Gaussian Dirty Paper Coding with Gaussian Dirty State Informations

Çağatay Dikici [a], M. Kıvanç Mıhçak [b], Suleyman S. Kozat [c,*]

[a] *Laboratoire des Signaux et Systemes, CNRS - SUPELEC Gif-sur-Yvette, 91192, France*

[b] *Electrical and Electronic Engineering Department of Boğaziçi University, Istanbul, 34342, Turkey*

[c] *Department of ECE, Koc University, Istanbul, 34450, Turkey Tel: 90 212 3381540*

Abstract

This paper considers a channel coding problem that models certain privacy-driven data hiding and semi-blind watermarking scenarios. Here, the alphabet is the real line and imperfect versions of the channel state which can model either the unmarked host or the information about the unmarked host are available to the (watermark) encoder and (watermark) decoder with an expected power constraint on the output of the encoder. We first present the general case capacity result for a memoryless channel with known statistics. Then, we specialize to the Gaussian channel case, where the "dirt" (imperfection) on the channel state is modeled as additive white Gaussian noise, and present closed-form single-letter capacity results together with asymptotic cases of interest. Applications of the proposed scheme also include communications with partially known interference.

Key words: Data hiding, watermarking, privacy-driven, dirty paper coding, capacity, Gaussian channel coding with Gaussian dirty state information, channel coding with side information.

* Corresponding author.
Email addresses: dikici@lss.supelec.fr (Çağatay Dikici), kivanc.mihcak@boun.edu.tr (M. Kıvanç Mıhçak), skozat@ku.edu.tr (Suleyman S. Kozat).

1 Introduction

We consider the channel coding problem with asymmetric "dirty" side information about the channel state at the transmitter and the receiver in the presence of a fixed channel and an expected cost (distortion) constraint imposed on the encoder in order to model certain privacy-driven data hiding and semi-blind watermarking scenarios. The transmitter (encoder) sends a message by using the available noisy channel state information and the receiver (decoder) decodes this message by using another noisy channel state information and the channel output; both the transmitter and the receiver know the joint distribution triplet of the original channel state information, the encoder-side noisy channel state information and the decoder-side noisy channel state information. Depending on the application, the channel state information can represent either the unmarked host or information correlated with the unmarked host as explained in Section 2. In the first part of the paper, we consider the case where the alphabet for all variables of interest is the real line and present the maximum rate of reliable communications under some mild technical assumptions and the aforementioned distortion constraint; this can be viewed as an extension of a special case of one of the results provided in [1]. In the second part of the paper, we confine ourselves to the Gaussian case where an expected squared error distortion constraint is imposed on the encoder and the original channel state information is assumed to be additive white Gaussian noise (AWGN) with a known power; furthermore both the encoder-side and the decoder-side noisy state information are produced from the original channel state via applying two independent AWGN sequences to it. In this case, closed-form single-letter capacity expressions are derived together with an analysis of the asymptotic cases of interest. As such, the framework studied in this paper provides *the fundamental theoretical limits* for three potential application scenarios, which are further elaborated in Section 2, as:

- A Gaussian data hiding scheme where the host data can be interpreted as the state information. The content owner, who does not know how to do watermark encoding/decoding, uses third parties for watermarking; and shares different noisy versions of the host signal with the encoder and the decoder for privacy reasons.

- A Gaussian semi-blind watermarking system where the host data can be interpreted as the noisy version of the state information and the watermark decoder has access to side information that is not equal to the host but a quantity that is correlated with it. Furthermore, the attacker may potentially have access to some information about the host.

- A channel coding application in the presence of a Gaussian channel where

the encoder and decoder are built before the intended usage and they receive different noisy information about channel characteristics.

Channel coding with state information known only to the encoder for the discrete alphabet case has been studied by Gel'fand and Pinsker [2] and Heegard and El Gamal [3]. Costa extended these results to the Gaussian case for continuous alphabets with a squared error distortion constraint on the encoder in [4]; he interpreted the state information known to the encoder as "dirt" (leading to the well-known term of "dirty paper coding" in the data hiding literature) and showed that the capacity in this case is the same as the one where the state information is known by both the encoder and the decoder. Duality between channel coding and source coding with side information was explored in [5], [6], [7]. An in-depth treatment of the subject of channel coding in the presence of side information can be found in [8]. In [1], Moulin and Wang presented a comprehensive analysis on the "generalized family of Gel'fand – Pinsker problems" where they analyzed several variants (with an emphasis from the data hiding point of view) differing in terms of the amount of side information available to the encoder, attacker and decoder, and provided capacity formulae and random-coding exponents. A strong connection between channel coding with side information and data hiding (where the unmarked host is treated as the channel state) has been discovered and further investigated in [9], [10], [11], [12], [13], [14], which forms one of the major motivations of this work.

The contributions of this paper are as follows:

1. We focus on the fixed discrete memoryless channel case of the setup of [1], extend it to *continuous* alphabets and subsequently present the capacity result (cf. Sec. 3).

2. We assume both the state and the channel are memoryless Gaussian and the constraint imposed on the encoder is the expected square of the Euclidean norm; the case, where two different dirty versions of the state (corrupted by AWGN) are available to the encoder and the decoder, respectively, is referred to as *G*aussian *D*irty *P*aper *C*oding with *A*symmetric *G*aussian *D*irty *S*tate information (short hand, GDPC-AGDS, of which capacity denoted by $C_{\text{GDPC-AGDS}}$); the case, where both of the aforementioned dirty versions of the state are available to both the encoder and the decoder, is referred to as *G*aussian *D*irty *P*aper *C*oding with *S*ymmetric *G*aussian *D*irty *S*tate information (short hand, GDPC-SGDS, of which capacity denoted by $C_{\text{GDPC-SGDS}}$). We derive both $C_{\text{GDPC-AGDS}}$ and $C_{\text{GDPC-SGDS}}$, and show (in a way, of which philosophy is analogous to that of [4]) that $C_{\text{GDPC-AGDS}} = C_{\text{GDPC-SGDS}}$ (cf. Sec. 4), which is the major contribution of this paper. This implies that, in the Gaussian case with expected square Euclidean norm, there is no rate loss in the asymmetric dirty paper coding setup (where the encoder and decoder have

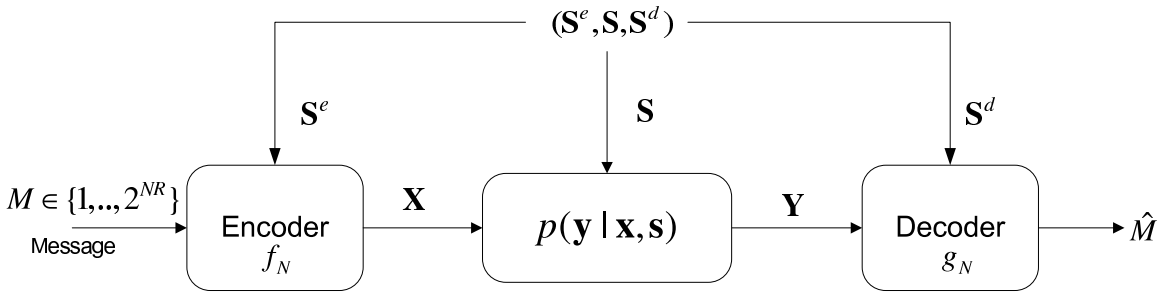

Fig. 1. Communication with (potentially asymmetric) side information at the encoder and decoder and fixed attack channel. An expected cost constraint is imposed on the encoder.

access to only partial and different information) with respect to the symmetric variant (where the encoder and decoder have access to the same information), as opposed to the general case for discrete alphabets [1].

After giving the problem statement in Section 2, we present the aforementioned results, together with an asymptotic analysis, in Sections 3 and 4. Then, we conclude in Section 5.

Notation: Boldface letters and corresponding regular letters with subscripts denote vectors (all of which are of length-N unless otherwise specified) and individual elements, respectively; e.g., the sequence of $\{a_1, a_2, \ldots, a_N\}$ is represented by $\mathbf{a}$. Capital letters and corresponding lowercase letters denote random variables and their realizations, respectively. $\mathrm{E}(\cdot)$, $\mathbb{1}_{(\cdot)}$, and $h(\cdot)$ denote expectation, standard indicator function, and differential entropy, respectively; $\log(\cdot)$ denotes natural logarithm unless otherwise specified. The abbreviations "i.i.d.", "p.d.f." and "w.l.o.g." are shorthands for the terms "independent identically distributed", "probability density function" and "without loss of generality", respectively.

2 Problem Statement

The problem considered in this paper is shown in Fig. 1. The original channel state information, the encoder-side noisy channel state information, and the decoder-side noisy channel state information are represented by length-N sequences $\mathbf{S}$, $\mathbf{S}^e$ and $\mathbf{S}^d$, respectively. The triplet $\left(\mathbf{S}^e, \mathbf{S}, \mathbf{S}^d\right)$ is assumed to consist of i.i.d. samples drawn from the bounded and continuous joint p.d.f. $p_{S^e,S,S^d}\left(s^e, s, s^d\right)$. The encoder codeword and the channel output are denoted by $\mathbf{X}$ and $\mathbf{Y}$, respectively. The channel is assumed to be memoryless with the corresponding conditional p.d.f. $p_{\mathbf{Y}|\mathbf{X},\mathbf{S}}(\mathbf{y}|\mathbf{x},\mathbf{s}) = \prod_{i=1}^{N} p_{Y|X,S}(y_i|x_i,s_i)$.

At the transmitter side, a message M is uniformly chosen from the discrete

finite set $\mathcal{M} = \left\{1, 2, \ldots, 2^{NR}\right\}$. Given the message M and the encoder-side state sequence $\mathbf{S}^e$, the encoder produces the codeword $\mathbf{X}$. The decoder input is the channel output, produced via the conditional p.d.f. $p_{\mathbf{Y}|\mathbf{X},\mathbf{S}}(\mathbf{y}|\mathbf{x},\mathbf{s})$ (specified above). The decoder knows the channel p.d.f. and has access to the decoder-side state sequence $\mathbf{S}^d$; given this information, it produces the decoded message $\hat{M}$. We assume that the alphabet for all sequences of interest is $\mathbb{R}^N$, and both the encoder and the decoder know the joint state distribution p.d.f. $p_{S^e,S,S^d}\left(s^e, s, s^d\right)$. We utilize a per-letter distortion metric $d^N(\cdot,\cdot)$ to quantify the cost introduced by the encoder, where $d^N(\mathbf{s}^e,\mathbf{x}) = \frac{1}{N}\sum_{i=1}^{N} d(s_i^e, x_i)$ and $d(\cdot,\cdot) : \mathbb{R}\times\mathbb{R} \to \mathbb{R}^+ \cup \{0\}$ is assumed to be continuous in its arguments.

Definition 2.1: A length-N rate-R RAASI (*R*eal-*A*lphabet *A*symmetric *S*ide *I*nformation) code with expected cost D is the triplet $(\mathcal{M}, f_N, g_N)$, where

- $\mathcal{M}$ is the message index set $\left\{1, 2, \ldots, 2^{NR}\right\}$,
- $f_N : \mathbb{R}^N \times \mathcal{M} \to \mathbb{R}^N$ is the (deterministic) encoder mapping, which produces the codeword $\mathbf{X} = f_N(M, \mathbf{S}^e)$ using the encoder-side state information $\mathbf{S}^e$ and the message M as the inputs, and which is subject to the expected cost constraint:

$$\mathrm{E}\left[d^N(\mathbf{S}^e, \mathbf{X})\right] = \sum_{m\in\mathcal{M}} \int_{\mathbb{R}^N} \frac{1}{2^{NR}} d^N(\mathbf{s}^e, f_N(\mathbf{s}^e, m))\, p_{\mathbf{S}^e}(\mathbf{s}^e)\, d\mathbf{s}^e \le D, \quad (2.1)$$

  where $p_{\mathbf{S}^e}(\mathbf{s}^e) = \int\int p_{\mathbf{S}^e,\mathbf{S},\mathbf{S}^d}\left(\mathbf{s}^e, \mathbf{s}, \mathbf{s}^d\right) d\mathbf{s}\, d\mathbf{s}^d$.
- $g_N : \mathbb{R}^N \times \mathbb{R}^N \to \mathcal{M}\cup\{e\}$ is the (deterministic) decoder mapping producing the estimate $\hat{M} = g_N\left(\mathbf{Y}, \mathbf{S}^d\right)$ given the channel output $\mathbf{Y}$ and the decoder-side state information $\mathbf{S}^d$ as the inputs. The decision $\hat{M} = e$ implies the error event during decoding.

Remark 2.1: The joint p.d.f. of $\left(M, \mathbf{S}^e, \mathbf{S}, \mathbf{S}^d, \mathbf{X}, \mathbf{Y}\right)$ is $p_{M,\mathbf{S}^e,\mathbf{S},\mathbf{S}^d,\mathbf{X},\mathbf{Y}}\left(m, \mathbf{s}^e, \mathbf{s}, \mathbf{s}^d, \mathbf{x}, \mathbf{y}\right) = p_M(m)\, p_{\mathbf{Y}|\mathbf{X},\mathbf{S}}(\mathbf{y}|\mathbf{x},\mathbf{s})\, p_{\mathbf{X}|\mathbf{S}^e,M}(\mathbf{x}|\mathbf{s}^e, m)\, p_{\mathbf{S}^e,\mathbf{S},\mathbf{S}^d}\left(\mathbf{s}^e, \mathbf{s}, \mathbf{s}^d\right)$, where $p_M(m) = 2^{-NR}$ for all m, and $p_{\mathbf{X}|\mathbf{S}^e,M}(\mathbf{x}|\mathbf{s}^e, m) = \mathbb{1}_{(\mathbf{x}=f_N(\mathbf{s}^e,m))}$ (since the encoder mapping is deterministic).

Definition 2.2: The average probability of error P_e^N for a length-N rate-R RAASI code $(\mathcal{M}, f_N, g_N)$ is $P_e^N = \Pr\left[M \ne \hat{M}\right]$, where the probability is computed over the joint p.d.f. of $\left(M, \mathbf{S}^e, \mathbf{S}, \mathbf{S}^d, \mathbf{X}, \mathbf{Y}\right)$.

Definition 2.3: Given a memoryless channel $p_{\mathbf{Y}|\mathbf{X},\mathbf{S}}(\mathbf{y}|\mathbf{x},\mathbf{s})$, a rate $R(D)$ is said to be achievable if there exists a length-N RAASI code $(\mathcal{M}, f_N, g_N)$ with expected cost D for which $P_e^N \to 0$ as $N \to \infty$.

Definition 2.4: Given a memoryless channel $p_{\mathbf{Y}|\mathbf{X},\mathbf{S}}(\mathbf{y}|\mathbf{x},\mathbf{s})$, the capacity $C(D)$

is the supremum of all achievable rates.

Remark 2.2: The aforementioned setup directly models two data hiding applications with the following interpretations:

Interpretation I: $\mathbf{S}^e$ represents the unmarked host; the decoder has access to side information $\mathbf{S}^d$, which is in general not equal to the host $\mathbf{S}^e$, but represents a quantity that is correlated with it, resulting in a potentially "semi-blind watermarking system" (see, for instance, [15, 16] for practical schemes illustrating semi-blind watermarking). Furthermore, the attacker may potentially have access to some information about the host, represented by $\mathbf{S}$. In that case, the constraint (2.1) amounts to the upper bound on the distortion introduced by data hiding and $\mathbf{X}$ represents the data-hidden sequence. This was the interpretation followed in [1].

Interpretation II: Consider a scenario, where the content owner hires a "data hiding service" from third parties due to the lack of resources or technical know-how, in which case the owner does not want to share the unmarked host with the service providers for privacy reasons. This scenario can be viewed as "privacy-driven data hiding". Then, this case may be represented by the introduced setup, where $\mathbf{S}$ denotes the unmarked host; the watermark encoder (resp. decoder) operates in the absence of $\mathbf{S}$, yet in the potential presence of a sequence $\mathbf{S}^e$ (resp. $\mathbf{S}^d$) that is correlated with the host. The encoder f_N produces the "information-carrying" signal $\mathbf{X}$, which is subsequently provided to the content owner. Then, the owner carries out data hiding via producing $\mathbf{X}+\mathbf{S}$, on which the attacker operates, producing $\mathbf{Y}$. Hence, actions of data hiding and attack are jointly captured via the conditional p.d.f. $p_{\mathbf{Y}|\mathbf{X},\mathbf{S}}(\mathbf{y}|\mathbf{x},\mathbf{s})$. In that case, via considering a special case of the distortion metric, $d^N(\mathbf{x},\mathbf{s}^e)=d^N(\mathbf{x})=\frac{1}{N}\sum_{i=1}^{N}d(x_i)$, the constraint (2.1) still amounts to the upper bound on the distortion introduced by data hiding. Privacy-driven data hiding constitutes the main motivation for the developments presented in Sec. 4 of this paper.

3 Capacity Result for Continuous Alphabets and Fixed Attack Channels

A special case of the results reported in [1] states that, the capacity of the setup presented in Sec. 2 (fixed channel, expected cost) for the case of *discrete* alphabets is given by

$$C(D)=\sup_{p_{X,U|S^e}(x,u|s^e)}\left[I\left(U;Y,S^d\right)-I\left(U;S^e\right)\right], \tag{3.1}$$

subject to the constraint $\mathrm{E}\left[d\left(S^e, X\right)\right] = \sum_{u,s^e,x} p_{X,U|S^e}\left(x,u|s^e\right) p_{S^e}\left(s^e\right) d\left(s^e,x\right) \leq D$ where U is an auxiliary random variable; all conditional distributions $\left\{p_{X,U|S^e}\right\}$ that satisfy the aforementioned constraint are termed as "admissible transmit channels". In this section, we extend this result, and under some mild technical assumptions show that the capacity of the setup presented in Sec. 2 (cf. Def. 2.4) for the case of *continuous* alphabets [1] is still given by (3.1) (where the mutual information is defined via the differential entropy over continuous probability distributions) subject to the constraint

$$\mathrm{E}\left[d\left(S^e, X\right)\right] = \int_u \int_{s^e} \int_x p_{X,U|S^e}\left(x,u|s^e\right) d\left(s^e,x\right) p_{S^e}\left(s^e\right) \leq D. \tag{3.2}$$

Our approach is analogous to the one used in Sec. V of [11].

Assume that, we confine ourselves to the class of "admissible transmit channels" $p_{X,U|S^e}\left(x,u|s^e\right)$, which are continuous, bounded and satisfy (3.2). Further, recall that, per the assumptions mentioned in Sec. 2, the considered alphabet is a finite dimensional Euclidean space, the joint p.d.f. $p_{S^e,S,S^d}\left(s^e,s,s^d\right)$ is bounded and continuous, and the distortion function $d\left(\cdot,\cdot\right)$ is continuous.

Given a probability measure for $\left(Y,X,U,S^e,S,S^d\right)$, the mutual information in case of continuous alphabets is defined as

$$I\left(U;Y,S^d\right) = \sup I\left(\bar{U};\bar{Y},\bar{S}^d\right) \quad \text{and} \quad I\left(U;S^e\right) = \sup I\left(\bar{U};\bar{S}^e\right), \tag{3.3}$$

where the supremum is over all finite partitions of the real line, yielding finite-alphabet random variables $\bar{U}$, $\bar{Y}$, $\bar{X}$, $\bar{S}^e$, $\bar{S}$, $\bar{S}^d$. Under the aforementioned assumptions, the mutual information expressions (3.3) and the objective $J \triangleq I\left(U;Y,S^d\right) - I\left(U;S^e\right)$ are all finite. For any $\epsilon > 0$ and for all admissible conditional p.d.f.s $p_{X,U|S^e}\left(x,u|s^e\right)$, select a finite partition of $\mathbb{R}$ such that

$$I\left(U;Y,S^d\right) - \epsilon < I\left(\bar{U};\bar{Y},\bar{S}^d\right) \leq I\left(U;Y,S^d\right), \tag{3.4}$$

$$I\left(U;S^e\right) - \epsilon < I\left(\bar{U};\bar{S}^e\right) \leq I\left(U;S^e\right), \tag{3.5}$$

$$\left|\mathrm{E}\left[d\left(\bar{S}^e,\bar{X}\right)\right] - \mathrm{E}\left[d\left(S^e,X\right)\right]\right| < \epsilon,$$

the existence of which is guaranteed by the aforementioned noted assumptions. Next, defining $J_\epsilon \triangleq I\left(\bar{U};\bar{Y},\bar{S}^d\right) - I\left(\bar{U};\bar{S}^e\right)$, and using the results of [1], the capacity in case of continuous alphabets is given

$$C\left(D\right) = \lim_{\epsilon \to 0} \sup_{p_{X,U|S^e}} J_\epsilon. \tag{3.6}$$

[1] Note that, although we consider the real line as the alphabet, the developments provided in this section apply to any continuous alphabet as long as the subsequent technical assumptions are satisfied.

Using (3.4) and (3.5) and straightforward algebra, we get $\left|J - J_\epsilon\right| \leq \epsilon$ for all admissible conditional p.d.f.s $p_{X,U|S^e}(x,u|s^e)$, which implies $\left|\sup_{p_{X,U|S^e}} J - \sup_{p_{X,U|S^e}} J_\epsilon\right| < \epsilon$. Thus, (3.6) reduces to (3.1), establishing that (3.1) subject to (3.2) is indeed the capacity in case of continuous alphabets. The results presented in Sec. 4 are based on this outcome.

4 Analytical Capacity Results for the Gaussian Case

In this section, we concentrate on a Gaussian variant of the setup introduced in Sec. 2 and present single-letter capacity expressions using the result given in Sec. 3. In particular, we assume the following (the distributions are all public and fixed):

(a) The triplet $\left(\mathbf{S}^e, \mathbf{S}, \mathbf{S}^d\right)$ is such that $\mathbf{S}^e = \mathbf{S} + \mathbf{Z}^e$; $\mathbf{S}^d = \mathbf{S} + \mathbf{Z}^d$; $\mathbf{S} \sim \mathcal{N}(\mathbf{0}, P_s\mathbf{I})$; $\mathbf{Z}^e \sim \mathcal{N}(\mathbf{0}, N_e\mathbf{I})$; $\mathbf{Z}^d \sim \mathcal{N}(\mathbf{0}, N_d\mathbf{I})$; $\mathbf{S}$, $\mathbf{Z}^e$, $\mathbf{Z}^d$ are independent; thus, $\mathbf{S}^e \leftrightarrow \mathbf{S} \leftrightarrow \mathbf{S}^d$ forms Markov chain in the given order.

(b) The channel p.d.f. $p_{\mathbf{Y}|\mathbf{X},\mathbf{S}}(\mathbf{y}|\mathbf{x},\mathbf{s})$ is such that $\mathbf{Y} = \mathbf{X} + \mathbf{S} + \mathbf{Z}^c$, where $\mathbf{Z}^c \sim \mathcal{N}(\mathbf{0}, N_c\mathbf{I})$ is independent of both $\mathbf{X}$ and $\mathbf{S}$.

(c) A special case of the distortion function $d(\cdot,\cdot)$ is considered such that $d(s_e, x) = x^2$.

Remark 4.1: The developments in this section are mainly intended for privacy-driven data hiding, which was discussed in Interpretation II of Remark 2.2: $\mathbf{S}$ is the host that belongs to a content owner, who, for privacy reasons, "masks" it via AWGN $\mathbf{Z}^e$ (resp. $\mathbf{Z}^d$) of which outcome is made available to the encoder (resp. decoder). The data-hidden sequence is $\mathbf{X} + \mathbf{S}$, on which the attacker applies AWGN, denoted by $\mathbf{Z}^c$, producing the decoder input $\mathbf{Y}$. This scenario is an extended version of the one considered by Costa [4] (extension being in the variation of the side information available to the encoder and the decoder); adopting his terminology, we use the term *G*aussian *D*irty *P*aper *C*oding (GDPC) with *G*aussian *D*irty *State* information (GDS) to refer to this setup. Note that, in this case, the constraint (3.2) reduces to

$$\mathrm{E}\left[X^2\right] = \int_u \int_{s^e} \int_x x^2 p_{X,U|S^e}(x,u|s^e)\, p_{S^e}(s^e) \leq D. \tag{4.1}$$

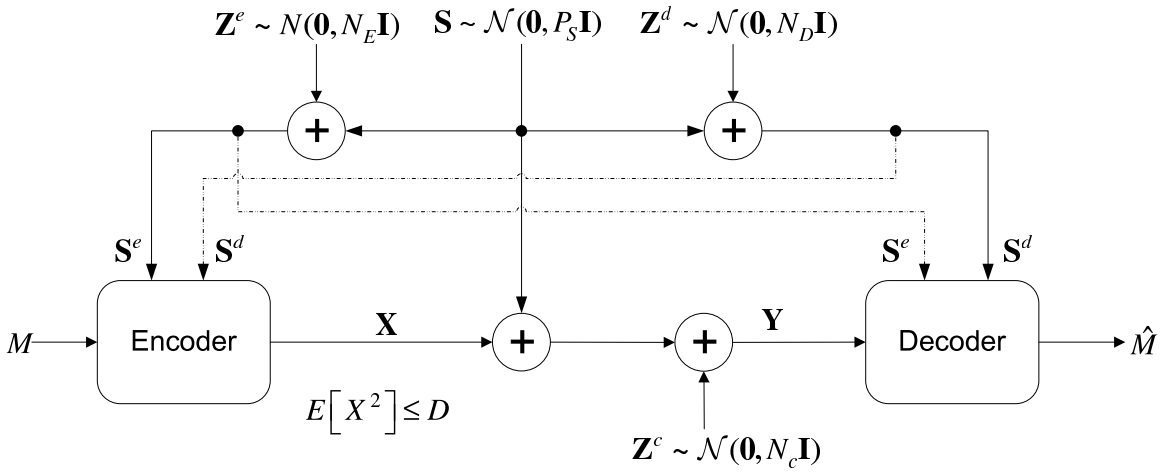

Fig. 2. Symmetric and Asymmetric Gaussian Setup. In GDPC-ADSI, $\mathbf{S}^e$ available to the encoder, $\mathbf{S}^d$ available to the decoder. In GDPC-SDSI, the pair $(\mathbf{S}^e, \mathbf{S}^d)$ available to the encoder and decoder.

4.1 Symmetric Setup

First, we consider the case where the side information available to the encoder and the decoder is symmetric; i.e., we assume that the pair $\left(\mathbf{S}^e, \mathbf{S}^d\right)$ is available to both the encoder and the decoder (See Fig. 2 for symmetric and asymmetric Gaussian setup). The resulting GDPC scenario with *S*ymmetric GDS is termed as GDPC-SGDS, with capacity $C_{\text{GDPC-SGDS}}$. Then, the cost function of (3.1) satisfies

$$\begin{aligned} &I\left(U; Y, S^e, S^d\right) - I\left(U; S^e, S^d\right) = h\left(U|S^e, S^d\right) - h\left(U|Y, S^e, S^d\right) \\ &= I\left(U; Y|S^e, S^d\right) \le I\left(X; Y|S^e, S^d\right) \end{aligned}$$

where the last inequality follows from noting that, $U \leftrightarrow X \leftrightarrow Y$ is a Markov chain in the specified order conditioned on $\left(S^e, S^d\right)$, and subsequently using data processing inequality. This implies that the inequality is satisfied with equality if and only if U is an invertible function of X, e.g., simply via choosing $U = X$. Then, $C_{\text{GDPC-SGDS}}$ would be the supremum of $I\left(X; Y|S^e, S^d\right)$ with respect to $p_{X|S^e,S^d}\left(x|s^e, s^d\right)$ subject to

$$\mathrm{E}\left[X^2\right] = \int_{s^e}\int_{s^d}\int_x x^2 p_{X|S^e,S^d}\left(x|s^e, s^d\right) p_{S^e,S^d}\left(s^e, s^d\right) \le D. \tag{4.2}$$

Proposition 4.1: The capacity of the GDPC-SGDS setup is given by

$$C_{\text{GDPC-SGDS}} = \frac{1}{2}\log\left(1 + \frac{D\left(P_sN_e + P_sN_d + N_eN_d\right)}{P_sN_eN_d + N_c\left(P_sN_e + P_sN_d + N_eN_d\right)}\right) \quad \text{nats.} \tag{4.3}$$

Proof: First, note that, in this case we have the two following Markov chains that characterize the setup:

$$S \leftrightarrow \left(S^e, S^d\right) \leftrightarrow X, \tag{4.4}$$

$$\left(S^e, S^d\right) \leftrightarrow (X, S) \leftrightarrow Y. \tag{4.5}$$

Next, observe that the cost function can be written as

$$I\left(X; Y|S^e, S^d\right) = h\left(Y|S^e, S^d\right) - h\left(Y|X, S^e, S^d\right). \tag{4.6}$$

Now, evaluating the first term of (4.6), we get

$$h\left(Y|S^e, S^d\right) = h\left(X + S + Z^c|S^e, S^d\right) = h\left(X + S + Z^c, S^e, S^d\right) - h\left(S^e, S^d\right). \tag{4.7}$$

Next, the second term of (4.6) yields

$$h\left(Y|X, S^e, S^d\right) = h\left(X + S + Z^c|X, S^e, S^d\right) = h\left(S + Z^c|X, S^e, S^d\right) = h\left(S + Z^c|S^e, S^d\right) \tag{4.8}$$

where the last equality is obtained via the Markov chain $(S + Z^c) \leftrightarrow S \leftrightarrow \left(S^e, S^d\right) \leftrightarrow X$, which follows from using (4.4) and noting that $S + Z^c$ is a function of S. Please note that $\left(S + Z^c, S^e, S^d\right) \sim \mathcal{N}\left(\mathbf{0}, \Sigma_{S+Z^c, S^e, S^d}\right)$, where

$$\Sigma_{S+Z^c, S^e, S^d} = \begin{pmatrix} P_s + N_c & P_s & P_s \\ P_s & P_s + N_e & P_s \\ P_s & P_s & P_s + N_d \end{pmatrix}. \tag{4.9}$$

Combining (4.7) and (4.8),

$$\begin{aligned} I\left(X; Y|S^e, S^d\right) &= h\left(X + S + Z^c, S^e, S^d\right) - h\left(S^e, S^d\right) - h\left(S + Z^c, S^e, S^d\right) + h\left(S^e, S^d\right), \\ &= h\left(X + S + Z^c, S^e, S^d\right) - h\left(S + Z^c, S^e, S^d\right), \qquad (4.10) \\ &= h\left(X + S + Z^c, S^e, S^d\right) - \frac{1}{2}\log\left((2\pi e)^3\left[P_s N_e N_d + N_c\left(P_s N_e + P_s N_d + N_e N_d\right)\right]\right), \qquad (4.11) \\ &\leq \frac{1}{2}\log\left((2\pi e)^3\left[P_s N_e N_d + (D + N_c)\left(P_s N_e + P_s N_d + N_e N_d\right)\right]\right), \qquad (4.12) \\ &\quad - \frac{1}{2}\log\left((2\pi e)^3\left[P_s N_e N_d + N_c\left(P_s N_e + P_s N_d + N_e N_d\right)\right]\right), \\ &= \frac{1}{2}\log\left(1 + \frac{D\left(P_s N_e + P_s N_d + N_e N_d\right)}{P_s N_e N_d + N_c\left(P_s N_e + P_s N_d + N_e N_d\right)}\right), \qquad (4.13) \end{aligned}$$

where the second term of (4.10) is a constant and can be calculated using (4.9), and the inequality (4.11) holds if $X \sim \mathcal{N}(0, D)$ and is independent of S, Z^c, Z^e and Z^d.

4.2 Asymmetric Setup

In this section, we provide the main result of the paper. We consider the asymmetric case; i.e., only $\mathbf{S}^e$ (resp. $\mathbf{S}^d$) is available to the encoder (resp. decoder). The resulting GDPC scenario with *A*symmetric GDS is termed as GDPC-AGDS, with capacity $C_{\text{GDPC-AGDS}}$. Then, $C_{\text{GDPC-AGDS}}$ would be the supremum of $I\left(U; Y, S^d\right) - I\left(U; S^e\right)$ with respect to $p_{X,U|S^e}(x, u|s^e)$ subject to (4.1).

Theorem 4.1: The capacity of the GDPC-AGDS setup is the same as that of GDPC-SGDS and is given by (4.3):

$$C_{\text{GDPC-AGDS}} = C_{\text{GDPC-SGDS}} \tag{4.14}$$

Proof: Let
$\mathcal{P}_{\alpha,\beta} \stackrel{\triangle}{=} \left\{ p_{X,U|S^e}(x, u|s^e) \,\middle|\, U = \beta X + \alpha S^e,\ X \sim \mathcal{N}(0, D)\ ,\ X \text{ independent of } S^e \right\}$ for all $\alpha, \beta \in \mathbb{R}^+$. Note that, per definition, all $p_{X,U|S^e}(x, u|s^e) \in \mathcal{P}_{\alpha,\beta}$ satisfy the constraint (4.1). Next, define

$$R_{\alpha,\beta} = \sup_{p_{X,U|S^e}(x,u|s^e) \in \mathcal{P}_{\alpha,\beta}} \left[I\left(U; Y, S^d\right) - I\left(U; S^e\right) \right]. \tag{4.15}$$

Thus, we have

$$R_{\alpha,\beta} \leq C_{\text{GDPC-AGDS}} \leq C_{\text{GDPC-SGDS}}, \tag{4.16}$$

where the left inequality follows since $\mathcal{P}_{\alpha,\beta}$ is a subset of all possible $p_{X,U|S^e}(x, u|s^e)$ subject to (4.1) and the right inequality follows since both the encoder and the decoder have access to more information in the symmetric setup than they do in the asymmetric setup.

Now, note that, for all $p_{X,U|S^e}(x, u|s^e) \in \mathcal{P}_{\alpha,\beta}$. we have $U = \beta X + \alpha S + \alpha Z^e$, $Y = X + S + Z^c$, $S^e = S + Z^e$, $S^d = S + Z^d$, where X, S, Z^c, Z^e, Z^d are all independent Gaussian with variances D, P_s, N_c, N_e, N_d, respectively. This implies $\left(U, Y, S^d\right) \sim \mathcal{N}\left(\mathbf{0}, \Sigma_{U,Y,S^d}\right)$, $\left(Y, S^d\right) \sim \mathcal{N}\left(\mathbf{0}, \Sigma_{Y,S^d}\right)$, $(U, S^e) \sim$

$\mathcal{N}(\mathbf{0}, \Sigma_{U,S^e})$, where

$$\Sigma_{U,Y,S^d} = \begin{pmatrix} \beta^2 D + \alpha^2 (P_s + N_e) & \beta D + \alpha P_s & \alpha P_s \\ \beta D + \alpha P_s & D + P_s + N_c & P_s \\ \alpha P_s & P_s & P_s + N_d \end{pmatrix}, \tag{4.17}$$

$$\Sigma_{U,S^e} = \begin{pmatrix} \beta^2 D + \alpha^2 (P_s + N_e) & \alpha (P_s + N_e) \\ \alpha (P_s + N_e) & P_s + N_e \end{pmatrix}, \tag{4.18}$$

and Σ_{Y,S^d} is the lower-right 2×2 submatrix of Σ_{U,Y,S^d}. Using (4.17), (4.18), and carrying out straightforward algebra, we get

$$I\left(U; Y, S^d\right) - I\left(U; S^e\right) = \frac{1}{2} \log \frac{D\left[\left(D + P_s + N_c\right)\left(P_s + N_d\right) - P_s^2\right]}{f(\theta)}, \tag{4.19}$$

where $\theta \triangleq \alpha/\beta$ and

$$\begin{aligned} f(\theta) \triangleq\ & (1-\theta)^2 D P_s N_d + N_c N_d \left[D + \theta^2 (P_s + N_e)\right] \\ & + \theta^2 N_e \left(D P_s + D N_d + P_s N_d + N_c P_s\right) + D N_c P_s. \end{aligned}$$

Thus, in order to maximize $I\left(U; Y, S^d\right) - I\left(U; S^e\right)$ with respect to (α, β) it suffices to minimize $f(\theta)$ with respect to θ. Using f quadratic with a positive leading coefficient (hence convex) in θ, we get

$$\begin{aligned} \theta_{min} \triangleq\ & \arg\min_{\theta} f(\theta) = D P_s N_d / \left[D P_s N_d + P_s N_c N_d \right. \\ & \left. + N_e \left(D P_s + D N_d + P_s N_d + N_c P_s + N_c N_d\right)\right]. \end{aligned}$$

Employing this result in (4.19), we reach $R_{\alpha,\beta} = C_{\text{GDPC-SGDS}}$; thus, recalling (4.16), we get (4.14).

Remark 4.2: Note that, the proof methodology is analogous to that of [4]. The capacity in [4], referred as C_{Costa}, is a special case of $C_{GDPC-AGDS}$ such that

$$C_{\text{Costa}} = \lim_{N_e \to 0} \lim_{N_d \to \infty} C_{GDPC-AGDS} = \frac{1}{2} \log \left(1 + \frac{D}{N_c}\right). \tag{4.20}$$

Remark 4.2: The case where both of the aforementioned dirty versions of the state available to both the encoder and the decoder are identical $\mathbf{S}^e = \mathbf{S}^d$, referred to as *G*aussian *D*irty *P*aper *C*oding with *I*dentical *S*ymmetric *G*aussian *D*irty *S*tate information (short hand, GDPC-ISGDS, of which capacity denoted by $C_{\text{GDPC-ISGDS}}$) can be analyzed using an asymptotic analysis

of $C_{\text{GDPC-SGDS}}$ such that the capacity is

$$C_{\text{GDPC-ISGDS}} = \lim_{N_e \to \delta} \lim_{N_d \to \infty} C_{\text{GDPC-SGDS}} = \lim_{N_e \to \infty} \lim_{N_d \to \delta} C_{\text{GDPC-SGDS}},$$
$$= \frac{1}{2} \ln \left(1 + \frac{D(P_s + \delta)}{P_s \delta + N_c (P_s + \delta)} \right) \quad \text{nats}, \tag{4.21}$$

where $\delta \in \mathbb{R}^+$.

5 Conclusions

This paper extends the channel setup of [1] to continuous alphabets case in order to model certain privacy-driven data hiding and semi-blind watermarking scenarios. Furthermore, the capacity term is evaluated for the Gaussian case under a mean square error distortion constraint. We show that there is no capacity loss in GDPC-ADSI scheme (where the encoder and decoder have access to only partial and different information) with respect to the GDPSC-SDSI scheme (where the encoder and decoder have access to the same information). The results are promising in order to design the practical GDPC-ADSI coding schemes that achieves the GDPSC-SDSI performance.

6 Acknowledgments

We thank Prof. Pierre Moulin for the technical discussions and motivation for this paper.

References

[1] P. Moulin and Y. Wang, "Capacity and random-coding exponents for channel coding with side information," *IEEE Transactions on Information Theory*, vol. 53, no. 4, pp. 1326–1347, 2007.

[2] S. I. Gel'fand and M. S. Pinsker, "Coding for channel with random parameters," *Problems of Control and Information Theory*, vol. 9, no. 1, pp. 19–31, 1980.

[3] C. Heegard and A. A. El Gamal, "On the capacity of computer memory with defects," *IEEE Transactions on Information Theory*, vol. IT-29, no. 5, pp. 731–739, Sep. 1983.

[4] M. Costa, "Writing on dirty paper," *IEEE Transactions on Information Theory*, vol. IT-29, no. 3, pp. 439–441, 1983.

[5] T. M. Cover and M. Chiang, "Duality between channel capacity and rate distortion with side information," *IEEE Transactions on Information Theory*, vol. 48, no. 6, pp. 1629–1638, June 2002.

[6] R. J. Barron, B. Chen, and G. W. Wornell, "The duality between information embedding and source coding with side information and some applications," *IEEE Transactions on Information Theory*, vol. 49, no. 5, pp. 1159–1180, May 2003.

[7] S. S. Pradhan, J. Chou, K. Ramchandran, "Duality between source coding and channel coding and its extension to the side information case," *IEEE Transactions on Information Theory*, vol. 49, no. 5, pp. 1181–1203, May 2003.

[8] G. Keshet, Y. Steinberg, and N. Merhav, "Channel Coding in the Presence of Side Information," *Foundations and Trends in Communications and Information Theory*, vol. 4, no. 6, pp. 445–586, 2007.

[9] F. M. J. Willems, "An information theoretical approach to information embedding," *Proc. 21st Symp. Information Theory in the Benelux*, Wassenaar, The Netherlands, pp. 255–260, May 2000.

[10] B. Chen and G. .W. Wornell, "Quantization index modulation methods: A Class of provably good methods for digital watermarking and information embedding," *IEEE Transactions on Information Theory*, vol. 47, no. 4, pp. 1423–1443, May 2001.

[11] P. Moulin and J. A. O'Sullivan, "Information-theoretic analysis of information hiding," *IEEE Transactions on Information Theory*, vol. 49, no. 3, pp. 563–593, Mar. 2003.

[12] A. S. Cohen and A. Lapidoth, "The Gaussian watermarking game," *IEEE Transactions on Information Theory*, vol. 48, no. 6, pp. 1639–1667, June 2002.

[13] A. Somekh-Baruch and N. Merhav, "On the error exponent and capacity games of private watermarking systems," *IEEE Transactions on Information Theory*, vol. 49, no. 3, pp. 537–562, Mar. 2003.

[14] A. Somekh-Baruch and N. Merhav, "On the capacity game of public watermarking systems," *IEEE Transactions on Information Theory*, vol. 50, no. 3, pp. 511–524, Mar. 2004.

[15] J. L. Cannons and P. Moulin, "Design and Statistical Analysis of a Hash-Aided Image Watermarking System," *IEEE Trans. on Image Processing*, Oct. 2004.

[16] M. K. Mihcak, R. Venkatesan, and T. Liu, "Watermarking via Optimization Algorithms for Quantizing Randomized Semi-Global Image Features," *ACM Multimedia Systems Journal*; vol. 11, no. 2, pp. 185–200, Dec. 2005.