Hybrid Digital/Analog Schemes for Secure Transmission with Side Information

Joffrey Villard*, Pablo Piantanida* and Shlomo Shamai (Shitz)[†]

* Department of Telecommunications	[†] Department of Electrical Engineering
SUPELEC	Technion - Israel Institute of Technology
91192 Gif-sur-Yvette, France	Technion city, Haifa 32000, Israel
Email: {joffrey.villard, pablo.piantanida}@supelec.fr	Email: sshlomo@ee.technion.ac.il

Abstract

Recent results on source-channel coding for secure transmission show that separation holds in several cases under some less-noisy conditions. However, it has also been proved through a simple counterexample that pure analog schemes can be optimal and hence outperform digital ones. According to these observations and assuming matched-bandwidth, we present a novel hybrid digital/analog scheme that aims to gather the advantages of both digital and analog ones. In the quadratic Gaussian setup when side information is only present at the eavesdropper, this strategy is proved to be optimal. Furthermore, it outperforms both digital and analog schemes and cannot be achieved via time-sharing. An application example to binary symmetric sources with side information is also investigated.

I. INTRODUCTION

The setup of source-channel coding for secure transmission consists of three nodes that measure an analog source as a function of time. One of them (referred to as Alice) wishes to transmit a compressed version of its observation to a second node (referred to as Bob) through a noisy (or wireless) channel. In addition, Bob can use his own observation as side information to decode the received message and refine his estimate of Alice's source. The third node (referred to as Eve) is an eavesdropper *i.e.*, a node that can listen to the messages sent by Alice through another noisy channel, as shown in Fig. 1. Considering Eve as an untrusted node, Alice wishes to leak the smallest amount of information about her source.

Among some major information-theoretic issues, the above scenario involves the notion of secrecy (and its application to source and channel coding), source coding with side information, as well as joint source/channel coding for transmission of sources over noisy channels. The information-theoretic notion of secrecy was introduced by Shannon [1] and used for secure communication over noisy channels by Wyner [2], who introduced the wiretap
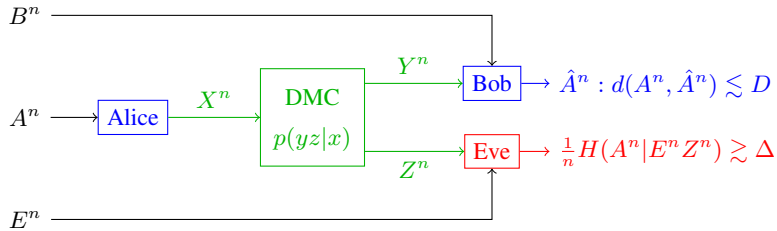
Figure 1: Secure transmission with side information.

channel, which was further extended by Csiszár and Körner [3]. On the other hand, source coding with side information has been introduced by Slepian and Wolf [4], and Wyner and Ziv [5]. Recent results [6], [7] consider such settings with an additional eavesdropper that must be kept as ignorant as possible of the transmitted source. Most of the existent work separately consider channel or source coding for secure transmission or compression. However, unlike simple point-to-point communication problems, there is no general result of separation for multiterminal settings under security constraints. Recent work [8], [9] about source-channel coding for secure transmission shows that separation holds in several cases under some less-noisy conditions. Whereas a simple counterexample in [9] showed that a pure analog scheme can improve digital schemes while being optimal. This observation motivates us to investigate hybrid digital/analog schemes for such setting, which by taking advantage of both analog and digital strategies may yield better performance. Indeed, such schemes have already been proved useful for point-to-point problems *e.g.*, to handle SNR mismatch (while they can perform as good as digital or analog ones at the true SNR) [10], [11], as well as for some multiterminal settings [12], [13].

In this paper, we consider the setup of joint source-channel coding for secure transmission of a source over a noisy channel with an eavesdropper, and in the presence of side information at the receiving terminals. We restrict our attention to the matched-bandwidth case *i.e.*, one channel use is allowed per source symbol, as depicted in Fig. 1. Our main goal is to understand how Alice can take simultaneous advantage of both statistical differences among side informations and channels. Section II recalls some prior results that yield an inner bound (digital scheme), and a general outer bound on the distortion-equivocation region. A novel hybrid digital/analog scheme and its single-letter inner bound is derived in Section III. Transmission of a Gaussian source over a Gaussian wiretap channel with side information (resp. binary source over a type-II wiretap channel) is studied in Section IV (resp. Section V).

Notations

For any sequence $(x_i)_{i \in \mathbb{N}^*}$, notation x^n stands for the collection $(x_1, x_2, \ldots, x_n)$. Entropy is denoted by $H(\cdot)$, and mutual information by $I(\cdot; \cdot)$. Let X, Y and Z be three random variables on some alphabets with probability distribution p. If $p(x|y, z) = p(x|y)$ for each x, y, z, then they form a Markov chain, which is denoted by $X \ominus Y \ominus Z$. The set of nonnegative real numbers is denoted by $\mathbb{R}_+$. For each $x \in \mathbb{R}$, notation $[x]_+$ stands for $\max(0; x)$. Notation h_2 stands for the binary entropy function. The binary exclusive-or operator is denoted by $\oplus$.

II. Problem Definition and Prior Results

A. Problem Definition

Let $\mathcal{A}$, $\mathcal{B}$, $\mathcal{E}$, $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$ be six finite sets. Alice, Bob, and Eve observe the sequences of random variables $(A_i)_{i \in \mathbb{N}^*}$, $(B_i)_{i \in \mathbb{N}^*}$, and $(E_i)_{i \in \mathbb{N}^*}$, respectively, which take values on $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{E}$, resp. For each $i \in \mathbb{N}^*$, the random variables A_i, B_i, and E_i are distributed according to the joint distribution $p(abe)$ on $\mathcal{A} \times \mathcal{B} \times \mathcal{E}$. Moreover, they are independent across time i. Alice can also communicate with Bob and Eve through a discrete memoryless channel $p(yz|x)$ with input X on $\mathcal{X}$, and outputs Y, Z on $\mathcal{Y}$, $\mathcal{Z}$, respectively. Let $d : \mathcal{A} \times \mathcal{A} \to [0\,;d_{\max}]$ be a finite distortion measure *i.e.*, $0 \leq d_{\max} < \infty$. Denote by d the component-wise mean distortion on $\mathcal{A}^n \times \mathcal{A}^n$ *i.e.*, for each $a^n, b^n \in \mathcal{A}^n$, $d(a^n, b^n) = \frac{1}{n} \sum_{i=1}^{n} d(a_i, b_i)$.

Definition 1 (Code and achievability): An n-code for source-channel coding in this setup is defined by

- A (stochastic) encoding function at Alice $F : \mathcal{A}^n \to \mathcal{X}^n$, defined by some transition probability $P_{X^n|A^n}(\cdot|\cdot)$,
- A decoding function at Bob $g : \mathcal{B}^n \times \mathcal{Y}^n \to \mathcal{A}^n$.

A tuple $(D, \Delta) \in \mathbb{R}_+^2$ is *achievable* if, for any $\varepsilon > 0$, there exists an n-code (F, g) s.t.:

$$\mathbb{E}\big[d(A^n, g(B^n, Y^n))\big] \leq D + \varepsilon \;,$$

$$\frac{1}{n} H(A^n | E^n Z^n) \geq \Delta - \varepsilon \;,$$

with channel input X^n as the output of the encoder $F(A^n)$. The set of all achievable tuples is denoted by $\mathcal{R}^*$ and is referred to as the *distortion-equivocation region*.

B. Prior Results

Recent results [9] provide inner and outer bounds on region $\mathcal{R}^*$ which do not match in general. In the matched-bandwidth case, the inner bound $\mathcal{R}_{\mathrm{dig}}$ is defined by the next theorem.

Theorem 1 (Digital Scheme [9]): The set of all tuples $(D, \Delta) \in \mathbb{R}_+^2$ such that there exist RVs U, V, Q, T, X on finite sets $\mathcal{U}$, $\mathcal{V}$, $\mathcal{Q}$, $\mathcal{T}$, $\mathcal{X}$ respectively, with joint distribution $p(uvqtabexyz) = p(u|v)p(v|a)p(abe)\,p(q|t)p(tx)$ $p(yz|x)$, and a function $\hat{A} : \mathcal{V} \times \mathcal{B} \to \mathcal{A}$, verifying the following inequalities, is achievable:

$$I(U; A|B) \leq I(Q; Y) \;,$$

$$I(V; A|B) \leq I(T; Y) \;,$$

$$D \geq \mathbb{E}\big[d(A, \hat{A}(V, B))\big] \;,$$

$$\Delta \leq H(A|UE) - \Big[I(V; A|UB) - \big(I(T; Y|Q) - I(T; Z|Q) \big) \Big]_+ \;.$$

The achievability of the above region follows by combining secure source coding [7] with coding for broadcast channels with common message [3]. This results in two independent (but not stand-alone) source and channel components, yielding statistically independent source and channel variables *i.e.*, "operational" separation holds. Such a scheme will be referred to as the *digital scheme*. In some special cases *e.g.*, when Eve has less noisy channel, or Bob has less noisy side information, this inner bound becomes tight [9] and traditional separation holds.

Nevertheless, when Bob has "better" channel and "worse" side information than Eve, it was observed in [9] through a simple example that a naive analog scheme, consisting of directly plugging the source on the channel, outperforms the digital one of Theorem 1. Furthermore, it turns to be optimal since it can be shown that it achieves the next outer bound $\mathcal{R}_{\text{out}}$.

Theorem 2 (Outer Bound [9]): For each achievable tuple (D, Δ), there exist random variables U, V, Q, T, X on finite sets $\mathcal{U}$, $\mathcal{V}$, $\mathcal{Q}$, $\mathcal{T}$, $\mathcal{X}$, respectively, and a function $\hat{A} : \mathcal{V} \times \mathcal{B} \to \mathcal{A}$, such that $p(uvqtabexyz) = p(uv|a)p(abe)\,p(q|t)p(tx)p(yz|x)$, and

$$I(V; A|B) \leq I(T; Y) \ ,$$

$$D \geq \mathbb{E}\big[d(A, \hat{A}(V, B))\big] \ ,$$

$$\Delta \leq H(A|UE) - \Big[I(V; A|B) - I(U; A|B) - \Big(I(T; Y|Q) - I(T; Z|Q)\Big)\Big]_{+} \ .$$

III. Hybrid Coding for Secure Transmission

Based on the observation made in [9] about the usefulness of *analog schemes*, we now propose a *hybrid digital/analog scheme* that yields the next inner bound $\mathcal{R}_{\text{hyb}} \subseteq \mathcal{R}^{*}$.

A. Main Result

Theorem 3 (Hybrid Scheme): The set of all tuples (D, Δ) in $\mathbb{R}_{+}^{2}$ such that there exist RVs U, V, X on finite sets $\mathcal{U}$, $\mathcal{V}$, $\mathcal{X}$, with joint PD $p(uvabexyz) = p(u|v)p(vx|a)\,p(abe)\,p(yz|x)$, $x = x(v, a)$, and a function $\hat{A} : \mathcal{V} \times \mathcal{B} \times \mathcal{Y} \to \mathcal{A}$, verifying the following inequalities, is achievable:

$$I(U; A) \leq I(U; BY) \ , \tag{1}$$

$$I(V; A|U) \leq I(V; BY|U) \ , \tag{2}$$

$$D \geq \mathbb{E}\big[d(A, \hat{A}(V, B, Y))\big] \ , \tag{3}$$

$$\Delta \leq H(A|UE) - I(V; A|U) - I(X; Z|UE) + \min\Big\{I(V; BY|U) \ ; \ I(V; AZ|U)\Big\} \ . \tag{4}$$

Channels $A \mapsto B$ and $X \mapsto Y$ can be viewed together as a state-dependent channel with input X, state A and output (B, Y). In this perspective, Alice and Bob form a communication system with channel state information known at the transmitter (CSIT), as depicted in Fig. 2. Roughly speaking, the proposed strategy consists in sending independent digital random noise W using a Gelfand-Pinsker code [14] for this equivalent state-dependent channel. Two auxiliary RVs (U, V) constitute the descriptions of A. Digital random noise W here helps to secure description V against Eve. As in the classical wiretap channel [3], [15], its rate satisfies some constraint that allows to characterize the equivocation rate at Eve. Finally, the auxiliary RV U is a subpart of V that can be seen as a *common* message which is considered to be known at Eve, as shown by the term $H(A|UE)$ in (4).
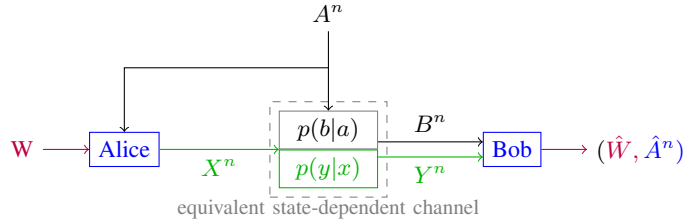
Figure 2: Alice and Bob as a communication system with state-dependent channel and CSIT.

B. Sketch of Proof

We provide a short sketch of proof of Theorem 3. Details will be given in an extended version of this paper. Let $R_1, R_2, R_f \in \mathbb{R}_+^*$ and assume that a local (independent and uniformly distributed) source with rate R_f is available at Alice.

1) Codebook generation: Randomly pick 2^{nR_1} sequences $u^n(r_1)$ from $T_\varepsilon^n(U)$. Then, for each $u^n(r_1)$, randomly pick $2^{n(R_2+R_f)}$ sequences $v^n(r_1, r_2, r_f)$ from $T_\varepsilon^n(V|u^n(r_1))$.

2) Encoding: Assume that source sequence A^n and random noise r_f are produced at Alice. Look for the first codeword $u^n(r_1)$ such that $(u^n(r_1), A^n) \in T_\varepsilon^n(U, A)$. Then look for the first codeword $v^n(r_1, r_2, r_f)$ such that $(v^n(r_1, r_2, r_f), A^n) \in T_\varepsilon^n(V, A|u^n(r_1))$ and send X^n, defined by the component-wise relation

$$X_i \triangleq x(v_i(r_1, r_2, r_f), A_i) .$$

By standard arguments, it can be proved that these two steps succeed with high probability if $R_1 > I(U; A)$ and $R_2 > I(V; A|U)$.

3) Decoding: Assume that Bob observes B^n and receives Y^n from Alice. Look for the unique codeword $u^n(r_1)$ such that $(u^n(r_1), B^n, Y^n) \in T_\varepsilon^n(U, B, Y)$. Then look for the unique codeword $v^n(r_1, r_2, r_f)$ such that $(v^n(r_1, r_2, r_f), B^n, Y^n) \in T_\varepsilon^n(V, B, Y|u^n(r_1))$. Compute the estimate $g(B^n, Y^n) \in \mathcal{A}^n$ using the component-wise relation

$$g_i(B^n, Y^n) \triangleq \hat{A}(v_i(r_1, r_2, r_f), B_i, Y_i) .$$

As noted in [13], the conventional random coding proof technique does not apply here, and the decoding error probability must be carefully handled. In the proposed joint coding scheme, a single codebook plays both roles of source and channel codebooks. For a given source sequence a^n, the indices (r_1, r_2) thus depend on the entire codebooks, and the averaging over the set of all possible codebooks cannot be performed in the usual way. Similarly to [13], it is not difficult to show that these two decoding steps succeed with high probability if $R_1 < I(U; BY)$ and $R_2 + R_f < I(V; BY|U)$.

4) Distortion at Bob: Provided the above constraints are verified, Bob can decode codeword $v^n(r_1, r_2, r_f)$ with an arbitrarily small probability of error, and compute estimate $g(Y^n, B^n)$ of A^n. Using standard properties of typical sequences, it can be easily proved that the mean distortion of this estimate approaches $\mathbb{E}[d(A, \hat{A}(V, B, Y))]$.

5) Equivocation rate at Eve: The equivocation at Eve can be divided in "source" and "channel" terms. Each one is studied using standard properties of typical sequences, and the arguments of [7] and [15, Section 2.3.*Step 3*]. The next constraint which ensures that Eve decodes $v^n(r_1, r_2, r_f)$ from (r_1, A^n, Z^n) is required to characterize the equivocation

$$R_2 + R_f < I(V; AZ|U) \ .$$

After some derivations, we can eventually prove that

$$\frac{1}{n} H(A^n | E^n Z^n) \geq H(A|UE) - I(X; Z|UE) + R_f - \varepsilon \ .$$

6) End of Proof: Gathering the above inequalities and performing Fourier-Motzkin elimination prove Theorem 3.

C. Special Cases

1) Analog schemes: The proposed scheme can reduce to a pure analog one (as the simple one of [9, Section VI]). Hence $\mathcal{R}_{\text{hyb}}$ contains tuples that may not be in $\mathcal{R}_{\text{dig}}$: $\mathcal{R}_{\text{hyb}} \not\subset \mathcal{R}_{\text{dig}}$.

2) Digital schemes: By defining the variables in Theorem 3 as pairs of independent source and channel components, we can obtain the structure of those in Theorem 1, but such variables do not verify all inequalities and thus $\mathcal{R}_{\text{dig}} \not\subset \mathcal{R}_{\text{hyb}}$.

3) Wiretap channel: Choosing independent source and channel variables with appropriate rates, region $\mathcal{R}_{\text{hyb}}$ reduces to the achievable region for the wiretap channel [15, Eq. (2.6)].

IV. Secure Transmission of a Gaussian Source over a Gaussian Wiretap Channel

A. System Model

In this section, we consider the transmission of a Gaussian source over a Gaussian wiretap channel. More precisely, the source at Alice A is standard Gaussian, and observations at Bob and Eve are the outputs of independent additive white Gaussian noise (AWGN) channels with input A and respective noise powers P_B and P_E. Communication channels from Alice to Bob and Charlie are AWGN channels with respective noise powers P_Y and P_Z. The average input power of this channel is limited to P.

Euclidean distance on $\mathbb{R}$ is used to measure distortion at Bob ($d(a, b) = (a - b)^2$, for each $a, b \in \mathbb{R}$). Differential entropy $h(\cdot)$ measures uncertainty yielding equivocation rates $\Delta \in \mathbb{R}$. We also introduce quantity $D_E \triangleq 2^{2\Delta}/(2\pi e)$, which provides a lower bound on the minimum mean-square error of any estimator of A at Eve.

Definition 2 (Achievability): In this section, a tuple $(D, D_E) \in \mathbb{R}_+^{*\,2}$ is said to be *achievable* if, for any $\varepsilon > 0$, there exists an n-code (F, g) s.t.:

$$\mathbb{E}\big[\|A^n - g(B^n, Y^n)\|^2\big] \leq D + \varepsilon \ ,$$

$$\frac{1}{n} h(A^n | E^n Z^n) \geq \frac{1}{2} \log\left(2\pi e\, D_E\right) - \varepsilon \ ,$$

$$\frac{1}{n} \sum_{i=1}^{n} \mathbb{E}\big[X_i^2\big] \leq P + \varepsilon \ ,$$

with channel input X^n as the output of the encoder $F(A^n)$.

	$P_B \leq P_E$	$P_B > P_E$
$P_Y < P_Z$	✓	?
$P_Y \geq P_Z$	✓	✓

Table I: Cases where $\mathcal{R}_{\text{dig}}$ is tight and separation holds.

Although Theorems 1–3 are stated and proved for finite alphabet, we take the liberty to use their statements as inner regions also for this case. The involved joint PDs should now also verify condition $\text{Var}\left[X\right] \leq P$. The corresponding regions will be denoted with an additional $\cdot^P$ *i.e.*, $\mathcal{R}_{\text{dig}}^P$, $\mathcal{R}_{\text{out}}^P$ and $\mathcal{R}_{\text{hyb}}^P$.

Notice that due to the Gaussian additive noises, and depending on the relative values of P_B, P_E (resp. P_Y, P_Z), one side information (resp. one channel) is a stochastically degraded version of the other. There exist four different cases and, from known results (see Section II-B), separation holds for three of them, as summarized in Table I. For instance, the case when Bob has "better" channel ($P_Y < P_Z$) and "worse" side information ($P_B > P_E$) than Eve is still open. We next propose a hybrid digital/analog scheme based on Theorem 3 that turns to be optimal when $P_Y < P_Z$ and $P_B \to \infty$.

B. Hybrid Coding

In this section, we consider hybrid coding with RVs U, V and X of Theorem 3 defined as $U = \emptyset$ and

$$V = \alpha A + \gamma N \ , \tag{5}$$

$$X = \sqrt{P}\big(\beta A - \gamma N\big) \ , \tag{6}$$

where $\gamma = \sqrt{1 - \beta^2}$, and $N \sim \mathcal{N}(0,1)$ is a standard Gaussian random variable independent of A. Note that $X \sim \mathcal{N}(0, P)$ writes as a deterministic function of A and V:

$$X = \sqrt{P}\big((\alpha + \beta)A - V\big) \ .$$

$\hat{A}$ is defined as the MMSE estimator of A from (V, Y).

The hybrid digital/analog scheme of Section III with the above variables reduces to the one depicted in Fig. 3.

C. Special Case: $P_Y < P_Z$, $P_B \to \infty$

From now on, we focus on the unsolved case (represented by "**?**" in Table I), where $P_Y < P_Z$. Then, if Bob does not have any side information $B = \emptyset$ (or equivalently $P_B \to \infty$):

- The hybrid digital/analog scheme of Section IV-B is optimal and yields Theorem 4.
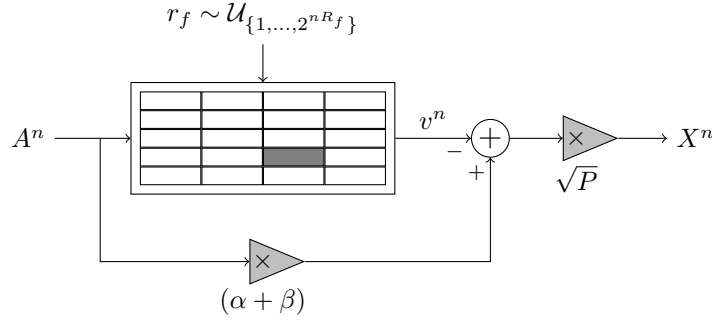- The digital scheme of [9] is strictly sub-optimal, as shown by Proposition 1 and Fig. 4.

Figure 3: Hybrid digital/analog scheme for secure transmission of a Gaussian source over a Gaussian wiretap channel.

Theorem 4 (Gaussian sources): If $P_Y < P_Z$ and $B = \emptyset$, a tuple $(D, D_E) \in \mathbb{R}_+^{*2}$ is achievable if and only if

$$D \geq \frac{1}{1 + \frac{P}{P_Y}} \ ,$$

$$D_E \leq \frac{1}{\max\left\{1 \,;\, \frac{1}{D} \cdot \frac{1 + \frac{P}{P_Z}}{1 + \frac{P}{P_Y}}\right\} + \frac{1}{P_E}} \ .$$

Proof: The converse proof relies on the (conditional) entropy power inequality and is omitted here. The direct part follows after Theorem 3 by choosing in the hybrid scheme of Section IV-B, for any distortion level $D \in \left[\frac{1}{1 + \frac{P}{P_Y}}, \frac{1 + \frac{P}{P_Z}}{1 + \frac{P}{P_Y}}\right]$:

$$\alpha \triangleq \frac{\beta + \gamma^2 \sqrt{\frac{1}{D}\left(\frac{P}{P_Y} - \frac{P}{P_Z}\right)}}{1 + \gamma^2 \frac{P}{P_Y}} - \beta \ ,$$

$$\beta \triangleq \sqrt{\frac{P_Z}{P}} \sqrt{1 + \frac{P}{P_Z} - D\left(1 + \frac{P}{P_Y}\right)} \ .$$

■

The next proposition provides a simple expression of region $\mathcal{R}_{\text{dig}}^P$ *i.e.*, the set of all tuples achievable by digital scheme [9].

Proposition 1: If $P_Y < P_Z$ and $B = \emptyset$, $(D, \Delta) \in \mathcal{R}_{\text{dig}}^P$ if and only if, for some $\mu \in \left[\frac{1}{1 + \frac{P}{P_Y}}; 1\right]$ and $D_E = \frac{2^{2\Delta}}{2\pi e}$:

$$D \geq \frac{1}{1 + \frac{P}{P_Y}} \ ,$$

$$D_E \leq \frac{1}{\frac{1}{\mu} + \frac{1}{P_E}} \cdot \min\left\{1 \,;\, \frac{D\left(1 + \frac{P}{P_Y}\right)}{1 + \mu\frac{P}{P_Z} - (1 - \mu)\frac{P_Y}{P_Z}}\right\} \ .$$

Remark 1: If $D \geq \frac{1 + \frac{P}{P_Z}}{1 + \frac{P}{P_Y}}$, then $\mu = 1$ is optimal in Proposition 1, yielding inequalities of Theorem 4. This implies that the digital scheme of [9] is optimal in this region. For such distortion levels, the quantity $D_E = \frac{1}{1 + \frac{1}{P_E}}$ $= \mathrm{Var}\,[A|E]$ is achievable, meaning that Eve cannot retrieve additional information from the communication between Alice and Bob.
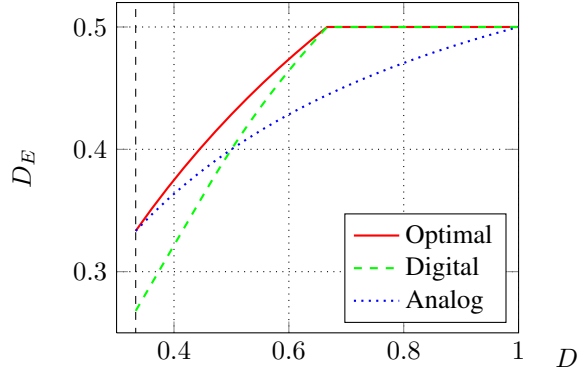
Figure 4: Quantity D_E as a function of the distortion level at Bob D ($P = 1$, $P_Y = 0.5$, $P_Z = 1$, $P_E = 1$).

Numerical Results: Fig. 4 represents the largest achievable D_E as a function of the distortion level at Bob D for

(i)   the optimal hybrid digital/analog scheme of Th. 4,

(ii)   the digital scheme of Prop. 1 (optimizing over μ),

(iii)   a pure analog scheme consisting of directly sending a scaled version of the source over the channel,

for parameter values $P = 1$, $P_Y = 0.5$, $P_Z = 1$, $P_E = 1$.

As a matter of fact, the proposed hybrid digital/analog scheme outperforms both pure analog and digital schemes.

Remark 2: While the analog scheme is optimal for $D = \frac{1}{1+\frac{P}{P_Y}}$ and, from Remark 1, the digital one is optimal for $D \geq \frac{1+\frac{P}{P_Z}}{1+\frac{P}{P_Y}}$, a time-sharing combination of these falls short to achieve the entire region, as shown by Fig. 4 and Theorem 4.

V. Secure Transmission of a Binary Source over a Type-II Wiretap Channel

A. System Model

Consider now the binary example first proposed in [9]. In this setup, the source is binary uniformly distributed ($A \sim \mathcal{B}\left(\frac{1}{2}\right)$) and the side information at Bob, resp. Eve, is the output of a binary erasure channel (BEC) with erasure probability $\beta \in [0,1]$, resp. a binary symmetric channel (BSC) with crossover probability $\epsilon \in [0, \frac{1}{2}]$, with input A. According to the values of (β, ϵ) these side informations satisfy the properties summarized in Fig. 5. The communication channel is similar to the one of [2]: It consists of a noiseless channel from Alice to Bob, and a BSC with crossover probability $\zeta \in [0, \frac{1}{2}]$, from Alice to Eve. Let the distortion level at Bob be zero *i.e.*, he performs *lossless* reconstruction.
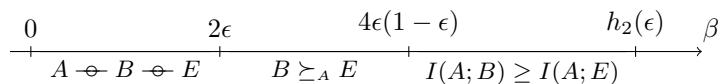

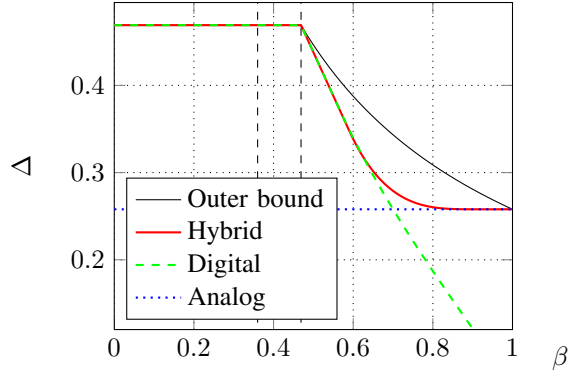Figure 5: Relative properties of the side informations.

Figure 6: Equivocation rate at Eve Δ as a function of the erasure probability β ($\epsilon = 0.1$, $\zeta = 0.1$).

B. Performance of Coding Schemes

Under the above assumptions, from [9, Proposition 3], the inner bound of Theorem 1 is maximized by choosing $V = A$ and a uniformly distributed binary auxiliary RV U (resp. Q), produced as the output of a BSC with crossover probability $u \in [0, \frac{1}{2}]$ (resp. $q \in [0, \frac{1}{2}]$), and input A (resp. X). Consider also the hybrid scheme of Theorem 3 choosing variables U, V and X as follows: $U = V \oplus W$, $V \overset{\perp\!\!\!\perp A}{\sim} \mathcal{B}(\frac{1}{2})$ and $X = V \oplus A$ where W is independent of A and V, and $W \sim \mathcal{B}(u)$ for some crossover probability $u \in [0, \frac{1}{2}]$.

Numerical Results: Fig. 6 represents the equivocation rate Δ as a function of the erasure probability β for

(i)   the outer bound *i.e.*, Theorem 2,

(ii)   the hybrid digital/analog scheme of Theorem 3 with U, V, X as defined above (and optimizing over u),

(iii) the digital scheme of [9, Proposition 3], optimizing over u and q,

(iv)   a pure analog scheme consisting of directly sending the source over the channel,

for parameter values $\epsilon = 0.1$, $\zeta = 0.1$.

As expected, if $\beta \leq 4\epsilon(1-\epsilon)$, B is less noisy than E, and the digital scheme is optimal, as well as the proposed hybrid one. Here, this result also seems to hold when B is only more capable than E *i.e.*, for $\beta \leq h_2(\epsilon)$.

For $\beta = 1$, as noted in [9], the naive pure analog scheme outperforms the digital one. According to the comments of Section III-C1, the proposed hybrid digital/analog scheme always performs as good as the analog one. In Fig. 6, the proposed hybrid digital/analog scheme also seems to perform as good as the digital one. However, according to the comments of Section III-C2, and depending on the parameters ϵ, ζ, this may not be the case for all values in $[h_2(\epsilon), 1]$.

REFERENCES

[1] C. Shannon, "Communication theory of secrecy systems," *BSTJ*, vol. 28, pp. 656–715, 1949.

[2] A. Wyner, "The wire-tap channel," *BSTJ*, vol. 54, no. 8, pp. 1355–1387, 1975.

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

[4] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. 19, no. 4, pp. 471–480, 1973.

[5] A. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Trans. Inf. Theory*, vol. 22, no. 1, pp. 1–10, 1976.

[6] V. Prabhakaran and K. Ramchandran, "On secure distributed source coding," in *Proc. ITW*, 2007, pp. 442–447.

[7] J. Villard and P. Piantanida, "Secure lossy source coding with side information at the decoders," in *Proc. Allerton*, 2010.

[8] N. Merhav, "Shannon's secrecy system with informed receivers and its application to systematic coding for wiretapped channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2723–2734, 2008.

[9] J. Villard, P. Piantanida, and S. Shamai, "Secure lossy source-channel wiretapping with side information at the receiving terminals," in *Proc. ISIT*, 2011.

[10] U. Mittal and N. Phamdo, "Hybrid digital-analog (HDA) joint source-channel codes for broadcasting and robust communications," *IEEE Trans. Inf. Theory*, vol. 48, no. 5, pp. 1082–1102, 2002.

[11] M. Wilson, K. Narayanan, and G. Caire, "Joint source channel coding with side information using hybrid digital analog codes," *IEEE Trans. Inf. Theory*, vol. 56, no. 10, pp. 4922–4940, 2010.

[12] D. Gündüz, J. Nayak, and E. Tuncel, "Wyner-Ziv coding over broadcast channels using hybrid digital/analog transmission," in *Proc. ISIT*, 2008.

[13] S. H. Lim, P. Minero, and Y.-H. Kim, "Lossy communication of correlated sources over multiple access channels," in *Proc. Allerton*, 2010.

[14] S. Gel'fand and M. Pinsker, "Coding for channel with random parameters," *Problem of Control and Inf. Theory*, vol. 9, pp. 19–31, 1980.

[15] Y. Liang, H. Poor, and S. Shamai, *Information theoretic security*.   Now Publishers, 2009.