Mathematical Problems of Computer Science 65, 16–29, 2026.
doi:10.51408/1963-0143

UDC 519.72

Rate-Reliability-Distortion-Equivocation Tradeoffs for Source with Secret Component and Side Information

Jemma S. Santrosyan

Vanadzor State University, Vanadzor, Armenia
e-mail: j.santrosian@gmail.com

Abstract

We consider the lossy source coding problem for one-way sources with correlated outputs and side information available at both the encoder and decoder. In this scenario, one component of the source must be transmitted to the receiver within a prescribed distortion level, while the other component must remain as confidential as possible from the receiver or a potential wiretapper. To characterize this trade-off, we introduce and analyze the rate-reliability-distortion-equivocation (RRDE) function, as well as the corresponding equivocation-reliability-distortion and rate-reliability-distortion functions. The results provide a unified information-theoretic framework that captures the interplay between compression efficiency, reconstruction fidelity, reliability, and secrecy.

Keywords: Rate-reliability-distortion-equivocation function, Lossy source coding, Data compression, Source coding with side information, Rate-distortion theory.
Article info: Received 27 March 2026; sent for review 7 April 2026; accepted 27 April 2026.

1. Introduction

Lossy source coding (also known as lossy compression) is a fundamental concept in information theory that deals with representing a source (e.g., an image, audio signal, or text) using fewer bits than the original, allowing some distortion or loss of information that is acceptable according to a given fidelity criterion [1].

A central concept in the theory of lossy source coding is the rate-distortion (RD) function, which characterizes the minimum coding rate required to satisfy a prescribed average distortion constraint. The RD function captures the fundamental trade-off between compression efficiency and reconstruction fidelity: as the allowable distortion increases, the required rate decreases, whereas stricter fidelity requirements necessitate higher transmission rates. These theoretical foundations originate in Shannon's seminal work [1], and were later developed extensively through the classical contributions of Slepian and Wolf [2], Wyner [3], and Wyner-Ziv [4]. Classical image and audio compression standards such as JPEG and MP3 exemplify the practical importance of the rate-distortion trade-off.

The presence of side information, namely additional data correlated with the source and available at the encoder, the decoder, or both, substantially enriches the source coding problem. By exploiting the statistical dependencies between the source and the side information, one can achieve more efficient compression or improved reconstruction quality. Source coding models with side information have found widespread applications in modern systems, including distributed sensor networks, multimedia communications, cooperative and relay-based wireless networks, privacy-preserving data compression and storage, as well as machine learning applications such as federated learning and distributed inference.

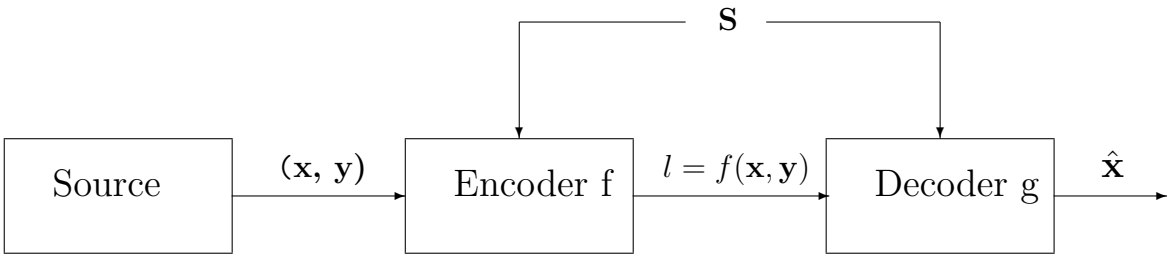

Fig. 1. One-way communication with correlated sources and common side information

Beyond the classical rate-distortion criterion, reliability plays an important role in source coding. Reliability quantifies the rate at which the decoding error probability decays as the block length increases. This leads to the notion of the rate-reliability-distortion (RRD) function, which describes the coding rate as a function of both the distortion level and a prescribed error exponent, or reliability parameter. This function has been investigated for various source models [5, 6].

In many practical scenarios, security is also a critical requirement. Security constraints arise when part of the source information must be protected from unintended receivers. This setting was first formalized by Yamamoto [7], who introduced the rate-distortion-equivocation (RDE) framework, where secrecy is measured via equivocation. In such models, one component of the source is reconstructed subject to distortion constraints, while another component is kept as uncertain as possible at the receiver. Subsequent research has extended this approach to cascade and branching communication systems, as well as to alternative security criteria based on distortion [8, 9, 10].

In our previous works, we studied the RRD and RDE functions. In particular, [11] analyzed the rate-reliability-distortion trade-off for correlated sources, while [12] introduced and investigated a secure source coding model in which secrecy is quantified using equivocation.

Building on these foundations and our previous work, this paper develops a unified framework that simultaneously accounts for rate, distortion, reliability, and secrecy. Specifically, we introduce the rate-reliability-distortion-equivocation (RRDE) function for a source coding model with a secret component and side information available at both the encoder and decoder. We characterize the set of achievable performance tuples and derive the corresponding equivocation-reliability-distortion and rate-reliability-distortion functions as special cases. This framework is particularly relevant for modern applications requiring secure and reliable data transmission, including distributed IoT networks, multimedia streaming with confidentiality constraints, secure communication protocols, and utility-privacy trade-off problems in data analysis [13]. By jointly accounting for side information, reliability, and secrecy, this work bridges classical source coding theory and contemporary challenges in secure communications.

The remainder of the paper is organized as follows. Section 2 introduces the main notations and definitions. The main results are presented in Section 3. The proofs are provided in the next section. Section 5 concludes the paper with a summary and discussion of possible extensions.

2. Notations and Definitions

The Discrete Memoryless Source (DMS) is defined as a sequence $\{(X_i, Y_i, S_i)\}_{i=1}^{\infty}$ of discrete independent identically distributed random variables (i. i. d.) X, Y, and S, taking values in finite sets $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{S}$, which are the source messages alphabets, respectively. Let

$$P^* = \{P^*(x, y, s), x \in \mathcal{X}, y \in \mathcal{Y}, s \in \mathcal{S}\}$$

be the generating probability distribution of the source outputs (X, Y, S). The source is memoryless, which means that for N-length vector pairs $\mathbf{x} = (x_1, x_2, ..., x_N) \in \mathcal{X}^N$,$\mathbf{y} = (y_1, y_2, ..., y_N) \in \mathcal{Y}^N$ and $\mathbf{s} = (s_1, s_2, ..., s_N) \in \mathcal{S}^N$

$$P^{*N}(\mathbf{x}, \mathbf{y}, \mathbf{s}) = \prod_{n=1}^{N} P^*(x, y, s).$$

The finite set $\hat{\mathcal{X}}$, different in general from $\mathcal{X}$, is the reproduction alphabet at the receiver. We will use the following distributions:

$$P = \{P(x, y, s) = P_0(s)P_1(x, y|s), x \in \mathcal{X}, y \in \mathcal{Y}, s \in \mathcal{S}\}$$

and the conditional distribution Q

$$Q = \{Q(\hat{x}|x, y, s), x \in \mathcal{X}, y \in \mathcal{Y}, \hat{x} \in \hat{X}, s \in \mathcal{S}\}.$$

A code (f_N, g_N) is defined by a pair of mappings: a coding

$$f_N : \mathcal{X}^N \times \mathcal{Y}^N \times \mathcal{S}^N \to \{1, 2, ..., L(N)\},$$

and decoding

$$g_N : \{1, 2, ..., L(N)\} \times \mathcal{S}^N \to \hat{\mathcal{X}},$$

where $L(N)$ is the code volume. Code rate is

$$R(f_N, g_N) = \frac{1}{N} \log L(N).$$

Throughout this paper, all log-s and exp-s are of base 2.

We consider the distortion measure

$$d : \mathcal{X} \times \hat{\mathcal{X}} \to [0; \infty)$$

between source and reconstruction messages. The distortion measure for N -length sequences is the average of the components' distortions

$$d(\mathbf{x}, \hat{\mathbf{x}}) = \frac{1}{N} \sum_{n=1}^{N} d(x, \hat{x}).$$

The task of this system is to ensure restoration of one of the components of source messages, i.e. X, at the receiver within a given distortion level Δ_d and with a small error probability in the case when the state sequence is available to both the encoder and the decoder. At the same time, the other source output Y should be kept as secret as possible from the receiver or wiretapper. This protection level is measured by the **equivocation rate**, defined as

$$R_e = \frac{1}{N} H(\mathbf{Y}|L(N), S),$$

where $H(\mathbf{Y}|L(N), S)$ is the conditional entropy [14]. In other words, the equivocation rate indicates the receiver's uncertainty about $\mathbf{y}$ given l and $\mathbf{s}$.

For the formulation of the result, we remind the following definitions [14].

The **entropy** of RV S is

$$H_{P_0}(S) = -\sum_{s\in\mathcal{S}} P_0(s)\log P_0(s).$$

The **conditional entropy** of RV X, Y relative to the random variable S is

$$H_P(X,Y|S) = -\sum_{x\in\mathcal{X},\, y\in\mathcal{Y},\, s\in\mathcal{S}} P(x,y,s)\log P_1(x,y|s).$$

The **conditional mutual information** of RV X, Y and $\hat{X}$ relative to the random variable S is

$$I_{P,Q}(X,Y;\hat{X}|S)$$

$$= \sum_{x\in\mathcal{X},\, y\in\mathcal{Y},\, \hat{x}\in\hat{\mathcal{X}},s\in\mathcal{S}} P(x,y,s)Q(\hat{x}|x,y,s)\log\frac{Q(\hat{x}|x,y,s)}{PQ(\hat{x}|s)},$$

where

$$PQ(\hat{x}|s) = \sum_{x\in\mathcal{X},y\in\mathcal{Y}} P_1(x,y|s)Q(\hat{x}|x,y,s).$$

The following property will be used below:

$$I_{P,Q}(X,Y;\hat{X}|S) = H_P(X,Y|S) - H_{P,Q}(X,Y|\hat{X},S).$$

The **Kullback-Leibler divergence** between the distributions P and P^* is defined as follows:

$$D(P||P^*) = \sum_{x\in\mathcal{X},y\in\mathcal{Y},s\in\mathcal{S}} P(x,y,s)\log\frac{P(x,y,s)}{P^*(x,y,s)}.$$

We define the **error probability** of the code (f_N, g_N) as

$$e(f_N, g_N, P^*, \Delta_d) = 1 - \min_{\mathbf{s}\in\mathcal{S}^N} P^{*N}(\mathcal{A}(\mathbf{s})),$$

where $\mathcal{A}(\mathbf{s})$ is the set of satisfactorily transmitted vectors for a given $\mathbf{s}$, which are reconstructed within the distortion constraint $\Delta_d \geq 0$:

$$\mathcal{A}(\mathbf{s}) = \{(\mathbf{x},\mathbf{y}) : g_N(f_N(\mathbf{x},\mathbf{y},\mathbf{s}),\mathbf{s}) = \hat{\mathbf{x}}, d(\mathbf{x},\hat{\mathbf{x}}) \leq \Delta_d\}.$$

Definition 1. The triple (R, Δ_d, Δ_e) is called E-achievable for given $P^*, E > 0, \Delta_d \geq 0, \Delta_e \geq 0$, if for every $\epsilon > 0, \delta > 0$, there exists a code (f_N, g_N) such that

$$\frac{1}{N} \log L(N) \leq R + \epsilon,$$

the error probability is exponentially small

$$e(f_N, g_N, P^*, \Delta_d) \leq \exp\{-N(E - \delta)\}$$

and the equivocation rate

$$R_e \geq \Delta_e - \epsilon.$$

We denote by $\mathcal{R}^*(E)$ the set of all **E-achievable triples**. We will consider the **distortion-equivocation E-achievable region**:

$$\mathcal{R}^*_{\Delta_d, \Delta_e}(E) = \{(\Delta_d, \Delta_e) : (R, \Delta_d, \Delta_e) \in \mathcal{R}^*(E) \text{ for some } R \geq 0\}.$$

Then the **RRDE function** is defined as

$$R^*(E, \Delta_d, \Delta_e) = \min_{(R, \Delta_d, \Delta_e) \in \mathcal{R}^*(E)} R.$$

At last, the **equivocation-reliability-distortion function** (ERD) is:

$$\Gamma^*(E, \Delta_d) = \max_{(\Delta_d, \Delta_e) \in \mathcal{R}^*_{\Delta_d, \Delta_e}(E)} \Delta_e.$$

3. Formulation of Results

Consider the following set of distributions P on $\mathcal{X} \times \mathcal{Y} \times \mathcal{S}$:

$$\alpha(E, P^*) = \{P : D(P||P^*) \leq E\}.$$

Let $\mathcal{Q}(P, \Delta_d, \Delta_e)$ be the set of all conditional PDs $Q_P(\hat{x}|x, y, s) = Q_P$, corresponding to the PD P, for which the following conditions hold:

$$\mathbf{E}d(X, \hat{X}) = \sum_{x,y,s,\hat{x}} P(x, y, s) Q_P(\hat{x}|x, y, s) d(x, \hat{x}) \leq \Delta_d, \tag{1}$$

$$H_{P,Q_P}(Y|\hat{X}, S) \geq \Delta_e.$$

Then

$$\mathcal{Q}(P, \Delta_d) = \bigcup_{H_{P,Q_P}(Y|X,S) \leq \Delta_e \leq H_{P,Q_P}(Y|S)} \mathcal{Q}(P, \Delta_d, \Delta_e).$$

The main result of this paper is presented in the following theorem.

Theorem 1. *For given source distribution P^*, every $E > 0$,*

$$\mathcal{R}^*(E) = \left\{ \begin{array}{l} (R, \Delta_d, \Delta_e) : \Delta_d \geq 0, \Delta_e \geq 0, \\ \\ 0 \leq R_e \leq \min\limits_{P \in \alpha(E, P^*)} \max\limits_{Q_P \in \mathcal{Q}(P, \Delta_d)} H_{P,Q_P}(Y, |\hat{X}, S), \\ \\ R \geq \max\limits_{P \in \alpha(E, P^*)} \min\limits_{Q_P \in \mathcal{Q}(P, \Delta_d, \Delta_e)} I_{P,Q_P}(X, Y; \hat{X}|S) \end{array} \right\}.$$

This result characterizes the fundamental trade-off between rate, distortion, reliability, and secrecy in the presence of side information. The proof is given in the Appendix, based on the method of types [15].

Corollary 2. *The ERD function equals*

$$\Gamma^*(E,\Delta_d)=\min_{P\in\alpha(E,P^*)}\max_{Q_P\in\mathcal{Q}(P,\Delta_d)}H_{P,Q_P}(Y|\hat{X},S).$$

Corollary 3.

$$\mathcal{R}^*_{\Delta_d,\Delta_e}(E)=\left\{\begin{array}{l} R(E,\Delta_d,\Delta_e):\Delta_d\geq 0,\\ \\ 0\leq\Delta_e\leq\Gamma^*(E,\Delta_d)\end{array}\right\}.$$

Corollary 4. *The RRDE function equals*

$$R^*(E,\Delta_d,\Delta_e)=\max_{P\in\alpha(E,P^*)}\min_{Q_P\in\mathcal{Q}(P,\Delta_d,\Delta_e)}I_{P,Q_P}(X,Y;\hat{X}|S).$$

Corollary 5. *The limits of the RRDE and ERD functions when E tends to 0, coincide with the RDR and ED functions stated in [7]:*

$$\lim_{E\to 0}R^*(E,\Delta_d,\Delta_e)=R^*(\Delta_d,\Delta_e)=\min_{Q^*_P\in\mathcal{Q}(P^*,\Delta_d,\Delta_e)}I_{P^*,Q^*_P}(X,Y;\hat{X}|S).$$

$$\lim_{E\to 0}\Gamma^*(E,\Delta_d)=\Gamma^*(\Delta_d)=\max_{Q_{P^*}\in\mathcal{Q}(P^*,\Delta_d)}H_{P^*,Q_{P^*}}(Y|\hat{X},S).$$

Corollary 6. *In the absence of a secret component, the achievable region coincides with [12]*

$$\mathcal{R}^*(E)=\left\{\begin{array}{l}(R,\Delta_d,\Delta_e):\Delta_d\geq 0,\Delta_e\geq 0,\\ \\ 0\leq R_e\leq\min\limits_{P\in\alpha(E,P^*)}\max\limits_{Q_P\in\mathcal{Q}(P,\Delta_d)}H_{P,Q_P}(Y|\hat{X}),\\ \\ R\geq\max\limits_{P\in\alpha(E,P^*)}\min\limits_{Q_P\in\mathcal{Q}(P,\Delta_d,\Delta_e)}I_{P,Q_P}(X,Y;\hat{X})\end{array}\right\}.$$

Corollary 7. *In the absence of side information at the decoder the result reduces to [11]*

$$R(E,\Delta,P^*)=\max_{P\in\alpha(E,P^*)}\min_{Q_P\in\mathcal{Q}(P,\Delta)}I_{P,Q_P}(X;\hat{X}|S).$$

For the proof of Theorem 1, we will use the following modification of the Covering Lemma [16], [5].

Lemma 1. *Let for $\epsilon>0$*

$$J(P,Q)=\exp\{N(I_{P,Q}(X,Y;\hat{X}|S)+\epsilon)\}.$$

Then, for every type P_0 state sequence $\mathbf{s}\in\mathcal{T}^N_{P_0}(S)$, conditional types P_1 and Q, there exists a collection of vectors

$$\{\hat{\mathbf{x}}_j\in\mathcal{T}^N_{P,Q}(\hat{X}|\mathbf{s}),j=1,...,J(P,Q)\},$$

such that the set

$$\{\mathcal{T}^N_{P,Q}(X,Y|\hat{\mathbf{x}}_j,\mathbf{s}),j=1,...,J(P,Q)\},$$

covers $\mathcal{T}^N_P(X,Y|\mathbf{s})$ for N large enough, that is

$$\mathcal{T}^N_P(X,Y|\mathbf{s})\subset\bigcup_{j=1}^{J(P,Q)}\mathcal{T}^N_{P,Q}(X,Y|\hat{\mathbf{x}}_j,\mathbf{s}).$$

4. Proof of Theorem 1

The proof of Theorem 1 consists of two parts: achievability (direct part) and converse (inverse part).

4.1 Achievability

First we shall prove that any triple (R, Δ_d, Δ_e) satisfying the conditions of Theorem 1 is E-achievable or that

$$\mathcal{R}^*(E) \supseteq \left\{ \begin{array}{l} (R, \Delta_d, \Delta_e) : \Delta_d \geq 0, \Delta_e \geq 0, \\ \\ 0 \leq R_e \leq \min\limits_{P \in \alpha(E,P^*)} \max\limits_{Q_P \in \mathcal{Q}(P,\Delta_d)} H_{P,Q_P}(Y|\hat{X}, S), \\ \\ R \geq \max\limits_{P \in \alpha(E,P^*)} \min\limits_{Q_P \in \mathcal{Q}(P,\Delta_d,\Delta_e)} I_{P,Q_P}(X, Y; \hat{X}|S) \end{array} \right\}.$$

Step 1: Type Partitioning

Let us represent the set of all source messages of length N as follows:

$$\mathcal{X}^N \times \mathcal{Y}^N \times \mathcal{S}^N = \bigcup_{P \in \mathcal{P}^N(X \times Y \times S)} \mathcal{T}_P^N(X, Y, S) = \bigcup_{P_0 \in \mathcal{P}^N(S)} \bigcup_{P_1 \in \mathcal{P}^N(X \times Y, P_0)} \mathcal{T}_P^N(X, Y, S),$$

where $\mathcal{P}^N(X \times Y \times S)$ is the set of possible types P of triples $(\mathbf{x}, \mathbf{y}, \mathbf{s}) \in \mathcal{X}^{\mathbf{N}} \times \mathcal{Y}^{\mathbf{N}} \times \mathcal{S}^{\mathbf{N}}$, $\mathcal{P}^{\mathbf{N}}(\mathbf{S})$ is the set of possible types P_0 of vectors $\mathbf{s} \in \mathcal{S}$, $\mathcal{P}^N(X \times Y, P_0)$ is the set of conditional types P_1 of pairs $(\mathbf{x}, \mathbf{y}) \in \mathcal{X}^{\mathbf{N}} \times \mathcal{Y}^{\mathbf{N}}$, for given P_0.

Using the properties of types and the definition of the set $\alpha(E, P^*)$ for each $\delta > 0$, the probability of observing sequences with types outside $\alpha(E + \delta, P^*)$ satisfies:

$$\begin{aligned} P^{*N}\left(\bigcup_{P \notin \alpha(E+\delta,P^*)} \mathcal{T}_P^N(X, Y, S) \right) &= \sum_{P \notin \alpha(E+\delta,P^*)} P^{*N}\left(\mathcal{T}_P^N(X, Y, S) \right) \\ &\leq (N+1)^{|\mathcal{X}||\mathcal{Y}||\mathcal{S}|} \exp\left\{ -N \min_{P \notin \alpha(E+\delta,P^*)} D(P||P*) \right\} \quad (2) \\ &\leq \exp\left\{ -NE - N\delta + |\mathcal{X}||\mathcal{Y}||\mathcal{S}| \log(N+1) \right\} \\ &\leq \exp\left\{ -N(E + \delta/2) \right\}, \end{aligned}$$

for sufficiently large N.

Step 2: Code Construction

For each $\Delta_d \geq 0$, fix type $P \in \alpha(E + \delta, P^*)$ and some $Q_P \in \mathcal{Q}(P, \Delta_d, \Delta_e)$. Let for each $\mathbf{s} \in \mathcal{T}_{P_0}^N(S)$

$$C(P, Q_P, j, \mathbf{s}) = \mathcal{T}_{P,Q_P}^N(X, Y|\hat{\mathbf{x}}_j, \mathbf{s}) - \bigcup_{j' < j} \mathcal{T}_{P,Q_P}^N(X, Y|\hat{\mathbf{x}}_{j'}, \mathbf{s}), \quad j = \overline{1, J(P, Q_P)}.$$

Define a code (f_N, g_N) for each $\mathbf{s} \in \mathcal{T}_{P_0}^N(S)$ and vector pairs of conditional type P_1 with encoding as:

$$f_N(\mathbf{x}, \mathbf{y}|\mathbf{s}) = \left\{ \begin{array}{l} j, \ \text{ when } (\mathbf{x}, \mathbf{y}) \in C(P, Q_P, j, \mathbf{s}), \ P \in \alpha(E + \delta, P^*), \\ \\ j_0, \ \text{ when } (\mathbf{x}, \mathbf{y}) \in \mathcal{T}_P^N(X, Y|\mathbf{s}), \ P \notin \alpha(E + \delta, P^*), \end{array} \right.$$

and decoding

$$g_N(j|\mathbf{s}) = \hat{\mathbf{x}}_j, \qquad g_N(j_0|\mathbf{s}) = \hat{\mathbf{x}}_0,$$

where the number j_0 and the reconstruction vector $\hat{\mathbf{x}}_0$ are fixed. Obviously, with such a code, an error occurs only when the number j_0 is sent.

Step 3: Distortion Constraint

According to the definition of the code and the inequality (1), for $P \in \alpha(E+\delta, P^*)$ and $Q_P \in \mathcal{Q}(P, \Delta_d, \Delta_e)$ we have:

$$\begin{aligned} d(\mathbf{x}, \hat{\mathbf{x}}_\mathbf{j}) &= \sum_{x,y,\hat{x},s} P(x,y,s) Q_P(\hat{x}|x,y,s) d(x,\hat{x}) \\ &= \mathbf{E}_{P,Q_P} d(X,\hat{X}) \le \Delta_d, \quad j = \overline{1, J(P,Q_P)}, \end{aligned}$$

which ensures that the distortion constraint is satisfied.

Step 4: Rate Analysis

According to Lemma 1, the number of vectors $\hat{\mathbf{x}}$, each $\mathbf{s}$ for type P and corresponding conditional type $Q_P \in \mathcal{Q}(P, \Delta_d, \Delta_e)$ is:

$$L_{P,Q_P}(N) = \exp\left\{N(I_{P,Q_P}(X,Y;\hat{X}|S) + \epsilon)\right\}.$$

Then, taking into account that the number of types has a polynomial estimate [15]

$$\begin{aligned} L(N) &\le \sum_{P \in \alpha(E+\delta,P^*)} \min_{Q_P \in \mathcal{Q}(P,\Delta_d,\Delta_e)} L_{P,Q_P}(N) \\ &\le (N+1)^{|\mathcal{X}||\mathcal{Y}||\mathcal{S}|} \max_{P \in \alpha(E+\delta,P^*)} \min_{Q_P \in \mathcal{Q}(P,\Delta_d,\Delta_e)} \exp\left\{N(I_{P,Q_P}(X,Y;\hat{X}|S) + \epsilon)\right\}. \end{aligned}$$

Hence, the corresponding limit for the transmission rate is:

$$\begin{aligned} &\frac{1}{N}\log L_{P,Q_P}(N) - \epsilon - \frac{1}{N}|\mathcal{X}||\mathcal{Y}||\mathcal{S}|\log(N+1) \\ &\le \max_{P \in \alpha(E+\delta,P^*)} \min_{Q_P \in \mathcal{Q}(P,\Delta_d,\Delta_e)} I_{P,Q_P}(X,Y;\hat{X}|S). \end{aligned} \tag{3}$$

Taking into account the arbitrariness of ϵ and δ and the continuity of the information expression (3), we get:

$$R^*(E,\Delta_d,\Delta_e) \le \max_{P \in \alpha(E,P^*)} \min_{Q_P \in \mathcal{Q}(P,\Delta_d,\Delta_e)} I_{P,Q_P}(X,Y;\hat{X}|S). \tag{4}$$

Step 5: Equivocation Analysis

Using type properties and entropy bounds, for this code the equivocation rate can be evaluated as follows:

$$\begin{aligned} &\frac{1}{N} H(\mathbf{Y}|L(N),S) \\ &\ge \sum_{\mathbf{s}} P_0(\mathbf{s}) \frac{1}{N} \sum_{j=1}^{L(N)} H_{P^*,Q_{P^*}}(Y|(\mathbf{x},\mathbf{y}) \in C(P,Q_P,j,\mathbf{s}))) P^*\{(\mathbf{x},\mathbf{y}) \in C(P,Q_P,j,\mathbf{s})\} \\ &= \sum_{\mathbf{s}} P_0(\mathbf{s}) \frac{1}{N} \sum_{j=1}^{L(N)} \end{aligned} \tag{5}$$

$$\left[-\sum_{\mathbf{y}:\mathbf{x},\mathbf{y}\in C(P,Q_P,j,\mathbf{s})} P^*\{\mathbf{y}|(\mathbf{x},\mathbf{y})\in C(P,Q_P,j,\mathbf{s})\}\log P^*\{\mathbf{y}|(\mathbf{x},\mathbf{y})\in C(P,Q_P,j,\mathbf{s})\}\right]$$
$$\times P^*\{(\mathbf{x},\mathbf{y})\in C(P,Q_P,j,\mathbf{s})\}.$$

For any $\mathbf{y}$ such that $\mathbf{x},\mathbf{y}\in C(P,Q_P,j,\mathbf{s})$ for some $\mathbf{x}$

$$P^*\{\mathbf{y}|(\mathbf{x},\mathbf{y})\in C(P,Q_P,j,\mathbf{s})\} = \frac{P^*\{(\mathbf{x},\mathbf{y})\in C(P,Q_P,j,\mathbf{s})|\mathbf{y}\}P^*\{\mathbf{y}\}}{P^*\{(\mathbf{x},\mathbf{y})\in C(P,Q_P,j,\mathbf{s})\}}$$

$$= \frac{\sum\limits_{(\mathbf{x},\mathbf{y})\in C(P,Q_P,j,\mathbf{s})} P^*\{\mathbf{x},\mathbf{y}|\mathbf{y},\mathbf{s}\}P^*\{\mathbf{y}\}}{\sum\limits_{(\mathbf{x},\mathbf{y})\in C(P,Q_P,j,\mathbf{s})} P^*\{\mathbf{x},\mathbf{y}|\mathbf{s}\}} \le \frac{\sum\limits_{\mathbf{x}\in\mathcal{T}^N_{P,Q_P}(X|\mathbf{y},\hat{\mathbf{x}}_j,\mathbf{s})} P^*\{\mathbf{x}|\mathbf{y},\mathbf{s}\}P^*\{\mathbf{y}\}}{\sum\limits_{(\mathbf{x},\mathbf{y})\in C(P,Q_P,j,\mathbf{s})} P^*\{\mathbf{x},\mathbf{y}|\mathbf{s}\}}. \quad (6)$$

As the probability of the pair $(\mathbf{x},\mathbf{y})$ is constant within the same type, from (6) we obtain that

$$P^*\{\mathbf{y}|(\mathbf{x},\mathbf{y})\in C(P,Q_P,j,\mathbf{s})\} \le \frac{|\mathcal{T}^N_{P,Q_P}(X|\mathbf{y},\hat{\mathbf{x}}_j,\mathbf{s})|}{|C(P,Q_P,j,\mathbf{s})|}$$

$$\le \frac{\exp[N(H_{P,Q_P}(X|Y,\hat{X},S)]}{(N+1)^{|\mathcal{X}||\mathcal{Y}||\mathcal{S}|}\exp[N(H_{P,Q_P}(X,Y|\hat{X},S)]} \le \exp[-N(H_{P,Q_P}(Y|\hat{X},S)-\epsilon)]. \quad (7)$$

Then, from (5), (7) and (2) we obtain that

$$\frac{1}{N}H(\mathbf{Y}|L(N),S)$$

$$\ge \sum_{\mathbf{s}} P_0(\mathbf{s})\frac{1}{N}\sum_{j=1}^{L(N)}\left[N\sum_{\mathbf{y}:(\mathbf{x},\mathbf{y})\in C(P,Q_P,j,\mathbf{s})} P^*\{\mathbf{y}|(\mathbf{x},\mathbf{y})\in C(P,Q_P,j,\mathbf{s})\}(H_{P,Q_P}(Y|\hat{X},S)-\epsilon)\right]$$
$$\times P^*\{(\mathbf{x},\mathbf{y})\in C(P,Q_P,j,\mathbf{s})\}$$
$$= \sum_{\mathbf{s}} P_0(\mathbf{s})P^*\{(\mathbf{x},\mathbf{y})\in \bigcup_{j=1}^{L(N)} C(P,Q_P,j,\mathbf{s})\}(H_{P,Q_P}(Y|\hat{X},S)-\epsilon)$$
$$\ge (1-\exp\{-N(E+\delta/2)\})(H_{P,Q_P}(Y|\hat{X},S)-\epsilon).$$

For N large enough, we obtain that

$$R_e \ge H_{P,Q_P}(Y|\hat{X},S)-\epsilon \ge \Delta_e-\epsilon. \quad (8)$$

According to (2), (4) and (8), we state that the triple (R,Δ_d,Δ_e) is E-achievable.

4.2 Converse

Now we show that any E-achievable triple satisfies:

$$\mathcal{R}^*(E)\subseteq\left\{\begin{array}{l}(R,\Delta_d,\Delta_e):\Delta_d\ge 0,\Delta_e\ge 0,\\ \\ 0\le R_e\le \min\limits_{P\in\alpha(E,P^*)}\max\limits_{Q_P\in\mathcal{Q}(P,\Delta_d)} H_{P,Q_P}(Y|\hat{X},S),\\ \\ R\ge \max\limits_{P\in\alpha(E,P^*)}\min\limits_{Q_P\in\mathcal{Q}(P,\Delta_d,\Delta_e)} I_{P,Q_P}(X,Y;\hat{X}|S)\end{array}\right\}.$$

Step 1: Setup

Let $\epsilon > 0$ be fixed. Consider a code (f_N, g_N) for each blocklength N with (R, Δ_d, Δ_e) E-achievable triple. We must show that for some $Q_P \in \mathcal{Q}(P, \Delta_d, \Delta_e)$ the following inequalities hold for N large enough:

$$\frac{1}{N}\log L(N) + \epsilon \geq \max_{P\in\alpha(E,P^*)} I_{P,Q_P}(X,Y;\hat{X}|S), \tag{9}$$

$$\frac{1}{N}H(\mathbf{Y}|L(N),S) - \epsilon \leq \min_{P\in\alpha(E,P^*)} H_{P,Q_P}(Y|\hat{X},S). \tag{10}$$

Step 2: Size of Typical Sets

Let $\mathcal{A}'(\mathbf{s})$ be the complement of the set $\mathcal{A}(\mathbf{s})$. The following statement is true:

$$\left|\mathcal{A}(\mathbf{s})\bigcap\mathcal{T}_P^N(X,Y|\mathbf{s})\right| = \left|\mathcal{T}_P^N(X,Y|\mathbf{s})\right| - \left|\mathcal{A}'(\mathbf{s})\bigcap\mathcal{T}_P^N(X,Y|\mathbf{s})\right|.$$

For $P \in \alpha(E-\epsilon, P^*)$

$$\begin{aligned}\left|\mathcal{A}'(\mathbf{s})\bigcap\mathcal{T}_P^N(X,Y|\mathbf{s})\right| &= \frac{P^{*N}\left\{\mathcal{A}'(\mathbf{s})\bigcap\mathcal{T}_P^N(X,Y|\mathbf{s})\right\}}{P^{*N}(\mathbf{x},\mathbf{y}|\mathbf{s})}\\ &\leq \exp\left\{N(H_P(X,Y|S)+D(P||P^*))\right\}\exp\left\{-N(E-\epsilon)\right\}\\ &\leq \exp\left\{N(H_P(X,Y|S)-\epsilon)\right\}.\end{aligned}$$

Hence,

$$\begin{aligned}\left|\mathcal{A}(\mathbf{s})\bigcap\mathcal{T}_P^N(X,Y|\mathbf{s})\right| &\geq (N+1)^{-|\mathcal{X}||\mathcal{Y}||\mathcal{S}|}\exp\left\{NH_P(X,Y|S)\right\} - \exp\left\{N(H_P(X,Y|S)-\epsilon)\right\}\\ &= \exp\left\{N(H_P(X,Y|S)-\epsilon)\right\}\left(\frac{\exp\{N\epsilon\}}{(N+1)^{|\mathcal{X}||\mathcal{Y}||\mathcal{S}|}}-1\right) \qquad (11)\\ &\geq \exp\left\{N(H_P(X,Y|S)-\epsilon)\right\}.\end{aligned}$$

For each $\mathbf{s}\in\mathcal{T}_{P_0}^N(S)$ and $\mathbf{x},\mathbf{y}\in\mathcal{A}(\mathbf{s})\bigcap\mathcal{T}_P^N(X,Y|\mathbf{s})$ corresponds a unique vector $\hat{\mathbf{x}}$ such that

$$\hat{\mathbf{x}} = g_N(f_N(\mathbf{x},\mathbf{y}|\mathbf{s}),\mathbf{s}) \ \text{ and } \ \hat{\mathbf{x}}\in\mathcal{T}_{P,Q}^N(\hat{X}|\mathbf{x},\mathbf{y},\mathbf{s}).$$

Step 3: Conditional Type Decomposition

Let us divide the set of all vectors $\left|\mathcal{A}(\mathbf{s})\bigcap\mathcal{T}_P^N(X,Y|\mathbf{s})\right|$ into subsets by conditional types Q_P. The class having maximum cardinality for given P, we denote by

$$\left(\left|\mathcal{A}(\mathbf{s})\bigcap\mathcal{T}_P^N(X,Y|\mathbf{s})\right|\right)_{Q_P}.$$

According to the number of conditional types Q, for sufficiently large N, we have:

$$\begin{aligned}\left|\mathcal{A}(\mathbf{s})\bigcap\mathcal{T}_P^N(X,Y|\mathbf{s})\right| &\leq (N+1)^{|\mathcal{X}||\mathcal{Y}||\mathcal{S}|}\left(\left|\mathcal{A}(\mathbf{s})\bigcap\mathcal{T}_P^N(X,Y|\mathbf{s})\right|\right)_{Q_P}\\ &\leq \exp\{N\epsilon/2\}\left(\left|\mathcal{A}(\mathbf{s})\bigcap\mathcal{T}_P^N(X,Y|\mathbf{s})\right|\right)_{Q_P}. \qquad (12)\end{aligned}$$

Let

$$\mathcal{D}(\mathbf{s}) = \left\{\hat{\mathbf{x}} : g_N(f_N(\mathbf{x},\mathbf{y}|\mathbf{s}),\mathbf{s}) = \hat{\mathbf{x}}, \text{for some } (\mathbf{x},\mathbf{y})\in\mathcal{A}(\mathbf{s})\bigcap\mathcal{T}_P^N(X,Y|\mathbf{s})\bigcap\mathcal{T}_{P,Q_P}^N(X,Y|\hat{\mathbf{x}},\mathbf{s})\right\}.$$

From the definition of the code $|\mathcal{D}(\mathbf{s})| \leq L(N)$, then

$$\begin{aligned}\left|\left(\mathcal{A}(\mathbf{s})\bigcap\mathcal{T}_P^N(X,Y|\mathbf{s})\right)\right|_{Q_P} &\leq \sum_{\hat{\mathbf{x}}\in\mathcal{D}(\mathbf{s})}\left|\mathcal{T}_{P,Q}^N(X,Y|\hat{\mathbf{x}},\mathbf{s})\right| \\ &\leq L(N)\exp\{NH_{P,Q_P}(X,Y|\hat{X},S)\}. \end{aligned} \tag{13}$$

Step 4: Lower Bound on Rate
From (11-13) follows

$$L(N) \geq \exp\{N(I_{P,Q_P}(X,Y;\hat{X}|S)-\epsilon)\}$$

for each $P \in \alpha(E-\epsilon, P*)$ and some Q_P for which $\mathbf{E}_{P,Q_P}d(X,\hat{X}) \leq \Delta_d$, because $\mathbf{x},\mathbf{y} \in \mathcal{A}(\mathbf{s})$.

Step 5: Equivocation Upper Bound
From the achievability it follows that

$$\Delta_e - \epsilon \leq \frac{1}{N}H(\mathbf{Y}|L(N),S) \leq H_{P,Q_P}(Y|\hat{X},S).$$

Thus, $Q_P \in \mathcal{Q}(P,\Delta_d,\Delta_e)$ and inequalities (9) and (10) are valid. The Achievable triples must satisfy the same constraints as in Theorem 1, completing the proof of Converse part.

Theorem 1 is proved.

5. Conclusion

In this paper, we developed a unified information-theoretic framework for lossy source coding with side information, incorporating reliability and secrecy constraints. We introduced the notion of E-achievable triples and derived a complete characterization of the rate-reliability-distortion-equivocation (RRDE) region.

The obtained results explicitly quantify the interplay between compression efficiency, reconstruction fidelity, decoding reliability, and confidentiality. In particular, we derived closed-form expressions for the RRDE and ERD functions and demonstrated that they naturally generalize classical rate-distortion and rate-distortion-equivocation results.

The proposed framework is well-suited for modern applications involving secure and reliable data transmission, such as distributed sensing systems, privacy-preserving data compression, and communication networks with confidentiality constraints.

Future work may include extensions to multi-user scenarios, continuous alphabets, and alternative secrecy measures such as strong secrecy or semantic security.

References

[1] C. E. Shannon, "Coding theorems for a discrete source with a fidelity criterion", *IRE National Convention Record*, vol. 7, pp.142–163, 1959.

[2] D. Slepyan and J. K. Wolf, "Noiseless coding of correlated information sources", *IEEE Transactions on Information Theory*, vol. 19, no.6, pp. 471 – 480, 1973.

[3] A. D. Wyner, "On source coding with side information at the decoder", *IEEE Transactions on Information Theory*, vol. 21, no. 5, pp. 294 – 300, 1975.

[4] A. D. Wyner and J.Ziv, "The rate distortion function for source coding with side information at the decoder", *IEEE Transactions on Information Theory*, vol. 22, no. 1, pp. 1 – 10, 1976.

[5] E. Haroutunian, M. Haroutunian and A. Harutyunyan, "Reliability Criteria in Information Theory and in Statistical Hypothesis Testing", *Foundations and Trends in Communications and Information Theory*, vol. 4, nos 2-3, pp. 97–263, 2007. doi: 10.1561/0100000008

[6] E. A. Haroutunian, A. N. Harutyunyan and A. R. Ghazaryan, "On rate-reliability-distortion function for a robust descriptions system", *IEEE Transactions on Information Theory*, vol. 46, no. 7, pp. 2690-2697, Nov. 2000, doi: 10.1109/18.887883.

[7] H. Yamamoto, "A source coding problem for sources with additional outputs to keep secret from the receiver or wiretappers", *IEEE Transactions on Information Theory*, vol. 29, no. 6, pp. 918–923, 1983.

[8] H. Yamamoto, "Source coding theory for cascade and branching communication systems", *IEEE Transactions on Information Theory*, vol. 27, no. 3, pp. 299–308, 1981.

[9] H. Yamamoto, "A rate-distortion problem for a communication system with a secondary decoder to be hindered", *IEEE Transactions on Information Theory*, vol. 34, no. 4, pp. 835–842, 1988.

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

[11] M. E. Haroutunian, J. S. Santrosyan and P. M. Hakobyan "Reliability criteria in source coding problem with secret component", *Mathematical Problems of Computer Science*, vol. 63, pp. 1424, 2025. doi:10.51408/1963-0128.

[12] M. Haroutunian, P. Hakobyan and J. Santrosyan, "Rate-reliability-distortion function for source with side information known to encoder and decoder", *Proceedings International Conference on Computer Science and Information Technologies*, pp. 155–158, 2025. doi: 10.51408/csit2025_38.

[13] L. Sankar, S. R. Rajagopalan and H. V. Poor, "Utility-privacy tradeoffs in databases: an information-theoretic approach", *IEEE Transactions on Information Theory*, vol. 8, no. 6, pp. 838–852, 2013.

[14] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Second Edition. Wiley, New York, 2006.

[15] I. Csiszár, "Method of types", *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2505-2523, 1998.

[16] I. Csiszár and J.Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, Academic Press, New York, 1981.

Գաղտնի բաղադրիչ և կողմնակի տեղեկատվություն ունեցող աղբյուրների համար արագություն–հուսալիություն–շեղում–անորոշություն փոխզիջումների տեսական ուսումնասիրություն

Ջեմմա Ս. Սանթրոսյան

Վանաձորի պետական համալսարան, Վանաձոր, Հայաստան
e-mail: j.santrosian@gmail.com

Ամփոփում

Մենք դիտարկում ենք կորուստներով աղբյուրի կոդավորման խնդիրը փոխկապակցված ելքերով միակողմանի աղբյուրների համար, որտեղ կողմնակի ինֆորմացիան հասանելի է թե՛ կոդավորիչին, թե՛ ապակոդավորիչին: Այս սցենարում աղբյուրի բաղադրիչներից մեկը պետք է փոխանցվի հասցեատիրոջը՝ շեղման սահմանված մակարդակի շրջանակներում, մինչդեռ մյուս բաղադրիչը պետք է առավելագույնս գաղտնի մնա հասցեատիրոջից կամ հնարավոր գաղտնալսողից: Այս փոխզիջումը բնութագրելու համար մենք ներմուծում և վերլուծում ենք հաղորդման արագություն-հուսալիություն-շեղում-անորոշություն ֆունկցիան, ինչպես նաև համապատասխան անորոշություն-հուսալիություն-շեղում և արագություն-հուսալիություն-շեղում ֆունկցիաները: Արդյունքները տրամադրում են միասնական ինֆորմացիոն-տեսական հիմք, որն արտացոլում է սեղմման արդյունավետության, վերականգնման ճշգրտության, հուսալիության և գաղտնիության փոխազդեցությունը:

Բանալի բառեր՝ արագություն-հուսալիություն-շեղում-անորոշություն ֆունկցիա, կորուստներով աղբյուրի կոդավորում, տվյալների սեղմում, կողմնակի ինֆորմացիայով աղբյուրի կոդավորում, արագություն-շեղում տեսություն:

Исследование компромиссов между скоростью, надежностью, искажением и неопределённостью для источников с секретной компонентой и побочной информацией

Джемма С. Сантросян

Ванадзорский государственный университет, Ванадзор, Армения
e-mail: j.santrosian@gmail.com

Аннотация

В данной работе рассматривается задача кодирования источника с потерями для односторонних источников с коррелированными выходами при наличии побочной информации как на кодере, так и на декодере. В данном сценарии один компонент источника должен быть передан получателю с соблюдением заданного уровня искажения, в то время как другой компонент должен оставаться максимально конфиденциальным для получателя или потенциального перехватчика. Для количественной характеристики данного компромисса вводится и анализируется функция скорость-надежность-искажение-неопределенность, а также соответствующие функции неопределенность-надежность-искажение и скорость-надежность-искажение. Полученные результаты представляют собой единую информационно-теоретическую базу, описывающую взаимосвязь между эффективностью сжатия, точностью восстановления, надежностью и секретностью.

Ключевые слова: функция скорость-надежность-искажение-неопределенность, кодирование источника с потерями, сжатие данных, кодирование источника с побочной информацией, теория скорость-искажение.