Strong Secrecy for Interference Channels Based on Channel Resolvability

Zhao Wang, Rafael F. Schaefer, *Senior Member, IEEE*, Mikael Skoglund, *Senior Member, IEEE*, Ming Xiao, *Senior Member, IEEE*, and H. Vincent Poor, *Fellow, IEEE*

***Abstract*—Interference channels with confidential messages are studied under strong secrecy constraints, based on the framework of channel resolvability theory. It is shown that if the random binning rate for securing a confidential message is above the resolution of its corresponding wiretapped channel, strong secrecy can be guaranteed. The information-spectrum method introduced by Han and Verdú is generalized to an arbitrary interference channel to obtain a direct channel resolvability result as a first step. For stationary and memoryless channels with discrete output alphabets, the results show that the achievable rates under weak and strong secrecy constraints are the same. This result is then generalized to channels with continuous output alphabets by deriving a reverse direction of Pinsker's inequality to bound the secrecy measure from above by a function of the variational distance of relevant distributions. As an application, Gaussian interference channels are studied in which the agreement between the best known weak and strong secrecy rate regions also appear. Following the footsteps of Csiszár, Hayashi and of Bloch and Laneman, these results provide further evidence that channel resolvability is a powerful and general framework for strong secrecy analysis in multiuser networks.**

***Index Terms*—Strong secrecy, interference channel, channel resolvability, reverse Pinsker's inequality, variational distance.**

I. Introduction

THE notion of information theoretic secrecy was first introduced by Wyner in the context of the degraded wiretap channel [1], in which a confidential message is sent from a transmitter to a legitimate receiver while keeping it secret from a degraded eavesdropper. Soon this problem was generalized to the non-degraded wiretap channel [2] and Gaussian wiretap channel [3], which laid the foundations for much subsequent research on information theoretic secrecy. Based on the original wiretap channel, in which the secrecy measure is defined as the leakage of confidential information at the eavesdropper normalized to the length of the codeword, the problem of transmitting confidential messages has been widely studied in multiuser networks, e.g., the discrete memoryless interference channel and broadcast channel with confidential messages [4], the fading broadcast channel [5], the multiple access channel with confidential messages [6], relay channels with confidential messages [7] and so on. In order to guarantee confidentiality, a series of random binning encoders has been applied to different networks, in which a proper quantity of randomness is placed in the codebook to protect the confidential messages. The common essence of the coding mechanisms in these results is tied to the capacity of the eavesdropper's channel, where the rate penalty for the random binning is slightly below the decoding ability of the eavesdropper. However, the above secrecy measure was pointed out by Maurer and Wolf [8] to be too weak for cryptographic applications. Meanwhile, the capacity-based secrecy coding encounters difficulty for general channel models, e.g., non-stationary or/and non-memoryless channels. In order to study communications under stronger constraints, the total leakage of confidential information was introduced as the strong secrecy measure in multiple works, e.g., [8]–[10]. Under such a strong secrecy constraint, there exist different methods for coding, such as privacy amplification [8], [11], the vanishing output variation approach [12], and channel resolvability [10], [13]–[15]. Among these approaches, we follow that of Hayashi [10] and Bloch and Laneman [13] to study the strong secrecy problem in interference channels, for which the secrecy problem is tied with the approximation method for output distributions, namely, the channel resolvability theory [16]. A recent review of the field of information theoretic secrecy can be found in [17].

A. Channel Resolvability

The concept of channel resolvability was first introduced by Wyner while investigating common randomness of two dependent random variables [18]. Subsequently, the theory of channel resolvability was thoroughly studied by Han and Verdú to determine *the number of random bits required per channel use in order to generate an input that achieves arbitrarily accurate approximation of the output statistics for any given*

Manuscript received May 21, 2015; revised February 26, 2018; accepted April 21, 2018. Date of publication May 9, 2018; date of current version June 20, 2018. This work was supported by the U.S. National Science Foundation under Grants CNS-1702808 and ECCS-1647198.

Z. Wang was with the Department of Communication Theory, School of Electrical Engineering, Royal Institute of Technology, 10044 Stockholm, Sweden. He is now with Ericsson Research, 16483 Stockholm, Sweden (e-mail: zhao.wang@ericsson.com).

R. F. Schaefer was with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA. He is now with the Information Theory and Applications Chair, Technische Universität Berlin, 10587 Berlin, Germany (e-mail: rafael.schaefer@tu-berlin.de).

M. Skoglund and M. Xiao are with the Department of Information Science and Engineering, Royal Institute of Technology, 10044 Stockholm, Sweden (e-mail: skoglund@kth.se; mingx@kth.se).

H. V. Poor is with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: poor@princeton.edu).

Communicated by A. Khisti, Associate Editor for Shannon Theory.

Digital Object Identifier 10.1109/TIT.2018.2834508

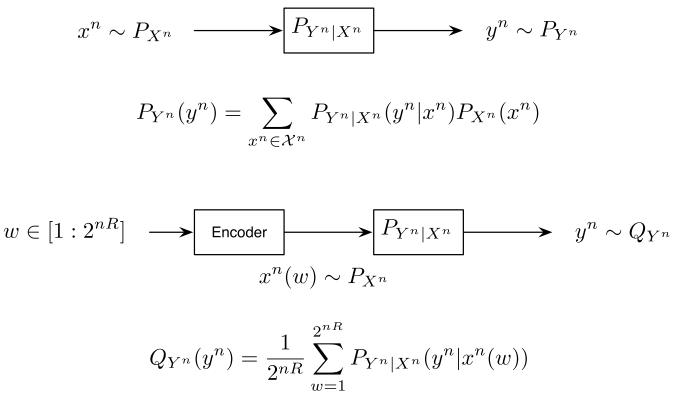

$x^n \sim P_{X^n}$
$P_{Y^n|X^n}$
$y^n \sim P_{Y^n}$
$P_{Y^n}(y^n) = \sum_{x^n \in \mathcal{X}^n} P_{Y^n|X^n}(y^n|x^n) P_{X^n}(x^n)$
$w \in [1 : 2^{nR}]$
Encoder
$P_{Y^n|X^n}$
$y^n \sim Q_{Y^n}$
$x^n(w) \sim P_{X^n}$
$Q_{Y^n}(y^n) = \frac{1}{2^{nR}} \sum_{w=1}^{2^{nR}} P_{Y^n|X^n}(y^n|x^n(w))$

Fig. 1. Approximation for output statistics: The variational distance between P_{Y^n} and Q_{Y^n} vanishes as n tending to infinity, if the rate R is larger than the *sup-information rate*, defined in (2) and Section II.

input process [16]. We adopt the notion of Han and Verdú to describe the framework of channel resolvability in this paper. To briefly interpret the notion of channel resolvability and its relation to the strong secrecy problem, let us consider the example shown in Fig. 1. Considering the channel defined by a sequence of transition probabilities $P_{Y^n|X^n}$, for any input process X^n drawn from the distribution P_{X^n}, the output distribution P_{Y^n} is the marginal distribution of $P_{Y^n|X^n} P_{X^n}$ as shown in the upper part of Fig. 1. In order to approximate the output statistics P_{Y^n}, in practice, a random number generator is used to generate the sample path of the input distribution, and the empirical estimates of the output statistics are computed from the output sample path. Therefore, a technical question to raise is, given the input statistics and the transition probability, how many bits per input sample are required to reproduce the target output statistics within a certain accuracy. Although, at first glance, the problem of approximating the output statistics would seem to have no connection to any codes or information transmission, Han and Verdú connected the approximation problem with Shannon theory via a random code construction: Let us generate a set of uniformly distributed messages with size 2^{nR}, and assign each message w to a codeword $x^n(w)$ generated according to the distribution P_{X^n}. Randomly choosing the message w from the message set and sending the codeword $x^n(w)$ to the channel, the induced output distribution is Q_{Y^n} as shown in the lower part of Fig. 1. Regarding Q_{Y^n} as the empirical approximation of P_{Y^n}, the question becomes how large R is required to be to achieve a certain accuracy. In order to measure the accuracy of the approximation, the specific measures used in [16] are variational distance and normalized Kullback-Leibler divergence. These measures are defined respectively in the following.

Definition 1 (Variational Distance): For two distributions P and Q defined on the same measurable space $(\Omega, \mathcal{F})$, the variational distance between P and Q is

$$d(P, Q) = \sum_{\omega \in \Omega} |P(\omega) - Q(\omega)| = 2 \sup_{E \in \mathcal{F}} |P(E) - Q(E)| .$$

Definition 2 (Kullback-Leibler Divergence): For two distributions P and Q defined on the same measurable space $(\Omega, \mathcal{F})$, where P is absolutely continuous with respect to Q, the Kullback-Leibler divergence is

$$D(P\|Q) = \int_{\Omega} \log \frac{dP}{dQ} dP,$$

where $\frac{dP}{dQ}$ is the Radon-Nikodym derivative of P with respect to Q. In the later part of the paper, we sometimes refer to the Kullback-Leibler divergence as *divergence* for brevity.

Based on these definitions, the required number of random bits for approximation is not only related to the input statistics, but is also relevant to the degree of approximation accuracy measured by the specific metric. It is shown in [16] that, if

$$R > \bar{\mathbf{I}}(\mathbf{X}; \mathbf{Y}), \tag{1}$$

where $\bar{\mathbf{I}}(\mathbf{X}; \mathbf{Y})$ represents the *sup-information rate*,

$$\bar{\mathbf{I}}(\mathbf{X}; \mathbf{Y}) = \inf \left\{ \alpha : \lim_{n \to \infty} \mathbb{P} \left[\frac{1}{n} \log \frac{P_{Y^n|X^n}(Y^n|X^n)}{P_{Y^n}(Y^n)} > \alpha \right] = 0 \right\}, \tag{2}$$

there exists at least one sequence of codebooks such that the variational distance between the two distributions P_{Y^n} and Q_{Y^n} tends to zero as $n \to \infty$, i.e., $\lim_{n\to\infty} d(P_{Y^n}, Q_{Y^n}) = 0$. Furthermore, if the channel has finite input alphabet, i.e., $|\mathcal{X}| < \infty$, it implies that the normalized divergence $\frac{1}{n} D(P_{Y^n} \| Q_{Y^n})$ tends to zero for sufficiently large n given (1) and (2). In [16], $\bar{\mathbf{I}}(\mathbf{X}; \mathbf{Y})$ is termed the *channel resolution* when the input distribution is P_{X^n}.

B. Resolvability and Secrecy

In Fig. 1, the resolvability result tells us that when the message rate is above the channel resolution, the statistics of the original output P_{Y^n} which is independent of the codebook, and the codebook-induced output Q_{Y^n} are arbitrarily close measured by variational distance or normalized divergence for sufficiently large n. We regard these two distributions as being *statistically indistinguishable* under the respective measure. The statistical indistinguishability of this pair of distributions can be further exploited in the context of information-theoretically secure communications. For example, let us consider a scenario illustrated by Fig. 1 in which the confidential message represented by a random variable W is transmitted via the channel with transition probability which can be marginalized as $P_{Y^n|X^n}$. Let us further assume that Y^n is the channel output sequence at the eavesdropper, and the input probability distribution P_{X^n} is known at the eavesdropper. In order to hide the confidential message, as a first step, a natural heuristic is to imitate the output distribution P_{Y^n} by the codebook-induced distribution Q_{Y^n} such that these two output statistics are arbitrarily close given sufficiently large n. Therefore, the confidential message should be encoded at a rate above the channel resolution of the eavesdropper's channel and below the channel capacity of the intended channel. To make this concept rigorous, following the conventional definition of information-theoretic security, the desired statistical indistinguishability is measured by the vanishing with increasing n of the normalized divergence $\frac{1}{n}D(P_{WY^n}\|P_W P_{Y^n})$ for weak secrecy and divergence $D(P_{WY^n}\|P_W P_{Y^n})$ for strong secrecy.

Therefore, there is a fundamental connection between channel resolvability and secrecy. In fact, as already indicated in [16], for many systems there is a direct implication that the notions of indistinguishability measured by the normalized divergence and variational distance render the same achievable channel resolution for the same input process. Thus, resolvability results have a strong connection with weak secrecy problems. However, for strong secrecy problems, directly applying channel resolvability results based on the variational distance or normalized divergence is not sufficient. The reason is that the total divergence measure (or the strong secrecy measure) is the strongest measure among these three. That being said, the vanishing of the total divergence when n tends to infinity implies the vanishing of the variational distance and obviously the normalized divergence, but *not vice versa* [13].

In this paper, we investigate the achievable rate with strong secrecy based on the channel resolvability method. In particular, we aim to construct a sequence of codebooks such that $\lim_{n\to\infty} d(P_{WY^n}, P_W P_{Y^n}) = 0$ and furthermore $\lim_{n\to\infty} I(W; Y^n) = \lim_{n\to\infty} D(P_{WY^n}\|P_W P_{Y^n}) = 0$. It is accomplished by exploiting the relationship of these two measures. Let P and Q represent two different probability distributions over the same sample space. It is well known that Pinsker's inequality [19] provides a lower bound on $D(P\|Q)$ based on $d(P, Q)$ such that the vanishing of $D(P\|Q)$ implies the vanishing of $d(P, Q)$, whereas the reverse direction does not hold in general. Accordingly, in our study the reverse direction of Pinsker's inequality is of particular interest. Bounding the divergence of two distributions $D(P\|Q)$ from above based on the variational distance $d(P, Q)$ is the key step throughout this paper.

The relation between channel resolvability and strong secrecy was originally addressed by Csiszár [9] and then Hayashi [10], and sequentially studied in [13], [14], and [15] for different types of wiretap channels and broadcast channels with confidential messages. It is worth noting that the information-spectrum toolbox presented by Han and Verdú is useful for studying general channels, i.e., channels with memory or/and non-stationary channels. For instance, in [13], the arbitrary wiretap channel was investigated based on the information-spectrum approach.

C. Summary of Contributions and Prior Work

We study the achievable secrecy rate region of interference channels with confidential messages under strong secrecy constraints. In this paper, we start from considering interference channels in a more general sense, for instance, channels are not stationary or memoryless. The (direct) channel resolvability theorem is first generalized to the two-user interference channel with arbitrary channel transition probabilities. Then, the stationary and memoryless interference channel with confidential messages is studied based on different assumptions on the transition probability. The contributions of the paper are summarized as follows:

- *Resolvability for arbitrary interference channels with confidential messages:* We first generalize the direct channel resolvability theorem to the two-user interference channel, for which there are no restrictions on the channel transition probability. We consider the scenario in which transmitter i $(i = 1, 2)$ intends to deliver a message W_i to receiver i, with a constraint on the output distributions that the variational distance $\lim_{n\to\infty} d(P_{W_i Y_j^n}, P_{W_i} P_{Y_j^n}) = 0$ $(i, j \in \{1, 2\}$ and $i \neq j)$. The achievable rate region is presented in a supporting lemma based on the information-spectrum method. This lemma holds regardless of whether or not the channel input/output alphabets are finite. We also show that the direct resolvability result guarantees weak secrecy for arbitrary interference channels.
- *Achievable secrecy rate region for interference channels with confidential messages:* Consider the two-user interference channel, in which W_i is intended for receiver i and to be kept secret from receiver j. The secrecy rate region is derived for the stationary and memoryless interference channel with confidential messages. The main difference between these results and channel resolvability is that the desired statistical indistinguishability is based on the strong secrecy measure $I(W_i; Y_j^n)$ instead of the variational distance. Therefore, the relationship of those measures plays an important role in the analysis. To consider discrete output alphabets, we adopt the method given by Csisźar [9] and Csisźar and Körner [20] directly to bound the targeted mutual information or equivalently the divergence from above as a function of the variational distance. For continuous output alphabets with finite support, we derive a new reverse Pinsker's inequality in order to provide an upper bound on the target strong secrecy measure by the variational distance. The principal step is to show that when the variational distance converges to zero fast enough with n, which is obtained by tailoring the supporting lemma, the mutual information also converges to zero in the limit of n, following a similar method in [13]. Our study directly implies that for discrete memoryless interference channels the best known achievable rate region with weak secrecy [4] guarantees strong secrecy. An application of the proposed reverse Pinsker's inequality is that it further aids the investigation of strong secrecy for Gaussian channels which have infinite output alphabets. The generalization from finite support to Gaussian channels follows from a careful truncation of the output alphabets, such that for the transmission based on a particular codebook, the desired divergence and variational distance of considered distributions concentrate on the truncated set with finite support. By this means, the derived reverse Pinsker's inequality can be applied to the truncated set with finite support. Our results show that for Gaussian interference channels, the known achievable rate region for weak secrecy is also achievable with strong secrecy constraints.
- *Prior work on the secrecy rate region of interference channels:* The problem of weak secrecy in interference channels has been widely studied. In [4], the discrete

memoryless interference channel with confidential messages has been studied, which provides the best known achievable secrecy rate region. In [21], the secrecy problem is studied for deterministic interference channels. Cognitive interference channels with secrecy constraints are studied in [22]. Secure degrees of freedom for Gaussian interference channels with confidential messages have been studied in [23], [24], and [25], where the optimal sum secure degrees of freedom of K-user Gaussian interference channel with confidential messages is derived in the latter. In the strong secrecy setting, Li and Matsumoto studied the strong secrecy rate region of discrete memoryless interference channels based on secure multiplex coding [26], where the privacy amplification approach [27] was adopted. Our results offer the same achievable rate region for discrete memoryless channels and Gaussian channels as in [26] and [28]. In [28], strong secrecy was guaranteed by a nested lattice codebook, in which the representation theorem [29] of nested lattice structures plays a critical rule for bounding the secrecy measure. Here in our paper, the coding schemes are still based on Shannon's random selection approach. The proof focuses on the relationship between the divergence and variational distance between a pair of output distributions. It is also important to note that our resolvability approach manages to show that the variational distance of target distributions tends to zero within the derived rate region for arbitrary channel transition probabilities. It is therefore also meaningful for future studies on channels with memory.

II. Preliminary Definitions

In this section, we introduce the definitions of quantities that will be used in the sequel. Let $\mathcal{X}$ and $\mathcal{Y}$ represent two finite alphabet sets. For $x^n \in \mathcal{X}^n$ and $y^n \in \mathcal{Y}^n$, $P_{X^n}(x^n)$ and $P_{Y^n}(y^n)$ represent the respective probability masses. For continuous alphabets, we assume that probability density functions exist, i.e., the corresponding probability measures are absolutely continuous with respect to Lebesgue measure. In what follows, unless otherwise noted, the definitions are provided based on discrete random variables. As the information-spectrum method we adopt in this paper does not impose any constraint on the alphabets, the results from the discrete case can be directly generalized to continuous cases as pointed out in [30], with restrictions and exceptions as we shall point out particularly. Throughout the paper, we use $\mathbb{R}$ and $\mathbb{R}^n$ to represent the set of real numbers and the n-dimensional space of real numbers, respectively. $\mathbb{R}^n_+$ represents the set of n-tuples of non-negative real numbers. We use lower case letters, e.g., x, to represent specific realizations of random variables denoted by upper case letters, e.g., X. Let f and g be two functions defined on some subset of real numbers. The big O condition $f(x) = O(g(x))$ as $x \to \infty$ holds if and only if there is a positive number M and a real number x_0 such that $|f(x)| \leq M|g(x)|, \forall x \geq x_0$. Throughout the paper, log represents the binary logarithm and ln represents the natural logarithm.

Definition 3 (Information Density [16], [30]): Given a joint distribution $P_{X^nY^n}(x^n, y^n) = P_{X^n}(x^n)\ P_{Y^n|X^n}(y^n|x^n)$, the information density is the following function defined on $\mathcal{X}^n \times \mathcal{Y}^n$:

$$i_{X^nY^n}(x^n, y^n) = \log\frac{P_{Y^n|X^n}(y^n, x^n)}{P_{Y^n}(y^n)}.$$

The distribution of the random variable $(\frac{1}{n})i_{X^nY^n}(X^n, Y^n)$ where X^n and Y^n have joint distribution $P_{X^nY^n}$ will be referred to as the information spectrum. The mutual information $I(X^n; Y^n)$ is defined as the following expectation:

$$\begin{aligned} I(X^n; Y^n) &= \mathbb{E}[i_{X^nY^n}(X^n, Y^n)] \\ &= \sum_{x^n \in \mathcal{X}^n, y^n \in \mathcal{Y}^n} P_{X^nY^n}(x^n, y^n)\log\frac{P_{Y^n|X^n}(y^n|x^n)}{P_{Y^n}(y^n)}. \end{aligned}$$

For the information density defined above, we define the following lim sup and lim inf in probability:

$$\begin{aligned} \overline{\mathbf{I}}(\mathbf{X}; \mathbf{Y}) &= \text{p-}\limsup_{n\to\infty} \frac{1}{n} i_{X^nY^n}(X^n, Y^n) \\ &= \inf\left\{\alpha : \lim_{n\to\infty} \mathbb{P}\left[\frac{1}{n} i_{X^nY^n}(X^n, Y^n) > \alpha\right] = 0\right\}, \\ \underline{\mathbf{I}}(\mathbf{X}; \mathbf{Y}) &= \text{p-}\liminf_{n\to\infty} \frac{1}{n} i_{X^nY^n}(X^n, Y^n) \\ &= \sup\left\{\beta : \lim_{n\to\infty} \mathbb{P}\left[\frac{1}{n} i_{X^nY^n}(X^n, Y^n) < \beta\right] = 0\right\}. \end{aligned}$$

$\overline{\mathbf{I}}(\mathbf{X}; \mathbf{Y})$ and $\underline{\mathbf{I}}(\mathbf{X}; \mathbf{Y})$ are referred to as the *sup-information rate* and *inf-information rate*, respectively.

III. Channel Model

Definition 4 (Interference Channel With Confidential Messages): Let us consider the interference channel $\mathbf{\Psi} = \{\Psi^n : \mathcal{X}_1^n \times \mathcal{X}_2^n \to \mathcal{Y}_1^n \times \mathcal{Y}_2^n\}_{n\in\mathbb{N}}$ which is a sequence of stochastic mappings from input alphabets $\mathcal{X}_1^n \times \mathcal{X}_2^n$ to output alphabets $\mathcal{Y}_1^n \times \mathcal{Y}_2^n$. We use the transition probability to represent this sequence of mappings:

$$\begin{aligned} \mathbf{\Psi} = \Bigg\{ &\Psi^n(y_1^n, y_2^n|x_1^n, x_2^n) : \\ &\Psi^n(y_1^n, y_2^n|x_1^n, x_2^n) = P_{Y_1^nY_2^n|X_1^nX_2^n}(y_1^n, y_2^n|x_1^n, x_2^n), \\ &\text{with } (x_1^n, x_2^n, y_1^n, y_2^n) \in \mathcal{X}_1^n \times \mathcal{X}_2^n \times \mathcal{Y}_1^n \times \mathcal{Y}_2^n \Bigg\}_{n=1}^{\infty}. \end{aligned}$$

We assume that $\{X_1^n = (X_{1,1}^{(n)}, X_{1,2}^{(n)}, \cdots, X_{1,n}^{(n)})\}_{n\in\mathbb{N}}$ and $\{X_2^n = (X_{2,1}^{(n)}, X_{2,2}^{(n)}, \cdots, X_{2,n}^{(n)})\}_{n\in\mathbb{N}}$ are general sources such that the consistency condition need not hold. For instance, the condition $X_{1,i}^{(n)} = X_{1,i}^{(m)}$ for all $m < n$ and $1 \leq i \leq m$ does not necessarily hold. Based on the channel transition probability $\Psi^n(y_1^n, y_2^n|x_1^n, x_2^n)$, we consider an interference channel with two transmitters, each intending to send one confidential message to its corresponding receiver, while keeping it secret from the other receiver. This channel is referred to as the *interference channel with confidential messages.*

A $(2^{nR_1}, 2^{nR_2}, n)$ code C_n for the considered channel is defined to consist of, for $i = 1, 2$,

- a set of messages at transmitter i: $\mathcal{W}_i = [1 : 2^{nR_i}]$,

- a stochastic encoder $f_i^{(n)}$ at transmitter i,
$$f_i^{(n)} : \mathcal{W}_i \to \mathcal{X}_i^n,$$
which maps the intended message $w_i \in \mathcal{W}_i$ to a codeword $x_i^n \in \mathcal{X}_i^n$, where the message set $\mathcal{W}_i$ is uniformly distributed, and
- a decoder $g_i^{(n)}$ at receiver i,
$$g_i^{(n)} : \mathcal{Y}_i^n \to \mathcal{W}_i,$$
that maps the output y_i^n to an estimated message $\hat{w}_i \in \mathcal{W}_i$.

The strong secrecy rate pair (R_1, R_2) is achievable for the considered channel if there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes $\{C_n\}$ such that

- the error probability satisfies
$$\lim_{n\to\infty} P_e^{(n)} = 0,$$
where $P_e^{(n)} = \mathbb{P}[(\hat{W}_1, \hat{W}_2) \neq (W_1, W_2)]$, and
- the strong secrecy measure satisfies, for $i \neq j$,
$$\lim_{n\to\infty} I(W_i; Y_j^n) = 0.$$

In this paper, we will also discuss the achievable rate under the weak secrecy constraint $\lim_{n\to\infty} \frac{1}{n} I(W_i; Y_j^n) = 0$, as well as the achievable rate with vanishing variational distance $\lim_{n\to\infty} d(P_{W_i Y_j^n}, P_{W_i} P_{Y_j^n}) = 0$. The definitions of codes and achievable rates follow by replacing the corresponding measures, respectively.

IV. A Supporting Lemma Based on Channel Resolvability

In this section, we present the direct resolvability lemma for arbitrary interference channels. First, the direct resolvability lemma is proved under the criterion of vanishing variational distance of output statistics. Then, its relation to secrecy is discussed. The importance of the direct resolvability result is that it not only indicates the weak secrecy rate region directly, but also serves as an intermediate step for strong secrecy studies. Because in a large part of the paper we will adopt variational distance between two distributions as one of the key metrics for the strong secrecy analysis, the technical motivation of this approach will be explained in this section.

A. Direct Resolvability Lemma in Variational Distance

Instead of studying the strong secrecy rate directly, we first take a detour to provide a supporting lemma based on channel resolvability. The proposed lemma sets the tone for the study of strong secrecy in interference channels.

Let us replace the secrecy measure $I(W_i; Y_j^n)$ with the variational distance between the distributions $P_{W_i Y_j^n}$ and $P_{W_i} P_{Y_j^n}$ for $(i \neq j)$, i.e., $d(P_{W_i Y_j^n}, P_{W_i} P_{Y_j^n})$. A closer look at the above variational distance tells us that when $d(P_{W_i Y_j^n}, P_{W_i} P_{Y_j^n})$ approaches zero, the confidential message W_i and the output at the undesired user Y_j^n are asymptotically independent. Intuitively, when W_i and Y_j^n are independent, information about the confidential message W_i in the sequence Y_j^n is zero. Therefore, the product distribution $P_{W_i} P_{Y_j^n}$ can be seen as our target distribution, and our goal is to make the true distribution $P_{W_i Y_j^n}$ arbitrarily close to it. Using the variational distance to measure the distance between two distributions, in [16], Han and Verdú introduced the concept of channel resolvability for approximating the output statistics of the point-to-point channel. The idea is generalized here for the interference channel in Definition 4. The main result is summarized in the following supporting lemma.

Lemma 1: For the interference channel as defined in Definition 4 by arbitrary transition probability $P_{Y_1^n Y_2^n | X_1^n X_2^n}(y_1^n, y_2^n | x_1^n, x_2^n)$, the following rate region $\mathcal{D}$ is achieved:

$$\mathcal{D} := \left\{ (R_1, R_2) \in \mathbb{R}_+^2 : \begin{array}{r} R_1 < \underline{\mathbf{I}}(\mathbf{V}_1; \mathbf{Y}_1 | \mathbf{U}) - \overline{\mathbf{I}}(\mathbf{V}_1; \mathbf{Y}_2 | \mathbf{V}_2, \mathbf{U}), \\ R_2 < \underline{\mathbf{I}}(\mathbf{V}_2; \mathbf{Y}_2 | \mathbf{U}) - \overline{\mathbf{I}}(\mathbf{V}_2; \mathbf{Y}_1 | \mathbf{V}_1, \mathbf{U}) \end{array} \right\} \quad (3)$$

with

$$\lim_{n\to\infty} d(P_{W_i Y_j^n}, P_{W_i} P_{Y_j^n}) = 0, \forall i, j \in \{1, 2\}, \quad i \neq j$$

for any distribution $P_{U^n V_1^n V_2^n X_1^n X_2^n}$ that can be factored as $P_{U^n} P_{V_1^n | U^n} P_{V_2^n | U^n} P_{X_1^n | V_1^n} P_{X_2^n | V_1^n}$.

Sketch of Proof: We are going to show first that the following rates are achievable:

$$0 \leq R_1 < \underline{\mathbf{I}}(\mathbf{X}_1; \mathbf{Y}_1 | \mathbf{U}) - \overline{\mathbf{I}}(\mathbf{X}_1; \mathbf{Y}_2 | \mathbf{X}_2, \mathbf{U}) \quad (4)$$
$$0 \leq R_2 < \underline{\mathbf{I}}(\mathbf{X}_2; \mathbf{Y}_2 | \mathbf{U}) - \overline{\mathbf{I}}(\mathbf{X}_2; \mathbf{Y}_1 | \mathbf{X}_1, \mathbf{U}). \quad (5)$$

Then (3) follows by the channel prefixing method as discussed in [2].

We start with creating a sequence of codebooks which are generated randomly. Let $R_1, R_1', R_2, R_2' > 0$. Define $\mathcal{W}_1 = [1 : 2^{nR_1}]$, $\mathcal{W}_2 = [1 : 2^{nR_2}]$, $\mathcal{W}_1' = [1 : 2^{nR_1'}]$ and $\mathcal{W}_2' = [1 : 2^{nR_2'}]$. Let $\gamma > 0$ be an arbitrary positive number.

- *Codebook generation:* Randomly generate a sequence u^n according to the distribution $P_{U^n}(u^n)$, which is shared among all transmitters and receivers as the time-sharing indicator. For transmitter i, $i \in \{1, 2\}$, generate $|\mathcal{W}_i||\mathcal{W}_i'|$ independent sequences $x_i^n \in \mathcal{X}_i^n$ according to the distribution $P_{X_i^n | U^n}(x_i^n | u^n)$. We label the sequences x_i^n as
$$x_i^n(w_i, w_i'), \; w_i \in \mathcal{W}_1, \; w_i' \in \mathcal{W}_i'.$$
- *Encoding:* In order to send a message pair $(w_1, w_2) \in \mathcal{W}_1 \times \mathcal{W}_2$, the transmitter i randomly chooses a value w_i' according to the uniform distribution on the set $\mathcal{W}_i'$ and sends the codeword $x_i^n(w_i, w_i')$ over the channel.
- *Decoding:* Define the following sets for $i = 1, 2$:
$$\mathcal{T}_{\gamma,i}^{(n)} := \left\{ (u^n, x_i^n, y_i^n) \in \mathcal{U}^n \times \mathcal{X}_i^n \times \mathcal{Y}_i^n : \frac{1}{n} \log \frac{P_{Y_i^n | X_i^n U^n}(y_i^n | x_i^n, u^n)}{P_{Y_i^n | U^n}(y_i^n | u^n)} \geq \frac{1}{n} \log |\mathcal{W}_i||\mathcal{W}_i'| + \gamma \right\}. \quad (6)$$
Based on the received signal y_i^n, the decoder i aims to find the unique $x_i^n(\hat{w}_i, \hat{w}_i')$ such that $(u^n, x_i^n, y_i^n) \in \mathcal{T}_{\gamma,i}^n$; otherwise, a random $\hat{w}_i$ is chosen.

A detailed proof of reliability and the vanishing of the variational distance is shown in Appendix B. For better understanding of the proof, we provide an outline for proving the vanishing of the variational distance between the targeted distributions here. Let us first set the time sharing random sequence $U^n = \emptyset$ and consider the case $i = 1$ and $j = 2$. Let $\{C_n\}_{n\in\mathbb{N}}$ represent a sequence of codebooks generated as above. We use over-lines to represent the channel input and output variables induced by the chosen sequence of codebooks. Based on Shannon's random selection approach, if we can show that the targeted variational distance vanishes by averaging the selection of the codebooks, there must exist at least one sequence of realizations for which the variational distance also vanishes. Specifically, if we can show that

$$\lim_{n\to\infty} \mathbb{E}_{C_n}\left[d(P_{W_i\bar{Y}_j^n}, P_{W_i}P_{\bar{Y}_j^n})\right] = 0, \quad i, j \in \{1, 2\}\ i \neq j, \tag{7}$$

then there exists at least one sequence of codes $\{C_n\}$ such that $\lim_{n\to\infty} d(P_{W_i\bar{Y}_j^n}, P_{W_i}P_{\bar{Y}_j^n}) = 0$. According to the triangle inequality for the variational distance, as provided in Lemma 6 of Appendix A, we have

$$\begin{aligned}
& d\left(P_{W_1\bar{Y}_2^n}, P_{W_1}P_{\bar{Y}_2^n}\right) \\
&\quad \leq d(P_{W_1\bar{Y}_2^n\bar{X}_2^n} P_{W_1}P_{\bar{Y}_2^n\bar{X}_2^n}) \\
&\quad = \mathbb{E}_{W_1\bar{X}_2^n}\left[d(P_{\bar{Y}_2^n|W_1\bar{X}_2^n}, P_{\bar{Y}_2^n|\bar{X}_2^n})\right] \\
&\quad \leq \mathbb{E}_{W_1\bar{X}_2^n}\left[d(P_{\bar{Y}_2^n|W_1\bar{X}_2^n}, P_{Y_2^n|X_2^n}) + d(P_{Y_2^n|X_2^n}, P_{\bar{Y}_2^n|\bar{X}_2^n})\right] \\
&\quad = \mathbb{E}_{W_1\bar{X}_2^n}\left[d(P_{\bar{Y}_2^n|W_1\bar{X}_2^n}, P_{Y_2^n|X_2^n})\right] \\
&\qquad + \mathbb{E}_{\bar{X}_2^n}\left[d(P_{Y_2^n|X_2^n}, P_{\bar{Y}_2^n|\bar{X}_2^n})\right] \\
&\quad \leq \mathbb{E}_{W_1\bar{X}_2^n}\left[d(P_{\bar{Y}_2^n|W_1\bar{X}_2^n}, P_{Y_2^n|X_2^n})\right] \\
&\qquad + \mathbb{E}_{\bar{X}_2^n}\left[d(P_{\bar{Y}_2^nW_1|\bar{X}_2^n}, P_{W_1}P_{Y_2^n|X_2^n})\right] \\
&\quad = 2\mathbb{E}_{W_1\bar{X}_2^n}\left[d(P_{\bar{Y}_2^n|W_1\bar{X}_2^n}, P_{Y_2^n|X_2^n})\right].
\end{aligned} \tag{8}$$

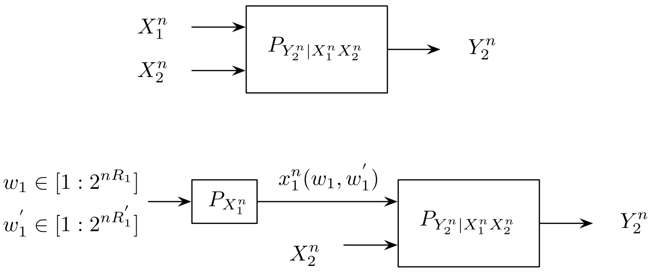
Therefore, it is sufficient to show that

$$\lim_{n\to\infty} \mathbb{E}_{C_n}\left\{\mathbb{E}_{W_1\bar{X}_2^n}\left[d(P_{\bar{Y}_2^n|W_1\bar{X}_2^n}, P_{Y_2^n|X_2^n})\right]\right\} = 0. \tag{9}$$

We generalize the channel resolvability theorem [16] to multiple users: In order to show (9), it is sufficient that the rate R_1' was larger than the resolution of the corresponding channel, i.e., $\bar{\mathbf{I}}(\mathbf{X}_1; \mathbf{Y}_2|\mathbf{X}_2)$. The equivalent channel is shown in Fig. 2. It is easy to see that the rate of the random message w_1' serves as a penalty term for the secrecy rate.

The case when $i = 2$ and $j = 1$ can be handled according to a symmetrical argument. ■

Remark 1: This supporting lemma does not impose any restriction on the structure of the channel transition probability (e.g., stationarity or memorylessness). Therefore the result holds in a general sense. As we show in the sequel, if we specify the channel transition probability, we can further study the achievable rate of the considered network with strong secrecy constraints based on the same theoretical framework.



$$\mathbb{E}_{W_1X_2^n}\left[d(P_{Y_2^n|X_2^nW_1}, P_{Y_2^n|X_2^n})\right] \to 0,\ \text{as } n \to \infty,\ \text{if } R_1' > \bar{\mathbf{I}}(\mathbf{X}_1; \mathbf{Y}_2|\mathbf{X}_2)$$

Fig. 2. The coding scheme over the equivalent channel with constraints on output statistics.

B. Direct Resolvability in Normalized Divergence and Weak Secrecy

So far, we have shown the achievable rate region for arbitrary interference channels under the vanishing variational distance $\lim_{n\to\infty} d(P_{W_iY_j^n}, P_{W_i}P_{Y_j^n}) = 0$. In fact, the result in Lemma 1 is meaningful in the context of secure communications. As discussed in [13], vanishing variational distance implies vanishing normalized divergence $\frac{1}{n}D(P_{W_iY_j^n}\|P_{W_i}P_{Y_j^n})$. Therefore, weak secrecy for arbitrary interference channels is guaranteed by the same achievable rate region $\mathcal{D}$ as defined in (3). For the sake of presentation, we summarize the result in the following proposition.

Proposition 1 (Weak Secrecy for Arbitrary Interference Channels): For the interference channel in Definition 4 with arbitrary transition probability $P_{Y_1^nY_2^n|X_1^nX_2^n}(y_1^n, y_2^n|x_1^n, x_2^n)$, the rate region $\mathcal{D}$ defined in (3) is achievable with $\lim_{n\to\infty} \frac{1}{n}D(P_{W_iY_j^n}\|P_{W_i}P_{Y_j^n}) = 0$, $\forall i, j \in \{1, 2\}, i \neq j$ for any distribution $P_{U^nV_1^nV_2^nX_1^nX_2^n}$ that can be factored as $P_{U^n}P_{V_1^n|U^n}P_{V_2^n|U^n}P_{X_1^n|V_1^n}P_{X_2^n|V_1^n}$.

Proof: This result is proved via showing the convergence of $\lim_{n\to\infty} \frac{1}{n}D(P_{W_iY_j^n}\|P_{W_i}P_{Y_j^n}) = 0$, provided that $\lim_{n\to\infty} d(P_{W_iY_j^n}, P_{W_i}P_{Y_j^n}) = 0$. The relation has been originally discussed in [19] and [30], and later studied in [13] for secrecy problems. We present the proof in Appendix C. ■

However, Lemma 1 cannot directly render that the strong secrecy constraints are satisfied. A technical explaination is that the vanishing variational distance constraint is generally weaker than the constraint of vanishing divergence, which is established by Pinsker's inequality which says that $D(P\|Q) \geq \frac{\log e}{2}d(P, Q)$ for two distributions P and Q defined on the same sample space. That being said, in order to satisfy the strong secrecy constraint the convergence of variational distance to zero is not sufficient. It is interesting to observe in the following section that for a specific class of transition probabilities, the result of Lemma 1 stands as a premise for strong secrecy. This is achieved by establishing the relationship of the divergence and the variational distance measures on a family of probability distributions.

V. Strong Secrecy for Interference Channels

Lemma 1 states that $d(P_{W_iY_j^n}, P_{W_i}P_{Y_j^n})$ can be arbitrarily close to zero if we carefully design the code within a certain rate region. In order to study strong secrecy of interference channels based on Lemma 1, a natural approach would be to provide an upper bound on the strong secrecy measure $D(P_{W_iY_j^n}\|P_{W_i}P_{Y_j^n})$ as a function of $d(P_{W_iY_j^n}, P_{W_i}P_{Y_j^n})$, such that when $d(P_{W_iY_j^n}, P_{W_i}P_{Y_j^n}) \to 0$, $D(P_{W_iY_j^n}\|P_{W_i}P_{Y_j^n})$ also tends to 0.

However, for the desired direction a reverse type of Pinsker's inequality does not exist in general. Specifically, for any $\epsilon > 0$, we can find P and Q such that $D(P\|Q) = \infty$ while $d(P, Q) = \epsilon$, where P and Q are two distributions. Therefore, certain restrictions on the studied distributions are required to obtain the inequality in the desired direction. In what follows, we will consider multiple channel models in which the reverse Pinsker's inequality can be derived accordingly and serves as a powerful approach to the analysis of strong secrecy constraints.

A. Stationary and Memoryless Interference Channel With Discrete Output Alphabets

In this section, we consider interference channels in which the channel transition probability is stationary and memoryless. Moreover, we restrict the output alphabet to be discrete with finite cardinality.

To study strong secrecy for interference channels in this case, we adopt the method given by Csiszár [9] by applying the following inequality.

Lemma 2 (Csiszár-Körner [9], [20]): Let P and Q denote two probability distributions on a discrete set $\mathcal{X}$. Let $H(P)$ and $H(Q)$ represent the entropies based on P and Q, respectively. Then, if $d(P, Q) \le \frac{1}{2}$,

$$|H(P) - H(Q)| \le -d(P, Q) \log \frac{d(P, Q)}{|\mathcal{X}|}, \tag{10}$$

where $|\mathcal{X}|$ is the cardinality of $\mathcal{X}$.

Remark 2: Based on this lemma, we have the following line of thought for bounding the strong secrecy measure $I(W_i; Y_j^n) = D(P_{W_iY_j^n}\|P_{W_i}P_{Y_j^n})$ from above by the variational distance. Considering the strong secrecy measure, based on Lemma 2, we have

$$\begin{aligned} D(P_{W_iY_j^n}\|P_{W_i}P_{Y_j^n}) &= H(Y_j^n) - H(Y_j^n|W_i) \\ &\le -d(P_{Y_j^n}, P_{Y_j^n|W_i}) \log \frac{d(P_{Y_j^n}, P_{Y_j^n|W_i})}{\left|\mathcal{Y}_j^n\right|}. \end{aligned}$$

Therefore, it suffices to show that there exists some $\alpha > 0$, so that $d(P_{W_i}P_{Y_j^n}, P_{W_iY_j^n}) \le e^{-n\alpha}$ for sufficiently large n, the proof of which depends on the stationary and memoryless structure of the channel. We note that in [13], Bloch and Laneman adopted a similar approach to establish the achievable secrecy rate for wiretap channels.

In order to handle channel coding problems in which the cost of the codewords must be taken into account, e.g., a transmission power constraint, following Han's approach [30], we introduce the following channel.

Definition 5 (Stationary Memoryless Channel With Additive Cost Functions): Let us consider the stationary and memoryless interference channel, where the channel transition probability is denoted as

$$\Psi^n(y_1^n, y_2^n|x_1^n, x_2^n) = \prod_{i=1}^{n} \Psi(y_{1,i}, y_{2,i}|x_{1,i}, x_{2,i}),$$

where $\Psi(y_{1,i}, y_{2,i}|x_{1,i}, x_{2,i}) = P_{Y_1Y_2|X_1X_2}(y_{1,i}, y_{2,i}|x_{1,i}, x_{2,i})$ is the probability mass function. There are also cost constraints based on the following additive cost functions:

$$\frac{1}{n}\sum_{i=1}^{n} c(x_i) \le P, \quad \text{with } c : \mathcal{X}_1 \cup \mathcal{X}_2 \to \mathbb{R}^+, \tag{11}$$

where P is a positive given constant. Such a constraint is referred to as the additive cost constraint P.

We are now in a position to present the following theorem.

Theorem 1: For the stationary memoryless interference channel with additive cost constraint P ($P > 0$), the following strong secrecy rate region $\mathcal{D}$ is achieved:

$$\mathcal{D} := \left\{ (R_1, R_2) \in \mathbb{R}_+^2 : \left. \begin{array}{l} R_1 < I(V_1; Y_1|U) - I(V_1; Y_2|V_2, U) \\ R_2 < I(V_2; Y_2|U) - I(V_2; Y_1|V_1, U) \end{array} \right\} \right. \tag{12}$$

for any distribution

$$P_U P_{V_1|U} P_{V_2|U} P_{X_1|V_1} P_{X_2|V_2}, \quad \text{and } \mathbb{E}[c(X_i)] \le P, \ \forall i \in \{1, 2\},$$

if the moment generating functions of $i_{V_iY_j|V_jU}$ and $c(X_i)$ exist.

Sketch of Proof: There are two critical steps in the proof. First, we modify the codebook generation as presented in the proof of Lemma 1. The purpose is to make the induced input process of the channel based on the generated codebooks satisfy the additive cost constraint P almost surely. The details of the modification of the codebook generation is given in Appendix D. Let C_n represent the codebook generated based on the described method for $n \in \mathbb{N}$. The second step is essentially the establishment of the following claim.

Claim 1: There exists at least one sequence of codebooks, denoted as $\{C_n\}$, which satisfies the constraint P and reliability, such that for sufficiently large n there exists some $\alpha > 0$ such that,

$$d(P_{W_i\bar{Y}_j^n}, P_{W_i}P_{\bar{Y}_j^n}) \le e^{-\alpha n},$$

where $\bar{Y}_j^n$ is the codebook induced output at receiver j.

Then following Lemma 2, the secrecy measure $D(P_{W_iY_j^n}\|P_{W_i}P_{Y_j^n})$ is shown to approach 0 as $n \to \infty$. We note that the key is to apply the Chernoff inequality (provided in Appendix A) to the proof of Lemma 1, based on the stationary and memoryless channel transition probability. Therefore, we need to make sure that the prerequisite of the Chernoff bound holds, i.e., that the moment generating functions for $i_{V_iY_j|V_jU}$ and $c(X_i)$ exist. The detailed proof is given in Appendix VI. ■

Remark 3: If we carefully choose the additive cost function and focus on the discrete memoryless interference channel, we have the following observations based on Theorem 1:

- Let $c(x_i) = |x_i|^2$ and choose a sufficiently large P. The cost constraint is automatically satisfied for any finite discrete distribution.

- The moment generating functions for $i_{V_iY_j|V_jU}$ and $c(X_i)$ exist for any discrete distribution.

Taking these two facts into account, we obtain that any distribution that achieves the boundary points of the derived secrecy rate region also achieves the same points at the boundary of the weak secrecy rate region presented in [4]. Therefore, the derived strong secrecy rate region ties with the best known weak secrecy rate region for the considered channel. In [26], the same result has been derived based on a secure multiplex coding scheme.

The result presented in Theorem 1 is not sufficient to be generalized to Gaussian channels directly. The major problem is that the inequality in Lemma 2 can only be applied to discrete distributions. In the next section, we will generalize the results to continuous alphabets and then focus on Gaussian interference channels.

B. Stationary and Memoryless Interference Channel on Continuous Output Alphabets

In order to generalize the result in Theorem 1 to continuous alphabets, a similar line of thought can be adopted here. Bounding the strong secrecy measure from above by the variational distance is critical to this generalization. In this section, we at first relax the discrete alphabet constraint to allow continuous input and output alphabets, yet with finite support for the output. The finite support of the output is finally dropped in the sequel when we study Gaussian channels.

To start with, an analog of Lemma 2 on continuous sets with finite support is presented.

Lemma 3: Let P and Q be two distributions on the set $\mathcal{X}^n \subset \mathbb{R}^n$ whose Lebesgue measure satisfies $\lambda(\mathcal{X}^n) < \infty$. Assuming $P, Q \ll \lambda$, let $p = \frac{dP}{d\lambda}$ and $q = \frac{dQ}{d\lambda}$ be the Radon-Nikodym derivatives of P and Q, respectively, that is, their densities with respect to Lebesgue measure. If p and q are bounded from above by c^n $(1 \le c < \infty)$ almost everywhere in $\mathcal{X}^n$, then

$$|h(P) - h(Q)| \le nd(P, Q)\left(\log\frac{\lambda(\mathcal{X}^n)}{d(P, Q)} + 2n\log c + \delta\right), \tag{13}$$

where $\delta = 2\log e + 1$, and $h(P)$ and $h(Q)$ are the differential entropies of P and Q, respectively.

Proof: Define $f(t) = -t\log t$, where $t \ge 0$. Let $\tau = |p - q|$, $\forall 0 \le p, q \le c^n$, then

$$|f(p) - f(q)| \le \begin{cases} \max(f(\tau), f(1-\tau)) = |\tau\log\tau|, \\ \qquad\qquad \text{if } 0 \le \tau \le \frac{1}{2}, 0 \le p, q \le 1, \\ \tau|f'(c^n)| = \tau\left|\log c^n + \frac{1}{\ln 2}\right|, \\ \qquad\qquad \text{otherwise.} \end{cases}$$

Therefore, we have

$$\begin{aligned} |h(P) - h(Q)| &= \left|\int_{\mathcal{X}^n} p\log p - q\log q \; d\lambda\right| \\ &\le \int_{\mathcal{X}^n} |p\log p - q\log q| \; d\lambda \\ &\le -\int_{\mathcal{E}_1} |p - q| \cdot \log|p - q| \; d\lambda \\ &\quad + \int_{\mathcal{E}_2} |p - q| \cdot \left|\log c^n + \frac{1}{\ln 2}\right| \; d\lambda, \end{aligned} \tag{14}$$

where (14) follows by defining two disjoint sets:

$$\mathcal{E}_1 = \left\{x^n : \tau \le \frac{1}{2}, 0 \le p(x^n), q(x^n) \le 1-\tau \text{ and } x^n \in \mathcal{X}^n\right\},$$
$$\mathcal{E}_2 = \left\{x^n : x^n \notin \mathcal{E}_1 \text{ and } x^n \in \mathcal{X}^n\right\},$$

and applying the upper bound on $|f(p) - f(q)|$ above. Define $\theta = \int_{\mathcal{E}_1} |p - q| \; d\lambda$. It is observed that $\theta \le \frac{1}{2}\lambda(\mathcal{E}_1)$. Based on (14), we further have

$$\begin{aligned} &-\int_{\mathcal{E}_1} |p - q| \cdot \log|p - q| \; d\lambda \\ &\quad = \theta\left(-\int_{\mathcal{E}_1} \frac{|p - q|}{\theta}\log\frac{|p - q|}{\theta} \; d\lambda\right) - \theta\log\theta \\ &\quad \le \theta\log\lambda(\mathcal{E}_1) - \theta\log\theta & (15) \\ &\quad \le \theta\log\left[\beta\cdot\lambda(\mathcal{X}^n)\right] - \theta\log\theta, \text{ for } \beta \ge 1. & (16) \end{aligned}$$

(15) follows from the fact that the uniform distribution provides maximum differential entropy for the bounded set $\mathcal{E}_1$, and (16) follows from the monotonicity with respect to λ.

Define the function $g(\theta) = \theta\log\left[\beta\cdot\lambda(\mathcal{X}^n)\right] - \theta\log\theta$ for $0 \le \theta \le d(P, Q)$. Setting $\beta = 2^{1+\log e}c^n$, we can write the derivative of $g(\theta)$ as follows:

$$\begin{aligned} g'(\theta) &= \log\frac{\beta\lambda(\mathcal{X}^n)}{\theta} - \log e = \log\frac{2^{1+\log e}c^n\lambda(\mathcal{X}^n)}{\theta} - \log e \\ &\ge \log\frac{d(P, Q)}{\theta} \ge 0, \quad \text{for } \theta \in [0, d(P, Q)], \end{aligned}$$

where $d(P, Q) \le 2c^n\lambda(\mathcal{X}^n)$ is applied. Therefore, $g(\theta)$ is monotonically increasing with θ in its domain. Therefore, $g(\theta) \le g(d(P, Q))$. Based on (16), we have

$$\begin{aligned} &-\int_{\mathcal{E}_1} |p - q| \cdot \log|p - q| \; d\lambda \\ &\quad \le d(P, Q)\left(\log\frac{\lambda(\mathcal{X}^n)}{d(P, Q)} + n\log c + \log e + 1\right), \end{aligned} \tag{17}$$

by substituting $\beta = 2^{1+\log e}c^n$ to $g(\theta)$.

Furthermore,

$$\begin{aligned} &\int_{\mathcal{E}_2} |p - q| \cdot \left|\log c^n + \frac{1}{\ln 2}\right| \; d\lambda \\ &\le \left|\log c^n + \frac{1}{\ln 2}\right| \int_{\mathcal{X}^n} |p - q| \; d\lambda = \left|\log c^n + \frac{1}{\ln 2}\right| \; d(P, Q) \end{aligned} \tag{18}$$

which follows from the definition of variational distance in the current case

$$d(P, Q) = \int_{\mathcal{X}^n} |p - q| \; d\lambda.$$

Combining (17) and (18), we have

$$\begin{aligned} &|h(P) - h(Q)| \\ &\quad \le d(P, Q)\left(\log\frac{\lambda(\mathcal{X}^n)}{d(P, Q)} + 2n\log c + 2\log e + 1\right). \end{aligned}$$

This concludes the proof. ∎

Remark 4: It is observed that when $\lambda(\mathcal{X}^n) \geq e^{-1}c^{-2n}$, the right-hand side of (13) is monotonically increasing with $d(P, Q)$. This can be shown by calculating the derivative with respect to $d(P, Q)$, and considering the fact that $d(P, Q) \leq 2$. Because $p, q \leq c^n$ almost everywhere, we have $c^n \int_{\mathcal{X}^n} d\lambda \geq 1$, which implies $\lambda(\mathcal{X}^n) \geq c^{-n} > e^{-1}c^{-2n}$. Consequently, the monotonicity with $d(P, Q)$ is guaranteed. For example, taking $\lambda(\mathcal{X}^n) = e^{n^2}$, $d(P, Q) \leq e^{-n\alpha}$ for some $\alpha = O(1)$, it can be shown that $|h(P) - h(Q)| \leq O(n^3 e^{-n\alpha})$ based on Lemma 3, which tends to 0 as $n \to \infty$.

Remark 5: A prerequisite condition in Lemma 3 is that the considered probability densities p and q are bounded almost everywhere in their sample space. For instance, Gaussian distributions will be one candidate, while the chi-square distribution with one degree of freedom does not qualify. We note that the reverse Pinsker's inequality has been studied with different constraints [31]–[35]. Among those, [31]–[33] studied the relationship of the entropy and variational distance for discrete distributions, while the recent work of Verdú [34] and of Sason [35] provides an interplay between relative entropy and variational distance. Different from these previous work, we use a different constraint on continuous distributions and focus on the asymptotic behavior of differential entropy and variational distance.

Based on Lemma 3, the proof of Theorem 1 can be immediately generalized to the continuous case in which the output alphabet has finite support, providing that output distributions have densities bounded almost everywhere. However, this is still not sufficient for the study of Gaussian channels, where the output alphabet has infinite support by definition. Directly applying Lemma 3 will not suffice for two distributions P and Q because $\lambda(\mathcal{X}^n)$ is infinite. Alternatively, if we can find two truncated distributions $\hat{P}$ and $\hat{Q}$ on a finite support $\mathcal{T}$ to approximate the original distributions with respect to the divergence and variational distance, the strong secrecy condition can then be proved via the properly truncated distributions. This approach will be presented in detail when we consider the following Gaussian interference channel.

Definition 6 (Gaussian Interference Channel With Confidential Messages): The Gaussian interference channel has the following channel input-output relation:

$$\begin{aligned} Y_1 &= X_1 + \rho_1 X_2 + Z_1, \\ Y_2 &= X_2 + \rho_2 X_1 + Z_2, \end{aligned}$$

where $\rho_1, \rho_2 \in [0, 1)$ are normalized channel coefficients and are known to all parties. Z_1 and Z_2 are independent Gaussian noises with zero means and unit variances. Here we consider only the weak interference scenario, i.e., $\rho_1, \rho_2 \in [0, 1)$, because otherwise secure communication is not possible. The transmitted signals X_1 and X_2 are subject to the average power constraint (i.e., additive cost function), such that for the transmitted sequences x_1^n and x_2^n,

$$\sum_{i=1}^{n} \frac{x_{k,i}^2}{n} \leq P, \quad \text{for } k = 1, 2.$$

The strong secrecy constraints remain consistent with Definition 4.

Proposition 2: The following strong secrecy rate region is achievable for the Gaussian interference channel:

$$\begin{aligned} 0 \leq R_1 &< \frac{1}{2}\log\left(1 + \frac{(1-\lambda_1)\beta_1 P}{(\lambda_1\beta_1 + \rho_1^2\beta_2)P + 1}\right) \\ &\quad - \frac{1}{2}\log\left(1 + \frac{\rho_2^2(1-\rho_1)\beta_1 P}{(\lambda_2\beta_2 + \rho_2^2\lambda_1\beta_1)P + 1}\right) \\ 0 \leq R_2 &< \frac{1}{2}\log\left(1 + \frac{(1-\lambda_2)\beta_2 P}{(\lambda_2\beta_2 + \rho_2^2\beta_1)P + 1}\right) \\ &\quad - \frac{1}{2}\log\left(1 + \frac{\rho_1^2(1-\rho_2)\beta_2 P}{(\lambda_1\beta_1 + \rho_1^2\lambda_2\beta_2)P + 1}\right) \end{aligned}$$

for arbitrary $\lambda_1, \lambda_2, \beta_1, \beta_2 \in [0, 1]$.

Proof: Let $R_1, R_1', R_2, R_2' > 0$, and $\mathcal{W}_1 = [1 : 2^{nR_1}]$, $\mathcal{W}_1' = [1 : 2^{nR_1'}]$, $\mathcal{W}_2 = [1 : 2^{nR_2}]$ and $\mathcal{W}_2' = [1 : 2^{nR_2'}]$. Fix the distributions P_{V_i} and P_{A_i} on sets $\mathcal{V}_i$ and $\mathcal{A}_i$, respectively, for $i = 1, 2$. Consider a sequence of codebooks $\{C_n\}$, in which

$$\begin{aligned} C_n = \big\{ & v_1^n(w_1), a_1^n(w_1'), v_2^n(w_2), a_2^n(w_2') : \\ & w_1 \in \mathcal{W}_1, w_1' \in \mathcal{W}_1', w_2 \in \mathcal{W}_2, w_2' \in \mathcal{W}_2' \big\}, \end{aligned}$$

and the sequences are generated as follows:

$$\begin{aligned} v_1^n &\sim \prod_{i=1}^{n} P_{V_1}(v_{1,i}), \quad v_2^n \sim \prod_{i=1}^{n} P_{V_2}(v_{2,i}) \\ a_1^n &\sim \prod_{i=1}^{n} P_{A_1}(a_{1,i}), \quad a_2^n \sim \prod_{i=1}^{n} P_{A_2}(a_{2,i}). \end{aligned}$$

The transmitted sequences for the confidential message w_i and the associated random message w_i' are determined based on C_n such that

$$\begin{aligned} x_1^n(w_1, w_1') &= v_1^n(w_1) + a_1^n(w_1'), \\ x_2^n(w_2, w_2') &= v_2^n(w_2) + a_1^n(w_2'), \end{aligned}$$

which moreover satisfy the average power constraints: $\sum_{i=1}^{n}(a_{k,i} + v_{k,i})^2 \leq nP$ for $k = 1, 2$.

We present the proof as a continuation of the proof for Theorem 1. Directly applying Theorem 1 and Claim 1, when

$$R_1 + R_1' < I(V_1; Y_1) \tag{19}$$

$$R_2 + R_2' < I(V_2; Y_2) \tag{20}$$

and

$$R_1' > I(V_1; Y_2|V_2) \tag{21}$$

$$R_2' > I(V_2; Y_1|V_1) \tag{22}$$

there exists at least one sequence of codebooks $\{C_n\}$ such that the reliability condition holds, and furthermore $\exists\alpha > 0, N > 0$ such that $\forall n > N$ the following inequality holds:

$$d(P_{W_i}P_{\bar{Y}_j^n}, P_{W_i\bar{Y}_j^n}) \leq e^{-n\alpha}.$$

Note that we use an overline to represent the output based on that particular codebook sequence $\{C_n\}$.

1) Proof of Strong Secrecy: In the following, we will show that based on that particular chosen codebook sequence, the strong secrecy constraints are satisfied, e.g., considering $i = 2$ and $j = 1$

$$\begin{aligned}\lim_{n\to\infty} I(W_2, \bar{Y}_1^n) &= \lim_{n\to\infty}\left(D(P_{\bar{Y}_1^n}P_{W_2}\|P_{\bar{Y}_1^n W_2})\right)\\ &= \lim_{n\to\infty}\mathbb{E}_{W_2}\left(h(\bar{Y}_1^n) - h(\bar{Y}_1^n|W_2 = w_2)\right) = 0.\end{aligned}$$

It suffices to show that for any $w_2 \in \mathcal{W}_2$, $h(\bar{Y}_1^n) - h(\bar{Y}_1^n|W_2 = w_2)$ decays exponentially fast with n.

Define the message set $\mathcal{W} = \mathcal{W}_1 \times \mathcal{W}_1' \times \mathcal{W}_2 \times \mathcal{W}_2'$, and $\overline{\mathcal{W}_2} = \mathcal{W}_1 \times \mathcal{W}_1' \times \mathcal{W}_2'$. The probability distribution of $\bar{Y}_1^n$, for any Borel measurable set $B_n \subset \mathbb{R}^n$, is given by

$$\begin{aligned}P_{\bar{Y}_1^n}(B_n) = \frac{1}{|\mathcal{W}|}&\sum_{(w_1,w_2,w_1',w_2')\in\mathcal{W}}\\ &P_{Y_1^n|X_1^nX_2^n}(B_n|a_1^n(w_1)+v_1^n(w_1'), a_2^n(w_2)+v_2^n(w_2')).\end{aligned}$$

For Gaussian channels, the transition probability distribution $P_{Y_1^n|X_1^nX_2^n}$ is absolutely continuous with respect to Lebesgue measure. Henceforth, $P_{\bar{Y}_1^n}(B_n)$ is also absolutely continuous with respect to Lebesgue measure. Therefore, its density function exists which is given by

$$\begin{aligned}&p_{\bar{Y}_1^n}(y^n)\\ &= \frac{1}{|\mathcal{W}|}\sum_{(w_1,w_2,w_1',w_2')\in\mathcal{W}}\\ &\quad p_{Z^n}\left(y^n - \left(a_1^n(w_1) + v_1^n(w_1')\right) - \rho_1\left(a_2^n(w_2) + v_2^n(w_2')\right)\right)\\ &= \frac{1}{|\mathcal{W}|}\sum_{(w_1,w_2,w_1',w_2')\in\mathcal{W}} p_{Z^n}\left(y^n - x_1^n(w_1,w_1') - \rho_1\ x_2^n(w_2,w_2')\right)\\ &= \frac{1}{|\mathcal{W}|}\sum_{(w_1,w_2,w_1',w_2')\in\mathcal{W}}\prod_{i=1}^n p_Z(y_i - x_{1,i} - \rho_1 x_{2,i}),\end{aligned}$$

where $p_Z \sim \mathcal{N}(0,1)$. Similarly, for the distribution of $P_{\bar{Y}_1^n|W_2=w_2}$ its probability density function can be written as

$$p_{\bar{Y}_1^n|W_2=w_2}(y^n) = \frac{1}{|\overline{\mathcal{W}_2}|}\sum_{(w_1,w_1',w_2')\in\overline{\mathcal{W}_2}}\prod_{i=1}^n p_Z(y_i - x_{1,i} - \rho_1 x_{2,i}).$$

The indices w_1, w_2, w_1' and w_2' are omitted in $x_{1,i}$ and $x_{2,i}$ without ambiguity.

In what follows, we will define a measurable set $\mathcal{T}_n \subset \mathbb{R}^n$, with $\lambda(\mathcal{T}_n) < \infty$ for finite n. The motivation is to focus on this measurable set such that the desired mutual information $I(W_2, \bar{Y}_1^n)$ and variation distance $d(P_{W_2}P_{\bar{Y}_1^n}, P_{W_2\bar{Y}_1^n})$ are concentrated on it.

For every $i \in [1:n]$, let

$$\begin{aligned}T^i &= \max_{\mathcal{W}}\left\{|v_{1,i}(w_1) + a_{1,i}(w_1')| + \rho_1|v_{2,i}(w_2) + a_{2,i}(w_2')|\right\}\\ &= \max_{\mathcal{W}}\left\{|x_{1,i}| + \rho_1|x_{2,i}|\right\}.\end{aligned}$$

By the average power constraint, it is worth noting that $T^i \le \sqrt{2nP}$. Because $\overline{\mathcal{W}_2} \cup w_2 \subseteq \mathcal{W}$, we have $T^i \ge \max_{\overline{\mathcal{W}_2}}\left\{|x_{1,i}| + \rho_i|x_{2,i}|\right\}$ given $W_2 = w_2$.

Let $\mathcal{T}^i = \left\{y : y \in (-T^i - \sqrt{2n}, T^i + \sqrt{2n})\right\}$. Define

$$\mathcal{T}_n = \left\{y^n : y_i \in \mathcal{T}^i, \forall i \in [1:n]\right\},$$

which is an n-dimensional Borel measurable set. Use $\overline{\mathcal{T}^i}$ and $\overline{\mathcal{T}_n}$ to represent the complement of $\mathcal{T}^i$ and $\mathcal{T}_n$, respectively. The properties regarding the partition presented in Lemma 4 will be used in the later proof.

Lemma 4: Let $\epsilon_n = e^{-n}$. Then the following properties hold:

1) Given $x_{1,i}, x_{2,i}$, and ρ_1, define $E = \left\{y - x_{1,i} - \rho_1\ x_{2,i} : \forall y \in \overline{\mathcal{T}^i}\right\}$. Then $P_Z(E) \le \epsilon_n$, where Z is normally distributed.

2) $P_{\bar{Y}_1^n}(\mathcal{T}_n) \ge (1-\epsilon_n)^n$ and $P_{\bar{Y}_1^n|W_2=w_2}(\mathcal{T}_n) \ge (1-\epsilon_n)^n$.

3) $P_{\bar{Y}_1^n}(\overline{\mathcal{T}_n}) \le 1 - (1-\epsilon_n)^n \le n\epsilon_n$, and $P_{\bar{Y}_1^n|W_2=w_2}(\overline{\mathcal{T}_n}) \le 1 - (1-\epsilon_n)^n \le n\epsilon_n$.

4) For $y^n \in \mathcal{T}_n$, the probability density functions $p_{\bar{Y}_1^n}(y^n) \ge (\frac{1}{\sqrt{2\pi}})^n e^{-tn^2}$, and $p_{\bar{Y}_1^n|W_2=w_2}(y^n) \ge (\frac{1}{\sqrt{2\pi}})^n e^{-tn^2}$, where $t = (2\sqrt{P} + \sqrt{2})^2$ and P represent the average power constraint.

5) For $y^n \in \overline{\mathcal{T}_n}$, the probability density functions satisfy

$$\begin{aligned}p_{\bar{Y}_1^n}(y^n) &\le \left(\frac{1}{\sqrt{2\pi}}\right)^n e^{-n}\\ p_{\bar{Y}_1^n|W_2=w_2}(y^n) &\le \left(\frac{1}{\sqrt{2\pi}}\right)^n e^{-n}.\end{aligned}$$

Proof: The proof is found in Appendix E. ■

For clarity of presentation, we define the following notation. For a continuous distribution P, and a Borel measurable set $B \subset \mathbb{R}$, let $h(P, B)$ represent the part of the differential entropy $h(P)$ on B, if it exists; i.e.,

$$h(P, B) := \int_B -p(x)\log p(x)dx.$$

Let $h_B(P)$ represent the differential entropy for the distribution obtained by truncating P on B; i.e.,

$$h_B(P) := \int_B -\frac{p(x)}{P(B)}\log\frac{p(x)}{P(B)}dx.$$

$d_B(P, Q)$ represents the variational distance between the pair of distributions by truncating P and Q on B:

$$\begin{aligned}d_B(P, Q) &:= 2\sup_{\mathcal{E}\subseteq B}\left|\frac{P(\mathcal{E})}{P(B)} - \frac{Q(\mathcal{E})}{Q(B)}\right|\\ &= \int_B\left|\frac{p(x)}{P(B)} - \frac{q(x)}{Q(B)}\right|dx,\end{aligned}$$

in which the last equality holds if and only if the density functions exist.

Based on the partition of $\mathcal{T}_n$ and $\overline{\mathcal{T}_n}$, we can divide $\mathbb{R}^n$ into two disjoint parts. We have

$$\begin{aligned}&h(\bar{Y}_1^n) - h(\bar{Y}_1^n|W_2 = w_2)\\ &= \int_{\mathcal{T}_n}\Big(-p_{\bar{Y}_1^n}(y^n)\log p_{\bar{Y}_1^n}(y^n)\\ &\quad + p_{\bar{Y}_1^n|W_2=w_2}(y^n)\log p_{\bar{Y}_1^n|W_2=w_2}(y^n)\Big)dy^n\\ &\quad + \int_{\overline{\mathcal{T}_n}}\Big(-p_{\bar{Y}_1^n}(y^n)\log p_{\bar{Y}_1^n}(y^n)\end{aligned}$$

$$
\begin{aligned}
&h(P_{\bar{Y}_1^n},\mathcal{T}_n) - h(P_{\bar{Y}_1^n|W_2=w_2},\mathcal{T}_n)\\
&= P_{\bar{Y}_1^n}(\mathcal{T}_n)\int_{\mathcal{T}_n} -\frac{p_{\bar{Y}_1^n}(y^n)}{P_{\bar{Y}_1^n}(\mathcal{T}_n)}\log\frac{p_{\bar{Y}_1^n}(y^n)}{P_{\bar{Y}_1^n}(\mathcal{T}_n)}dy^n - P_{\bar{Y}_1^n}(\mathcal{T}_n)\log P_{\bar{Y}_1^n}(\mathcal{T}_n)\\
&\quad - P_{\bar{Y}_1^n|W_2=w_2}(\mathcal{T}_n)\int_{\mathcal{T}_n} -\frac{p_{\bar{Y}_1^n|W_2=w_2}(y^n)}{P_{\bar{Y}_1^n|W_2=w_2}(\mathcal{T}_n)}\log\frac{p_{\bar{Y}_1^n|W_2=w_2}(y^n)}{P_{\bar{Y}_1^n|W_2=w_2}(\mathcal{T}_n)}dy^n + P_{\bar{Y}_1^n|W_2=w_2}(\mathcal{T}_n)\log P_{\bar{Y}_1^n|W_2=w_2}(\mathcal{T}_n)\\
&= P_{\bar{Y}_1^n}(\mathcal{T}_n)h_{\mathcal{T}_n}(P_{\bar{Y}_1^n}) - P_{\bar{Y}_1^n|W_2=w_2}(\mathcal{T}_n)h_{\mathcal{T}_n}(P_{\bar{Y}_1^n}|W_2=w_2)\\
&\quad - P_{\bar{Y}_1^n}(\mathcal{T}_n)\log P_{\bar{Y}_1^n}(\mathcal{T}_n) + P_{\bar{Y}_1^n|W_2=w_2}(\mathcal{T}_n)\log P_{\bar{Y}_1^n|W_2=w_2}(\mathcal{T}_n)\\
&= \Big(h_{\mathcal{T}_n}(P_{\bar{Y}_1^n}) - h_{\mathcal{T}_n}(P_{\bar{Y}_1^n|W_2=w_2})\Big)P_{\bar{Y}_1^n}(\mathcal{T}_n) + h_{\mathcal{T}_n}(P_{\bar{Y}_1^n|W_2=w_2})\int_{\mathcal{T}_n} p_{\bar{Y}_1^n}(y^n) - p_{\bar{Y}_1^n|W_2=w_2}(y^n)\ dy^n\\
&\quad - P_{\bar{Y}_1^n}(\mathcal{T}_n)\log P_{\bar{Y}_1^n}(\mathcal{T}_n) + P_{\bar{Y}_1^n|W_2=w_2}(\mathcal{T}_n)\log P_{\bar{Y}_1^n|W_2=w_2}(\mathcal{T}_n)\\
&\le \Big(h_{\mathcal{T}_n}(P_{\bar{Y}_1^n}) - h_{\mathcal{T}_n}(P_{\bar{Y}_1^n|W_2=w_2})\Big)P_{\bar{Y}_1^n}(\mathcal{T}_n) + h_{\mathcal{T}_n}(P_{\bar{Y}_1^n|W_2=w_2})d(P_{\bar{Y}_1^n}, P_{\bar{Y}_1^n|W_2=w_2})\\
&\quad + 2(1-e^{-n})^n\log(1-e^{-n})^n \qquad (23)\\
&\le h_{\mathcal{T}_n}(P_{\bar{Y}_1^n}) - h_{\mathcal{T}_n}(P_{\bar{Y}_1^n|W_2=w_2}) + e^{-n\alpha}|h_{\mathcal{T}_n}(P_{\bar{Y}_1^n|W_2=w_2})| + 2(1-e^{-n})^n\log(1-e^{-n})^n \qquad (24)
\end{aligned}
$$

$$
\begin{aligned}
&\quad + p_{\bar{Y}_1^n|W_2=w_2}(y^n)\log p_{\bar{Y}_1^n|W_2=w_2}(y^n)\Big)\,dy^n\\
&= h(P_{\bar{Y}_1^n},\mathcal{T}_n) - h(P_{\bar{Y}_1^n|W_2=w_2},\mathcal{T}_n) + h(P_{\bar{Y}_1^n},\overline{\mathcal{T}_n})\\
&\quad - h(P_{\bar{Y}_1^n|W_2=w_2},\overline{\mathcal{T}_n}).
\end{aligned}
$$

Taking the limit in n, we have

$$
\begin{aligned}
&\lim_{n\to\infty}\big(h(\bar{Y}_1^n) - h(\bar{Y}_1^n|W_2=w_2)\big)\\
&\quad\le \limsup_{n\to\infty}\Big(h(P_{\bar{Y}_1^n},\mathcal{T}_n) - h(P_{\bar{Y}_1^n|W_2=w_2},\mathcal{T}_n)\Big)\\
&\qquad + \limsup_{n\to\infty}\Big(h(P_{\bar{Y}_1^n},\overline{\mathcal{T}_n}) - h(P_{\bar{Y}_1^n|W_2=w_2},\overline{\mathcal{T}_n})\Big). \qquad (25)
\end{aligned}
$$

Based on the following lemma, it is sufficient to show that the above limit goes to 0.

Lemma 5: For distributions $P_{\bar{Y}_1^n}$ and $P_{\bar{Y}_1^n|W_2=w_2}$, and sets $\mathcal{T}_n$ and $\overline{\mathcal{T}_n}$ as defined, we have

1) $\limsup_{n\to\infty}\Big(h(P_{\bar{Y}_1^n},\mathcal{T}_n) - h(P_{\bar{Y}_1^n|W_2=w_2},\mathcal{T}_n)\Big) \le 0,$

2) $\limsup_{n\to\infty}\Big(h(P_{\bar{Y}_1^n},\overline{\mathcal{T}_n}) - h(P_{\bar{Y}_1^n|W_2=w_2},\overline{\mathcal{T}_n})\Big) \le 0.$

Proof of Lemma 5.1: We start the proof with the inequalities shown at the top of the page, which follow from the definition of differential entropy. (23), as shown at the top of this page follows from the following facts. First,

$$
\begin{aligned}
&\int_{\mathcal{T}_n} p_{\bar{Y}_1^n}(y^n) - p_{\bar{Y}_1^n|W_2=w_2}(y^n)dy^n\\
&\quad\le \int_{\mathcal{T}_n}\Big|p_{\bar{Y}_1^n}(y^n) - p_{\bar{Y}_1^n|W_2=w_2}(y^n)\Big|\,dy^n\\
&\quad\le \int_{\mathbb{R}^n}\Big|p_{\bar{Y}_1^n}(y^n) - p_{\bar{Y}_1^n|W_2=w_2}(y^n)\Big|\,dy^n\\
&\quad= d(P_{\bar{Y}_1^n}, P_{\bar{Y}_1^n|W_2=w_2}).
\end{aligned}
$$

Secondly, let $f(p) := -p\log p$, which is a non-negative monotonically decreasing function in p when $p \to 1^-$. Because $P_{\bar{Y}_1^n}(\mathcal{T}_n) \ge (1-e^{-n})^n$ and $P_{\bar{Y}_1^n|W_2=w_2}(\mathcal{T}_n) \ge (1-e^{-n})^n$, this leads to

$$
\begin{aligned}
&-P_{\bar{Y}_1^n}(\mathcal{T}_n)\log P_{\bar{Y}_1^n}(\mathcal{T}_n)\\
&\qquad + P_{\bar{Y}_1^n|W_2=w_2}(\mathcal{T}_n)\log P_{\bar{Y}_1^n|W_2=w_2}(\mathcal{T}_n)\\
&\quad := f(P_{\bar{Y}_1^n}(\mathcal{T}_n)) - f(P_{\bar{Y}_1^n|W_2=w_2}(\mathcal{T}_n))\\
&\quad \le 2(1-e^{-n})^n\log(1-e^{-n})^n.
\end{aligned}
$$

(24), as shown at the top of this page follows from the facts that $P_{\bar{Y}_1^n}(\mathcal{T}_n) \le 1$, and $d(P_{\bar{Y}_1^n}, P_{\bar{Y}_1^n|W_2=w_2}) \le e^{-\alpha n}$. In (24), at first we have $|h_{\mathcal{T}_n}(P_{\bar{Y}_1^n|W_2=w_2})|$ bounded as follows:

$$
\begin{aligned}
h_{\mathcal{T}_n}(P_{\bar{Y}_1^n|W_2=w_2}) &\le -\min_{y^n}\log\left(\frac{p_{\bar{Y}_1^n|W_2=w_2}(y^n)}{P_{\bar{Y}_1^n|W_2=w_2}(\mathcal{T}_n)}\right)\\
&\le -\log\frac{(\frac{1}{\sqrt{2\pi}})^n e^{-tn^2}}{P_{\bar{Y}_1^n|W_2=w_2}(\mathcal{T}_n)}\\
&\le -n\log\left(\frac{1}{\sqrt{2\pi}}e^{-tn}\right)\\
&= O(n^2).
\end{aligned}
$$

On the other hand,

$$
\begin{aligned}
&h_{\mathcal{T}_n}(P_{\bar{Y}_1^n|W_2=w_2})\\
&\quad\ge P_{\bar{Y}_1^n|W_2=w_2}(\mathcal{T}_n)^2\\
&\qquad\cdot\Big(-\max_{y^n}\log(p_{\bar{Y}_1^n|W_2=w_2}(y^n)) + \log(P_{\bar{Y}_1^n|W_2=w_2}(\mathcal{T}_n))\Big)\\
&\quad\ge P_{\bar{Y}_1^n|W_2=w_2}(\mathcal{T}_n)^2\\
&\qquad\cdot\Big(-\log(\frac{1}{\sqrt{2\pi}})^n + \log(P_{\bar{Y}_1^n|W_2=w_2}(\mathcal{T}_n)))\Big)\\
&\quad= O(n),
\end{aligned}
$$

which follows from the fact that $\max_{y^n}\log(p_{\bar{Y}_1^n|W_2=w_2}(y^n)) \le \log(\frac{1}{\sqrt{2\pi}})^n$, where the maximum value is achieved when all the Gaussian density peaks overlap.

Therefore, $|h_{\mathcal{T}_n}(P_{\bar{Y}_1^n|W_2=w_2})| = O(n^2)$. Substituting into (24), and taking the lim sup of both sides, we have

$$\begin{aligned}&\limsup_{n\to\infty}\left(h(P_{\bar{Y}_1^n},\mathcal{T}_n)-h(P_{\bar{Y}_1^n|W_2=w_2},\mathcal{T}_n)\right)\\&\quad\le\limsup_{n\to\infty}\left(h_{\mathcal{T}_n}(P_{\bar{Y}_1^n})-h_{\mathcal{T}_n}(P_{\bar{Y}_1^n|W_2=w_2})\right).\end{aligned}\tag{26}$$

The importance of the above steps is that we have bounded the partial integral on the left hand side of (26) from above by the difference of the differential entropy of the pair of truncated distributions on the partition $\mathcal{T}_n$. In what follows, we focus on the differential entropy terms on the partition $\mathcal{T}_n$, which has finite measure for any $n<\infty$. Up to this point, the following claim will directly lead to Lemma 5.1.

Claim 2:

$$\limsup_{n\to\infty}\left(h_{\mathcal{T}_n}(P_{\bar{Y}_1^n})-h_{\mathcal{T}_n}(P_{\bar{Y}_1^n|W_2=w_2})\right)\le 0.$$

In order to show the above claim, the following property of the variational distance of the same pair of truncated distributions is used. The key observation is that it decays to zero exponentially fast with n.

Claim 3: There exists an $N>0$ and $\beta>0$ such that for all $n>N$, the following holds:

$$d_{\mathcal{T}_n}(P_{\bar{Y}_1^n},P_{\bar{Y}_1^n|W_2=w_2})\le e^{-n\beta}.$$

Proof of Claim 3:

$$\begin{aligned}&d_{\mathcal{T}_n}(P_{\bar{Y}_1^n},P_{\bar{Y}_1^n|W_2=w_2})\\&=\int_{\mathcal{T}_n}\left|\frac{p_{\bar{Y}_1^n}(y^n)}{P_{\bar{Y}_1^n}(\mathcal{T}_n)}-\frac{p_{\bar{Y}_1^n|W_2=w_2}(y^n)}{P_{\bar{Y}_1^n|W_2=w_2}(\mathcal{T}_n)}\right|dy^n\\&=\int_{\mathcal{T}_n}\frac{1}{P_{\bar{Y}_1^n}(\mathcal{T}_n)}\left|p_{\bar{Y}_1^n}(y^n)-\frac{P_{\bar{Y}_1^n}(\mathcal{T}_n)p_{\bar{Y}_1^n|W_2=w_2}(y^n)}{P_{\bar{Y}_1^n|W_2=w_2}(\mathcal{T}_n)}\right|dy^n\\&\le\frac{1}{P_{\bar{Y}_1^n}(\mathcal{T}_n)}\int_{\mathcal{T}_n}\left|p_{\bar{Y}_1^n}(y^n)-p_{\bar{Y}_1^n|W_2=w_2}(y^n)\right|dy^n\\&\quad+\left|\frac{1}{P_{\bar{Y}_1^n}(\mathcal{T}_n)}(1-\frac{P_{\bar{Y}_1^n}(\mathcal{T}_n)}{P_{\bar{Y}_1^n|W_2=w_2}(\mathcal{T}_n)})\right|\int_{\mathcal{T}_n}p_{\bar{Y}_1^n|W_2=w_2}(y^n)dy^n\\&\le\frac{1}{P_{\bar{Y}_1^n}(\mathcal{T}_n)}\Big(d(P_{\bar{Y}_1^n},P_{\bar{Y}_1^n|W_2=w_2})\\&\quad+\left|P_{\bar{Y}_1^n|W_2=w_2}(\mathcal{T}_n)-P_{\bar{Y}_1^n}(\mathcal{T}_n)\right|\Big)\\&\le\frac{1}{P_{\bar{Y}_1^n}(\mathcal{T}_n)}(e^{-n\alpha}+ne^{-n})\\&\le e^{-n\beta},\quad\text{for some}\quad\beta>0.\end{aligned}\tag{27}$$

(27) follows from the fact that for some $\alpha>0$, there exist an N such that for all $n>N$

$$d(P_{\bar{Y}_1^n},P_{\bar{Y}_1^n|W_2=w_2})\le e^{-n\alpha},\tag{28}$$

based on resolvability. And

$$\begin{aligned}(1-e^{-n})^n&\le P_{\bar{Y}_1^n}(\mathcal{T}_n)\le 1\\(1-e^{-n})^n&\le P_{\bar{Y}_1^n|W_2=w_2}(\mathcal{T}_n)\le 1,\end{aligned}$$

thus

$$|P_{\bar{Y}_1^n}(\mathcal{T}_n)-P_{\bar{Y}_1^n|W_2=w_2}(\mathcal{T}_n)|\le 1-(1-e^{-n})^n\le ne^{-n}$$

by Lemma 4.3. The proof of Claim 3 is complete.

Proof of Claim 2: By the reverse Pinsker's inequality in Lemma 3, because $P_{\bar{Y}_1^n}$ and $P_{\bar{Y}_1^n|W_2=w_2}$ are finite everywhere, there exists some constant $c>0$, such that

$$\begin{aligned}&h_{\mathcal{T}_n}(P_{\bar{Y}_1^n})-h_{\mathcal{T}_n}(P_{\bar{Y}_1^n|W_2=w_2})\\&\quad\le nd_{\mathcal{T}_n}(P_{\bar{Y}_1^n},P_{\bar{Y}_1^n|W_2=w_2})\\&\qquad\cdot\left(\log\frac{\lambda(\mathcal{T}_n)}{d_{\mathcal{T}_n}(P_{\bar{Y}_1^n},P_{\bar{Y}_1^n|W_2=w_2})}+n\log c\right)\\&\quad\le ne^{-n\beta}\log(\lambda(\mathcal{T}_n))-ne^{-n\beta}\log(e^{-n\beta})+n^2e^{-\alpha n}\log c\\&\quad=ne^{-n\beta}\log(O(n^{\frac{n}{2}}))-ne^{-n\beta}\log(e^{-n\beta})+n^2e^{-\alpha n}\log c\\&\quad=O(n^2\log ne^{-n\beta}).\end{aligned}$$

Taking the lim sup of both sides, we have $\limsup_{n\to\infty}\left(h_{\mathcal{T}_n}(P_{\bar{Y}_1^n})-h_{\mathcal{T}_n}(P_{\bar{Y}_1^n|W_2=w_2})\right)\le 0$. ■

The proof of Lemma 5.1 is concluded after Claim 2. ■

Proof of Lemma 5.2: In order to show that

$$\limsup_{n\to\infty}\left(h(P_{\bar{Y}_1^n},\overline{\mathcal{T}_n})-h(P_{\bar{Y}_1^n|W_2=w_2},\overline{\mathcal{T}_n})\right)\le 0,\tag{29}$$

it suffices to show that $\limsup_{n\to\infty}\left|h(P_{\bar{Y}_1^n},\overline{\mathcal{T}_n})\right|=0$ and $\limsup_{n\to\infty}\left|h(P_{\bar{Y}_1^n|W_2=w_2},\overline{\mathcal{T}_n})\right|=0$.

For $y^n\in\overline{\mathcal{T}_n}$, the probability density function can be bounded as follows. Let $\mu_i=x_{1,i}+\rho_1\ x_{2,i}$, and define the set $\mathcal{J}:=\{j:y_j\in\overline{\mathcal{T}^j}\}$, then

$$\begin{aligned}&p_{\bar{Y}_1^n}(y^n)\\&\quad=\frac{1}{|\mathcal{W}|}\sum_{\mathcal{W}}\left(\prod_{i=1}^n p_Z(y_i-\mu_i)\right)\\&\quad=\frac{1}{|\mathcal{W}|}\sum_{\mathcal{W}}\left(\left(\frac{1}{\sqrt{2\pi}}\right)^n\right.\\&\qquad\left.\cdot\exp\left(-\frac{\sum_{j\in\mathcal{J}}(y_j-\mu_j)^2+\sum_{i\notin\mathcal{J}}(y_i-\mu_i)^2}{2}\right)\right),\\&\quad\le\max_{w\in\mathcal{W}}\left(\left(\frac{1}{\sqrt{2\pi}}\right)^n\right.\\&\qquad\left.\cdot\exp\left(-\frac{\sum_{j\in\mathcal{J}}(y_j-\mu_j)^2+\sum_{i\notin\mathcal{J}}(y_i-\mu_i)^2}{2}\right)\right)\\&\quad=\prod_{j\in\mathcal{J}}p_j(y_j)\prod_{i\notin\mathcal{J}}p_i(y_i),\quad\text{for } y_j\in\overline{\mathcal{T}^j},\ \text{and } y_i\in\mathcal{T}^i,\end{aligned}\tag{30}$$

in which (30) follows by choosing a combination of transmitted sequences, i.e., μ^n, which is the closest to y^n with respect to the Euclidean distance among all possible combinations in the codebook. The last equality follows from the definition

$$\begin{aligned}p_j(y_j)&:=\frac{1}{\sqrt{2\pi}}\exp\left(-\frac{(y_j-\mu_j)^2}{2}\right),\quad\text{for } y_j\in\overline{\mathcal{T}^j}\\p_i(y_i)&:=\frac{1}{\sqrt{2\pi}}\exp\left(-\frac{(y_i-\mu_i)^2}{2}\right),\quad\text{for } y_i\in\mathcal{T}_i.\end{aligned}$$

As $f(p) := -p\log p > 0$ when $p \to 0^+$, then $h(P_{\bar{Y}_1^n}, \overline{\mathcal{T}_n}) > 0$ because $p_{\bar{Y}_1^n}(y^n) \le (\frac{1}{\sqrt{2\pi}})^n e^{-n}$ as shown in Lemma 4.5.

Since $f(p)$ increases monotonically in p when $p \to 0^+$, we have

$$\begin{aligned} h(P_{\bar{Y}_1^n}, \overline{\mathcal{T}_n}) &= \int_{\overline{\mathcal{T}_n}} -p_{\bar{Y}_1^n}(y^n)\log p_{\bar{Y}_1^n}(y^n) dy^n \\ &\le \int_{\overline{\mathcal{T}_n}} - \prod_{j\in\mathcal{J}} p_j(y_j) \prod_{i\notin\mathcal{J}} p_i(y_i) \\ &\quad \cdot \log\left(\prod_{j\in\mathcal{J}} p_j(y_j) \prod_{i\notin\mathcal{J}} p_i(y_i)\right) dy^n \\ &= \prod_{i\notin\mathcal{J}} P_i(\mathcal{T}^i) \sum_{j\in\mathcal{J}} \prod_{k\in\mathcal{J}, k\neq j} P_k(\overline{\mathcal{T}^k}) \\ &\quad \cdot \int_{\overline{\mathcal{T}^j}} -p_j(y_j)\log p_j(y_j) dy_j \\ &\quad + \prod_{j\in\mathcal{J}} P_j(\overline{\mathcal{T}^j}) \sum_{i\notin j} \prod_{k\notin\mathcal{J}, k\neq i} P_k(\mathcal{T}^k) \\ &\quad \cdot \int_{\mathcal{T}^i} -p_i(y_i)\log p_i(y_i) dy_i \\ &\le \sum_{j\in\mathcal{J}} h(P_j, \overline{\mathcal{T}^j}) + (2e^{-n})^{|\mathcal{J}|} \sum_{i\notin\mathcal{J}} h(P_i, \mathcal{T}^i) \\ &\le e^{-n\epsilon}, \quad \text{for some } \epsilon > 0, \end{aligned}$$

where the last inequality holds because

$$\begin{aligned} &h(P_j, \overline{\mathcal{T}^j}) > 0, \text{ as } -p\log p > 0 \text{ when } p \to 0^+ \\ &h(P_j, \overline{\mathcal{T}^j}) = O(ne^{-n}), \\ &h(P_j, \mathcal{T}^j) = \ln\sqrt{2\pi e} - h(P_j, \overline{\mathcal{T}^j}) \le \ln\sqrt{2\pi e}, \end{aligned}$$

which follow from the properties shown in Lemma 4.

Therefore, we have $|h(P_{\bar{Y}_1^n}, \overline{\mathcal{T}_n})| \le e^{-n\epsilon}$. Following a similar proof, we can show that $|h(P_{\bar{Y}_1^n|W_2=w_2}, \overline{\mathcal{T}_n})| \le e^{-n\gamma}$ for some $\gamma > 0$.

Taking the limit,

$$\begin{aligned} &\limsup_{n\to\infty} \left(h(P_{\bar{Y}_1^n}, \overline{\mathcal{T}_n}) - h(P_{\bar{Y}_1^n|W_2=w_2}, \overline{\mathcal{T}_n})\right) \\ &\quad \le \limsup_{n\to\infty} \left|h(P_{\bar{Y}_1^n}, \overline{\mathcal{T}_n})\right| + \limsup_{n\to\infty} \left|h(P_{\bar{Y}_1^n|W_2=w_2}, \overline{\mathcal{T}_n})\right| = 0. \end{aligned}$$

The proof of Lemma 5.2 is complete. ■

To conclude, based on Lemma 5 and inequality (25), for the chosen sequence of codebooks $\{C_n\}$ the strong secrecy constraint is satisfied.

2) Artificial Noise Transmission: What remains to prove is that the actual rate region in Proposition 2 is achieved. We present an artificial noise aided scheme to tie the same achievable rate region with weak secrecy constraints [4]. The strategy is to split the transmission power P into two parts, one for transmitting the confidential message and one for generating artificial noise. Let

$$\begin{aligned} P_{1,V} &= (1-\lambda_1)\beta_1 P, \quad \text{and } P_{1,A} = \lambda_1\beta_1 P \\ P_{2,V} &= (1-\lambda_2)\beta_2 P, \quad \text{and } P_{2,A} = \lambda_2\beta_2 P, \end{aligned}$$

where $\lambda_i, \beta_i \in [0,1]$ for $i = 1,2$. Set U to be an optimization operator which chooses λ_i and β_i. Setting $P_{V_i} \sim \mathcal{N}(0, P_{i,V})$ and $P_{A_i} \sim \mathcal{N}(0, P_{i,A})$, and calculating (19)-(22) the rate region in Proposition 2 is established. ■

Remark 6: Proposition 2 is meaningful in the following aspects:

- The generalization from discrete channels to Gaussian channels is regardless of input distributions that generate the random codebooks. Therefore, the rate region as shown in (12) holds for any input distributions as factorized in Theorem 1 for Gaussian channels. The results can be generalized to K-user ($K > 2$) stationary and memoryless Gaussian interference channels directly following a similar analysis, the achievable strong secrecy rate region of which is given by

$$\begin{aligned} \mathcal{D} := \Big\{ &(R_1, R_2, \ldots, R_K) \in \mathbb{R}_+^K, \forall k \in [1:K], \\ &R_k < I(V_k; Y_k|U) - \max_{j\in[1:K]\setminus k} I(V_k; Y_j|V_{[1:K]\setminus k}, U) \Big\} \end{aligned}$$

  for any input distribution

$$P_U \prod_{k\in[1:K]} P_{V_k|U} P_{X_k|V_k},$$

  which satisfies the additive constraint $\mathbb{E}[c(X_k] \le P$ provided that the moment generating functions of $i_{V_kY_k|V_{[1:K]\setminus k}U}$ and $c(X_k)$ exist. $V_{[1:K]\setminus k}$ represents the collection of $V_i, \forall i \in [1:K] \setminus k$. Therefore, the strong secrecy rate region coincides with the weak secrecy rate region shown in [25] under mild conditions.
- The key steps of the proof of Proposition 2 essentially investigate the relationships among divergence, differential entropy, and variational distance of a family of probability distributions. The principle is to find a proper subset of the output alphabets such that the desired measures are concentrated on it. Together with the proposed reverse Pinsker's inequality in Lemma 3, the generalization from discrete alphabets to continuous alphabets is completely different from the quantization method in [36].

VI. Conclusion

The problem of transmitting confidential messages in interference channels has been studied under strong secrecy constraints. Starting from generalizing the channel resolvability theory to arbitrary interference channels, we have derived the achievable secrecy rate region for the stationary and memoryless interference channel with additive cost functions. It is interesting to note that the derived secrecy rate region for the discrete memoryless channel remains the same as the best known region under weak secrecy constraints. However, the optimality of it has not yet been proved. Note that we have used the information-spectrum method to analyze secrecy in the considered network, and strong secrecy has been guaranteed by penalizing the confidential message a binning rate above the resolution of its eavesdropper's channel.

The presented theoretical framework of analyzing strong secrecy for interference channels contains two major steps. The first step is based on the resolvability theory that by sampling the input process with a rate higher than the channel resolution the output statistics is well approximated in terms of the variational distance or normalized divergence. A direct application of the resolvability result is that it implies the achievable rate region for weak secrecy of arbitrary interference channels with confidential messages. The second step has been focused on the generalization from the resolvability result to strong secrecy via exploiting the relationship between variational distance and mutual information. A reverse direction of Pinsker's inequality has been proposed in order to bound the mutual information, in other words, the divergence of two probability distributions, from above as a function of the variational distance between them. The proposed reverse Pinsker's inequality together with a truncation method are leveraged in the study of Gaussian interference channels. It is worth noting that the achievable rate region for strong secrecy also ties with the best known weak secrecy rate region for Gaussian interference channels. Our study has provided further evidence that the channel resolvability framework is a powerful tool for strong secrecy analysis in multiuser networks.

Appendix A
Preliminary Lemmas

Lemma 6 (Triangle Inequality for Variational Distance): Let X_1, X_2 and X_3 be random variables defined on the same alphabet set $\mathcal{X}$, with different distributions respectively. The following inequalities hold:

$$d(P_{X_1}, P_{X_3}) \leq d(P_{X_1}, P_{X_2}) + d(P_{X_2}, P_{X_3}),$$
$$d(P_{X_1}, P_{X_2}) \leq d(P_{X_1}P_{X_3}, P_{X_2X_3}) = \mathbb{E}_{X_3}\left[d(P_{X_1}, P_{X_2|X_3})\right].$$

Lemma 7 (Data-processing Inequality for Variational Distance): Let X_1 and X_2 be random variables defined on the alphabet set $\mathcal{X}$. And let Z_1 and Z_2 be two random variables defined on the set $\mathcal{Z}$, which are defined as follows: $\forall(z, x) \in \mathcal{Z} \times \mathcal{X}$

$$P_{Z_iX_i}(z, x) = P_{Z|X}(z|x)P_{X_i}(x),\ i = 1, 2.$$

Then, $d(P_{Z_1}, P_{Z_2}) \leq d(P_{X_1}, P_{X_2})$.

Lemma 8 (Han-Verdú [16]): Let P and Q be two distributions defined on the same sample space. Then for every $\mu > 0$,

$$d(P, Q) \leq \frac{2}{\log e}\mu + 2\mathbb{P}\left[\log\frac{P(X)}{Q(X)} > \mu\right],$$

where the random variable X is distributed according to P.

Lemma 9 (Markov Inequality): If X is any non-negative integrable random variable and $a > 0$, then

$$\mathbb{P}[X \geq a] \leq \frac{\mathbb{E}[X]}{a}.$$

Lemma 10 (Chernoff Inequality): Let $X_1, X_2, \ldots X_n$ be independently and identically generated according to P_X. Assuming that the moment generating function $\mathbb{E}[e^{tX}]$ exists, then, $\forall\delta > 0$, there exists an $\alpha(\delta) > 0$ such that

$$\mathbb{P}\left[\frac{1}{n}\sum_{i=1}^{n} X_i > \mathbb{E}(X) + \delta\right] \leq e^{-\alpha(\delta)n}.$$

Lemma 11 (Tail Bound for Normal Distribution): Let $X \sim \mathcal{N}(0, 1)$. Then the following upper bound on the tail probability is satisfied:

$$\mathbb{P}[X > a] \leq \frac{\exp(-a^2/2)}{a\sqrt{2\pi}}.$$

Appendix B
Proof of Lemma 1

In this section, we will present a detailed proof of Lemma 1 given the codebook generation method presented therein. The proof consists of two parts: reliability and vanishing variational distance.

Reliability: Let $|\mathcal{W}_i\|\mathcal{W}_i'| = 2^{n(\underline{\mathbf{I}}(\mathbf{X}_i;\mathbf{Y}_i|\mathbf{U})-2\gamma)}$. We have

$$\mathcal{T}_{\gamma,i}^{(n)} = \Big\{(u^n, x_i^n, y_i^n) : \frac{1}{n}i_{X_i^nY_i^n|U^n}(x_i^n, y_i^n|u^n) \geq \underline{\mathbf{I}}(\mathbf{X}_i; \mathbf{Y}_i|\mathbf{U}) - \gamma\Big\},$$

based on the definition of $\mathcal{T}_{\gamma,i}^n$.

Define two types of error events as follows: based on the sent messages pair (w_i, w_i'),

$$\mathcal{E}_1 = \{(u^n, x_i^n(w_i, w_i'), y_i^n) \notin \mathcal{T}_{\gamma,i}^{(n)}\}$$
$$\mathcal{E}_2 = \{(u^n, x_i^n(\tilde{w}_i, \tilde{w}_i'), y_i^n) \in \mathcal{T}_{\gamma,i}^{(n)},\ \text{for } (\tilde{w}_i, \tilde{w}_i') \neq (w_i, w_i')\}.$$

We have the error probability $P_e^{(n)} \leq \mathbb{P}[\mathcal{E}_1] + \mathbb{P}[\mathcal{E}_2]$ by the union bound. By the definition of $\underline{\mathbf{I}}(\mathbf{X}_i; \mathbf{Y}_i|\mathbf{U})$, it is clear that $\lim_{n\to\infty}\mathbb{P}[\mathcal{E}_1] = 0$. Because the message pair (w_i, w_i') is chosen uniformly, it is sufficient to consider only the case $(w_i, w_i') = (1, 1)$. Let x_i^n represent the sequence corresponding to $(\tilde{w}_i, \tilde{w}_i') \neq (1, 1)$. For the event $\mathcal{E}_2$, we have

$$\begin{aligned}
&\mathbb{P}[\mathcal{E}_2] \\
&\quad\leq |\mathcal{W}_i\|\mathcal{W}_i'|\mathbb{P}\left[(u^n, x_i^n(\tilde{w}_i, \tilde{w}_i'), y_i^n) \in \mathcal{T}_{\gamma,i}^{(n)}\right] \\
&\quad= 2^{n(\underline{\mathbf{I}}(\mathbf{X}_i;\mathbf{Y}_i|\mathbf{U})-2\gamma)} \sum_{(u^n,x_i^n,y_i^n)\in\mathcal{T}_{\gamma,i}^{(n)}} P_{X_i^nY_i^nU^n}(x_i^n, y_i^n, u^n) \\
&\quad= 2^{n(\underline{\mathbf{I}}(\mathbf{X}_i;\mathbf{Y}_i|\mathbf{U})-2\gamma)} \\
&\qquad\cdot \sum_{(u^n,x_i^n,y_i^n)\in\mathcal{T}_{\gamma,i}^{(n)}} P_{Y_i^n|U^n}(y_i^n|u^n)P_{X_i^n|U^n}(x_i^n|u^n)P_{U^n}(u^n) &(31)\\
&\quad\leq 2^{n(\underline{\mathbf{I}}(\mathbf{X}_i;\mathbf{Y}_i|\mathbf{U})-2\gamma)} \\
&\qquad\cdot \sum_{(u^n,x_i^n,y_i^n)\in\mathcal{T}_{\gamma,i}^{(n)}} P_{Y_i^n|X_i^nU^n}(y_i^n|x_i^n, u^n)2^{-n(\underline{\mathbf{I}}(\mathbf{X}_i;\mathbf{Y}_i|\mathbf{U})-\gamma)} \\
&\qquad\cdot P_{X_i^n|U^n}(x_i^n|u^n)P_{U^n}(u^n) &(32)\\
&\quad\leq 2^{-n\gamma},
\end{aligned}$$

where (31) follows from the fact that y_i^n is independent of x_i^n given u^n for the unsent codewords, and (32) follows from the definition of $\mathcal{T}_{\gamma,i}^{(n)}$. Therefore, as $n \to \infty$, $P_e^{(n)}$ tends to zero. We note that this result is a conditioned version of Feinstein's Lemma [37].

Consequently, we can conclude that $R_i + R_i' = \underline{\mathbf{I}}(\mathbf{X}_i; \mathbf{Y}_i|\mathbf{U}) - 2\gamma$ is achieved for the reliability constraint.

Variational Distance for Output Distributions: Let $\{C_n\}_{n\in\mathbb{N}}$ represent a sequence of codes randomly generated according to the codebook generation method presented above:

$$C_n = \left\{(u^n, c_i^n(w_i, w_i')) : \forall(w_i, w_i') \in \mathcal{W}_i \times \mathcal{W}_i', i = 1, 2\right\},$$

where $c_i^n \in \mathcal{X}_i^n$. In order to identify the channel input and output when using a codeword from C_n, we represent the corresponding channel input and output variables as $\bar{X}_i^n$ and $\bar{Y}_i^n$, $i = 1, 2$, respectively, and the time sharing variables as $\bar{U}^n$. Based on the codebook C_n, the joint probability $P_{\bar{Y}_1^n\bar{Y}_2^n\bar{X}_1^n\bar{X}_2^n\bar{U}^nW_1W_2}$ (on its support) can be factored as follows, for $(u^n, c_1^n, c_2^n) \in C_n$:

$$\begin{aligned}
&P_{\bar{Y}_1^n\bar{Y}_2^n\bar{X}_1^n\bar{X}_2^n\bar{U}^nW_1W_2}(y_1^n, y_2^n, c_1^n, c_2^n, u^n, w_1, w_2)\\
&\quad= \Psi^n(y_1^n, y_2^n|x_1^n, x_2^n)P_{\bar{X}_1^n|\bar{U}^nW_1}(c_1^n|u^n, w_1)\\
&\qquad P_{\bar{X}_2^n|\bar{U}W_2}(c_2^n|u^n, w_2)P_{\bar{U}^n}(u^n)P_{W_1W_2}(w_1, w_2)\\
&\quad= \frac{1}{|\mathcal{W}_1'||\mathcal{W}_2'|}\sum_{w_1'\in\mathcal{W}_1'}\sum_{w_2'\in\mathcal{W}_2'} P_{W_1W_2}(w_1, w_2)\\
&\qquad \cdot \Psi^n(y_1^n, y_2^n|c_1^n(w_1, w_1'), c_2^n(w_2, w_2')).
\end{aligned}$$

The last equality follows from the fact that given C_n, $P_{\bar{U}^n}(u^n) = 1$ for $u^n \in C_n$, and $P_{\bar{X}_i^n|\bar{U}^nW_i}(c_i^n|u^n, w_i) = \frac{1}{|\mathcal{W}_i'|}\sum_{w_i'\in\mathcal{W}_i'} P_{\bar{X}_i^n|\bar{U}^nW_iW_i'}(c_i^n|u^n, w_i, w_i')$, where $P_{\bar{X}_i^n|\bar{U}^nW_iW_i'}(c_i^n|u^n, w_i, w_i') = \mathbf{1}\{c_i^n = c_i^n(w_i, w_i')\}$, and $\mathbf{1}\{\cdot\}$ is the indicator function.

We aim to show that

$$\lim_{n\to\infty} \mathbb{E}_{C_n}\left[d(P_{W_i\bar{Y}_j^n}, P_{W_i}P_{\bar{Y}_j^n})\right] = 0, \quad i, j\in\{1, 2\}\ i\neq j. \tag{33}$$

From (8), it suffices to show that (without loss of generality setting $i = 1, j = 2$)

$$\lim_{n\to\infty} \mathbb{E}_{C_n}\left[\mathbb{E}_{W_1\bar{X}_2^n\bar{U}^n}\left[d(P_{\bar{Y}_2^n|W_1\bar{X}_2^n\bar{U}^n}, P_{Y_2^n|X_2^nU^n})\right]\right] = 0. \tag{34}$$

In (34), the components are presented as follows:

- the conditional output distribution based on the code C_n is

$$\begin{aligned}
&P_{\bar{Y}_2^n|W_1\bar{X}_2^n\bar{U}^n}(y_2^n|w_1, c_2^n, u^n)\\
&\quad= \sum_{x_1^n\in C_n} P_{\bar{Y}_2^n|\bar{X}_1^n\bar{X}_2^n\bar{U}^nW_1}(y_2^n|x_1^n, c_2^n, u^n, w_1)\\
&P_{\bar{X}_1^n|\bar{X}_2^n\bar{U}^nW_1}(x_1^n|c_2^n, u^n, w_1)\\
&\quad= \sum_{x_1^n\in C_n} \Psi^n(y_2^n|x_1^n, c_2^n)P_{\bar{X}_1^n|\bar{U}^nW_1}(x_1^n|u^n, w_1)\\
&\quad= \frac{1}{|\mathcal{W}_1'|}\sum_{w_1'=1}^{|\mathcal{W}_1'|} \Psi^n(y_2^n|c_1^n(w_1, w_1'), c_2^n)\\
&\quad= \frac{1}{|\mathcal{W}_1'|}\sum_{w_1'=1}^{|\mathcal{W}_1'|} P_{Y_2^n|X_1^nX_2^nU^n}(y_2^n|c_1^n(w_1, w_1'), c_2^n, u^n),
\end{aligned}$$

where the last inequality follows because of the Markov chain condition: $U^n - (X_1^n, X_2^n) - Y_2^n$. $\Psi^n(y_2^n|x_1^n, x_2^n)$ represents the marginal distribution defined by the channel transition probability $P_{Y_2^n|X_1^n,X_2^n}(y_2^n|x_1^n, x_2^n)$.

- the target distribution is

$$\begin{aligned}
&P_{Y_2^n|X_2^nU^n}(y_2^n|x_2^n, u^n)\\
&\quad= \sum_{x_1^n\in\mathcal{X}_1^n} \Psi^n(y_2^n|x_1^n, x_2^n)P_{X_1^n|X_2^nU^n}(x_1^n|x_2^n, u^n)\\
&\quad= \sum_{x_1^n\in\mathcal{X}_1^n} \Psi^n(y_2^n|x_1^n, x_2^n)P_{X_1^n|U^n}(x_1^n|u^n).
\end{aligned}$$

According to Lemma 8, we have the following bound (let $\mu > 0$):

$$\mathbb{E}_{C_n}\left\{\mathbb{E}_{W_1\bar{X}_2^n\bar{U}^n}\left[d(P_{\bar{Y}_2^n|W_1\bar{X}_2^n\bar{U}^n}, P_{Y_2^n|X_2^nU^n})\right]\right\} \leq \frac{\mu}{\log e} + 2A_n,$$

where

$$\begin{aligned}
A_n = \mathbb{E}_{C_n}\Bigg\{&\mathbb{E}_{W_1\bar{X}_2^n\bar{U}_n}\\
&\left[\mathbb{P}\left[\log\frac{P_{\bar{Y}_2^n|W_1=w_1,\bar{X}_2=c_2^n,\bar{U}^n=u^n}(\bar{Y}_2^n)}{P_{Y_2^n|X_2^n=c_2^n,U^n=u^n}(\bar{Y}_2^n)} > \mu\right]\right]\Bigg\},
\end{aligned}$$

and $\bar{Y}_2^n$ is distributed according to $P_{\bar{Y}_2^n|W_1=w_1,\bar{X}_2^n=c_2^n,\bar{U}^n=u^n}$. Considering the independence of codewords and the symmetry of the codebook generation, we can choose $w_1 = 1$ for simplicity. Consequently, A_n is expanded as shown at the top of the next page.

We can represent the identification function in the following way:

$$\begin{aligned}
&\mathbf{1}\left\{\log\frac{P_{\bar{Y}_2^n|W_1=1,\bar{X}_2^n=c_2^n,\bar{U}^n=u^n}(y_2^n)}{P_{Y_2^n|X_2^n=c_2^n,U^n=u^n}(y_2^n)} > \mu\right\}\\
&\quad= \mathbf{1}\left\{\log\frac{1}{|\mathcal{W}_1'|}\sum_{i=1}^{|\mathcal{W}_1'|}\frac{\Psi^n(y_2^n|c_1^n(1, i), c_2^n)}{P_{Y_2^n|X_2^nU^n}(y_2^n|c_2^n, u^n)} > \mu\right\}\\
&\quad= \mathbf{1}\left\{\log\frac{1}{|\mathcal{W}_1'|}\sum_{i=1}^{|\mathcal{W}_1'|}\frac{P_{Y_2^n|X_1^nX_2^nU^n}(y_2^n|c_1^n(1, i), c_2^n, u^n)}{P_{Y_2^n|X_2^nU^n}(y_2^n|c_2^n, u^n)} > \mu\right\}\\
&\quad= \mathbf{1}\Bigg\{\frac{1}{|\mathcal{W}_1'|}\exp\left(i_{X_1^nY_2^n|X_2^nU^n}(c_1^n(1, 1), y_2^n|c_2^n, u^n)\right)\\
&\qquad\quad + \frac{1}{|\mathcal{W}_1'|}\sum_{i=2}^{|\mathcal{W}_1'|}\exp\left(i_{X_1^nY_2^n|X_2^nU^n}(c_1^n(1, i), y_2^n|c_2^n, u^n)\right)\\
&\quad > 1 + 2\tau\Bigg\},
\end{aligned} \tag{35}$$

where $\tau = \frac{2^\mu - 1}{2} > 0$.

By substituting the identification function (35) into A_n, we can bound A_n as follows:

$$\begin{aligned}
A_n \leq\ &\mathbb{P}\left[\frac{1}{|\mathcal{W}_1'|}\exp\left(i_{X_1^nY_2^n|X_2^nU^n}(X_1^n, Y_2^n|X_2^n, U^n)\right) > \tau\right]\\
&+\mathbb{P}\Bigg[\frac{1}{|\mathcal{W}_1'|}\sum_{i=2}^{|\mathcal{W}_1'|}\exp\left(i_{X_1^nY_2^n|X_2^nU^n}(X_1^n(1, i), Y_2^n|X_2^n, U^n)\right)\\
&\qquad > 1 + \tau\Bigg],
\end{aligned}$$

where X_1^n and Y_2^n are related through the channel Ψ^n, and $\{X_1^n(1, i), Y_2^n\}$ $(i \in \{2, \ldots, |\mathcal{W}_1'|\})$ are independent. By the

$$\begin{aligned}
A_n &= \mathbb{E}_{C_n}\left[P_{\bar{Y}_2^n|W_1=1,\bar{X}_2^n=c_2^n,\bar{U}^n=u^n}\left[\log\frac{P_{\bar{Y}_2^n|W_1=1,\bar{X}_2^n=c_2^n,\bar{U}^n=u^n}(\bar{Y}_2^n)}{P_{Y_2^n|X_2^n=c_2^n,U^n=u^n}(\bar{Y}_2^n)} > \mu\right]\right]\\
&= \sum_{u^n\in\mathcal{U}^n} P_{U^n}(u^n)\sum_{c_2^n\in\mathcal{X}_2^n} P_{X_2^n|U^n}(c_2^n|u^n)\prod_{w_1'=1}^{|\mathcal{W}_1'|}\sum_{c_1^n(1,w_1')\in\mathcal{X}_1^n} P_{X_1^n|U^n}(c_1^n(1,w_1')|u^n)\\
&\quad\cdot\sum_{y_2^n\in\mathcal{Y}_2^n} P_{\bar{Y}_2|W_1=1,\bar{X}_2^n=c_2^n,\bar{U}^n=u^n}(y_2^n)\\
&\quad\cdot\mathbf{1}\left\{\log\frac{P_{\bar{Y}_2^n|W_1=1,\bar{X}_2^n=c_2^n,\bar{U}^n=u^n}(y_2^n)}{P_{Y_2^n|X_2^n=c_2^n,U^n=u^n}(y_2^n)} > \mu\right\}\\
&= \frac{1}{|\mathcal{W}_1'|}\sum_{w_1'=1}^{|\mathcal{W}_1'|}\sum_{u^n\in\mathcal{U}^n} P_{U^n}(u^n)\sum_{c_2^n\in\mathcal{X}_2^n} P_{X_2^n|U^n}(c_2^n|u^n)\sum_{c_1^n(1,1)\in\mathcal{X}_1^n} P_{X_1^n|U^n}(c_1^n(1,1)|u^n)\\
&\quad\cdot\sum_{c_1^n(1,2)\in\mathcal{X}_1^n}\cdots\sum_{c_1^n(1,|\mathcal{W}_1'|)\in\mathcal{X}_1^n} P_{X_1^n|U^n}(c_1^n(1,|\mathcal{W}_1'|)|u^n)\sum_{y_2^n\in\mathcal{Y}_2^n}\Psi^n(y_2^n|c_1^n(1,w_1'),c_2^n)\\
&\quad\cdot\mathbf{1}\left\{\log\frac{P_{\bar{Y}_2^n|W_1=1,\bar{X}_2^n=c_2^n,\bar{U}^n=u^n}(y_2^n)}{P_{Y_2^n|X_2^n=c_2^n,U^n=u^n}(y_2^n)} > \mu\right\}\\
&= \sum_{u^n\in\mathcal{U}^n} P_{U^n}(u^n)\sum_{c_2^n\in\mathcal{X}_2^n} P_{X_2^n|U^n}(c_2^n|u^n)\sum_{c_1^n(1,2)\in\mathcal{X}_1^n}\cdots\sum_{c_1^n(1,|\mathcal{W}_1'|)\in\mathcal{X}_1^n} P_{X_1^n|U^n}(c_1^n(1,|\mathcal{W}_1'|)|u^n)\\
&\quad\cdot\sum_{c_1^n(1,1)\in\mathcal{X}^n}\sum_{y_2^n\in\mathcal{Y}_2^n} P_{X_1^nY_2^n|X_2^nU^n}(c_1^n(1,1),y_2^n|c_2^n,u^n)\\
&\quad\cdot\mathbf{1}\left\{\log\frac{P_{\bar{Y}_2^n|W_1=1,\bar{X}_2^n=c_2^n,\bar{U}^n=u^n}(y_2^n)}{P_{Y_2^n|X_2^n=c_2^n,U^n=u^n}(y_2^n)} > \mu\right\}.
\end{aligned}$$

direct resolvability theorem in [16], the above two probabilities approach zero if

$$|\mathcal{W}_1'| \geq 2^{n\bar{\mathbf{I}}(\mathbf{X}_1;\mathbf{Y}_2|\mathbf{X}_2,\mathbf{U})+n\gamma}$$

for arbitrary $\gamma > 0$, which implies that $R_1' \geq \bar{\mathbf{I}}(\mathbf{X}_1;\mathbf{Y}_2|\mathbf{X}_2,\mathbf{U})+\gamma$. Consequently, A_n tends to zero as $n \to 0$ which guarantees that the sufficient condition (34) for the vanishing variational distance holds.

By a similar method, we can show that $R_2' \geq \bar{\mathbf{I}}(\mathbf{X}_2;\mathbf{Y}_1|\mathbf{X}_1,\mathbf{U}) + \gamma$ to make the target variational distance vanish as $n \to \infty$. Combining the rate constraints for reliability and output distribution, we conclude that (4) and (5) can be achieved.

Appendix C
Proof of Proposition 1

In this section, we provide the proof that if $\lim_{n\to\infty} d(P_{W_iY_j^n}, P_{W_i}P_{Y_j^n}) = 0$, then $\lim_{n\to\infty} \frac{1}{n} D(P_{W_iY_j^n}\|P_{W_i}P_{Y_j^n}) = 0$.

Let P and Q be two distributions defined on the same measurable space $(\mathcal{A},\mathcal{F})$, with P absolutely continuous with respect to Q, i.e., $P << Q$. Let $\epsilon > 0$ be an arbitrary positive number. Define a set E,

$$E = \left\{a \in \mathcal{A} : \left|1 - (\frac{dP}{dQ}(a))^{-1}\right| > \frac{\epsilon}{1+\epsilon}\right\}.$$

According to the definition, we have

$$\begin{aligned}
d(P,Q) &= \int_{\mathcal{A}}\left|\frac{dP}{dQ}-1\right|dQ \geq \int_E\left|\frac{dP}{dQ}-1\right|dQ\\
&= \int_E\left|\frac{dP}{dQ}-1\right|dP(\frac{dP}{dQ})^{-1} = \int_E\left|1-(\frac{dP}{dQ})^{-1}\right|dP\\
&\geq \frac{\epsilon}{1+\epsilon}P(E) \geq \frac{\epsilon}{1+\epsilon}P(E^*)
\end{aligned} \tag{36}$$

where the last inequality follows from the definition

$$E^* = \left\{a \in \mathcal{A} : \log(\frac{dP}{dQ}(a)) > \epsilon\right\},$$

and the fact that $E^* \subseteq E$. Let (P_n, Q_n) represent the sequence of a pair of distributions for $n \in \mathbb{N}$. We therefore have the relation that for any $\epsilon > 0$, if $\lim_{n\to\infty} d(P_n, Q_n) = 0$, then $\lim_{n\to} P_n(E^*) = 0$. Note that in the original proof of Pinsker, the absolute continuity condition $P << Q$ was dropped. The idea is to split the sample space into two disjoint parts, in one of which $P << Q$, and otherwise in the other. The details of the proof are given in [19]. Overall, the relation (36) holds in a general sense regardless of the continuity of measures.

Let $\gamma > 0$ be an arbitrary positive number. Let us write the weak secrecy constraint as follows by dropping the subscripts in W_i and Y_j^n $(i \neq j)$:

$$
\begin{aligned}
&\frac{1}{n} I(W; Y^n) \\
&\quad = \mathbb{E}\left\{ \frac{1}{n} i_{WY^n}(W, Y^n) \mathbf{1}[i_{WY^n}(W, Y^n) \leq \epsilon] \right\} \\
&\qquad + \mathbb{E}\left\{ \frac{1}{n} i_{WY^n}(W, Y^n) \mathbf{1}[\epsilon < i_{WY^n}(W, Y^n) \leq n(R+\gamma)] \right\} \\
&\qquad + \mathbb{E}\left\{ \frac{1}{n} i_{WY^n}(W, Y^n) \mathbf{1}[i_{WY^n}(W, Y^n) \geq n(R+\gamma)] \right\} \\
&\quad \leq \frac{\epsilon}{n} + (R+\gamma) \mathbb{P}\left[i_{WY^n}(W, Y^n) > \epsilon \right] \\
&\qquad + \mathbb{E}\left\{ \frac{1}{n} i_{WY^n}(W, Y^n) \mathbf{1}[i_{WY^n}(W, Y^n) \geq n(R+\gamma)] \right\} \qquad (37)
\end{aligned}
$$

where $R = \frac{1}{n} \log |\mathcal{W}|$ for the message set $\mathcal{W}$. Because of (36), we know that when $d(P_{WY^n}, P_W P_{Y^n}) \to 0$ for sufficiently large n, then $\mathbb{P}\left[i_{WY^n}(W, Y^n) > \epsilon \right] \to 0$. Therefore, the second term of (37) tends to zero for sufficiently large n. The vanishing of the third term follows by exploiting the fact that $i_{WY^n}(w, y^n) \leq \log \frac{1}{P_W(w)} = nR$ for any $w \in \mathcal{W}$. The desired relation of convergence is proved.

APPENDIX D
PROOF OF THEOREM 1

In this section, we present a detailed proof of Theorem 1, which is based on the proof of Lemma 1. The key step is to modify the codebook generation method in the proof of Lemma 1 with the additional consideration of the additive cost constraint. The purpose is to construct the input process such that it satisfies additive cost constraint almost surely. Based on the modified codebook generation, we further show that there exists a sequence of codebooks $\{C_n\}$ such that the variational distance of the targeted distributions decays exponentially with respect to n. Henceforth, the information divergence can be bounded according to Lemma 2 as in Remark 2.

A. Modifications in the Codebook Generation

Let $\delta > 0$. Fix a distribution P_U on $\mathcal{U}$. Fix the conditional distributions $P_{X_i|U}$ on $\mathcal{X}_i \times \mathcal{U}$ such that $\mathbb{E}[c(X_i)] \leq P - \delta$ for $i = 1, 2$, respectively. Furthermore, fix the product distributions $P_{U^n}(u^n) = \prod_{i=1}^n P_U(u_i)$, $P_{X_1^n|U^n} = \prod_{i=1}^n P_{X_1|U}(x_{1,i}|u_i)$, and $P_{X_2^n|U^n} = \prod_{i=1}^n P_{X_2|U}(x_{2,i}|u_i)$. We construct new distributions such that the additive cost constraint can be satisfied with probability 1. Let us define the following sets:

$$
\mathcal{P}_{1,n} = \left\{ x^n \in \mathcal{X}_1^n : \frac{1}{n} \sum_{i=1}^n c(x_i) \leq P \right\},
$$

$$
\mathcal{P}_{2,n} = \left\{ x^n \in \mathcal{X}_2^n : \frac{1}{n} \sum_{i=1}^n c(x_i) \leq P \right\}.
$$

Due to the law of large numbers, it is clear that $\mathbb{P}[X_1^n \in \mathcal{P}_{1,n}] \to 1$ and $\mathbb{P}[X_2^n \in \mathcal{P}_{2,n}] \to 1$, as $n \to \infty$. By the Chernoff bound in Lemma 10, there exist $\alpha_1(\delta) > 0$ and $\alpha_2(\delta) > 0$, such that

$$
\begin{aligned}
\mathbb{P}[X_1^n \in \mathcal{P}_{1,n}] &\geq 1 - e^{-n\alpha_1(\delta)}, \\
\mathbb{P}[X_2^n \in \mathcal{P}_{2,n}] &\geq 1 - e^{-n\alpha_2(\delta)}.
\end{aligned}
$$

Note that we here assume that the moment generating functions for $c(X_1)$ and $c(X_2)$ exist. Define the following set:

$$
\begin{aligned}
\mathcal{G}_n := \Big\{ u^n \in \mathcal{U}^n : \mathbb{P}_{X_1^n|U^n=u^n}[x_1^n \notin \mathcal{P}_{1,n}|u^n] < e^{-n\frac{\alpha_1(\delta)}{2}} \\
\text{and } \mathbb{P}_{X_2^n|U^n=u^n}[x_2^n \notin \mathcal{P}_{2,n}|u^n] < e^{-n\frac{\alpha_2(\delta)}{2}} \Big\}.
\end{aligned}
$$

Then we have

$$
\begin{aligned}
\mathbb{P}[U^n \notin \mathcal{G}_n] &= P_{U^n}(\mathcal{G}_n^c) \\
&= P_{U^n}\Big(\Big\{ \mathbb{P}_{X_1^n|U^n}[x_1^n \notin \mathcal{P}_{1,n}|u^n] \geq e^{-n\frac{\alpha_1(\delta)}{2}} \Big\} \\
&\qquad \bigcup \Big\{ \mathbb{P}_{X_2^n|U^n}[x_2^n \notin \mathcal{P}_{2,n}|u^n] \geq e^{-n\frac{\alpha_2(\delta)}{2}} \Big\} \Big) \\
&\leq P_{U^n}\Big(\mathbb{P}_{X_1^n|U^n}[x_1^n \notin \mathcal{P}_{1,n}|u^n] \geq e^{-n\frac{\alpha_1(\delta)}{2}} \Big) \\
&\quad + P_{U^n}\Big(\mathbb{P}_{X_2^n|U^n}[x_2^n \notin \mathcal{P}_{2,n}|u^n] \geq e^{-n\frac{\alpha_2(\delta)}{2}} \Big) \\
&\leq e^{n\frac{\alpha_1(\delta)}{2}} \mathbb{E}_{U^n}\Big[\mathbb{P}_{X_1^n|U^n}[x_1^n \notin \mathcal{P}_{1,n}|u^n] \Big] \\
&\quad + e^{n\frac{\alpha_2(\delta)}{2}} \mathbb{E}_{U^n}\Big[\mathbb{P}_{X_2^n|U^n}[x_2^n \notin \mathcal{P}_{2,n}|u^n] \Big] \\
&= e^{n\frac{\alpha_1(\delta)}{2}} \mathbb{P}[X_1^n \notin \mathcal{P}_{1,n}] + e^{n\frac{\alpha_2(\delta)}{2}} \mathbb{P}[X_2^n \notin \mathcal{P}_{2,n}] \\
&\leq e^{-n\frac{\alpha_1(\delta)}{2}} + e^{-n\frac{\alpha_1(\delta)}{2}} \leq 2e^{-n\frac{\alpha(\delta)}{2}} := 1 - \varepsilon_n,
\end{aligned}
$$

where the second inequality follows from Markov's inequality as shown in Lemma 9, and $\alpha(\delta) = \min\{\alpha_1(\delta), \alpha_2(\delta)\}$. Therefore, we have $\varepsilon_n \to 1$ as $n \to \infty$.

Now let us define new random variables $\tilde{U}^n$, $\tilde{X}_i^n$ and $\tilde{Y}_i^n$ $(i = 1, 2)$ as follows. First, we construct $\tilde{U}^n$: choose $u^n \in \mathcal{U}^n$ according to the distribution

$$
P_{\tilde{U}^n}(u^n) = \begin{cases} \frac{1}{\mathbb{P}[U^n \in \mathcal{G}_n]} P_{U^n}(u^n) & \text{for } u^n \in \mathcal{G}_n \\ 0 & \text{for } u^n \notin \mathcal{G}_n. \end{cases}
$$

Then, we construct $\tilde{X}_i^n$ as follows, for $u^n \in \mathcal{G}_n$ such that

$$
P_{\tilde{X}_i^n|\tilde{U}^n}(x_i^n|u^n) = \begin{cases} \frac{1}{\mathbb{P}[X_i^n \in \mathcal{P}_{i,n}|u^n]} P_{X_i^n|U^n}(x_i^n|u^n), & \forall x_i^n \in \mathcal{P}_{i,n} \\ 0, & \forall x_i^n \notin \mathcal{P}_{i,n} \text{ and } x_i^n \in \mathcal{X}_i^n. \end{cases}
$$

Let us construct the input based on the process $\tilde{X}_i^n$. We have $\mathbb{P}\left[\frac{1}{n} \sum_{i=1}^n c(\tilde{X}_i) \leq P \right] = 1$. Furthermore, the following inequalities hold for all $(x_i^n, u^n) \in \mathcal{X}_i^n \times \mathcal{G}_n$:

$$
P_{\tilde{U}^n}(u^n) \leq \frac{P_U^n(u^n)}{\varepsilon_n} \qquad (38)
$$

$$
P_{\tilde{X}_i^n|\tilde{U}^n}(x_i^n|u^n) \leq \frac{P_{X_i^n|U^n}(x_i^n|u^n)}{\varepsilon_n}. \qquad (39)
$$

Consequently, the output distribution $P_{\tilde{Y}_i^n}$ is constructed according to the input. For all $(y_1^n, y_2^n, x_1^n, x_2^n, u^n) \in \mathcal{Y}_1^n \times \mathcal{Y}_2^n \times \mathcal{X}_1^n \times \mathcal{X}_2^n \times \mathcal{G}_n$, we have

$$
\begin{aligned}
&P_{\tilde{U}^n \tilde{X}_1^n \tilde{X}_2^n \tilde{Y}_1^n \tilde{Y}_2^n}(u^n, x_1^n, x_2^n, y_1^n, y_2^n) \\
&\quad = P_{\tilde{U}^n}(u^n) P_{\tilde{X}_1^n|\tilde{U}^n}(x_1^n|u^n) P_{\tilde{X}_2^n|\tilde{U}^n}(x_2^n|u^n) \Psi^n(y_1^n, y_2^n|x_1^n, x_2^n).
\end{aligned}
$$

TABLE I

NOTATION USED IN THE PROOF OF THEOREM 1

Notation	Meaning
X	the basis distribution
$\tilde{X}$	the newly constructed distribution based on X satisfying additive cost constraints almost surely
$\bar{X}$	the specific input induced by the chosen codebook based on $\tilde{X}$

Based on the newly constructed distributions, we repeat the steps in the proof of Lemma 1. The rates are specified as follows: for any $\gamma > 0$, $i \neq j$ and $i, j \in \{1, 2\}$,

$$R_i = I(X_i; Y_i|U) - I(X_i; Y_j|X_j, U) - 3\gamma,$$
$$R_i' = I(X_i; Y_j|X_j, U) + \gamma.$$

Before going further, let us summarize the notation that will be used to represent different distributions, using the variable X as an example in Table I.

B. Reliability

Following the standard method in the proof of Lemma 1 (the conditional version of Feinstein's Lemma), the achievable rate region $R_i + R_i' \leq \bar{\mathbf{I}}(\mathbf{X}_i; \mathbf{Y}_i|\mathbf{U}) - 2\gamma$ guarantees the reliability condition. Moreover, as shown in [30] the following relation exists: $\bar{\mathbf{I}}(\mathbf{X}_i; \mathbf{Y}_i|\mathbf{U}) \geq I(X_i; Y_i|U)$. Therefore, the choice of $R_i + R_i' = I(X_i; Y_i|U) - 2\gamma$ satisfies the reliability constraints.

C. Strong Secrecy

Strong secrecy is shown by the establishment of Claim 1 which suffices if the following lemma holds.

Lemma 12 (Exponentially Decay): For any $\gamma > 0$, $\exists N > 0$ and $\alpha > 0$ such that for all $n \geq N$

$$\mathbb{E}_{C_n}[d(P_{W_i\bar{Y}_j^n}, P_{W_i}P_{\bar{Y}_j^n})] \leq e^{-n\alpha}, \quad i \neq j$$

if $R_i' \geq I(X_i; Y_j|X_j, U) + \gamma$.

Based on the above lemma, we shall use the upper bound in Lemma 2 to show that for sufficiently large n, $\exists\beta > 0$, such that there exists at least a sequence of codebooks that satisfies the additive constraint and induces

$D(P_{W_i\bar{Y}_j^n}\|P_{W_i}P_{\bar{Y}_j^n}) \leq e^{-n\beta}$, if $R_i' \geq I(X_i; Y_j|X_j, U) + \gamma$ for $i, j \in \{1, 2\}$ and $i \neq j$. Strong secrecy constraints have been shown to hold. Combining the reliability and strong secrecy constraints, it is shown that the secrecy rate region in (12) is achieved.

Proof of Lemma 12: Let us consider the case $i = 1$ and $j = 2$. Let $\gamma > 0$, and recall that $|\mathcal{W}_1'| = 2^{nI(X_1;Y_2|X_2,U)+n\gamma}$. The proof follows a similar method given in [13]. Note that from (8), we have

$$\begin{aligned}
&\mathbb{E}_{C_n}\left[d(P_{W_1\bar{Y}_2^n}, P_{W_1}P_{\bar{Y}_2^n})\right] \\
&\quad\leq 2\mathbb{E}_{C^n}\left[d(P_{\bar{Y}_2^n|W_1\bar{X}_2^n\bar{U}^n}, P_{\tilde{Y}_2^n|\tilde{X}_2^n\tilde{U}^n})\right] \\
&\quad\leq 2\mathbb{E}_{C_n}\Big[d(P_{\bar{Y}_2^n|W_1\bar{X}_2^n\bar{U}^n}, P_{Y_2^n|X_2^nU^n}) \\
&\qquad\qquad + d(P_{Y_2^n|X_2^nU^n}, P_{\tilde{Y}_2^n|\tilde{X}_2^n\tilde{U}^n})\Big] \\
&\quad:= T_1 + T_2,
\end{aligned}$$

where $T_1 := 2\mathbb{E}_{C_n}\left[d(P_{\bar{Y}_2^n|W_1\bar{X}_2^n\bar{U}^n}, P_{Y_2^n|X_2^nU^n})\right]$, and $T_2 := 2\mathbb{E}_{C_n}\left[d(P_{Y_2^n|X_2^nU^n}, P_{\tilde{Y}_2^n|\tilde{X}_2^n\tilde{U}^n})\right]$.

For the first term T_1, by Lemma 8 we have, for every $\mu > 0$

$$\mathbb{E}_{C_n}\left[d(P_{\bar{Y}_2^n|W_1\bar{X}_2^n\bar{U}^n}, P_{Y_2^n|X_2^nU^n})\right] \leq \frac{2\mu}{\log e} + 2A_n$$

where

$$\begin{aligned}
A_n \leq \mathbb{P}&\Big[\frac{1}{|\mathcal{W}_1'|}\exp\left(i_{\tilde{X}_1^n\tilde{Y}_2^n|\tilde{X}_2^n\tilde{U}^n}(\tilde{X}_1^n, \tilde{Y}_2^n|\tilde{X}_2^n, \tilde{U}^n)\right) > \tau\Big] \\
&+\mathbb{P}\Big[\frac{1}{|\mathcal{W}_1'|}\sum_{i=2}^{|\mathcal{W}_1'|}\exp\left(i_{\tilde{X}_1^n\tilde{Y}_2^n|\tilde{X}_2^n\tilde{U}^n}(\tilde{X}_1^n(1,i), \tilde{Y}_2^n|\tilde{X}_2^n, \tilde{U}^n)\right) \\
&\qquad > 1 + \tau\Big],
\end{aligned}$$

for $\tau = \frac{2^{\mu}-1}{2}$. Recalling that $|\mathcal{W}_1'| = 2^{nI(X_1;Y_2|X_2,U)+n\gamma}$, the first term in A_n is bounded as follows: $\exists\alpha_\gamma > 0$, such that

$$\begin{aligned}
&\mathbb{P}\left[\frac{1}{|\mathcal{W}_1'|}\exp\left(i_{\tilde{X}_1^n\tilde{Y}_2^n|\tilde{X}_2^n\tilde{U}^n}(\tilde{X}_1^n, \tilde{Y}_2^n|\tilde{X}_2^n, \tilde{U}^n)\right) > \tau\right] \\
&\quad\leq \frac{1}{\varepsilon_n^3}\mathbb{P}\Big[\frac{1}{n}i_{X_1^nY_2^n|X_2^nU^n}(X_1^n, Y_2^n|X_2^n, U^n) \\
&\qquad\qquad > I(X_1; Y_2|X_2, U) + \left(\gamma + \frac{\log\tau}{n}\right)\Big] \\
&\quad\leq \frac{1}{\varepsilon_n^3}e^{-n\alpha_\gamma} \qquad (40)
\end{aligned}$$

where the first inequality follows from factoring the distribution as follows:

$$\begin{aligned}
&P_{\tilde{Y}_2^n\tilde{X}_1^n\tilde{X}_2^n\tilde{U}^n}(y_2^n, x_1^n, x_2^n, u^n) \\
&\qquad\leq P_{Y_2^n|X_1^nX_2^n}(y_2^n|x_1^n, x_2^n) \\
&\frac{P_{X_1^n|U^n}(x_1^n|u^n)}{\varepsilon_n}\frac{P_{X_2^n|U^n}(x_2^n|u^n)}{\varepsilon_n}\frac{P_{U^n}(u^n)}{\varepsilon_n} \\
&\qquad= \frac{1}{\varepsilon_n^3}P_{Y_2^nX_1^nX_2^nU^n}(y_2^n, x_1^n, x_2^n, u^n),
\end{aligned}$$

with the inequality following from the distributions' construction (38) and (39). Furthermore (40) follows from the Chernoff inequality based on the assumption that the moment generating function of $i_{X_1^nY_2^n|X_2^nU^n}$ $(x_1^n, y_2^n|x_2^n, u^n)$ exists.

For the second term in A_n, we need to note that $\tilde{X}_1^n(1, i)$ is independent of $\tilde{Y}_2^n$ given $\tilde{X}_2^n, \tilde{U}^n$. Specifically, the distribution can be factored as

$$\begin{aligned}
&P_{\tilde{U}^n}(u^n)P_{\tilde{X}_1^n|\tilde{U}^n}(x_1^n|u^n)P_{\tilde{X}_2^n|\tilde{U}^n}(x_2^n|u^n)P_{\tilde{Y}_2^n|\tilde{X}_2^n\tilde{U}^n}(y_2^n|x_2^n,u^n)\\
&\quad\le \frac{1}{\varepsilon_n^3}P_{U^n}(u^n)P_{X_1^n|U^n}(x_1^n|u^n)P_{X_2^n|U^n}(x_2^n|u^n)\\
&\qquad\cdot\sum_{x_1^n\in\mathcal{X}_1^n}P_{\tilde{Y}_2^n\tilde{X}_1^n|\tilde{X}_2^n\tilde{U}^n}(y_2^n,x_1^n|x_2^n,u^n)\\
&\quad= \frac{1}{\varepsilon_n^3}P_{U^n}(u^n)P_{X_1^n|U^n}(x_1^n|u^n)P_{X_2^n|U^n}(x_2^n|u^n)\\
&\qquad\cdot\sum_{x_1^n\in\mathcal{X}_1^n}P_{\tilde{Y}_2^n|\tilde{X}_1^n\tilde{X}_2^n}(y_2^n|x_1^n,x_2^n)P_{\tilde{X}_1^n|\tilde{U}^n}(x_1^n|u^n)\\
&\quad\le \frac{1}{\varepsilon_n^4}P_{U^n}(u^n)P_{X_1^n|U^n}(x_1^n|u^n)P_{X_2^n|U^n}(x_2^n|u^n)\\
&\qquad\cdot\sum_{x_1^n\in\mathcal{X}_1^n}\Psi^n(y_2^n|x_1^n,x_2^n)P_{X_1^n|U^n}(x_1^n|u^n)\\
&\quad= \frac{1}{\varepsilon_n^4}P_{U^n}(u^n)P_{X_1^n|U^n}(x_1^n|u^n)P_{X_2^n|U^n}(x_2^n|u^n)\\
&\qquad\cdot P_{Y_2^n|X_2^nU^n}(y_2^n|x_2^n,u^n)\\
&\quad:= \frac{1}{\varepsilon_n^4}\pi_{Y_2^nX_1^nX_2^nU^n}(y_2^n,x_1^n,x_2^n,u^n). \qquad (41)
\end{aligned}$$

Therefore, for the second term in A_n, we bound it in the following way:

$$\begin{aligned}
&\mathbb{P}\left[\frac{1}{|\mathcal{W}_1'|}\sum_{i=2}^{|\mathcal{W}_1'|}\exp\left(i_{\tilde{X}_1^n\tilde{Y}_2^n|\tilde{X}_2^n\tilde{U}^n}(\tilde{X}_1^n(1,i),\tilde{Y}_2^n|\tilde{X}_2^n,\tilde{U}^n)\right)>1+\tau\right]\\
&\le\frac{1}{\varepsilon_n^4}\sum_{\mathcal{Y}_2^n,\mathcal{X}_1^n,\mathcal{X}_2^n,\mathcal{U}^n}\pi_{Y_2^nX_1^nX_2^nU^n}(y_2^n,x_1^n,x_2^n,u^n)\\
&\quad\cdot\mathbf{1}\left\{\frac{1}{|\mathcal{W}_1'|}\sum_{i=2}^{|\mathcal{W}_1'|}\exp\left(i_{X_1^nY_2^n|X_2^nU^n}(x_1^n(1,i),y_2^n|x_2^n,u^n)\right)>1+\tau\right\} \qquad (42)\\
&\le\frac{1}{\varepsilon_n^4}\mathbb{P}\left[\frac{1}{n}i_{X_1^nY_2^n|X_2^nU^n}(x_1^n,y_2^n|x_2^n,u^n)\right.\\
&\qquad\qquad\left.>I(X_1;Y_2|X_2,U)+\gamma\right]\\
&\quad+\frac{1}{\tau^2\varepsilon_n^4}\mathbb{P}\left[\frac{1}{n}i_{X_1^nY_2^n|X_2^n,U^n}(x_1^n,y_2^n|x_2^n,u^n)\right.\\
&>\left.I(X_1;Y_2|X_2,U)+\frac{\gamma}{2}\right]+\frac{e^{-n\frac{\gamma}{2}}}{\tau^2\varepsilon_n^4} \qquad (43)\\
&\le\frac{1}{\varepsilon_n^4}e^{-n\alpha_\gamma}+\frac{1}{\tau^2\varepsilon_n^4}e^{-n\alpha_\gamma}+\frac{1}{\tau^2\varepsilon_n^4}e^{-n\frac{\gamma}{2}}. \qquad (44)
\end{aligned}$$

(42) comes from substituting (41) into the probability distribution. (43) follows from the proof given by Han and Verdú in the direct resolvability theorem [16], and (44) follows from the Chernoff inequality.

Based on (40) and (44), we can show that there exists $\alpha_n > 0$ such that when n is sufficiently large

$$T_1 = 2\mathbb{E}_{C_n}\left[d(P_{\bar{Y}_2^n|W_1\bar{X}_2^n\bar{U}^n},P_{Y_2^n|X_2^nU^n})\right]\le e^{-n\alpha_n}. \qquad (45)$$

To bound T_2, we have the following inequalities:

$$\begin{aligned}
&d(P_{Y_2^n|X_2^n=x_2^n,U^n=u^n},P_{\tilde{Y}_2^n|\tilde{X}_2^n=x_2^n,\tilde{U}^n=u^n})\\
&\quad\le d(P_{X_2^nX_1^nU^n|X_2^n=x_2^n,U^n=u^n},P_{\tilde{X}_2^n\tilde{X}_1^n\tilde{U}^n|\tilde{X}_2^n=x_2^n,\tilde{U}^n=u^n}) \qquad (46)\\
&\quad= d(P_{X_1^n|U^n=u^n},P_{\tilde{X}_1^n|\tilde{U}^n=u^n})\\
&\quad= \sup_{\mathcal{A}\subseteq\mathcal{X}_1^n}\sum_{\mathcal{B}\in\{\mathcal{A},\mathcal{A}^c\}}\left|\mathbb{P}_{X_1^n|U^n=u^n}[\mathcal{B}]-\mathbb{P}_{\tilde{X}_1^n|\tilde{U}^n=u^n}[\mathcal{B}]\right|\\
&\quad= \sup_{\mathcal{A}\subseteq\mathcal{X}_1^n}\sum_{\mathcal{B}\in\{\mathcal{A},\mathcal{A}^c\}}\Big|\mathbb{P}_{X_1^n|U^n=u^n}[\mathcal{B}\cap\mathcal{P}_{1,n}]\\
&\qquad+\mathbb{P}_{X_1^n|U^n=u^n}[\mathcal{B}\cap\mathcal{P}_{1,n}^c]-\mathbb{P}_{\tilde{X}_1^n|\tilde{U}^n=u^n}[\mathcal{B}\cap\mathcal{P}_{1,n}]\Big|\\
&\quad\le \sup_{\mathcal{A}\subseteq\mathcal{X}_1^n}\sum_{\mathcal{B}\in\{\mathcal{A},\mathcal{A}^c\}}\Bigg(\mathbb{P}_{X_1^n|U^n=u^n}[\mathcal{B}\cap\mathcal{P}_{1,n}]\left(\frac{1}{\varepsilon_n}-1\right)\\
&\qquad+\mathbb{P}_{X_1^n|U^n=u^n}[\mathcal{B}\cap\mathcal{P}_{1,n}^c]\Bigg) \qquad (47)\\
&\quad\le\left(\frac{1}{\varepsilon_n}-1\right)+(1-\varepsilon_n)\le e^{-n\beta_n}, \qquad (48)
\end{aligned}$$

for some $\beta_n > 0$. (46) follows by the data processing inequality in Lemma 7, and (47) follows by the distribution construction (39).

Combining the bounds on T_1 and T_2, i.e., (45) and (48), we conclude that $\exists\alpha > 0$ such that for sufficiently large n, $\mathbb{E}_{C_n}[d(P_{W_1}P_{\bar{Y}_2^n},P_{W_1\bar{Y}_2^n})]\le e^{-n\alpha}$, if $R_1'\ge I(X_1;Y_2|X_2,U)+\gamma$. ■

Appendix E
Proof of Lemma 4

In this section, we present the proof of the properties for the partition $\underline{\mathcal{T}_n}$ and $\overline{\mathcal{T}_n}$ as shown in Lemma 4.

1) For $y\in\overline{\mathcal{T}^i}$, where

$$\overline{\mathcal{T}^i}=\left\{y:y\in(-\infty,-T^i-\sqrt{2n}]\cup[T^i+\sqrt{2n},\infty)\right\},$$

$\forall x_1^n\in C_n, x_2^n\in C_n$, we have

$$|y-x_{1,i}-\rho_1x_{2,i}|\ge\sqrt{2n},$$

because $|x_{1,i}+\rho_1\ x_{2,i}|\le T^i$. For $Z\sim N(0,1)$, by the tail bound on the Gaussian distribution, we have

$$\begin{aligned}
&P_Z\left(\left\{y-x_{1,i}-\rho_1\ x_{2,i}:y\in\overline{\mathcal{T}^i}\right\}\right)\\
&\qquad=P_Z((-\infty,-\sqrt{2n}]\cup[\sqrt{2n},\infty))\le\sqrt{\frac{2}{\pi}}\frac{e^{-n}}{n}\le e^{-n}.
\end{aligned}$$

2) Let $f_Z(y)=\min_{i\in[1:n]}p_Z(y-x_{1,i}-\rho_1\ x_{2,i})$ for any $y\in\mathcal{T}^i$. Then we have,

$$\begin{aligned}
&P_{\bar{Y}_1^n}(\mathcal{T}_n)\\
&\quad=\int_{\mathcal{T}_n}\frac{1}{|\mathcal{W}|}\sum_{(w_1,w_2,w_1',w_2')\in\mathcal{W}}\prod_{i=1}^n p_Z(y_i-x_{1,i}-\rho_1\ x_{2,i})dy^n\\
&\quad=\frac{1}{|\mathcal{W}|}\sum_{(w_1,w_2,w_1',w_2')\in\mathcal{W}}\int_{\mathcal{T}_n}\prod_{i=1}^n p_Z(y_i-x_{1,i}-\rho_1\ x_{2,i})dy^n
\end{aligned}$$

$$
\begin{aligned}
&\geq \frac{1}{|\mathcal{W}|} \sum_{(w_1,w_2,w_1',w_2')\in\mathcal{W}} \int_{\mathcal{T}_n} \prod_{i=1}^{n} f_Z(y_i)dy^n \\
&= \prod_{i=1}^{n} \int_{\mathcal{T}^i} f_Z(y_i)dy_i \\
&\geq \left(1 - \max_{i\in[1:n]} P_Z\left(\left\{y - x_{1,i} - \rho_1\ x_{2,i} : y \in \overline{\mathcal{T}^i}\right\}\right)\right)^n \\
&\geq (1-\epsilon_n)^n.
\end{aligned}
$$

The last inequality holds due to *1)*. A similar argument holds for $P_{\bar{Y}_1^n|W_2=w_2}(\mathcal{T}_n)$.

3) From *2)*, it is clear that $P_{\bar{Y}_1^n}(\overline{\mathcal{T}_n}) \leq 1-(1-\epsilon_n)^n$. The second inequality, known as *Bernoulli's inequality*, can be proved by induction.

4) This follows by the definition of $\mathcal{T}_n$. For $y_i \in \mathcal{T}^i$,

$$|y - x_{1,i} - \rho_1 x_{2,i}| \leq 2T^i + \sqrt{2n} = (2\sqrt{P}+\sqrt{2})n^{\frac{1}{2}}.$$

Substituting this bound into $p_{\bar{Y}_1^n}(y^n)$ and $p_{\bar{Y}_1^n|W_2=w_2}(y^n)$ for $y^n \in \mathcal{T}_n$, we obtain the desired result:

$$
\begin{aligned}
p_{\bar{Y}_1^n}(y^n) &\geq \left(\frac{1}{\sqrt{2\pi}}\right)^n e^{-tn^2}, \\
p_{\bar{Y}_1^n|W_2=w_2}(y^n) &\geq \left(\frac{1}{\sqrt{2\pi}}\right)^n e^{-tn^2},
\end{aligned}
$$

where $t = (2\sqrt{P}+\sqrt{2})^2$.

5) For any $y^n \in \overline{\mathcal{T}_n}$, there exists at least one i such that $y_i \in \bar{\mathcal{T}}^i$, so that following the definition for any x_1^n and $x_2^n \in C_n$,

$$|y_i - x_{1,i} - \rho_1 x_{2,i}| \geq \sqrt{2n},$$

because $|x_{1,i} + \rho_1\ x_{2,i}| \leq T^i$. Therefore, the density function $p_Z(y_i - x_{1,i} - \rho_1\ x_{2,i}) \leq \frac{1}{\sqrt{2\pi}} \exp(-n), \forall y_i \in \bar{\mathcal{T}}^i$. Substituting this inequality to $p_{\bar{Y}_1^n}(y^n)$, we have the claim directly

$$
\begin{aligned}
p_{\bar{Y}_1^n}(y^n) &\leq \left(\frac{1}{\sqrt{2\pi}}\right)^n e^{-n} \\
p_{\bar{Y}_1^n|W_2=w_2}(y^n) &\leq \left(\frac{1}{\sqrt{2\pi}}\right)^n e^{-n}.
\end{aligned}
$$

ACKNOWLEDGMENT

The authors would like to thank Dr. Qiwen Wang of the Swedish Royal Institute of Technology (KTH) for discussions on the reverse Pinsker's inequality.

REFERENCES

[1] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[3] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[4] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

[5] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communications over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[6] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[7] Y. Oohama, "Coding for relay channels with confidential messages," in *Proc. IEEE Inf. Theory Workshop*, Cairns, QLD, Australia, Sep. 2001, pp. 87–89.

[8] U. M. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Proc. 19th Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*. Bruges, Belgium, May 2000, pp. 351–368.

[9] I. Csiszár, "Almost independence and secrecy capacity," *Problems Inf. Transmiss.*, vol. 32, no. 1, pp. 40–47, 1996.

[10] M. Hayashi, "General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1562–1575, Apr. 2006.

[11] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

[12] H. Boche and R. F. Schaefer, "Wiretap channels with side information—Strong secrecy capacity and optimal transceiver design," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 8, pp. 1397–1408, Aug. 2013.

[13] M. R. Bloch and J. N. Laneman, "Strong secrecy from channel resolvability," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 8077–8098, Dec. 2013.

[14] J. Hou and G. Kramer, "Informational divergence approximations to product distributions," in *Proc. 13th Can. Workshop Inf. Theory*, Jun. 2013, pp. 76–81.

[15] J. Hou and G. Kramer, "Effective secrecy: Reliability, confusion and steal," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2014, pp. 1–5.

[16] T. S. Han and S. Verdú, "Approximation theory of output statistics," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 752–770, May 1993.

[17] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proc. Nat. Acad. Sci. USA*, vol. 114, no. 1, pp. 19–26, Jan. 2017.

[18] A. D. Wyner, "The common information of two dependent random variables," *IEEE Trans. Inf. Theory*, vol. 21, no. 2, pp. 163–179, Mar. 1975.

[19] M. S. Pinsker, *Information and Information Stability of Random Variables and Processes*. Izv. Akad. Nauk, 1960,

[20] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[21] R. D. Yates, D. Tse, and Z. Li, "Secret communication on interference channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, ON, Canada, Jul. 2008, pp. 374–378.

[22] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai (Shitz), and S. Verdú, "Capacity of cognitive interference channels with and witwith secrecy," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 604–619, Feb. 2009.

[23] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3323–3332, Jun. 2011.

[24] R. Bassily and S. Ulukus, "Ergodic secret alignment," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1594–1611, Mar. 2012.

[25] J. Xie and S. Ulukus, "Secure degrees of freedom of K-user Gaussian interference channels: A unified view," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2647–2661, May 2015.

[26] X. Li and R. Matsumoto, "Secure multiplex coding over interference channel with confidential messages," in *Proc. Int. Zurich Seminar Commun.*, Mar. 2012, pp. 75–78.

[27] M. Hayashi and R. Matsumoto, "Secure multiplex coding with dependent and non-uniform multiple messages," in *Proc. 50th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2012, pp. 954–959.

[28] X. He and A. Yener, "Interference channels with strong secrecy," in *Proc. 47th Annu. Allerton Conf. Commun., Control, Comput.*, Sep./Oct. 2009, pp. 811–818.

[29] X. He and A. Yener, "Providing secrecy with lattice codes," in *Proc. 46th Annu. Allerton Conf. Commun., Control, Comput.*, Sep. 2008, pp. 1199–1206.

[30] T. S. Han *et al.*, *Information-Spectrum Methods in Information Theory*, vol. 50. Springer, 2013.

[31] S.-W. Ho and R. W. Yeung, "The interplay between entropy and variational distance," *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 5906–5929, Dec. 2010.

[32] V. V. Prelov, "On inequalities between mutual information and variation," *Problems Inf. Transmiss.*, vol. 43, no. 1, pp. 12–23, 2007.

[33] I. Sason, “Entropy bounds for discrete random variables via maximal coupling,” *IEEE Trans. Inf. Theory*, vol. 59, no. 11, pp. 7118–7131, Nov. 2013.

[34] S. Verdú, “Total variation distance and the distribution of relative information,” in *Proc. Inf. Theory Appl. Workshop (ITA)*, San-Diego, CA, USA, Feb. 2014, pp. 1–3.

[35] I. Sason. (2015). “On reverse Pinsker inequalities.” [Online]. Available: https://arxiv.org/abs/1503.07118

[36] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[37] A. Feinstein, “A new basic theorem of information theory,” *Trans. IRE Prof. Group Inf. Theory*, vol. 4, no. 4, pp. 2–22, Sep. 1954.

Zhao Wang received the Bachelor and Master degrees in Engineering from the University of Electronic Science and Technology of China (UESTC), Chengdu, in 2007 and 2010, respectively. He received the Ph.D degree in Telecommunications from the Royal Institute of Technology (KTH), Sweden, in 2015. He is currently affiliated with Ericsson research at Stockholm.

Rafael F. Schaefer (S’08–M’12–SM’17) received the Dipl.-Ing. degree in electrical engineering and computer science from the Technische Universität Berlin, Germany, in 2007, and the Dr.-Ing. degree in electrical engineering from the Technische Universität München, Germany, in 2012. From 2007 to 2010, he was a Research and Teaching Assistant with the Technische Universität Berlin and from 2010 to 2013, with the Technische Universität München. From 2013 to 2015, he was a Post-Doctoral Research Fellow with Princeton University. Since 2015, he has been an Assistant Professor with the Technische Universität Berlin. Among his publications is the recent book *Information Theoretic Security and Privacy of Information Systems* (Cambridge University Press, 2017). He was a recipient of the VDE Johann-Philipp-Reis Prize in 2013. He received the best paper award of the German Information Technology Society (ITG-Preis) in 2016. He was one of the exemplary reviewers of the IEEE COMMUNICATION LETTERS in 2013. He is currently an Associate Editor of the IEEE TRANSACTIONS OF COMMUNICATIONS and an Associate Member of the IEEE Information Forensics and Security Technical Committee.

Mikael Skoglund (S’93–M’97–SM’04) received the Ph.D. degree in 1997 from Chalmers University of Technology, Sweden. In 1997, he joined the Royal Institute of Technology (KTH), Stockholm, Sweden, where he was appointed to the Chair in Communication Theory in 2003. At KTH, he heads the Department of Information Science and Engineering.

Dr. Skoglund has worked on problems in source-channel coding, coding and transmission for wireless communications, Shannon theory, information and control, and statistical signal processing. He has authored and co-authored more than 140 journal and some 340 conference papers.

Dr. Skoglund has served on numerous technical program committees for IEEE sponsored conferences. During 2003–08 he was an associate editor with the IEEE TRANSACTIONS ON COMMUNICATIONS and during 2008–12 he was on the editorial board for the IEEE TRANSACTIONS ON INFORMATION THEORY. He is general co-chair for the upcoming IEEE ITW 2019.

Ming Xiao (S’02–M’07–SM’12) received Bachelor and Master degrees in Engineering from the University of Electronic Science and Technology of China, ChengDu in 1997 and 2002, respectively. He received Ph.D degree from Chalmers University of Technology, Sweden, in November 2007. From 1997 to 1999, he worked as a network and software engineer at ChinaTelecom. From 2000 to 2002, he also held a position in the SiChuan Communications Administration. From November 2007 to now, he has been with the Department of Information Science and Engineering, School of Electrical Engineering and Computer Science, Royal Institute of Technology, Sweden, where he is currently an Associate Professor. Since 2012, he has been an Associate Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE COMMUNICATIONS LETTERS (Senior Editor Since Jan. 2015) and IEEE WIRELESS COMMUNICATIONS LETTERS (2012-2016). He was the lead Guest Editor for the IEEE JSAC Special issue on “Millimeter Wave Communications for Future Mobile Networks” in 2017.

H. Vincent Poor (S’72–M’77–SM’82–F’87) received the Ph.D. degree in electrical engineering and computer science from Princeton University in 1977. From 1977 until 1990, he was on the faculty of the University of Illinois at Urbana-Champaign. Since 1990 he has been on the faculty at Princeton’s, where he is the Michael Henry Strater University Professor of Electrical Engineering. During 2006 to 2016, he served as Dean of Princeton’s School of Engineering and Applied Science. He has also held visiting appointments at several other institutions, most recently at Berkeley and Cambridge. His research interests are in the areas of information theory and signal processing, and their applications in wireless networks, energy systems and related fields. Among his publications in these areas is the recent book *Information Theoretic Security and Privacy of Information Systems* (Cambridge University Press, 2017).

Dr. Poor is a member of the National Academy of Engineering and the National Academy of Sciences, and is a foreign member of the Chinese Academy of Sciences, the Royal Society, and other national and international academies. In 1990, he served as President of the IEEE Information Theory Society, in 2004-07 as the Editor-in-Chief of these TRANSACTIONS, and in 2009 as General Co-chair of the IEEE International Symposium on Information Theory, held in Seoul, South Korea. Recent recognition of his work includes the 2017 IEEE Alexander Graham Bell Medal, Honorary Professorships from Peking University and Tsinghua University, both conferred in 2017, and a D.Sc. *honoris causa* from Syracuse University awarded in 2017.