu_3}{2} \left( K - B_1^* \right)^{-1} + \frac{\mu_1 + \mu_2}{2} \left( K + \tilde{K}_Y - B_1^* \right)^{-1}$
\[ = \frac{\mu_2 + \mu_3}{2} \left( K + K_Y - B_1^* \right)^{-1} \]
\[ + \frac{\mu_1}{2} \left( K + K_Z - B_1^* \right)^{-1} + M_1. \] \hspace{1cm} (43)
Furthermore, from the first and second statement of Lemma 2,
\[ 0 \prec \tilde{K}_Y \preceq \{K_Y, K_Z\}. \] \hspace{1cm} (44)

Notice the KKT conditions of (21) as well. We can use Lemma 4 to obtain the following lower bound on (39b):

$\mu_1 h(Z|V) + (\mu_2 + \mu_3) h(Y|V)$
\[ - (\mu_1 + \mu_2) h(\tilde{Y}|V) - \mu_3 h(X|V). \]
\[
\begin{align*}
&\geq \frac{\mu_1}{2} \log |K + K_Z - B_1^*| \\
&\quad + \frac{\mu_2 + \mu_3}{2} \log |K + K_X - B_1^*| \\
&\quad - \frac{\mu_1 + \mu_2}{2} \log |K + \tilde{K}_Y - B_1^*| - \frac{\mu_3}{2} \log |K - B_1^*|.
\end{align*}
\] (45)

3) The lower bound of (39c): From the first statement of Lemma 2, we can decompose \( \mathbf{Y} \) into two parts: \( \mathbf{Y} = \mathbf{Y} + \mathbf{Y} \), where \( \mathbf{Y} \) is a Gaussian random vector with covariance \( \mathbf{K}_Y - \mathbf{K}_Y \), and it is assumed to be independent of \( (\mathbf{Y}, \mathbf{U}) \). The difference between \( h(\mathbf{Y}|\mathbf{U}) \) and \( h(\mathbf{Y}|\mathbf{Y}) \) may be written as

\[
h(\mathbf{Y}|\mathbf{U}) - h(\mathbf{Y}|\mathbf{Y}) = h(\mathbf{Y} + \mathbf{Y}|\mathbf{U}) - h(\mathbf{Y}|\mathbf{Y})
\]

(a) follows from the forth statement of Lemma 2.

(b) follows from Markov chain \( V \to U \to X \to Y \), and the fact that conditioning reduces entropy.

Thus, (49) implies (39c) is lower bounded by 0.

Now we are ready to show the extremal inequality (29) via combining all the lower bounds together.

\[
(\mu_1 + \mu_2)h(\mathbf{Y}|\mathbf{U}) - \mu_1 h(\mathbf{Z}|\mathbf{U}) - \mu_2 h(\mathbf{X}|\mathbf{U})
\]

\[
+ \mu_1 h(\mathbf{Z}|\mathbf{V}) + (\mu_3 - \mu_1) h(\mathbf{Y}|\mathbf{V}) - \mu_3 h(\mathbf{X}|\mathbf{V})
\]

\[
\geq \frac{\mu_1 + \mu_2}{2} \log |K + \tilde{K}_Y - B_1^* - B_2^*| - \frac{\mu_1}{2} \log |K + K_Z - B_1^* - B_2^*| - \frac{\mu_2 + \mu_3}{2} \log |K + K_X - B_1^*| - \frac{\mu_3}{2} \log |K - B_1^*|.
\] (50)

where (a) follows from the forth statement of Lemma 2.

IV. CONCLUSION

In this paper, we consider the vector Gaussian secret key generation problem with limited rate constrained public and private communications. A single-letter characterization is obtained. The proof is based on suitable applications of the enhancement argument, and the proof of a new extremal inequality, which should be decoupled into two different forms of extremal inequalities.

ACKNOWLEDGMENT

The work was supported by the National Natural Science Foundation of China under Grant 61901105, the Natural Science Foundation of Jiangsu Province under Grant BK20190343, the Youth Fund of MOE (Ministry of Education in China) Project of Humanities and Social Sciences (Project No. 20YJC630245), and the Fundamental Research Funds for the Central Universities under Grant 30919013229.

REFERENCES

[1] U. M. Maurer, “Secret key agreement by public discussion from common information,” IEEE Trans. Inf. Theory, vol. 39, no. 3, pp. 733–742, May 1993.

[2] R. Ahlswede and I. Csiszár, “Common randomness in information theory and cryptography. I: secret sharing,” IEEE Trans. Inf. Theory, vol. 39, no. 4, pp. 1121–1132, Sep. 1993.

[3] I. Csiszár and P. Narayan, “Common randomness and secret key generation with a helper,” IEEE Trans. Inf. Theory, vol. 46, no. 2, pp. 344–366, Mar. 2000.

[4] H. Weingarten, Y. Steinberg, and S. Shamai, “The capacity region of the Gaussian multiple-input multiple-output broadcast channel,” IEEE Trans. Inf. Theory, vol. 52, no. 9, pp. 3936–3964, Sep. 2006.

[5] T. Liu and P. Viswanath, “An extremal inequality motivated by multiterminal information-theoretic problems,” IEEE Trans. Inf. Theory, vol. 53, no. 5, pp. 1839–1851, May 2007.

[6] T. Liu and S. Shamai, “A note on the secrecy capacity of the multiple-antenna wiretap channel,” IEEE Trans. Inf. Theory, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[7] R. Liu, T. Liu, H. V. Poor, and S. Shamai, “A vector generalization of Costa’s entropy-power inequality with applications,” IEEE Trans. Inf. Theory, vol. 56, no. 4, pp. 1865–1879, Apr. 2010.

[8] E. Ekrem and S. Ulukus, “Secure lossy transmission of vector Gaussian sources,” IEEE Trans. Inf. Theory, vol. 59, no. 9, pp. 5466–5487, Sep. 2013.

[9] S. Watanabe and Y. Oohama, “Secret key agreement from vector Gaussian sources by rate limited public communication,” IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 541–550, Sep. 2011.

[10] H. Weingarten, T. Liu, S. Shamai, Y. Steinberg, and P. Viswanath, “The capacity region of the degraded multiple-input multiple-output compound broadcast channel,” IEEE Trans. Inf. Theory, vol. 55, no. 11, pp. 5011–5023, Nov. 2009.

[11] H. Chong and Y. Liang, “An extremal inequality and the capacity region of the degraded compound Gaussian MIMO broadcast channel with multiple users,” IEEE Trans. Inf. Theory, vol. 60, no. 10, pp. 6131–6143, Oct. 2014.

[12] D. Cao and W. Kang, “Secret key generation from correlated sources and secure link,” in Proc. Int. Conf. Wireless Commun. Signal Process., Oct. 2017, pp. 1–5.

[13] Y. Xu and D. Cao, “Secret key generation from vector Gaussian sources with public and private communications,” preprint. [Online]. Available: arXiv:2004.05086.