Secure Semantic Communication over Wiretap Channel

Denis Kozlov, Mahtab Mirmohseni and Rahim Tafazolli
5/6GIC, Institute for Communication Systems (ICS), University of Surrey, Guildford, United Kingdom

***Abstract*—Semantic communication is an emerging feature for future networks like 6G, which emphasizes the meaning of the message in contrast to the traditional approach where the meaning of the message is irrelevant. Yet, the open nature of a wireless channel poses security risks for semantic communications. In this paper, we derive information-theoretic limits for the secure transmission of semantic source over wiretap channel. Under separate equivocation and distortion conditions for semantics and observed data, we present the general outer and inner bounds on the rate-distortion-equivocation region. We also reduce the general region to a case of Gaussian source and channel and provide numerical evaluations.**

***Index Terms*—Semantic Communications, Wiretap Channel, Rate-Distortion-Equivocation Region.**

I. Introduction

Semantic communications represents a promising approach for the next generation of wireless networks, particularly within the realm of 6G technology. In this paradigm, the semantic content of messages is given significant consideration, marking a departure from traditional communication methods [1]–[3].

Despite its potential, wireless semantic communication still faces substantial security challenges due to the inherent openness of communication channels, leaving them susceptible to eavesdropping. In addition, semantics can carry more sensitive information. Thus, the security requirement could be different for the semantics compared with the observed source. This makes the problem challenging and novel, requiring attention and exploration by researchers [3], [4].

In this work, we derive the information-theoretic limits governing the secrecy of semantic communication. To achieve this, we model a source as the intrinsic (semantic) part and extrinsic (observed) part, building upon previous work that introduced this source model [5], [6]. To illustrate this model with a concrete example, a semantic part may be represented by a textual description of an image, coupled with an observed part generated by a neural network in response to the text prompt.

Our research centers on a wiretap channel scenario, wherein we consider a passive eavesdropper as the adversary. Within the model of wiretap channel and general semantic source (which is modeled as two correlated random variables (r.v.s) with joint distribution), we analyze the trade-off between equivocation and distortion for the semantic and observed components separately, particularly in the context of joint source-channel coding (JSCC). Specifically, we derive inner and outer bounds for rate, equivocations, and distortions pairs.

This research was supported by the 5/6GIC, Institute for Communication Systems (ICS), University of Surrey.

Related works. Wyner's work in 1975 laid the groundwork for secure communication over wiretap channels [7], while subsequent advancements generalized this model to broadcast channels with common and confidential messages [8]. In [9], the wiretap model is extended to incorporate JSCC and the one-time pad technique, bringing an important result that a separation principle holds: first a rate-distortion achieving code can be applied, then one-time pad can be applied for a given key-rate, and it is finished by using a wiretap code. Further extensions to the JSCC model, including scenarios with side information at the decoders, have been explored in [10], [11]. The lossy compression aspect of semantic sources was covered in [5].

Challenges of secure semantic communications from a machine learning (ML) perspective were covered in [12], [13]. Authors of [14] proposed a way for encrypting semantic data in a deep learning JSCC scenario. Also, encryption and obfuscation algorithm for semantic communication was presented in [15].

To the best of our knowledge, there is no work on secure JSCC of semantic sources over wiretap channel with passive eavesdroppers under separate equivocation and distortion conditions for semantics and observed source.

II. Problem statement

Consider a model shown in Fig. 1, where a transmitter wishes to send the semantic and observed data to a receiver (Bob), subject to some distortion constraints while keeping them hidden from an eavesdropper (Eve) with some equivocation constraints. Thus, the source consists of intrinsic (semantics) state and extrinsic observation which are modeled as a sequence of i.i.d. r.v.s S^k and U^k, respectively. They are correlated through joint distribution $p_{S,U}(s,u)$ defined on product alphabet $\mathcal{S} \times \mathcal{U}$.

Main (Bob's) and wiretap (Eve's) channels are modeled as a discrete memoryless channel (DMC) with input X on $\mathcal{X}$ and outputs Y on $\mathcal{Y}$ and Z on $\mathcal{Z}$ given transition probability $p_{Y,Z|X}$. In this work, we consider a degraded channel model: $p_{Y,Z|X} = p_{Y|X} p_{Z|X}$.

There are two cases for encoder input. In the first case, the encoder has access to both semantics s^k and observation u^k, while in the second case, the encoder is only given u^k and has no access to a semantic sample s^k.

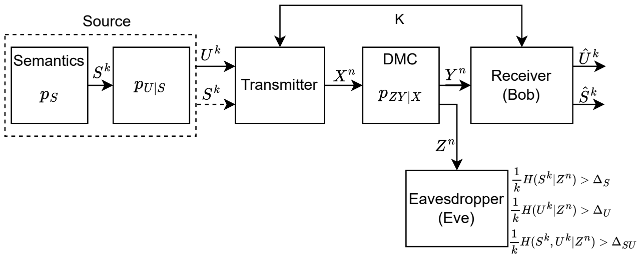

Fig. 1. System Model

The case 1 encoder $f_1 : S^k \times U^k \times K \to X^n$ maps the semantic and observed sequence and a key to a channel input sequence X^n. The case 2 encoder $f_2 : U^k \times K \to X^n$, acts only on the observed sequence and key.

The transmitter and receiver have access to a shared key which is modeled as random variable K with alphabet $\mathcal{K}$. This key is used to secure part of the data with a one-time pad technique.

We define decoding function as $\hat{f} : Y^n \times K \to (\hat{S}^k, \hat{U}^k)$ which maps Bob's received signal Y^n and the shared key to estimated semantic and observed sources $\hat{S}^k$ and $\hat{U}^k$ defined on alphabets $\hat{\mathcal{S}}, \hat{\mathcal{U}}$.

From the decoder function definition we have:

$$H(\hat{S}^k, \hat{U}^k | Y^n, K) = 0. \tag{1}$$

Additionally, we set distortion measure for semantics $d_S : \mathcal{S} \times \hat{\mathcal{S}} \to \mathbb{R}^+$ and for observation $d_U : \mathcal{U} \times \hat{\mathcal{U}} \to \mathbb{R}^+$. We follow the same naming for the block average distortion: $d_S(s^k, \hat{s}^k) = \frac{1}{k}\sum_{i=1}^k d_S(s_i, \hat{s}_i)$ and $d_U(u^k, \hat{u}^k) = \frac{1}{k}\sum_{i=1}^k d_U(u_i, \hat{u}_i)$.

The goal of this work is to characterize the following region:

$$\mathcal{R} \doteq \{(R, R_k, D_S, D_U, \Delta_S, \Delta_U, \Delta_{SU}) \text{ is achievable}\},$$

where a tuple $(R, R_k, D_S, D_U, \Delta_S, \Delta_U, \Delta_{SU})$ is achievable if there exist source-channel (k, n)-code $(f_1, \hat{f})$ (or $(f_2, \hat{f})$ for the second encoder input type) s.t.:

$$n/k \leq R + \epsilon, \tag{2}$$

$$\frac{1}{k}\log|\mathcal{K}| \leq R_k + \epsilon, \tag{3}$$

$$\mathbb{E}\, d_S(S^k, \hat{S}^k) \leq D_S + \epsilon, \tag{4}$$

$$\mathbb{E}\, d_U(U^k, \hat{U}^k) \leq D_U + \epsilon, \tag{5}$$

$$\frac{1}{k}H(S^k|Z^n) \geq \Delta_S - \epsilon, \tag{6}$$

$$\frac{1}{k}H(U^k|Z^n) \geq \Delta_U - \epsilon, \tag{7}$$

$$\frac{1}{k}H(S^k, U^k|Z^n) \geq \Delta_{SU} - \epsilon, \tag{8}$$

are satisfied for any $\epsilon > 0$. Condition (2) restricts channel expansion ratio (inverse of rate), that is channel uses per source symbol. Equation (3) restricts the rate of the key which is used to protect data with the one-time pad technique. Average distortion for semantics and observation is restricted by conditions (4) and (5). Equivocation for semantics and observation as well as joint one, restricted by conditions (6), (7) and (8), respectively.

III. Preliminaries

In this section, we provide some useful lemmas.

Lemma 1 ([16, Theorem 3.5]): The rate-distortion function for discrete memoryless source (DMS) U has the following form:

$$R_U(D_U) = \inf_{\substack{p_{\hat{U}|U} \\ \mathbb{E}\, d_U(U,\hat{U}) \leq D_U}} I(U; \hat{U}).$$

To meet distortion conditions optimally in terms of rate for both semantics and observation, we can employ the multiple-description rate-distortion function.

Definition 1: The multiple-description rate-distortion function:

$$R(D_S, D_U) \doteq \inf\{R : (R, D_S, D_U) \text{ is achievable}\},$$

where tuple (R, D_S, D_U) is considered to be achievable if there exists a code such that (2), (4) and (5) are satisfied for any $\epsilon > 0$.

Lemma 2 ([17, Theorem 2]):

$$R(D_S, D_U) = \inf_{\substack{p_{\hat{S},\hat{U}|S,U} \\ \mathbb{E}\, d_U(U,\hat{U}) \leq D_U \\ \mathbb{E}\, d_S(S,\hat{S}) \leq D_S}} I(S, U; \hat{S}, \hat{U}),$$

Lemma 3 ([5, Theorem 1]): The case 2 of the encoder input rate-distortion function can be rewritten as follows:

$$R(D_S, D_U) = \inf_{\substack{p_{\hat{S},\hat{U}|U} \\ \mathbb{E}\, d_U(U,\hat{U}) \leq D_U \\ \mathbb{E}\, \hat{d}_S(U,\hat{S}) \leq D_S}} I(U; \hat{S}, \hat{U}),$$

where $\hat{d}_S(U, \hat{S}) = \sum_{s \in S} p_{S|U}(s|U) d_S(s, \hat{S})$ is a modified distortion metric.

IV. Main Result

In this section, we present the general outer and inner bound for a system model defined in Section II.

Theorem 1: (Converse). For both cases of encoder input, any achievable tuple $(R, R_k, D_S, D_U, \Delta_S, \Delta_U, \Delta_{SU})$ must satisfy:

$$\begin{cases} R_U(D_U) \leq RI(X;Y), & (9) \\ R_S(D_S) \leq RI(X;Y), & (10) \\ R(D_S, D_U) \leq RI(X;Y), & (11) \\ \Delta_U \leq R_k + R[I(X;Y) - I(X;Z)] & \\ \quad -R_U(D_U) + H(U), & (12) \\ \Delta_S \leq R_k + R[I(X;Y) - I(X;Z)] & \\ \quad -R_S(D_S) + H(S), & (13) \\ \Delta_{SU} \leq R_k + R[I(X;Y) - I(X;Z)] & \\ \quad -R(D_S, D_U) + H(S, U). & (14) \end{cases}$$

The proof of Theorem 1 is provided in the Appendix.

One can see that the equivocation in the converse region consists of three basic terms. The first one, R_k, shows how much equivocation we achieve using the one-time pad technique with a key rate R_k. The second one is the secrecy capacity ($R[I(X;Y) - I(X;Z)]$). And the last one (i.e. $H(U) - R_U(D_U)$), describes the part of equivocation due to loss in source encoding.

Theorem 2: (Inner bound). When the transmitter has access to both semantics and observation (case 1 of encoder input), a tuple $(R, D_S, D_U, \Delta_S, \Delta_U, \Delta_{SU})$ is achievable if there exist auxiliary r.v.s $A_c, A_p, B_c, B_p, Q_c, Q_p, W_c, X$ with joint distribution $p(a_c, a_p, b_c, b_p, q_c, q_p, w_c, x)$ and functions $\tilde{S} : A_c^k \times A_p^k \to \hat{S}^k$ and $\tilde{U} : A_c^k \times A_p^k \times B_c^k \times B_p^k \to \hat{U}^k$ such that the following inequalities hold:

$$\begin{cases} I(S;A_c) < RI(Q_c;Y), \\ I(S;A_c,A_p) < RI(Y;Q_c,Q_p), \\ I(U;B_c|S,A_c) < RI(W_c;Y|Q_c), \\ I(U;B_c|S,A_c) + I(U;B_p|S,A_c,A_p,B_c) < \\ \qquad < R[I(W_c;Y|Q_c) + I(X;Y|Q_c,Q_p,W_c)] \\ D_S \geq \mathbb{E}\, d_S(S,\tilde{S}(A_c,A_p)), \\ D_U \geq \mathbb{E}\, d_U(U,\tilde{U}(A_c,A_p,B_c,B_p)), \\ \Delta_S \leq H(S|Ac,Ap) + R(H(Z|X) - H(Z|Qc)) \\ \qquad +RI(Qp;Y|Qc), \\ \Delta_U \leq H(U) - I(A_c,A_p;S) - I(B_c;U|A_c) \\ \qquad -I(B_p;U|S,A_c,A_p,B_c) + RH(Z|X) \\ \qquad -RH(Z|Q_c,W_c) + RI(Q_p;Y|Q_c) \\ \qquad +RI(X;Y|Q_c,Q_p,W_c), \\ \Delta_{SU} \leq H(S,U) - I(S;A_c,A_p) - I(U;B_p|S,A_c,A_p,B_c) \\ \qquad -I(U;B_c|S,A_c) + R(H(Z|X) - H(Z|Qc,Wc)) \\ \qquad +RI(Q_p;Y|Q_c) + RI(X;Y|Q_c,Q_p,W_c). \end{cases}$$

Achievability proof outline. Consider a codebook with source, channel, and wiretap codes. Wiretap code is embedded in the channel encoder and introduces additional random noise to cover private parts of the data from the eavesdropper. We introduce source encoder auxiliary r.v.s A_c, A_p, B_c, B_p, and channel encoder auxiliary r.v.s Q_c, Q_p, W_c for codebook generation. The r.v.s A_c and A_p reflect the distribution of i.i.d. codewords (denoted by a_c^k and a_p^k) for the common and private parts of semantics, while B_c and B_p are used for the common and private parts of the observation, for codewords denoted as b_c^k and b_p^k, correspondingly.

Then we use a technique similar to superposition coding: for each sequence a_c^k we generate a_p^k and b_c^k, then for each a_c^k, a_p^k, b_c^k we generate b_p^k. All of these sequences are selected from typical sets.

The channel encoder codebook has a layered structure related to the source encoder. That is, we generate sequence q_c^n from Q_c distribution, for each q_c^n we generate q_p^n and w_c^n using Q_p and W_c, given q_c^n, q_p^n, w_c^n we generate x^n according to X. Sequences q_p^n and x^n additionally covered with noise.

To encode data, we choose source encoder sequences that are jointly typical with encoder input. Then using the mapping, we obtain the channel code sequences and transmit x^n. The decoding is based on the joint typically with channel output y^n.

For this codebook and encoding/decoding procedure, we show that the probability of encoding/decoding errors goes to zero under some rate conditions with $k \to \infty$.

Finally, we bound the average distortion and equivocations. For the complete proof of achievability see Appendix.

V. Gaussian Case

In this section, we consider the Gaussian source and channel with quadratic distortion measure.

A. System model.

Let source be distributed according to normal distribution $(S,U) \sim \mathcal{N}(0,K)$ with covariance matrix,

$$K = \begin{pmatrix} P_S & \sigma_{SU} \\ \sigma_{SU} & P_U \end{pmatrix}.$$

We set distortion measure $d_s(x,y) = d_u(x,y) = (x-y)^2$, and we model the channel as,

$$\begin{aligned} &\mathbb{E}(X^2) \leq P, \\ &Y = X + N_1, \quad N_1, \sim \mathcal{N}(0,P_{N_1}), \\ &Z = Y + N_2, \quad N_2, \sim \mathcal{N}(0,P_{N_2}), \end{aligned}$$

where P is the power constraint for channel input, P_{N_1} is the noise power for the main channel, and P_{N_2} is the noise power for the eavesdropper channel, we define $P_N = P_{N_1} + P_{N_2}$.

B. Rate-equivocation-distortion region

For the Gaussian system model, we derive the following outer bound from Theorem 1.

Proposition 1: (Converse). In the case when the encoder has access only to observation u^k (case 2 of encoder input), for the Gaussian source and channel, to fulfill conditions (2)-(8) any code must satisfy:

$$\begin{cases} D_S \geq \eta, \\ D_U \geq P_U \left(\frac{P_{N_1}}{P+P_{N_1}}\right)^R, \\ D_S \geq P_S \left(\frac{P_{N_1}}{P+P_{N_1}}\right)^R, \\ \max\left[\frac{P_U}{D_U}, \frac{\sigma_{SU}^2}{P_U(D_S-\eta)}\right] \leq \left(1+\frac{P}{P_{N_1}}\right)^R, \\ \Delta_U \leq R_k + RC_s + \frac{1}{2}\log(2\pi e D_U), \\ \Delta_S \leq R_k + RC_s + \frac{1}{2}\log(2\pi e D_S), \\ \Delta_{SU} \leq R_k + RC_s + \frac{1}{2}\log\left[(2\pi e)^2|K|\right] - \\ \qquad -\frac{1}{2}\max\left[\log\frac{P_U}{D_U}, \log\frac{\sigma_{SU}^2}{P_U(D_S-\eta)}\right], \end{cases}$$

where $\eta = P_S - \frac{\sigma_{SU}^2}{P_U}$, and $C_s = \frac{1}{2}\log\frac{P_N(P+P_{N_1})}{P_{N_1}(P+P_N)}$ is the secrecy channel capacity.

Proposition 2: (Inner bound). When the encoder has access to both u^k and s^k (case 1 of encoder input), for the Gaussian source and channel, the tuple $(R, D_S, D_U, \Delta_S, \Delta_U, \Delta_{SU})$ is achievable if:

$$\begin{cases}
\left(1+\frac{\alpha_1^2 P_s}{\beta_1^2 P_{\tilde{A}_p}}\right) \leq \left(1+\frac{P_{Q_c}+P_{\tilde{Q}_p}}{P_{\tilde{W}_c}+P_{\tilde{X}+P_{N_1}}}\right)^R, \\
\left(1+\frac{\alpha_2^2 P_U}{\beta_2^2 P_{\tilde{B}_p}}\right) \leq \left(1+\frac{P_{\tilde{W}_c}}{P_{\tilde{X}}+P_{\tilde{Q}_p}+P_{N_1}}\right)^R \left(1+\frac{P_{\tilde{X}}}{P_{N_1}}\right)^R, \\
D_S \geq P_S - \frac{\alpha_1^2 P_S}{(\alpha_1^2 P_S+\beta_1^2 P_{\tilde{A}_p})^2}, \\
D_U \geq P_U - \frac{(\alpha_2^2 P_U+\gamma\sigma_{SU})^2}{P_U(\alpha_2^2 P_U+\gamma^2 P_S+2\alpha_2\gamma\sigma_{SU})^2}, \\
\Delta_S \leq \frac{R}{2}\log\left(\frac{P+P_{N_1}}{P_{\tilde{W}_c}+P_{\tilde{X}}+P_{N_1}}\frac{P_N}{P-P_{Q_c}+P_N}\right) \\
\quad +\frac{1}{2}\log\left(2\pi e\frac{\beta_1^2 P_S P_{\tilde{A}_p}}{\alpha_1^2 P_S+\beta_1^2 P_{\tilde{A}_p}}\right), \\
\Delta_U \leq \frac{1}{2}\log\left(\frac{\beta_2^2 P_U}{\beta_1^2 P_S}\frac{P_{\tilde{B}_p}}{P_{\tilde{A}_p}}\frac{\alpha_1^2 P_S+\beta_1^2 P_{\tilde{A}_p}}{\alpha_2^2 P_U+\beta_2^2 P_{\tilde{B}_p}}\right) \\
\quad +\frac{R}{2}\log\left(\frac{P_{N_1}+P_{N_2}}{P_{\tilde{Q}_p+P_{\tilde{X}}+P_{N_1}+P_{N2}}}\frac{P+P_{N_1}}{P_{\tilde{W}_c}+P_{\tilde{X}}+P_{N_1}}\frac{P_{\tilde{X}}+P_{N_1}}{P_{N_1}}\right), \\
\Delta_{SU} \leq \frac{1}{2}\log\left((2\pi e)^2|K|\frac{\beta_1^2 P_{\tilde{A}_p}}{\alpha_1^2 P_S+\beta_1^2 P_{\tilde{A}_p}}\frac{\beta_2^2 P_{\tilde{B}_p}}{\alpha_2^2 P_U+\beta_2^2 P_{\tilde{B}_p}}\right) \\
\quad +\frac{R}{2}\log\left(\frac{P_N}{P_{\tilde{Q}_p+P_{\tilde{X}}+P_N}}\left(1+\frac{P_{\tilde{Q}_p}}{P_{\tilde{W}_c}+P_{\tilde{X}}+P_{N_1}}\right)\left(1+\frac{P_{\tilde{X}}}{P_{N_1}}\right)\right).
\end{cases}$$

The inner bound is derived from Theorem 2 by choosing the following auxiliary r.v.s. The source encoder variables: $A_c = \emptyset$, $\quad B_c = \emptyset$, $A_p = \alpha_1 S + \beta_1 \tilde{A}_p$, where $\tilde{A}_p \sim \mathcal{N}(0, P_{\tilde{A}_p})$ and $B_p = \alpha_2 U + \beta_2 \tilde{B}_p + \gamma S$, given $\tilde{B}_p \sim \mathcal{N}(0, P_{\tilde{B}_p})$.

The channel encoder variables:

$$\begin{aligned}
&Q_c \sim \mathcal{N}(0, P_{Qc}), \\
&Q_p = Q_c + \tilde{Q}_p, \quad \tilde{Q}_p \sim \mathcal{N}(0, P_{\tilde{Q}_p}), \\
&W_c = Q_c + \tilde{W}_c, \quad \tilde{W}_c \sim \mathcal{N}(0, P_{\tilde{W}_c}), \\
&X = Q_c + \tilde{W}_c + \tilde{Q}_p + \tilde{X}, \quad \tilde{X} \sim \mathcal{N}(0, P_{\tilde{X}}),
\end{aligned}$$

where $P = P_{\tilde{X}} + P_{Qc} + P_{\tilde{W}_c} + P_{\tilde{Q}_p}$.

Function $\tilde{S}$ defined as minimum mean square error (MMSE) estimator of S from A_c and A_p, and $\tilde{U}$ is the MMSE estimator of U from B_c, B_p.

C. Numerical evaluation

Fig. 2 shows outer bound obtained numerically from Proposition 1 for the case of $\Delta_S = H(S)$ and $\Delta_U = H(U)$. Fig. 3 shows the inner bound (Proposition 2) for the same parameters but for case 1 encoder input. The other parameters are: $P_S = 0.3$, $P_U = 1$, $\sigma_{SU} = 0.8$, $P = 1$, $P_{N_1} = 0.10$, $P_{N_2} = 0.40$.

VI. Conclusion

This paper presents an information-theoretic framework for the secure transmission of semantic sources over wiretap channel. We characterize the rate-distortion-equivocation region to see the theoretically possible trade-off between distortion and secrecy requirements for semantic communications. We present bounds on a general inner and outer rate-distortion-equivocation region and reduce them to the Gaussian source and channel model to bring closer a general model to a practical wireless communication setup.

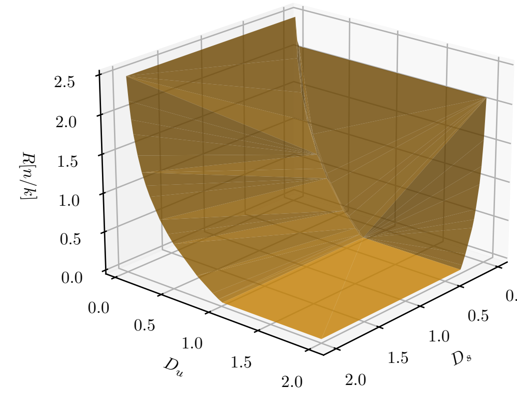

Fig. 2. Outer bound for Gaussian case and case 2 encoder input

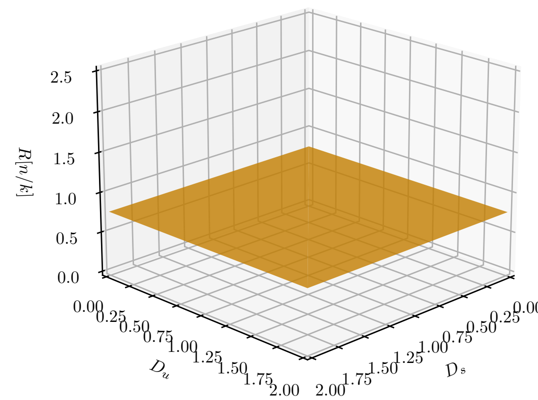

Fig. 3. Inner bound (every point above plane is achievable) for Gaussian case and case 1 encoder input

Appendix
Proof of Theorem 1

The following set of inequalities will be used in our proof:

$$I(X^n; Y^n) \leq \sum_{i=1}^{n} I(X_i; Y_i) \leq nI(X; Y), \tag{15}$$

$$\frac{1}{k} I(U^k; \hat{U}^k) \geq \frac{1}{k} \sum_{i=1}^{k} I(U_i; \hat{U}_i) \geq R_U(D_U + \epsilon), \tag{16}$$

$$\frac{1}{k} I(S^k; \hat{S}^k) \geq \frac{1}{k} \sum_{i=1}^{k} I(S_i; \hat{S}_i) \geq R_S(D_S + \epsilon), \tag{17}$$

$$\sum_{i=1}^{k} I(S_i; \hat{S}_i) \leq \sum_{i=1}^{k} I(U_i; \hat{U}_i) \leq \sum_{i=1}^{n} I(X_i; Y_i), \tag{18}$$

where $\epsilon > 0$.

First, we proof inequality in (9) as:

$$\begin{aligned}
R_U(D_U + \epsilon) \leq^{(16)} \frac{1}{k} \sum_{i=1}^{k} I(U_i; \hat{U}_i) \leq^{(18)} \frac{1}{k} \sum_{i=1}^{n} I(X_i; Y_i) \\
\leq^{(15)} \frac{n}{k} I(X; Y) \leq^{(2)} (R + \epsilon) I(X; Y). \quad (19)
\end{aligned}$$

To obtain (10), we follow the same steps as in the proof of (9) with (17) instead of (16).

The proof of (12) is as follows:

$$
\begin{aligned}
k(R_k+\epsilon) &\geq^{(3)} \log|\mathcal{K}| \geq H(K) \geq H(K|Y^n)\\
&\geq H(K|Y^n) - H(K|Y^n\hat{U}^k)\\
&= H(K,Y^n) - H(Y^n)\\
&\quad - H(K,Y^n,\hat{U}^k) + H(Y^n,\hat{U}^k)\\
&= H(\hat{U}^k|Y^n) - H(\hat{U}^k|Y^nK) =^{(1)} H(\hat{U}^k|Y^n)\\
&\geq^{(7)} H(\hat{U}^k|Y^n) - [H(U^k|Z^n) - k(\Delta_U-\epsilon)]\\
&= H(\hat{U}^k,Y^n) - H(Y^n) - H(U^k,Z^n)\\
&\quad + H(Z^n) + k(\Delta_U-\epsilon)\\
&= H(Y^n|\hat{U}^k) + H(\hat{U}^k) - H(Y^n)\\
&\quad - H(Z^n|U^k) - H(U^k) + H(Z^n)\\
&\quad + k(\Delta_U-\epsilon)\\
&= I(U^k;Z^n) - I(\hat{U}^k;Y^n) + H(\hat{U}^k|U^k)\\
&\quad - H(U^k) + I(U^k;\hat{U}^k) + k(\Delta_U-\epsilon).
\end{aligned} \tag{20}
$$

The first three terms in (20) can be rewritten as follows:

$$
\begin{aligned}
&I(U^k;Z^n) - I(\hat{U}^k;Y^n) + H(\hat{U}^k|U^k) =\\
&= I(U^k;Z^n) - H(Y^n) + H(Y^n|\hat{U}^k) + H(\hat{U}^k|U^k)\\
&\geq I(U^k;Z^n) - H(Y^n) + H(Y^n|\hat{U}^kU^k)\\
&\quad + H(\hat{U}^k|U^k)\\
&= I(U^k;Z^n) - H(Y^n) + H(Y^n,\hat{U}^k|U^k)\\
&\geq I(U^k;Z^n) - I(U^k;Y^n).
\end{aligned}
$$

With the help of Lemma 1 (see Appendix), we have:

$$
I(U^k;Z^n) - I(U^k;Y^n) \geq n[I(X;Z) - I(X;Y)]. \tag{21}
$$

Substituting (21) to (20) we obtain:

$$
\begin{aligned}
k(R_k+\epsilon) &\geq^{(20,16)} n[I(X;Z) - I(X;Y)] - kH(U)+\\
&\quad + kR_U(D_U+\epsilon) + k(\Delta_U-\epsilon)
\end{aligned} \tag{22}
$$

$$
\begin{aligned}
R_k + 2\epsilon &\geq \frac{n}{k}[I(X;Z) - I(X;Y)] - H(U)+\\
&\quad + R_U(D_U+\epsilon) + \Delta_U\\
&\geq^{(2)} (R+\epsilon)[I(X;Z) - I(X;Y)] - H(U)+\\
&\quad + R_U(D_U+\epsilon) + \Delta_U.
\end{aligned} \tag{23}
$$

To prove (13), we skip some steps due to its similarity with steps in proof of (12) (we use S^k instead of U^k).

$$
\begin{aligned}
k(R_k+\epsilon) &\geq ... \geq H(\hat{S}^k|Y^n) - H(\hat{S}^k|Y^nK)\\
&\geq^{(6)} H(\hat{S}^k|Y^n) - [H(S^k|Z^n) - k(\Delta_S-\epsilon)]\\
&= I(S^k;Z^n) - I(\hat{S}^k;Y^n) - H(S^k)+\\
&\quad + I(S^k;\hat{S}^k) + H(\hat{S}^k|S^k) + k(\Delta_S-\epsilon)\\
&\geq ... \geq n[I(X;Z) - I(X;Y)] - kH(S)+\\
&\quad + I(S^k;\hat{S}^k) + k(\Delta_S-\epsilon)
\end{aligned} \tag{24}
$$

$$
\begin{aligned}
&\geq^{(17)} n[I(X;Z) - I(X;Y)] - kH(S)+\\
&\quad + kR_S(D_S+\epsilon) + k(\Delta_S-\epsilon).
\end{aligned} \tag{25}
$$

Now we proceed with the proof of (11). Our proof will rely on the following inequality:

$$
\frac{1}{k}I(S^k,U^k;\hat{S}^k,\hat{U}^k) \geq \frac{1}{k}\sum_{i=1}^{k} I(S_i,U_i;\hat{S}_i,\hat{U}_i) \geq R(D_S,D_U). \tag{26}
$$

Thus, (11):

$$
\begin{aligned}
R(D_S+\epsilon, D_U+\epsilon) &\leq^{(26)} \frac{1}{k}\sum_{i=1}^{k} I(S_i,U_i;\hat{S}_i,\hat{U}_i)\\
&\leq^{(a)} \frac{1}{k}\sum_{i=1}^{n} I(X_i;Y_i) \leq^{(15)} \frac{n}{k}I(X;Y)\\
&\leq^{(2)} (R+\epsilon)I(X;Y),
\end{aligned} \tag{27}
$$

where (a) is due to the data processing inequality.

Finally, the proof of (14) is,

$$
\begin{aligned}
&k(R_k+\epsilon) \geq ... \geq H(K|Y^n) - H(K|Y^n,\hat{S}^k,\hat{U}^k)\\
&= H(\hat{S}^k,\hat{U}^k|Y^n) - H(\hat{S}^k,\hat{U}^k|Y^nK) =^{(1)} H(\hat{S}^k,\hat{U}^k|Y^n)\\
&\geq^{(8)} H(\hat{S}^k,\hat{U}^k|Y^n) - [H(S^k,U^k|Z^n) - k(\Delta_{SU}-\epsilon)]\\
&= H(\hat{S}^k,\hat{U}^k,Y^n) - H(Y^n) - H(S^k,U^k,Z^n)\\
&\quad + H(Z^n) + k(\Delta_{SU}-\epsilon)\\
&= H(Y^n|\hat{S}^k,\hat{U}^k) + H(\hat{S}^k,\hat{U}^k) - H(Y^n)\\
&\quad - H(Z^n|S^k,U^k) - H(S^k,U^k) + H(Z^n)\\
&\quad + k(\Delta_{SU}-\epsilon)\\
&= I(S^k,U^k;Z^n) - I(\hat{S}^k,\hat{U}^k;Y^n) + H(\hat{S}^k,\hat{U}^k|S^k,U^k)\\
&\quad - H(S^k,U^k) + I(S^k,U^k;\hat{S}^k,\hat{U}^k) + k(\Delta_{SU}-\epsilon).
\end{aligned} \tag{28}
$$

The first three terms in (28) are,

$$
\begin{aligned}
&I(S^k,U^k;Z^n) - I(\hat{S}^k,\hat{U}^k;Y^n) + H(\hat{S}^k,\hat{U}^k|S^k,U^k)\\
&\geq n[I(X;Z) - I(X;Y)].
\end{aligned}
$$

Substituting in (28), we have:

$$
\begin{aligned}
k(R_k+\epsilon) &\geq^{(26)} n[I(X;Z) - I(X;Y)] - kH(S,U)\\
&\quad + kR(D_S,D_U) + k(\Delta_{SU}-\epsilon),
\end{aligned}
$$

$$
\begin{aligned}
R_k + 2\epsilon &\geq (R+\epsilon)[I(X;Z) - I(X;Y)] - H(S,U)\\
&\quad + R(D_S,D_U) + \Delta_{SU}.
\end{aligned}
$$

Letting $\epsilon \to 0$ completes the converse proof.

Appendix
Proof of Theorem 2

Now we consider achievability proof for case 1 of encoder input (encoder has access to both u^k and s^k).

Source codebook:

We introduce 4 r.v.s A_c, A_p and B_c, B_p defined on alphabets $\mathcal{A}_c$, $\mathcal{A}_p$ and $\mathcal{B}_c$, $\mathcal{B}_p$. Random variables A_c and B_c correspond to a codebook distribution of a common message part for semantics and source. While A_p and B_p represent private a part of semantics and source. Let R_{ac}, R_{ap}, R_{bc}, R_{bp} be positive rates.

To construct a source codebook, we start by randomly and independently picking $2^{kR_{ac}}$ typical $\mathcal{T}_\delta^k(A_c)$ sequences from A_c distribution. We call such sequence $a_c^k(s_{ac})$, where $s_{ac} \in [1,2,...,2^{kR_{ac}}]$

For each sequence $a_c^k(s_{ac})$ we pick $2^{kR_{ap}}$ typical $\mathcal{T}_\delta^k(A_p|a_c^k(s_{ac}))$ sequences from A_p distribution and name it $a_p^k(s_{ac}, s_{ap})$, $s_{ap} \in [1,2,...,2^{kR_{ap}}]$.

For each $a_c^k(s_{ac})$ we pick $2^{kR_{bc}}$ sequences $b_c^k(s_{ac}, s_{bc}) \in \mathcal{T}_\delta^k(B_c|a_c^k(s_{ac}))$, $s_{bc} \in [1,2,...,2^{kR_{bc}}]$.

We finish codebook by picking for each previous sequences, $2^{kR_{bp}}$ sequences $b_p^k(s_{ac}, s_{ap}, s_{bc}, s_{bp}) \in \mathcal{T}_\delta^k(B_p|a_c^k(s_{ac}), a_p^k(s_{ac}, s_{ap}), b_c^k(s_{ac}, s_{bc}))$, $s_{bp} \in [1,2,...,2^{kR_{bp}}]$.

This codebook is revealed to Bob and Eve.

Channel codebook:

Let Q_c, Q_p and W_c be r.v. for channel codebook generation defined on $\mathcal{Q}_c$, $\mathcal{Q}_p$, $\mathcal{W}_c$. Let $R_{qc}, R_{qp}, R_{wc}, R_{wp}, R_1, R_2$ be positive rates s.t:

$$R_1 < (R+\epsilon)I(Q_p; Z|Q_c),$$
$$R_2 < (R+\epsilon)I(X; Z|W_c).$$

From $\mathcal{T}_\delta^n(Q_c)$ we pick $2^{kR_{qc}}$ sequences named $q_c^n(r_{qc})$, where $r_{qc} \in [1,2,...,2^{kR_{qc}}]$ is a index of a sequence.

For each $q_c^n(r_{qc})$ we pick $2^{k(R_{qp}+R_1)}$ sequences $q_p^n(r_{qc}, r_{qp}, r_1) \in \mathcal{T}_\delta^n(Q_p|q_c^n(r_{qc}))$.

Also for each $q_c^n(r_{qc})$ we randomly pick $2^{kR_{wc}}$ sequences $w_c^n(r_{qc}, r_{wc}) \in \mathcal{T}_\delta^n(W_c|q_c^n(r_{qc}))$.

And, finally, for each $q_c^n(r_{qc}), q_p^n(r_{qc}, r_{qp}, r_1), w_c^n(r_{qc}, r_{wc})$ we pick $2^{k(R_{wp}+R_2)}$ sequences $x^n(r_{qc}, r_{qp}, r_1, r_{wc}, r_{wp}, r_2) \in \mathcal{T}_\delta^n(X|q_c^n(r_{qc}), q_p^n(r_{qc}, r_{qp}, r_1), w_c^n(r_{qc}, r_{wc}))$.

This codebook is revealed to Bob and Eve. Further to shorten notations we will skip indices in sequence names.

Source encoding:

We have (s^k, u^k) as encoder input. We search for the first jointly typical sequence a_c^k s.t. $(a_c^k, s^k) \in \mathcal{T}_\delta^k(A_c, S)$.

Then, given a_c^k, we find first a_p^k sequence s.t. $(a_p^k, s^k) \in \mathcal{T}_\delta^k(A_p, S|a_c^k)$.

Also, given codeword a_c^k, we proceed by finding first codeword b_c^k s.t. $(b_c^k, u^k) \in \mathcal{T}_\delta^k(B_c, U|S, a_c^k)$.

And, given all previous codewords a_c^k, a_p^k and b_c^k, we finish source encoding by finding first $(b_p^k, u^k) \in \mathcal{T}_\delta^k(B_p, U|S, a_c^k, a_p^k, b_c^k)$.

Channel encoding:

We choose arbitrary one-to-one mapping $(r_{qc}, r_{qp}, r_{wc}, r_{wp}) = g(s_{ac}, s_{ap}, s_{bc}, s_{bp})$ which is used to map source indices to channel indices. We assume that there exist mappings $(r_{qc}, r_{qp}) = g_1(s_{ac}, s_{ap})$ and $(r_{wc}, r_{wp}) = g_2(s_{bc}, s_{bp})$.

Now, given channel indexes $(r_{qc}, r_{qp}, r_{wc}, r_{wp})$ as a result of mapping g, we sequentially select q_c^n, q_p^n, w_c^n, x^n, from channel codebook. Alice transmit sequence $x^n \doteq x^n(r_{qc}, r_{qp}, r_1, r_{wc}, r_{wp}, r_2)$, where r_1 and r_2 selected at random with uniform distribution.

Decoding:

Bob receives y^n. He sequentially searches in his codebook for a codewords s.t.:

1) $(q_c^n, y^n) \in \mathcal{T}_\delta^n(Q_c, Y)$,
2) $(q_p^n, y^n) \in \mathcal{T}_\delta^n(Q_p, Y|q_c^n)$,
3) $(w_c^n, y^n) \in \mathcal{T}_\delta^n(W_c, Y|q_c^n)$,
4) $(x^n, y^n) \in \mathcal{T}_\delta^n(X, Y|q_c^n, q_p^n, w_c^n)$.

Then, given channel indexes $(r_{qc}, r_{qp}, r_{wc}, r_{wp})$, Bob using inverse mapping g^{-1} gets source decoder indexes $(s_{ac}, s_{ap}, s_{bc}, s_{bp})$ and decodes:

$$\hat{s}^k = \tilde{S}(a_c^k, a_p^k),$$
$$\hat{u}^k = \tilde{U}(a_c^k, a_p^k, b_c^k, b_p^k),$$

where $\tilde{S}: A_c^k \times A_p^k \to \hat{S}^k$ and $\tilde{U}: A_c^k \times A_p^k \times B_c^k \times B_p^k \to \hat{U}^k$ are functions.

Errors at encoding and decoding:

We consider the following events which correspond to errors at the encoding or decoding stages.

Encoder errors:

$$\mathcal{E}_1 \doteq \{\nexists a_c^k : (a_c^k, s^k) \in \mathcal{T}_\delta^k(A_c, S)\},$$
$$\mathcal{E}_2 \doteq \{\nexists a_p^k : (a_p^k, s^k) \in \mathcal{T}_\delta^k(A_p, S|a_c^k)\},$$
$$\mathcal{E}_3 \doteq \{\nexists b_c^k : (b_c^k, u^k) \in \mathcal{T}_\delta^k(B_c, U|S, a_c^k)\},$$
$$\mathcal{E}_4 \doteq \{\nexists b_p^k : (b_p^k, u^k) \in \mathcal{T}_\delta^k(B_p, U|S, a_c^k, a_p^k, b_c^k)\}.$$

Decoder errors:

$$\mathcal{E}_5 \doteq \{\exists \hat{q}_c^n \neq q_c^n : \hat{q}_c^n, q_c^n \in \mathcal{T}_\delta^n(Q_c, Y)\},$$
$$\mathcal{E}_6 \doteq \{\exists \hat{q}_p^n \neq q_p^n : \hat{q}_p^n, q_p^n \in \mathcal{T}_\delta^n(Q_p, Y|q_c^n)\},$$
$$\mathcal{E}_7 \doteq \{\exists \hat{w}_c^n \neq w_c^n : \hat{w}_c^n, w_c^n \in \mathcal{T}_\delta^n(W_c, Y|q_c^n)\},$$
$$\mathcal{E}_8 \doteq \{\exists \hat{x}^n \neq x^n : \hat{x}^n, x^n \in \mathcal{T}_\delta^n(X, Y|q_c^n, q_p^n, w_c^n)\}.$$

We upper bound probability of an "error" event as follows:

$$Pr\{\mathcal{E}\} = P_{\mathcal{E}} \leq \sum_{i=1}^{8} P_{\mathcal{E}_i},$$

where $P_{\mathcal{E}_i} = Pr\{\mathcal{E}_i\}$.

Given $k \to \infty$, it can be shown that:

1) if $R_{ac} > I(A_c; S)$
   then $P_{\mathcal{E}_1} \to 0$,
2) if $R_{ap} > I(A_p; S|A_c)$
   then $P_{\mathcal{E}_2} \to 0$,
3) if $R_{bc} > I(B_c; U|S, A_c)$
   then $P_{\mathcal{E}_3} \to 0$,
4) if $R_{bp} > I(B_p; U|S, A_c, A_p, B_c)$
   then $P_{\mathcal{E}_4} \to 0$,
5) if $R_{qc} < (R+\epsilon)I(Q_c; Y)$
   then $P_{\mathcal{E}_5} \to 0$,
6) if $R_{qp} + R_1 < (R+\epsilon)I(Q_p; Y|Q_c)$
   then $P_{\mathcal{E}_6} \to 0$,
7) if $R_{wc} < (R+\epsilon)I(W_c; Y|Q_c)$
   then $P_{\mathcal{E}_7} \to 0$,
8) if $R_{wp} + R_2 < (R+\epsilon)I(X; Y|Q_c, Q_p, W_c)$
   then $P_{\mathcal{E}_8} \to 0$.

Analysis of expected distortion for semantics:

$$
\begin{aligned}
&\mathbb{E}\, d_s\left(S^k, \hat{S}^k\right) = \mathbb{E}\, d_s\left(S^k, \hat{f}_s(Y^n)\right) \\
&=^{(a)} P_{\mathcal{E}}\, \mathbb{E}\left\{ d_s\left(S^k, \hat{f}_s(Y^n)\right) | \mathcal{E} \right\} \\
&\qquad + P_{\bar{\mathcal{E}}}\, \mathbb{E}\left\{ d_s\left(S^k, \hat{f}_s(Y^n)\right) | \bar{\mathcal{E}} \right\} \\
&\le P_{\mathcal{E}} d_{S,m} + P_{\bar{\mathcal{E}}}\, \mathbb{E}\left\{ d_s\left(S^k, \hat{f}_s(Y^n)\right) | \bar{\mathcal{E}} \right\} \\
&=^{(b)} P_{\mathcal{E}} d_{S,m} + P_{\bar{\mathcal{E}}}\, \mathbb{E}\left\{ d_s\left(S^k, \tilde{S}(A_c^k, A_p^k)\right) | \bar{\mathcal{E}} \right\} \\
&\le^{(c)} P_{\mathcal{E}} d_{S,m} + P_{\bar{\mathcal{E}}}(1+\epsilon_1)\, \mathbb{E}\left\{ d_s\left(S, \tilde{S}(A_c, A_p)\right) | \bar{\mathcal{E}} \right\} \\
&\le^{(d)} P_{\mathcal{E}} d_{S,m} + (1+\epsilon_1)\, \mathbb{E}\, d_s\left(S, \tilde{S}(A_c, A_p)\right),
\end{aligned}
$$

where $d_{S,m} = \max_{\mathcal{C}, S^k, Y^n} d_s\left(S^k, \hat{f}_s(Y^n)\right)$, (a) due to law of total expectation, (b) because $\hat{f}_s(Y^n) = \tilde{S}(A_c^k, A_p^k)$ given no error occurs $\bar{\mathcal{E}}$, (c) due to typical average lemma and $(s^k, a_c^k, a_p^k) \in \mathcal{T}_\delta^k(S, A_c, A_p)$, (d) due to $\mathbb{E}(X|A) \le \frac{\mathbb{E}\, X}{P_A}$.

We conclude that the following is sufficient to satisfy distortion condition (4) for semantics:

$$
D_S \ge \mathbb{E}\, d_s\left(S, \tilde{S}(A_c, A_p)\right),
$$

given $k \to \infty$

Analysis of expected distortion for observation:

$$
\begin{aligned}
&\mathbb{E}\, d_u\left(U^k, \hat{U}^k\right) = \mathbb{E}\, d_u\left(U^k, \hat{f}_u(Y^n)\right) \\
&=^{(a)} P_{\mathcal{E}}\, \mathbb{E}\left\{ d_u\left(S^k, \hat{f}_s(Y^n)\right) | \mathcal{E} \right\} \\
&\qquad + P_{\bar{\mathcal{E}}}\, \mathbb{E}\left\{ d_u\left(U^k, \hat{f}_u(Y^n)\right) | \bar{\mathcal{E}} \right\} \\
&\le P_{\mathcal{E}} d_{U,m} + P_{\bar{\mathcal{E}}}\, \mathbb{E}\left\{ d_u\left(U^k, \hat{f}_u(Y^n)\right) | \bar{\mathcal{E}} \right\} \\
&=^{(b)} P_{\mathcal{E}} d_{U,m} + P_{\bar{\mathcal{E}}}\, \mathbb{E}\left\{ d_u\left(U^k, \tilde{U}(A_c^k, A_p^k, B_c^k, B_p^k)\right) | \bar{\mathcal{E}} \right\} \\
&\le^{(c)} P_{\bar{\mathcal{E}}}(1+\epsilon_1)\, \mathbb{E}\left\{ d_u\left(S, \tilde{U}(A_c^k, A_p^k, B_c^k, B_p^k)\right) | \bar{\mathcal{E}} \right\} \\
&\qquad + P_{\mathcal{E}} d_{U,m} \\
&\le^{(d)} P_{\mathcal{E}} d_{U,m} + (1+\epsilon_1)\, \mathbb{E}\, d_u\left(U, \tilde{U}(A_c, A_p, B_c, B_p)\right),
\end{aligned}
$$

where $d_{U,m} = \max_{\mathcal{C}, U^k, Y^n} d_u\left(U^k, \hat{f}_u(Y^n)\right)$, (a) due to law of total expectation, (b) because $\hat{f}_u(Y^n) = \tilde{U}(A_c^k, A_p^k, B_c^k, B_p^k)$ given $\bar{\mathcal{E}}$, (c) due to typical average lemma and $(u^k, a_c^k, a_p^k, b_c^k, b_p^k) \in \mathcal{T}_\delta^k(U, A_c, A_p, B_c, B_p)$, (d) due to $\mathbb{E}(X|A) \le \frac{\mathbb{E}\, X}{P_A}$.

Thus, to satisfy distortion condition (5) it is sufficient to have:

$$
D_U \ge \mathbb{E}\, d_u\left(U, \tilde{U}(A_c, A_p, B_c, B_p)\right),
$$

given $k \to \infty$

Equivocation analysis for observation:

Here we treat sequence indices s_{**} and r_{**} as random variables. We start by analyzing equivocation for observation U^k:

$$
\begin{aligned}
H(U^k|Z^n) &= H(U^k|M_u, Z^n) + I(U^k; M_u|Z^n) \\
&= H(U^k|M_u) + H(M_u|Z^n) - H(M_u|U^k, Z^n) \\
&\quad - I(U^k; Z^n|M_u),
\end{aligned} \tag{29}
$$

where $M_u \doteq (s_{bc}, s_{bp})$ is an encoded (by source encoder) message for observation.

First term of (29):

$$
\begin{aligned}
&H(U^k|M_u) = H(U^k|s_{bc}, s_{bp}) = H(S^k, U^k) \\
&\quad - I(s_{bc}, s_{bp}; S^k, U^k) - H(S^k|U^k, s_{bc}, s_{bp}) \\
&=^{(a)} H(S^k, U^k) - H(s_{bc}, s_{bp}) - H(S^k|U^k, s_{bc}, s_{bp}) \\
&= H(S^k, U^k) - H(s_{bc}) - H(s_{bp}) + I(s_{bc}; s_{bp}) \\
&\quad - H(S^k|U^k, s_{bc}, s_{bp}),
\end{aligned} \tag{30}
$$

where (a) because (s_{bc}, s_{bp}) is a function of (s^k, u^k)

For second term (29) we have:

$$
\begin{aligned}
&H(M_u|Z^n) = H(s_{bc}, s_{bp}|Z^n) =^{(a)} H(r_{wc}, r_{wp}|Z^n) \\
&\ge^{(b)} H(X^n|r_{wc}) + H(Z^n|X^n) - H(X^n|r_{wc}, r_{wp}, Z^n) \\
&\quad - H(Z^n|r_{wc}) \\
&= H(X^n|r_{wc}) + H(Z^n|X^n) - H(X^n|r_{wc}, r_{wp}, Z^n) \\
&\quad - H(Z^n|r_{qc}, r_{wc}) - I(Z^n; r_{qc}|r_{wc}),
\end{aligned} \tag{31}
$$

where (a) due to g_2 mapping, (b) for same reasons as in [18, eq. 2.38]. Substituting (30) and (31) into (29) we have:

$$
\begin{aligned}
&H(U^k|Z^n) \ge H(S^k, U^k) - H(s_{bc}) - H(s_{bp}) + I(s_{bc}; s_{bp}) \\
&\quad - H(S^k|U^k, s_{bc}, s_{bp}) + H(X^n|r_{wc}) + H(Z^n|X^n) \\
&\quad - H(X^n|r_{wc}, r_{wp}, Z^n) - H(Z^n|r_{qc}, r_{wc}) - I(Z^n; r_{qc}|r_{wc}) \\
&\quad - H(s_{bc}, s_{bp}|U^k, Z^n) - I(U^k; Z^n|s_{bc}, s_{bp}).
\end{aligned} \tag{32}
$$

Now we reduce some terms in (32).

$$
\begin{aligned}
&H(S^k, U^k) - H(S^k|U^k, s_{bc}, s_{bp}) - H(s_{bc}, s_{bp}|U^k, Z^n) \\
&=^{(a)} H(U^k) + I(S^k; s_{bc}, s_{bp}; Z^n|U^k),
\end{aligned} \tag{33}
$$

where (a) because (s_{bc}, s_{bp}) is a function of (s^k, u^k).

$$
\begin{aligned}
&H(X^n|r_{wc}, r_{wp}, Z^n) + I(U^k; Z^n|s_{bc}, s_{bp}) \\
&\le^{(a)} H(X^n|r_{wc}, r_{wp}, Z^n) + I(X^n; Z^n|r_{wc}, r_{wp}) \\
&= H(X^n|r_{wc}, r_{wp}),
\end{aligned} \tag{34}
$$

where (a) due to data processing inequality and g_2 mapping.

$$
I(Z^n; r_{qc}|r_{wc}) \le H(r_{qc}|r_{wc}) = H(r_{qc}) - I(r_{qc}; r_{wc}). \tag{35}
$$

Returning to (32) with (33), (34) and (35):

$$
\begin{aligned}
&H(U^k|Z^n) \ge H(U^k) - H(s_{bc}) - H(s_{bp}) + I(s_{bc}; s_{bp}) \\
&\quad + H(X^n|r_{wc}) + H(Z^n|X^n) - H(Z^n|r_{qc}, r_{wc}) \\
&\quad - H(r_{qc}) + I(r_{qc}; r_{wc}) - H(X^n|r_{wc}, r_{wp}) \\
&\quad + I(S^k; s_{bc}, s_{bp}; Z^n|U^k).
\end{aligned} \tag{36}
$$

Now we bound each term of (36):

1) $H(U^k) = kH(U)$ (U^k is i.i.d.),
2) $H(s_{bc}) \le kR_{bc}$,
3) $H(s_{bp}) \le kR_{bp}$,
4) $H(X^n|r_{wc}) \ge k(R_{qc}+R_{qp}+R_1+R_{wp}+R_2) - 1 - \epsilon_1$ (X^n is nearly uniform and [18, Lemma 2.5]),
5) $H(Z^n|X^n) = nH(Z|X)$ (channel is memoryless),
6) $H(Z^n|r_{qc}, r_{wc}) \le nH(Z|Q_c, W_c) + n\epsilon_2$ (see [18, eq. 2.50-2.52]),
7) $H(r_{qc}) \le kR_{qc}$,
8) $H(X^n|r_{wc}, r_{wp}) \le k(R_{qc}+R_{qp}+R_1+R_2)$,
9) $I(s_{bc}; s_{bp}) + I(r_{qc}; r_{wc}) + I(S^k; s_{bc}, s_{bp}; Z^n|U^k) \ge 0$.

Collecting all terms we have:

$$\begin{aligned}H(U^k|Z^n) &\ge kH(U) - kR_{bc} - kR_{bp} + kR_{qc} + kR_{qp} + kR_1 \\ &\quad + kR_{wp} + kR_2 - 1 - \epsilon_1 + nH(Z|X) - nH(Z|Q_c, W_c) \\ &\quad - n\epsilon_2 - kR_{qc} - k(R_{qc}+R_{qp}+R_1+R_2) \\ &= kH(U) - kR_{bc} - kR_{bp} + kR_{wp} - kR_{qc} + nH(Z|X) \\ &\quad - nH(Z|Q_c, W_c) - n\epsilon_3 - 1.\end{aligned}$$

Thus, to satisfy equivocation for source, it is sufficient to have:

$$\begin{aligned}\Delta_U &\le H(U) - R_{bc} - R_{bp} + R_{wp} - R_{qc} \\ &\quad + (R+\epsilon)(H(Z|X) - H(Z|Q_c, W_c)) - \epsilon,\end{aligned}$$

given $k \to \infty$.

Equivocation analysis for semantics:

For semantic equivocation, we have:

$$\begin{aligned}H(S^k|Z^n) &= H(S^k|M_s, Z^n) + I(S^k; M_s|Z^n) \\ &= H(S^k|M_s) + H(M_s|Z^n) - H(M_s|S^k, Z^n) \\ &\quad - I(S^k; Z^n|M_s),\end{aligned} \tag{37}$$

where $M_s \doteq (s_{ac}, s_{ap})$ is an encoded (by source encoder) message for semantics. First term of (37):

$$\begin{aligned}H(S^k|M_s) &= H(S^k|s_{ac}, s_{ap}) \\ &= H(S^k, U^k) - I(s_{ac}, s_{ap}; S^k, U^k) - H(U^k|S^k, s_{ac}, s_{ap}) \\ &=^{(a)} H(S^k, U^k) - H(s_{ac}, s_{ap}) - H(U^k|S^k, s_{ac}, s_{ap}) \\ &= H(S^k, U^k) - H(s_{ac}) - H(s_{ap}) + I(s_{ac}; s_{ap}) \\ &\quad - H(U^k|S^k, s_{ac}, s_{ap}),\end{aligned} \tag{38}$$

where (a) because (s_{ac}, s_{ap}) is a function of (s^k, u^k). Second term of (37):

$$\begin{aligned}H(M_s|Z^n) &= H(s_{ac}, s_{ap}|Z^n) =^{(a)} H(r_{qc}, r_{qp}|Z^n) \\ &\ge^{(b)} H(X^n|r_{qc}) + H(Z^n|X^n) \\ &\quad - H(X^n|r_{qc}, r_{qp}, Z^n) - H(Z^n|r_{qc}),\end{aligned} \tag{39}$$

where (a) due to g_1 mapping, (b) see [18, eq. 2.38]. Gathering all terms, we have:

$$\begin{aligned}H(S^k|Z^n) &\ge H(S^k, U^k) - H(s_{ac}) - H(s_{ap}) + I(s_{ac}; s_{ap}) \\ &\quad - H(U^k|S^k, s_{ac}, s_{ap}) + H(X^n|r_{qc}) + H(Z^n|X^n) \\ &\quad - H(X^n|r_{qc}, r_{qp}, Z^n) - H(Z^n|r_{qc}) \\ &\quad - H(s_{ac}, s_{ap}|S^k, Z^n) - I(S^k; Z^n|s_{ac}, s_{ap}).\end{aligned} \tag{40}$$

We reduce some terms in (40).

$$\begin{aligned}&H(S^k, U^k) - H(U^k|S^k, s_{ac}, s_{ap}) - H(s_{ac}, s_{ap}|S^k, Z^n) \\ &=^{(a)} H(S^k) + I(U^k; s_{ac}, s_{ap}; Z^n|S^k),\end{aligned} \tag{41}$$

where (a) because (s_{ac}, s_{ap}) is a function of (s^k, u^k).

$$\begin{aligned}&H(X^n|r_{qc}, r_{qp}, Z^n) + I(S^k; Z^n|s_{ac}, s_{ap}) \\ &\le^{(a)} H(X^n|r_{qc}, r_{qp}, Z^n) + I(X^n; Z^n|r_{qc}, r_{qp}) \\ &= H(X^n|r_{qc}, r_{qp}),\end{aligned} \tag{42}$$

where (a) due to data processing inequality and g_1 mapping. Substituting (41) and (42) into (40) we obtain:

$$\begin{aligned}H(S^k|Z^n) &\ge H(S^k) - H(s_{ac}) - H(s_{ap}) + I(s_{ac}; s_{ap}) \\ &\quad + H(X^n|r_{qc}) + H(Z^n|X^n) - H(Z^n|r_{qc}) \\ &\quad - H(X^n|r_{qc}, r_{qp}) + I(U^k; s_{ac}, s_{ap}; Z^n|S^k).\end{aligned} \tag{43}$$

Now we bound each term of (43):

1) $H(S^k) = kH(S)$ (S^k is i.i.d.),
2) $H(s_{ac}) \le kR_{ac}$,
3) $H(s_{ap}) \le kR_{ap}$,
4) $H(X^n|r_{qc}) \ge k(R_{wc}+R_{qp}+R_1+R_{wp}+R_2) - 1 - \epsilon_1$ (X^n is nearly uniform and [18, Lemma 2.5]),
5) $H(Z^n|X^n) = nH(Z|X)$ (channel is memoryless),
6) $H(Z^n|r_{qc}) \le nH(Z|Q_c) + n\epsilon_2$ (see [18, eq. (2.50-2.52)]),
7) $H(X^n|r_{qc}, r_{qp}) \le k(R_{wc}+R_{wp}+R_1+R_2)$,
8) $I(U^k; s_{ac}, s_{ap}; Z^n|S^k) \ge 0$,
9) $I(s_{ac}; s_{ap}) \ge 0$.

Returning to (43) we have:

$$\begin{aligned}H(S^k|Z^n) &\ge kH(S) - kR_{ac} - kR_{ap} \\ &\quad + k(R_{wc}+R_{qp}+R_1+R_{wp}+R_2) - 1 - \epsilon_1 \\ &\quad + nH(Z|X) - nH(Z|Q_c) - n\epsilon_2 \\ &\quad - k(R_{wc}+R_{wp}+R_1+R_2) \\ &= kH(S) - kR_{ac} - kR_{ap} + kR_{qp} \\ &\quad + nH(Z|X) - nH(Z|Q_c) - n\epsilon_3 - 1.\end{aligned}$$

Thus, to satisfy equivocation for semantics, it is sufficient to have:

$$\begin{aligned}\Delta_S &\le H(S) - R_{ac} - R_{ap} + R_{qp} \\ &\quad + (R+\epsilon)(H(Z|X) - H(Z|Q_c)) - \epsilon,\end{aligned}$$

given $k \to \infty$.

Joint equivocation analysis:

$$\begin{aligned}H(S^k, U^k|Z^n) &= H(S^k, U^k|M) + H(M|Z^n) \\ &\quad - I(S^k, U^k; Z^n|M) \\ &=^{(a)} H(S^k, U^k|M) + H(M|Z^n),\end{aligned} \tag{44}$$

where $M = (s_{ac}, s_{bc}, s_{ap}, s_{bp})$ and (a) due to $(S^k, U^k) \to M \to Z^n$.

First term of (44):

$$H(S^k, U^k|M) =^{(a)} H(S^k, U^k) - H(M),$$

where (a) because M is a function of (S^k, U^k).

Second term of (44):

$$H(M|Z^n) \geq^{(a)} H(X^n|r_c) + H(Z^n|X^n) - H(X^n|r_c, r_p, Z^n) - H(Z^n|r_c),$$

where $r_c = (r_{qc}, r_{wc})$, $r_p = (r_{qp}, r_{wp})$, (a) due to g mapping, the fact that $H(r_c, r_p|X^n) = 0$ and $X^n \to Y^n \to Z^n$.

Returning to (44) we have:

$$H(S^k, U^k|Z^n) \geq H(S^k, U^k) - H(M) + H(X^n|r_c) + H(Z^n|X^n) - H(X^n|r_c, r_p, Z^n) - H(Z^n|r_c). \quad (45)$$

Now we bound each term of (45):

1) $H(S^k, U^k) = kH(S, U)$ (S^k and U^k are i.i.d),
2) $H(M) \leq k(R_{ac} + R_{bc} + R_{ap} + R_{bp})$,
3) $H(X^n|r_c) \geq k(R_{qp} + R_{wp} + R_1 + R_2) - 1 - \epsilon_1$ (X^n is nearly uniform, [18, Lemma 2.5]),
4) $H(Z^n|X^n) = nH(Z|X)$,
5) $H(X^n|r_c, r_p, Z^n) \leq \epsilon_2$ (due to Fano's inequality, see [18, eq. (2.49)]),
6) $H(Z^n|r_c) \leq nH(Z|Q_c, W_c) + n\epsilon_3$ (see [18, eq. (2.50-2.52)]).

Finally, we obtain:

$$\frac{1}{k}H(S^k, U^k|Z^n) \geq H(S, U) - R_{ac} - R_{bc} - R_{ap} - R_{bp} + (R + \epsilon)\left(H(Z|X) - H(Z|Q_c, W_c)\right) + \epsilon + R_{qp} + R_{wp} + R_1 + R_2.$$

Thus, to satisfy joint equivocation, it is sufficient to have:

$$\Delta_{SU} \leq H(S, U) - R_{ac} - R_{bc} - R_{ap} - R_{bp} + R_{qp} + R_{wp} + R_1 + R_2 + (R + \epsilon)\left(H(Z|X) - H(Z|Q_c, W_c)\right) - \epsilon.$$

Summary of conditions:

$$\begin{cases} R_{**}, R_1, R_2 > 0 \\ R_{ac} + R_{ap} = R_{qc} + R_{qp} \\ R_{bc} + R_{bp} = R_{wc} + R_{wp} \\ R_{ac} < R_{qc} \\ R_{bc} < R_{wc} \\ R_{ac} > I(A_c; S) \\ R_{ap} > I(A_p; S|A_c) \\ R_{bc} > I(B_c; U|S, A_c) \\ R_{bp} > I(B_p; U|S, A_c, A_p, B_c) \\ R_{qc} < RI(Q_c; Y) \\ R_{qp} + R_1 < RI(Q_p; Y|Q_c) \\ R_{wc} < RI(W_c; Y|Q_c) \\ R_{wp} + R_2 < RI(X; Y|Q_c, Q_p, W_c) \\ R_1 < RI(Q_p; Z|Q_c) \\ R_2 < RI(X; Z|W_c) \\ D_S \geq \mathbb{E}\, d_S(S, \tilde{S}(A_c, A_p)) \\ D_U \geq \mathbb{E}\, d_U(U, \tilde{U}(A_c, A_p, B_c, B_p)) \\ \Delta_S \leq H(S) - R_{ac} - R_{ap} + R_{qp} \\ \qquad +(R + \epsilon)(H(Z|X) - H(Z|Q_c)) - \epsilon \\ \Delta_U \leq H(U) - R_{bc} - R_{bp} + R_{wp} - R_{qc} \\ \qquad +(R + \epsilon)(H(Z|X) - H(Z|Q_c, W_c)) - \epsilon \\ \Delta_{SU} \leq H(S, U) - R_{ac} - R_{bc} - R_{ap} - R_{bp} + R_{qp} + R_{wp} \\ \qquad +R_1 + R_2 + (R + \epsilon)\left(H(Z|X) - H(Z|Q_c, W_c)\right) - \epsilon. \end{cases}$$

The above system of inequalities can be reduced to the following system:

$$\begin{cases} I(S; A_c) < RI(Q_c; Y), \\ I(S; A_c, A_p) < RI(Y; Q_c, Q_p), \\ I(U; B_c|S, A_c) < RI(W_c; Y|Q_c), \\ I(U; B_c|S, A_c) + I(U; B_p|S, A_c, A_p, B_c) < \\ \qquad < R[I(W_c; Y|Q_c) + I(X; Y|Q_c, Q_p, W_c)] \\ D_S \geq \mathbb{E}\, d_S(S, \tilde{S}(A_c, A_p)), \\ D_U \geq \mathbb{E}\, d_U(U, \tilde{U}(A_c, A_p, B_c, B_p)), \\ \Delta_S \leq H(S|Ac, Ap) + R(H(Z|X) - H(Z|Qc)) \\ \qquad +RI(Qp; Y|Qc), \\ \Delta_U \leq H(U) - I(A_c, A_p; S) - I(B_c; U|A_c) \\ \qquad -I(B_p; U|S, A_c, A_p, B_c) + RH(Z|X) \\ \qquad -RH(Z|Q_c, W_c) + RI(Q_p; Y|Q_c) \\ \qquad +RI(X; Y|Q_c, Q_p, W_c), \\ \Delta_{SU} \leq H(S, U) - I(S; A_c, A_p) - I(U; B_p|S, A_c, A_p, B_c) \\ \qquad -I(U; B_c|S, A_c) + R(H(Z|X) - H(Z|Qc, Wc)) \\ \qquad +RI(Q_p; Y|Q_c) + RI(X; Y|Q_c, Q_p, W_c). \end{cases}$$

APPENDIX
LEMMA 4

Lemma 4: For $U^k \to X^n \to Y^n \to Z^n$ Markov chain the following holds [8]:

$$I(U^k; Z^n) - I(U^k; Y^n) \geq n[I(X;Z) - I(X;Y)]. \quad (46)$$

Proof:

$$\begin{aligned}
&I(U^k; Y^n) = \sum_{i=1}^{n} I(U^k; Y_i | Y^{i-1}),\\
&I(U^k; Y_i | Y^{i-1}) = I(U^k, \tilde{Z}^{i+1}; Y_i | Y^{i-1})\\
&\quad - I(\tilde{Z}^{i+1}; Y_i | Y^{i-1}, U^k)\\
&= I(U^k; Y_i | Y^{i-1}, \tilde{Z}^{i+1})\\
&\quad + I(\tilde{Z}^{i+1}; Y_i | Y^{i-1}) - I(\tilde{Z}^{i+1}; Y_i | U^k, Y^{i-1}),
\end{aligned}$$

where $\tilde{Z}^i = (Z_i, Z_{i+1}, ..., Z_n)$. Following the same steps for $I(U^k; Z^n)$ we have:

$$\begin{aligned}
I(U^k; Y^n) &= \sum_{i=1}^{n} A + \sum_{i=1}^{n} B - \sum_{i=1}^{n} C,\\
I(U^k; Z^n) &= \sum_{i=1}^{n} D + \sum_{i=1}^{n} F - \sum_{i=1}^{n} G,
\end{aligned}$$

where:

$$\begin{aligned}
A &= I(U^k; Y_i | Y^{i-1}, \tilde{Z}^{i+1}),\\
B &= I(\tilde{Z}^{i+1}; Y_i | Y^{i-1}),\\
C &= I(\tilde{Z}^{i+1}; Y_i | U^k, Y^{i-1}),\\
D &= I(U^k; Z_i | Y^{i-1}, \tilde{Z}^{i+1}),\\
F &= I(Y^{i-1}; Z_i | \tilde{Z}^{i+1}),\\
G &= I(Y^{i-1}; Z_i | \tilde{Z}^{i+1} U^k).
\end{aligned}$$

Due to Csiszár Sum Identity [16] we have:

$$\begin{aligned}
\sum_{i=1}^{n} B &= \sum_{i=1}^{n} F,\\
\sum_{i=1}^{n} C &= \sum_{i=1}^{n} G.
\end{aligned}$$

Then:

$$\begin{aligned}
&I(U^k; Z^n) - I(U^k; Y^n) = \sum_{i=1}^{n} I(U^k; Z_i | Y^{i-1}, \tilde{Z}^{i+1}) -\\
&\quad - \sum_{i=1}^{n} I(U^k; Y_i | Y^{i-1}, \tilde{Z}^{i+1})\\
&= nI(U^k; Z|V) - nI(U^k; Y|V), \quad (47)
\end{aligned}$$

where J is uniform r.v. with alphabet $\mathcal{J} = \{1, ..., n\}$, $Z = Z_J$, and $V = (Y^{i-1}, \tilde{Z}^{i+1}, J)$.

Due to $V \to W \to X \to Y \to Z$ Markov chain, where $W = (V, U^k)$, we can rewrite (47) as,

$$\begin{aligned}
&nI(W;Z|V) - nI(W;Y|V) = n[I(W;Z) - I(V;Z) -\\
&\quad - I(W;Y) + I(V;Y)]\\
&= n[I(X;Z) - I(X;Z|W) - I(V;Z) -\\
&\quad - I(X;Y) + I(X;Y|W) + I(V;Y)]\\
&\geq^{(48)} n[I(X;Z) - I(X;Y)]
\end{aligned}$$

where the last inequality holds since the channel is less noisy:

$$I(V;Y) \geq I(W;Z) \text{ and } I(X;Y|U^k) \geq I(X;Z|U^k) \quad (48)$$

The proof is complete.

REFERENCES

[1] Z. Qin, X. Tao, J. Lu, W. Tong, and G. Y. Li, "Semantic communications: Principles and challenges," 2022.

[2] D. Gündüz, Z. Qin, I. E. Aguerri, H. S. Dhillon, Z. Yang, A. Yener, K. K. Wong, and C.-B. Chae, "Beyond transmitting bits: Context, semantics, and task-oriented communications," *IEEE Journal on Selected Areas in Communications*, vol. 41, no. 1, pp. 5–41, 2023.

[3] T. M. Getu, G. Kaddoum, and M. Bennis, "A survey on goal-oriented semantic communication: Techniques, challenges, and future directions," *IEEE Access*, vol. 12, pp. 51 223–51 274, 2024.

[4] Z. Yang, M. Chen, G. Li, Y. Yang, and Z. Zhang, "Secure semantic communications: Fundamentals and challenges," 2023.

[5] J. Liu, S. Shao, W. Zhang, and H. V. Poor, "An indirect rate-distortion characterization for semantic sources: General model and the case of gaussian observation," 2022.

[6] J. Liu, W. Zhang, and H. V. Poor, "A rate-distortion framework for characterizing semantic information," in *2021 IEEE International Symposium on Information Theory (ISIT)*, 2021, pp. 2894–2899.

[7] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

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

[9] H. Yamamoto, "Rate-distortion theory for the shannon cipher system," *IEEE Transactions on Information Theory*, vol. 43, no. 3, pp. 827–835, 1997.

[10] N. Merhav, "Shannon's secrecy system with informed receivers and its application to systematic coding for wiretapped channels," in *2007 IEEE International Symposium on Information Theory*, 2007, pp. 2481–2485.

[11] J. Villard, P. Piantanida, and S. Shamai, "Secure transmission of sources over noisy channels with side information at the receivers," *IEEE Transactions on Information Theory*, vol. 60, no. 1, pp. 713–739, 2014.

[12] Y. E. Sagduyu, T. Erpek, S. Ulukus, and A. Yener, "Is semantic communication secure? a tale of multi-domain adversarial attacks," *IEEE Communications Magazine*, vol. 61, no. 11, pp. 50–55, 2023.

[13] M. Shen, J. Wang, H. Du, D. Niyato, X. Tang, J. Kang, Y. Ding, and L. Zhu, "Secure semantic communications: Challenges, approaches, and opportunities," *IEEE Network*, pp. 1–1, 2023.

[14] T.-Y. Tung and D. Gündüz, "Deep joint source-channel and encryption coding: Secure semantic communications," in *ICC 2023 - IEEE International Conference on Communications*, 2023, pp. 5620–5625.

[15] Q. Qin, Y. Rong, G. Nan, S. Wu, X. Zhang, Q. Cui, and X. Tao, "Securing semantic communications with physical-layer semantic encryption and obfuscation," 2023.

[16] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge University Press, 2011.

[17] A. Gamal and T. Cover, "Achievable rates for multiple descriptions," *IEEE Transactions on Information Theory*, vol. 28, no. 6, pp. 851–857, 1982.

[18] Y. Liang, H. V. Poor, and S. S. (Shitz), "Information theoretic security," *Foundations and Trends® in Communications and Information Theory*, vol. 5, no. 4–5, pp. 355–580, 2009. [Online]. Available: http://dx.doi.org/10.1561/0100000036