



The Secret Key Capacity of a Class of Noisy Channels with Correlated Sources

Germán Bassi, Pablo Piantanida, Shlomo Shamai

► To cite this version:

Germán Bassi, Pablo Piantanida, Shlomo Shamai. The Secret Key Capacity of a Class of Noisy Channels with Correlated Sources. Entropy, 2019, 21 (8), pp.732. 10.3390/e21080732 . hal-02940461

HAL Id: hal-02940461

<https://centralesupelec.hal.science/hal-02940461>

Submitted on 16 Sep 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

Article

The Secret Key Capacity of a Class of Noisy Channels with Correlated Sources

Germán Bassi ^{1,*} , Pablo Piantanida ^{2,3}  and Shlomo Shamai (Shitz) ⁴ 

¹ School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology, 100 44 Stockholm, Sweden

² CentraleSupélec–French National Center for Scientific Research (CNRS)–Université Paris-Sud, 3 Rue Joliot-Curie, F-91192 Gif-sur-Yvette, France

³ Montreal Institute for Learning Algorithms (MILA), Université de Montréal, 2920 Chemin de la Tour, Montréal, QC H3T 1N8, Canada

⁴ Department of Electrical Engineering, Technion–Israel Institute of Technology, Haifa 32000, Israel

* Correspondence: germanb@kth.se

Received: 3 June 2019; Accepted: 25 July 2019; Published: 26 July 2019



Abstract: This paper investigates the problem of secret key generation over a wiretap channel when the terminals observe correlated sources. These sources are independent of the main channel and the users overhear them before the transmission takes place. A novel outer bound is proposed and, employing a previously reported inner bound, the secret key capacity is derived under certain less-noisy conditions on the channel or source components. This result improves upon the existing literature where the more stringent condition of degradedness is required. Furthermore, numerical evaluation of the achievable scheme and previously reported results for a binary model are presented; a comparison of the numerical bounds provides insights on the benefit of the chosen scheme.

Keywords: information-theoretic security; secret key agreement; secret key capacity; wiretap channel; correlated sources

1. Introduction

The wiretap channel, introduced by Wyner [1], is the basic model for analyzing secrecy in wireless communications. In this model, the transmitter, named Alice, wants to communicate reliably with Bob while keeping the transmitted message—or part of it—secret from an eavesdropper, named Eve, overhearing the communication through another channel. Secrecy is characterized by the amount of information that is not leaked, which can be measured by the equivocation rate—the remaining uncertainty about the message at the eavesdropper. The secrecy capacity of the wiretap channel is thus defined as the maximum transmission rate that can be attained with zero leakage. In their influential paper [2], Csiszár and Körner determined the rate-equivocation region of a general broadcast channel with any arbitrary level of security, which also establishes the secrecy capacity of the wiretap channel. These schemes guarantee secrecy by exploiting an artificial random noise that saturates the eavesdropper’s decoding capabilities.

On the other hand, Shannon [3] showed that it is also possible to achieve a positive secrecy rate by means of a *secret key*. Alice and Bob can safely communicate over a noiseless public broadcast channel as long as they share a secret key. The rate of this key, however, must be at least as large as the rate of the message to attain zero leakage. The main question that arises in this scenario is therefore: how do the legitimate users safely share the secret key? The answer is that the users should not communicate the key itself, which would then be compromised. Instead, they should only convey enough information to allow themselves to agree upon a key without disclosing, at the same time,

any relevant information about it to the eavesdropper (for further discussion, the reader is referred to [4,5]).

In this work, we study the problem of secret key generation over a wiretap channel with correlated sources at each terminal. These sources are assumed to be independent of the main channel and there is no additional public broadcast channel of finite or infinite rate, as seen in Figure 1. It is assumed that each node acquires the n -sequence observation of its corresponding source before the communication begins.

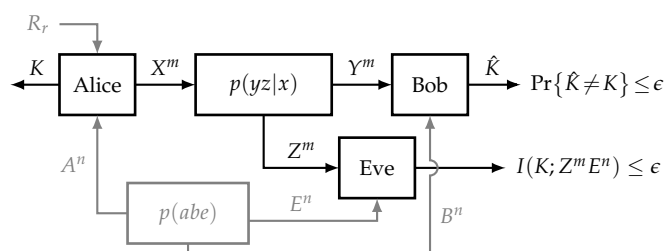


Figure 1. System model for the problem of secret key generation. Every node has access to one of the correlated sources (A, B, E), whereas R_r is the local randomness only used by Alice.

1.1. Related Work

Maurer [6] and Ahlswede and Csiszár [7] were among the first to study the use of correlated observations available at the legitimate users as a means to agree upon a key. In addition to the correlated observations, the terminals may communicate over a public broadcast channel of infinite capacity to which the eavesdropper has also access. Two models are proposed in [7]: the “source model”, where the users observe correlated random sources controlled by nature, and the “channel model”, where the users observe inputs and outputs of a noisy channel controlled by one of the users. In [8], Csiszár and Narayan studied the first model but assumed that the public broadcast channel has finite capacity and there is a third “helper” node who is not interested in recovering the key but rather helping Alice and Bob. The same authors also analyzed the channel model with only one [9] or with multiple channel inputs [10]. Capacity results are presented in [8–10] assuming that there is only one round of communication over the public channel. General inner and outer bounds for both source and channel models with interaction over the public channel were introduced by Gohari and Anantharam [11,12].

More recently, Khisti et al. [13] investigated the situation where there is no helper node, the users communicate over a wiretap channel, and a separate public discussion channel may or may not be available. The simultaneous transmission of a secret message along with a key generation scheme using correlated sources was analyzed by Prabhakaran et al. [14]. They obtained a simple expression that reveals the trade-off between the achievable secrecy rate and the achievable rate of the secret key. The corresponding Gaussian channel with correlated Gaussian sources but independent of the channel components is recently studied in [15]. Closed form expressions for both secret key generation and secret message transmission are derived. On the other hand, Salimi et al. [16] considered simultaneous key generation of two independent users over a multiple access channel with feedback, where each user eavesdrops the other. In addition, the receiver can actively send feedback, through a private noiseless (or noisy) link, to increase the size of the shared keys.

The authors of [13–15] did not assume interactive communication, i.e., there is only one round of communication. Salimi et al. [16], however, allowed the end user to respond once through the feedback link. Other authors have analyzed key generation schemes that rely on several rounds of transmissions. Tyagi [17] characterized the minimum communication rate required to generate a maximum-rate secret key with r rounds of interactive communication. He showed that this rate is equal to the *interactive common information* (a quantity he introduces) minus the secret key capacity. In his model, two users observe i.i.d. correlated sources and communicate over an error-free channel. Hayashi et al. [18]

studied a similar problem but consider general (not necessarily i.i.d.) source sequences of finite length. Their proposed protocol attains the secret key capacity for general observations as well as the second-order asymptotic term of the maximum feasible secret key length for i.i.d. observations. They also proved that the standard one-way communication protocol fails to attain the aforementioned asymptotic result. Courtade and Halford [19] analyzed the related problem of how many rounds of public transmissions are required to generate a specific number of secret keys. Their model assumes that there are n terminals connected through an error-free public channel, where each terminal is provided with a number of messages before transmission that it uses to generate the keys. More recently, Boche et al. [20] investigated the computability of the secret key in the source model with only one forward communication. They showed that the corresponding secret key capacity is not Turing computable when the public communication is rate-limited, and consequently there is no algorithm that can simulate or compute the secret key capacity.

As previously mentioned, the focus of the present work is on sources that are independent of the main channel; nonetheless, some works have addressed the general situation of correlated sources and channels. Prior work on secrecy for channels with state include Chen and Vinck's [21] and Liu and Chen's [22] analyses of the wiretap channel with state. These works employ Gelfand and Pinsker's scheme [23] to correlate the transmitted codeword with the channel state at the same time that it saturates the eavesdropper's decoding capabilities. A single-letter expression of the secrecy capacity for this model is still unknown, although a multi-letter bound was provided by Muramatsu [24] and a novel lower bound is recently reported in [25]. As a matter of fact, the complexity of this problem also lies in the derivation of an outer bound that can handle simultaneously secrecy and channels with state.

To the best of our knowledge, only a handful of works have studied the problem of key generation for channels with state. The previously mentioned result of Prabhakaran et al. [14] is one of these examples. Zibaeenejad [26] analyzed a similar scenario where there is also a public channel of finite capacity between the users and he provides an inner and an outer bound for this model. Although the inner bound is developed for a channel with state, it is possible to apply it to the model used in the present work, i.e., sources independent of the main channel. However, some steps of the proof reported in [26] appear to be obscure and a constraint seems to be missing in the final expression; the resulting achievable rate was recently shown in [27] to be in certain cases unachievable. As a consequence, we decided not to compare our inner bound to this previously reported scheme.

1.2. Contributions and Organization of the Paper

In this work, we introduce a novel outer bound (Theorem 2) for the problem of secret key generation over a wiretap channel with correlated sources at each terminal. The correlated sources are assumed to be independent of the main channel and, thanks to a previously reported inner bound (Theorem 1), we obtain the capacity region (Propositions 1–3) whenever the channel and/or source components satisfy the specific *less-noisy* conditions described in Table 1. In contrast, the proposed schemes in [13–16] are optimal only when the stronger *degradedness* condition holds true for the channel and source components.

The results and tools introduced in this work have connections to ones in a previous work of ours [28], where we studied both the secrecy capacity and the secret key capacity of the wiretap channel with generalized feedback. In [28], we determined some capacity regions for the problem dealt here as a secondary result of the main problem. It is not surprising that, by being the main focus of the present work, the capacity results shown here are more general than those in [28]. Furthermore, we go deeper into the analysis of secret key agreement schemes and we show, in Section 4, the suboptimality of a previously published achievable scheme.

This paper is organized as follows. Section 2 provides some definitions and the previously reported inner bound. In Section 3, we first present the outer bound for the problem of secret key agreement and then we enumerate the cases where we obtain the capacity region. Section 4 illustrates

with a binary example the benefit of the present inner bound over a previously reported scheme. Finally, Section 5 summarizes and concludes the work, while some technical proofs are deferred to the appendices.

1.3. Notation and Conventions

Throughout this work, we use the standard notation of El Gamal and Kim [29]. Specifically, given two integers i and j , the expression $[i : j]$ denotes the set $\{i, i + 1, \dots, j\}$, whereas for real values a and b , $[a, b]$ denotes the closed interval between a and b . We use the notation $x_i^j = (x_i, x_{i+1}, \dots, x_j)$ to denote the sequence of length $j - i + 1$ for $1 \leq i \leq j$. If $i = 1$, we drop the subscript for succinctness, i.e., $x^j = (x_1, x_2, \dots, x_j)$. Lowercase letters such as x and y are mainly used to represent constants or realizations of random variables, capital letters such as X and Y stand for the random variables in itself, and calligraphic letters such as $\mathcal{X}$ and $\mathcal{Y}$ are reserved for sets, codebooks, or special functions.

The set of nonnegative real numbers is denoted by $\mathbb{R}_+$. The probability distribution (PD) of the random vector X^n , $p_{X^n}(x^n)$, is succinctly written as $p(x^n)$ without subscript when it can be understood from the argument x^n . Given three random variables X , Y , and Z , if its joint PD can be decomposed as $p(xyz) = p(x)p(y|x)p(z|y)$, then they form a Markov chain, denoted by $X \dashv Y \dashv Z$. The random variable Y is said to be *less noisy* than Z w.r.t. X if $I(U; Y) \geq I(U; Z)$ for each random variable U such that $U \dashv X \dashv (Y, Z)$; this relation is denoted by $Y \succeq_X Z$. Entropy is denoted by $H(\cdot)$ and mutual information, $I(\cdot; \cdot)$. The expression $[x]^+$ denotes $\max\{x, 0\}$. Given $u, v \in [0, 1]$, the function $h_2(u) \triangleq -u \log_2 u - (1 - u) \log_2 (1 - u)$ is the binary entropy function and $u * v \triangleq u(1 - v) + v(1 - u)$. We denote typical and conditional typical sets by $\mathcal{T}_\delta^n(X)$ and $\mathcal{T}_\delta^n(Y|x^n)$, respectively.

2. Preliminaries

2.1. Problem Definition

Consider the *wiretap channel with correlated sources* at every node (A, B, E) , as shown in Figure 1. The legitimate users (Alice and Bob) want to agree upon a secret key $K \in \mathcal{K}$ while an eavesdropper (Eve) is overhearing the communication. Let $\mathcal{A}$, $\mathcal{B}$, $\mathcal{E}$, $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$ be six finite sets. Alice, Bob, and Eve observe the random sequences (sources) A^n , B^n , and E^n , respectively, drawn i.i.d. according to the joint distribution $p(abe)$ on $\mathcal{A} \times \mathcal{B} \times \mathcal{E}$. Alice communicates with Bob through m instances of a discrete memoryless channel with input $X \in \mathcal{X}$ and output $Y \in \mathcal{Y}$. Eve is listening the communication through another channel with input $X \in \mathcal{X}$ and output $Z \in \mathcal{Z}$. This channel is defined by its transition probability $p(yz|x)$ and it is independent of the sources' distribution.

Definition 1 (Code). A $(2^{nR_k}, n, m)$ secret key code c_n for this model consists of:

- a key set $\mathcal{K}_n \triangleq [1 : 2^{nR_k}]$, where R_k is the rate of the secret key;
- a source of local randomness $R_r \in \mathcal{R}_r$ at Alice;
- an encoding function $\varphi: \mathcal{A}^n \times \mathcal{R}_r \rightarrow \mathcal{X}^m$;
- a key generation function $\psi_a: \mathcal{A}^n \times \mathcal{R}_r \rightarrow \mathcal{K}_n$; and
- a key generation function $\psi_b: \mathcal{B}^n \times \mathcal{Y}^m \rightarrow \mathcal{K}_n$.

The rate of such a code is defined as the number of channel uses per source symbol $\frac{m}{n}$.

Given a code, let $K = \psi_a(A^n, R_r)$ and $X^m = \varphi(A^n, R_r)$; then, the performance of the $(2^{nR_k}, n, m)$ secret key code c_n is measured in terms of its average probability of error

$$P_e(c_n) \triangleq \Pr\{\psi_b(B^n, Y^m) \neq K | c_n\}, \quad (1)$$

in terms of the information leakage

$$L_k(c_n) \triangleq I(K; E^n Z^m | c_n), \quad (2)$$

and in terms of the uniformity of the keys

$$U_k(c_n) \triangleq nR_k - H(K|c_n). \quad (3)$$

Definition 2 (Achievability). A tuple $(\eta, R_k) \in \mathbb{R}_+^2$ is said to be achievable for this model if, for every $\epsilon > 0$ and sufficiently large n , there exists a $(2^{nR_k}, n, m)$ secret key code c_n such that

$$\frac{m}{n} \leq \eta + \epsilon, \quad P_e(c_n) \leq \epsilon, \quad L(c_n) \leq \epsilon, \quad \text{and} \quad U(c_n) \leq \epsilon. \quad (4)$$

The set of all achievable tuples is denoted by $\mathcal{R}^*$ and is referred to as the secret key region.

2.2. Inner Bound

The following theorem gives an inner bound on $\mathcal{R}^*$, i.e., it defines the region $\mathcal{R}_{\text{in}} \subseteq \mathcal{R}^*$.

Theorem 1 ([30], Theorem 2). A tuple $(\eta, R_k) \in \mathbb{R}_+^2$ is achievable if there exist random variables U, V, Q, T , and X on finite sets $\mathcal{U}, \mathcal{V}, \mathcal{Q}, \mathcal{T}$, and $\mathcal{X}$, respectively, with joint distribution $p(uvqtxyzabe) = p(q|t)p(tx)p(yz|x)p(abe)p(v|a)p(u|v)$, which verify

$$R_k \leq \eta [I(T; Y|Q) - I(T; Z|Q)] + I(V; B|U) - I(V; E|U) \quad (5)$$

subject to

$$I(U; A|B) \leq \eta I(Q; Y), \quad (6a)$$

$$I(V; A|B) \leq \eta I(T; Y). \quad (6b)$$

Moreover, it suffices to consider sets $\mathcal{U}, \mathcal{V}, \mathcal{Q}$, and $\mathcal{T}$ such that $|\mathcal{U}| \leq |\mathcal{A}| + 2$, $|\mathcal{V}| \leq (|\mathcal{A}| + 1)(|\mathcal{A}| + 2)$, $|\mathcal{Q}| \leq |\mathcal{X}| + 2$, and $|\mathcal{T}| \leq (|\mathcal{X}| + 1)(|\mathcal{X}| + 2)$.

Sketch of Proof. Alice employs the two-layer description (U, V) to compress the source A and she transmits it through the two-layer channel codeword (Q, T) . Each layer of the description must fit in the corresponding layer of the channel codeword according to Equation (6). In brief, the encoder randomly picks codewords $u^n(s_1)$ from $\mathcal{T}_\delta^n(U)$ and, for each one, it randomly picks codewords $v^n(s_1, s_2)$ from $\mathcal{T}_\delta^n(V|u^n(s_1))$. After observing the source sequence a^n , the encoder selects the indices $(\hat{s}_1, \hat{s}_2)$ of the codewords that are jointly typical with a^n . The codewords $u^n(s_1)$ and $v^n(s_1, s_2)$ are distributed in bins, i.e., $u^n(s_1) \in \mathcal{B}_1(r_1)$ and $v^n(s_1, s_2) \in \mathcal{B}_2(s_1, r_2, r_p)$, and it is the bin indices $(\hat{r}_1, \hat{r}_2, \hat{r}_p)$ which are transmitted through the noisy channel. The channel codewords $q^m(r_1, r_2)$ are randomly picked from $\mathcal{T}_\delta^m(Q)$ and, for each $q^m(r_1, r_2)$, the codewords $t^m(r_1, r_2, r_p, k_2, r_f)$ are randomly picked from $\mathcal{T}_\delta^m(T|q^m(r_1, r_2))$. In addition to the bin indices from the two-layer description of the source, the encoder uses the noisy channel to transmit a part of the secret key (k_2) , which is protected using a wiretap code; the dummy index r_f corresponds to the artificial noise used to exhaust the decoding capabilities of the eavesdropper. Once the decoder successfully decodes the channel and source codewords using its side information b^n , it can obtain the other part of the key (k_1) from another bin index of the source codeword, i.e., $v^n(s_1, s_2) \in \mathcal{B}_2(s_1, r_2, k_1)$. We note that the achievable secret key rate in Equation (5) is a combination of the secret bits transmitted through the noisy channel in the manner of the wiretap channel and the secret bits obtained by the reconstruction of the source at Bob.

The inner bound in [30] is obtained using the *weak* secrecy and uniformity conditions, i.e., $L(c_n) \leq n\epsilon$ and $U(c_n) \leq n\epsilon$. However, an improved proof of the inner bound is found in [31], which shows that the *strong* secrecy and uniformity conditions in Equation (4) also hold true. We refer the interested reader to [30,31] for a detailed proof of the inner bound. $\square$

Remark 1. By setting $U = \emptyset$, the region in Theorem 1 recovers the results in ([13], Theorems 1 and 4), when the eavesdropper has access to a correlated source, and ([14], Theorem 2), when there is no secret message to be transmitted. The advantage of having two layers of description is that Theorem 1 can potentially achieve higher secret key rates (see Section 4) and it recovers the result of Csiszár and Narayan [8] (see Remark 6).

Remark 2. The inner bound in Theorem 1 is a special case of the inner bound recently proposed in [27] for a more general system model.

Remark 3. The region in Theorem 1 also recovers the result in ([32], Theorem 1) which was published after the original submission of Bassi et al. [30]. In that work, Alice and Bob communicate over a public noiseless channel of rate R_1 and a secure noiseless channel of rate R_2 . The proposed achievable scheme in [32] sends the codeword Q through the public channel, i.e., $I(Q; Y) = R_1$, and the codeword T through the secure channel, i.e., $I(T; Y|Q) = R_2$ and $I(T; Z|Q) = 0$. The reader may verify that, by using the aforementioned quantities and $\eta = 1$, both regions are equal.

3. Main Results

In this section, we first introduce an outer bound for the secret key region (Theorem 2). We then study some special cases where the inner bound of Theorem 1 turns out to achieve the (optimal) secret key region (Propositions 1–3).

3.1. Outer Bound

The following theorem gives an outer bound on $\mathcal{R}^*$, i.e., it defines the region $\mathcal{R}_{\text{out}} \supseteq \mathcal{R}^*$.

Theorem 2. An outer bound on the secret key region for this channel model is given by

$$R_k \leq \max_{p \in \mathcal{P}} \{ \eta [I(T; Y) - I(T; Z)] + I(V; B|U) - I(V; E|U) \} \quad (7)$$

subject to

$$I(V; A|B) \leq \eta I(X; Y), \quad (8)$$

where $\mathcal{P}$ is the set of all input probability distributions given by

$$\mathcal{P} = \{ p(tx y z u v a b e) = p(tx)p(yz|x)p(a b e)p(v|a)p(u|v) \} \quad (9)$$

with $|\mathcal{T}| \leq |\mathcal{X}|$, $|\mathcal{U}| \leq |\mathcal{A}| + 1$, and $|\mathcal{V}| \leq (|\mathcal{A}| + 1)^2$.

Proof. Refer to Appendix A for details. $\square$

Theorem 2 shows that the secret key generated between Alice and Bob has two components. The first two terms on the r.h.s. of Equation (7) represent the part of the key that is securely transmitted through the noisy channel (given by the random variable T) as in the wiretap channel. On the other hand, the last two terms on the r.h.s. of Equation (7) characterize the part of the key that is securely extracted from the correlated sources (given by the random variables U and V). Since the source and channel variables are independent in the model, it should not be surprising that the variable T is independent of (U, V) . However, given that the users need to agree on common extracted bits from the source, the noisy channel imposes the restriction in Equation (8) on the amount of information exchanged during that agreement.

Remark 4. The regions $\mathcal{R}_{\text{out}}$ and $\mathcal{R}_{\text{in}}$ do not coincide in general. This is due to the presence of the condition in Equation (6a) in the inner bound, and the looser condition in Equation (8) in the outer bound with respect to Equation (6b). We present in Section 3.2 a few special cases where these differences disappear and both regions coincide.

Remark 5. We note that, although the model defines source and channel sequences of potentially different lengths, the final bounds in Equations (7) and (8) are single-letter and they are calculated using the single-letter probability distribution in Equation (9). The difference in sequence length is captured by the coefficient η defined in Equation (4).

3.2. Optimal Characterization of the Secret Key Rate

The inner bound $\mathcal{R}_{\text{in}}$ is optimal under certain less-noisy conditions on the channel and/or source components. These special cases are summarized in Table 1 and explained in the sequel.

Table 1. Regimes where Theorem 1 is optimal. No secret key is achievable if $Z \succeq_X Y$ and $E \succeq_A B$.

$Z \succeq_X Y$		$Y \succeq_X Z$	
$E \succeq_A B$	$B \succeq_A E$	$E \succeq_A B$	$B \succeq_A E$
$R_k = 0$	Proposition 1	Proposition 2	Proposition 3

3.2.1. Eve Has a Less Noisy Channel

If Eve has a less noisy channel than Bob, i.e., $Z \succeq_X Y$, the information transmitted over the channel is compromised. Therefore, the amount of secret key that can be generated only depends on the statistical differences between the sources.

Proposition 1. If $Z \succeq_X Y$, a tuple $(\eta, R_k) \in \mathbb{R}_+^2$ is achievable if and only if there exist random variables U , V , and X on finite sets $\mathcal{U}$, $\mathcal{V}$, and $\mathcal{X}$, respectively, with joint distribution $p(uvabxyz) = p(u|v)p(v|a)p(a|b)p(x)p(yz|x)$, which verify

$$R_k \leq I(V; B|U) - I(V; E|U) \quad (10a)$$

$$\text{subject to } I(V; A|B) \leq \eta I(X; Y). \quad (10b)$$

Proof. Given the less-noisy condition on Eve's channel, i.e., $I(T; Y) \leq I(T; Z)$ for any RV T such that $T \oplus X \oplus (YZ)$, the bound in Equation (7) is maximized with $T = \emptyset$. On the other hand, the region in Equation (10) is achievable by setting auxiliary RVs $Q = T = X$ in $\mathcal{R}_{\text{in}}$. $\square$

Remark 6. The secret key capacity of the wiretap channel with a public noiseless channel of rate R ([8], Theorem 2.6) turns out to be a special case of Proposition 1, where $X = Y = Z$ and defining $\eta H(X) = \eta \log |\mathcal{X}| \equiv R$.

3.2.2. Eve Has a Less Noisy Source

If Eve has a less noisy source than Bob, i.e., $E \succeq_A B$, the amount of secret key that can be generated depends on the amount of secure information transmitted through the wiretap channel.

Proposition 2. If $E \succeq_A B$, a tuple $(\eta, R_k) \in \mathbb{R}_+^2$ is achievable if and only if there exist random variables T and X on finite sets $\mathcal{T}$ and $\mathcal{X}$, respectively, with joint distribution $p(tx yz) = p(tx)p(yz|x)$, which verify

$$R_k \leq \eta [I(T; Y) - I(T; Z)]. \quad (11)$$

Proof. Given the less-noisy condition on Eve's source, i.e., $I(V; B) \leq I(V; E)$ for any RV V such that $V \oplus A \oplus (BE)$, the bound in Equation (7) is maximized with $U = V$ and independent of the sources. The region in Equation (11) is achievable by using the same auxiliary RVs in the inner bound as in the outer bound. $\square$

Remark 7. The bound in Equation (11) is equal to the secrecy capacity of the wiretap channel.

Remark 8. Even though the bound in Equation (11) becomes independent of the sources sequences (A^n, B^n, E^n) , we assume $n \neq 0$, and thus the rate η is finite.

3.2.3. Bob Has a Less Noisy Channel and Source

If Bob has a less noisy channel and source than Eve, i.e., $Y \succeq_X Z$ and $B \succeq_A E$, the lower layers of the channel and source codewords are no longer needed.

Proposition 3. If $Y \succeq_X Z$ and $B \succeq_A E$, a tuple $(\eta, R_k) \in \mathbb{R}_+^2$ is achievable if and only if there exist random variables V and X on finite sets $\mathcal{V}$ and $\mathcal{X}$, respectively, with joint distribution $p(vabxyz) = p(v|a)p(abe)p(x)p(yz|x)$, which verify

$$R_k \leq \eta [I(X; Y) - I(X; Z)] + I(V; B) - I(V; E) \quad (12a)$$

$$\text{subject to } I(V; A|B) \leq \eta I(X; Y). \quad (12b)$$

Proof. Given the less-noisy conditions on Bob's channel and source, the bound in Equation (7) is maximized with $U = \emptyset$ and $T = X$. The region in Equation (12) is achievable by also setting auxiliary RVs $U = Q = \emptyset$ and $T = X$ in the inner bound. $\square$

Remark 9. Proposition 3 extends the results from ([13], Theorem 4) and ([14], Theorem 3) which assume the more stringent conditions of degradedness: $A \rightarrow B \rightarrow E$ and $X \rightarrow Y \rightarrow Z$.

4. Secret Key Agreement over a Wiretap Channel with BEC/BSC Sources

As mentioned in Remark 1, the inner bound introduced in Section 2.2 employs two layers of description, and thus it is an improvement over previously reported results. In this section, we compare the performance of this achievable scheme with the scheme in [13] for a specific binary source and channel model.

4.1. System Model

Consider the communication system depicted in Figure 2. The main channel consists of a noiseless link from Alice to Bob and a binary symmetric channel (BSC) with crossover probability $\zeta \in [0, \frac{1}{2}]$ from Alice to Eve (see Figure 2a). Additionally, the three nodes have access to correlated sources; in particular, Alice observes a binary uniformly distributed source, i.e., $A \sim \mathcal{B}(\frac{1}{2})$, which is the input of two parallel channels, as shown in Figure 2b. Bob observes the output of a binary erasure channel (BEC) with erasure probability $\beta \in [0, 1]$, and Eve, a BSC with crossover probability $\epsilon \in [0, \frac{1}{2}]$. For simplicity, we assume $\eta = 1$ in the sequel.

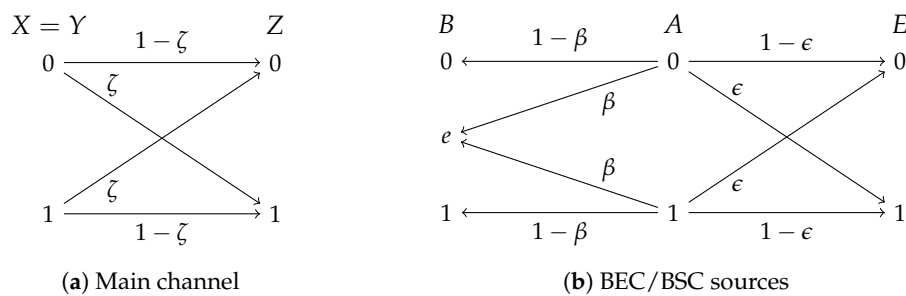


Figure 2. System model for the wiretap channel with BEC/BSC sources.

Remark 10. The sources (A, B, E) satisfy different properties according to the values of the parameters (β, ϵ) [33], specifically:

- If $0 \leq \beta < 2\epsilon$, E is a degraded version of B , i.e., $A \rightarrow B \rightarrow E$.
- If $2\epsilon \leq \beta < 4\epsilon(1 - \epsilon)$, B is less noisy than E , i.e., $B \succeq_A E$.
- If $4\epsilon(1 - \epsilon) \leq \beta < h_2(\epsilon)$, B is more capable than E .

4.2. Performance of the Coding Scheme

The following proposition provides a simple expression of the inner bound from Theorem 1. The expression is obtained by simplifying the maximization process of the input distribution, and thus it might not be optimal. However, this suffices to show the higher rates achieved by this scheme as we see later.

Proposition 4. The tuple $(\eta = 1, R_k) \in \mathcal{R}_{in}$ if there exist $u, v, q \in [0, \frac{1}{2}]$ such that:

$$R_k \leq (1 - \beta)[h_2(v * u) - h_2(v)] + h_2(v * \epsilon) - h_2(v * u * \epsilon) + h_2(\zeta) + h_2(q) - h_2(\zeta * q), \quad (13a)$$

$$\text{subject to } \beta[1 - h_2(v * u)] \leq 1 - h_2(q). \quad (13b)$$

Proof. The bound in Equation (13) is directly calculated from Equations (5) and (6a) with the following choice of input random variables: $T = X$, $Q = X \oplus Q'$, $V = A \oplus V'$, and $U = V \oplus U'$. Here, $X \sim \mathcal{B}(\frac{1}{2})$, $Q' \sim \mathcal{B}(q)$, $V' \sim \mathcal{B}(v)$, and $U' \sim \mathcal{B}(u)$, and each random variable is independent of each other and (A, B, E) . The condition in Equation (6b) in the inner bound becomes redundant with the aforementioned choice of input distribution. $\square$

As previously mentioned, we provide next the inner bound presented in ([13], Theorem 4) as a means of comparison. This inner bound is similar to Theorem 1 but with only one layer of description for the source A ; thus, its achievable region is denoted $\mathcal{R}_{in-1L}$. We note that Theorem 4 from [13] is actually a capacity result assuming that $A \rightarrow B \rightarrow E$ and $X \rightarrow Y \rightarrow Z$. In our present example, only the second Markov chain holds independently of the value of the parameters β and ϵ , but this does not invalidate the use of the inner bound.

Proposition 5 ([13], Theorem 4). The tuple $(\eta = 1, R_k) \in \mathcal{R}_{in-1L}$ if and only if

$$R_k \leq [h_2(\epsilon) - \beta]^+ + h_2(\zeta). \quad (14)$$

Proof. See Appendix B. $\square$

Remark 11. Proposition 5 is a special case of Proposition 4 with $u = q = \frac{1}{2}$, and $v = 0$ or $v = \frac{1}{2}$. As mentioned in Remark 1, the inner bound ([13], Theorem 4) is a special case of Theorem 1 with $U = \emptyset$ (thus $u = \frac{1}{2}$). Moreover, given that in this model the Markov chain $X \rightarrow Y \rightarrow Z$ holds, the channel codebook of Proposition 5 only has one layer (thus $q = \frac{1}{2}$). On the other hand, there are two layers of description in Proposition 4, and whenever $U \neq \emptyset$ (i.e., $u < \frac{1}{2}$), we have that $Q \neq \emptyset$ (i.e., $q < \frac{1}{2}$). This relationship is determined by Equation (13b).

We performed numerical optimization of the bound in Equation (13) for different values of β while fixing $\zeta = 0.01$ and $\epsilon = 0.05$; the results are shown in Figure 3 along with the bound in Equation (14). We see in the figure the advantage of having two layers of description for the source A . The proposed scheme in Proposition 4 attains higher secret key rates than the scheme with only one layer of description (Proposition 5) for intermediate values of β . It is in this regime, when the source B is no longer less noisy than E , that two layers of description are needed.

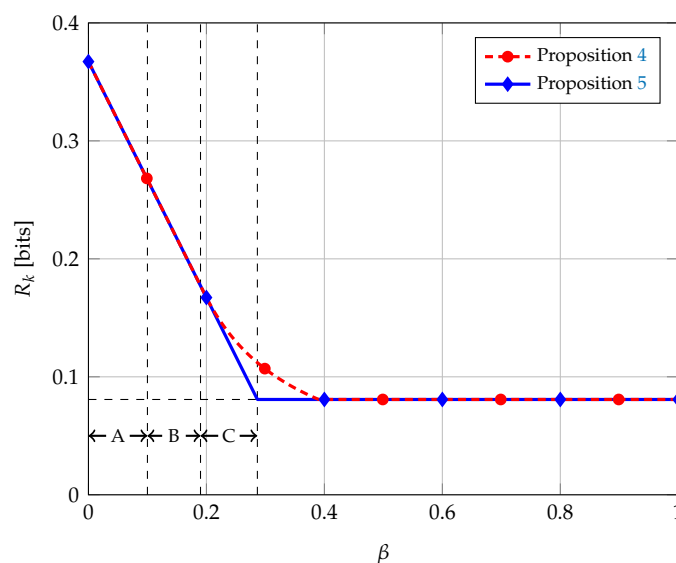


Figure 3. Achievable secret key rates for the wiretap channel with BEC/BSC sources, with $\zeta = 0.01$ and $\epsilon = 0.05$. In Region A, $A \oplus B \oplus E$; in Region B, $B \succeq_A E$; and, in Region C, B is more capable than E . The horizontal dotted line corresponds to the secrecy capacity of the main channel, i.e., $h_2(\zeta)$.

5. Summary and Concluding Remarks

In this work, we investigated the problem of secret key generation over a noisy channel in presence of correlated sources (independent of the main channel) at all terminals. We introduced a novel outer bound for this channel model, which allowed us to show that a particular achievable scheme is optimal for all classes of less-noisy sources and channels (Propositions 1–3). In Section 4, we further compared the performance of the aforementioned achievable scheme with a previously reported result for a simple binary model. Numerical computation of the corresponding bounds provided interesting insights on the regimes where the achievable scheme outperforms the previous one.

This work, however, does not address the scenario where the sources and the noisy channel are correlated. The extension of the previously mentioned result of Prabhakaran et al. [14] by using two description layers is a natural consequence. Indeed, this extension—posterior to the short version of the present work in [30]—has been recently addressed in [27]. By using two description layers, the proposed achievable scheme recovers the present inner bound for $\eta = 1$ provided that the sources are independent of the channel.

Author Contributions: Conceptualization, G.B. and P.P.; formal analysis, G.B.; supervision, P.P. and S.S.; validation, P.P.; writing—original draft preparation, G.B.; and writing—review and editing, G.B., P.P., and S.S.

Funding: The work of G.B. was funded in part by the Knut and Alice Wallenberg foundation and the Swedish Foundation for Strategic Research, and the work of S.S. was supported by the European Union’s Horizon 2020 Research and Innovation Programme, grant agreement no. 694630.

Acknowledgments: G.B. is grateful to Mikael Skoglund for valuable discussions at the early stage of this work.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

i.i.d.	independent and identically distributed
r.h.s.	right-hand side
w.r.t.	with respect to

Appendix A. Proof of Theorem 2

The outer bound is derived by following similar steps to those in ([28], Theorem 4) which assumes $\eta = 1$. It is reproduced here for completeness.

Let (η, R_k) be an achievable tuple according to Definition 2, and $\epsilon > 0$. Then, there exists a $(2^{nR_k}, n, m)$ secret key code c_n with functions $\varphi(\cdot)$, $\psi_a(\cdot)$, and $\psi_b(\cdot)$ such that

$$X^m = \varphi(A^n, R_r), \quad (\text{A1a})$$

$$K = \psi_a(A^n, R_r), \quad (\text{A1b})$$

$$\hat{K} = \psi_b(B^n, Y^m), \quad (\text{A1c})$$

that verify

$$\frac{m}{n} \leq \eta + \epsilon, \quad (\text{A2a})$$

$$\Pr\{K \neq \hat{K}\} \leq \epsilon, \quad (\text{A2b})$$

$$I(K; E^n Z^m) \leq \epsilon, \quad (\text{A2c})$$

$$nR_k - H(K) \leq \epsilon, \quad (\text{A2d})$$

where we have dropped the conditioning on the codebook c_n from Equations (A2b)–(A2d) and all subsequent calculations for clarity. Before continuing, we present the following remark that is useful to establish Markov chains between the random variables.

Remark A1. From the fact that random variables A_i, B_i, E_i are independent across time and the channel $X \mapsto (Y, Z)$ is memoryless and without feedback, the joint distribution of $(K, A^n, B^n, E^n, X^m, Y^m, Z^m)$ can be written as follows. For each $i \in [1 : n]$ and each $j \in [1 : m]$, we have

$$p(k, a^n, b^n, e^n, x^m, y^m, z^m) = p(a^{i-1}, b^{i-1}, e^{i-1}) p(a_i, b_i, e_i) p(a_{i+1}^n, b_{i+1}^n, e_{i+1}^n) \\ \times p(k, x^m | a^n) p(y^{j-1}, z^{j-1} | x^{j-1}) p(y_j, z_j | x_j) p(y_{j+1}^m, z_{j+1}^m | x_{j+1}^m), \quad (\text{A3})$$

where $P_\varphi(x^m | a^n) = \sum_{\forall k} p(k, x^m | a^n)$ and $P_{\psi_a}(k | a^n) = \sum_{\forall x^m} p(k, x^m | a^n)$ are the distributions of the stochastic functions in Equations (A1a) and (A1b), respectively.

We may now carry on with the derivation of the outer bound. First, consider,

$$nR_k \leq H(K) + \epsilon \quad (\text{A4a})$$

$$= H(K | E^n Y^m) + I(K; E^n Y^m) + \epsilon \\ \leq H(K | E^n Y^m) + I(K; E^n Y^m) - I(K; E^n Z^m) + 2\epsilon \quad (\text{A4b})$$

$$= H(K | E^n Y^m) + I(K; Y^m | E^n) - I(K; Z^m | E^n) + 2\epsilon \\ \leq H(K | E^n Y^m) - H(K | B^n Y^m) + I(K; Y^m | E^n) - I(K; Z^m | E^n) + n\epsilon' \quad (\text{A4c})$$

$$= \underbrace{I(K; B^n | Y^m) - I(K; E^n | Y^m)}_{R_s} + \underbrace{I(K; Y^m | E^n) - I(K; Z^m | E^n)}_{R_c} + n\epsilon', \quad (\text{A4d})$$

where

- Equation (A4a) stems from the uniformity of the keys in Equation (A2d).
- Equation (A4b) is due to the security condition in Equation (A2c).
- Equation (A4c) follows from Equations (A1) and (A2b), and Fano's inequality, $H(K | B^n Y^m) \leq n\epsilon$.

We now study separately the “source” term R_s and the “channel” term R_c . Hence,

$$R_s = \sum_{i=1}^n I(K; B_i | Y^m B^{i-1}) - I(K; E_i | Y^m E_{i+1}^n) \\ = \sum_{i=1}^n I(K; B_i | Y^m B^{i-1} E_{i+1}^n) - I(K; E_i | Y^m B^{i-1} E_{i+1}^n) \quad (\text{A5a})$$

$$= \sum_{i=1}^n I(V_i; B_i | U_i) - I(V_i; E_i | U_i) \quad (\text{A5b})$$

$$= n[I(V_J; B_J | U_J J) - I(V_J; E_J | U_J J)] \quad (\text{A5c})$$

$$= n[I(V; B | U) - I(V; E | U)], \quad (\text{A5d})$$

where

- Equation (A5a) is due to Csiszár sum identity.
- Equation (A5b) follows from the definition of the auxiliary RVs $U_i = (Y^m B^{i-1} E_{i+1}^n)$ and $V_i = (KU_i)$.
- Equation (A5c) introduces the auxiliary RV J uniformly distributed over $[1 : n]$ and independent of all the other variables.
- Equation (A5d) stems from the definition of random variables $U = (U_J J)$, $V = (V_J J)$, $B = B_J$, and $E = E_J$.

This establishes the “source” term in Equation (A4d) with auxiliary RVs (U, V) that satisfy the following Markov chain

$$U_i \text{---} V_i \text{---} A_i \text{---} (B_i E_i). \quad (\text{A6})$$

The first part of Equation (A6) is trivial given the definition $V_i = (KU_i)$, whereas the second part follows from the i.i.d. nature of the sources and that they are correlated to the main channel only through the encoder’s input in Equation (A1a), see Equation (A3),

$$(KY^m B^{i-1} E_{i+1}^n) \text{---} A_i \text{---} (B_i E_i). \quad (\text{A7})$$

The “channel” term R_c can be single-letterized similarly,

$$R_c = m[I(T; Y | Q) - I(T; Z | Q)], \quad (\text{A8})$$

where we first define the auxiliary RVs $Q_i = (E^n Y^{i-1} Z_{i+1}^m)$ and $T_i = (KQ_i)$, we then introduce the auxiliary RV L uniformly distributed over $[1 : m]$, and we finally define $Q = (Q_L L)$, $T = (T_L L)$, $Y = Y_L$, and $Z = Z_L$. The auxiliary RVs in this term, i.e., (Q, T) , satisfy the following Markov chain

$$Q_i \text{---} T_i \text{---} X_i \text{---} (Y_i Z_i), \quad (\text{A9})$$

where the nontrivial part is due to the memoryless property of the channel and Equation (A1b), provided the joint probability distribution satisfies Equation (A3). Since neither Q nor T appears on other parts of the outer bound, we may expand R_c as

$$R_c = m \sum_{q \in \mathcal{Q}} p_Q(q) [I(T; Y | Q = q) - I(T; Z | Q = q)] \\ \leq m \max_{q \in \mathcal{Q}} [I(T; Y | Q = q) - I(T; Z | Q = q)] \\ = m[I(T^*; Y) - I(T^*; Z)], \quad (\text{A10})$$

where in the last step we choose auxiliary RV $T^* \sim p_{T|Q}(\cdot | q)$.

Gathering Equations (A4), (A5), (A8), and (A10), the rate of the secret key writes

$$R_k \leq I(V; B | U) - I(V; E | U) + \frac{m}{n} [I(T; Y) - I(T; Z)] + \epsilon'. \quad (\text{A11})$$

If we let $(n, m) \rightarrow \infty$ and take arbitrarily small ϵ' , we obtain the bound in Equation (7).

To obtain Equation (8), we use the following Markov chain that is a consequence of Equation (A1a), provided the joint probability satisfies Equation (A3):

$$(B^n E^n) \text{---} A^n \text{---} X^m \text{---} (Y^m Z^m). \quad (\text{A12})$$

Due to the data processing inequality, we have

$$I(A^n; Y^m) \leq I(X^m; Y^m) \leq m I(X; Y), \quad (\text{A13})$$

where in the last inequality we use the memoryless property of the channel. Next, consider

$$I(A^n; Y^m) = I(A^n B^n; Y^m) \quad (\text{A14a})$$

$$\begin{aligned} &\geq I(A^n; Y^m | B^n) \\ &= I(A^n; KY^m | B^n) - I(A^n; K | B^n Y^m) \\ &\geq I(A^n; KY^m | B^n) - n\epsilon \end{aligned} \quad (\text{A14b})$$

$$\geq n[I(A; V | B) - \epsilon], \quad (\text{A14c})$$

where

- Equation (A14a) follows from the Markov chain in Equation (A12).
- Equation (A14b) stems from $H(K | B^n Y^m) \leq n\epsilon$ due to Equations (A1) and (A2b), and $H(K | A^n B^n Y^m) \geq 0$.

For the last step, i.e., Equation (A14c), consider

$$I(KY^m; A^n | B^n) = I(KY^m; A^n E^n | B^n) \quad (\text{A15a})$$

$$\begin{aligned} &= \sum_{i=1}^n I(KY^m; A_i E_i | B^n A_{i+1}^n E_{i+1}^n) \\ &\geq \sum_{i=1}^n I(KY^m B^{i-1} E_{i+1}^n; A_i E_i | B_i) \end{aligned} \quad (\text{A15b})$$

$$= \sum_{i=1}^n I(V_i; A_i E_i | B_i) \quad (\text{A15c})$$

$$\begin{aligned} &\geq \sum_{i=1}^n I(V_i; A_i | B_i) \\ &= n I(V_J; A_J | B_J) \end{aligned} \quad (\text{A15d})$$

$$= n I(V_J; A_J | B_J) \quad (\text{A15e})$$

$$= n I(V; A | B), \quad (\text{A15f})$$

where

- Equation (A15a) stems from the Markov chain $(B^n E^n) \text{---} A^n \text{---} (KY^m)$.
- Equation (A15b) follows from the sources being i.i.d., i.e., $(A_i E_i) \text{---} B_i \text{---} (B^{i-1} B_{i+1}^n A_{i+1}^n E_{i+1}^n)$.
- Equation (A15c) is due to the auxiliary RV $V_i = (KY^m B^{i-1} E_{i+1}^n)$.
- Equation (A15d) introduces the auxiliary RV J uniformly distributed over $[1 : n]$ and independent of all the other variables.
- Equation (A15e) follows from the independence of J and $(A_J B_J)$.
- Equation (A15f) stems from the definition of random variables $V = (V_J J)$, $B = B_J$, and $A = A_J$.

Putting Equations (A13) and (A14) together, we obtain:

$$I(V; A | B) \leq \frac{m}{n} I(X; Y) + \epsilon, \quad (\text{A16})$$

which gives the condition in Equation (8) as we let $(n, m) \rightarrow \infty$ and take an arbitrarily small ϵ .

Although the definition of the auxiliary RVs (TUV) used in the proof makes them arbitrarily correlated, the bounds in Equations (7) and (8) only depend on the marginal PDs $p(tx)$ and $p(uv|a)$.

Consequently, we can restrict the set of possible joint PDs to Equation (9), i.e., independent source and channel variables, and still achieve the maximum.

The bounds on the cardinality of the alphabets $\mathcal{T}$, $\mathcal{U}$, and $\mathcal{V}$ for the auxiliary RVs follow from Fenchel–Eggleston–Carathéodory’s theorem and the standard cardinality bounding technique ([29], Appendix C); therefore, their proof is omitted. This concludes the proof of Theorem 2. $\square$

Appendix B. Proof of Proposition 5

For completeness, we first present the inner bound from ([13], Theorem 4) but rewritten using the notation of the present work:

$$R_k \leq \max_{p(x)p(v|a)} \{I(V;B) - I(V;E) + \eta I(X;Y|Z)\} \quad (\text{A17a})$$

$$\text{subject to } I(V;A|B) \leq \eta I(X;Y). \quad (\text{A17b})$$

In the sequel, we assume $\eta = 1$.

The main channel in the system model depicted in Figure 2a is not only degraded but also Y equals X ; thus, the last term on the r.h.s. of Equation (A17a) may be expanded as follows

$$I(X;Y|Z) = H(X|Z) = H(X) + H(Z|X) - H(Z). \quad (\text{A18})$$

Since X is the input of a BSC of parameter ζ and output Z , it is clear that

$$I(X;Y|Z) \leq H(Z|X) = h_2(\zeta), \quad (\text{A19})$$

with equality if and only if $X \sim \mathcal{B}\left(\frac{1}{2}\right)$. Furthermore, this choice of X maximizes the r.h.s. of Equation (A17b) and makes the condition redundant:

$$I(V;A|B) \leq H(A|B) = \beta H(A) = \beta \leq 1 = H(X), \quad (\text{A20})$$

given that $A \sim \mathcal{B}\left(\frac{1}{2}\right)$ and $0 \leq \beta \leq 1$.

It remains to be determined what the maximizing value of the first two terms on the r.h.s. of Equation (A17a) is. Let us first assume that B is *more capable* than E , i.e., $0 \leq \beta < h_2(\epsilon)$ according to Remark 10. Then, we may write

$$\begin{aligned} I(V;B) - I(V;E) &= I(A;B) - I(A;E) - [I(A;B|V) - I(A;E|V)] \\ &\leq I(A;B) - I(A;E) \end{aligned} \quad (\text{A21a})$$

$$= H(A|E) - H(A|B) \quad (\text{A21b})$$

$$= h_2(\epsilon) - \beta, \quad (\text{A21c})$$

where the inequality is due to $I(A;B|V) \geq I(A;E|V)$ for all $p(v,a)$ given the more capable assumption. The bound in Equation (A21) holds with equality if and only if $V = A$. We also note that Equation (A21) is a monotonically decreasing function of β and it is zero when $\beta = h_2(\epsilon)$. For $\beta > h_2(\epsilon)$, the bound in Equation (A21) is no longer valid; however, we can rightfully argue that, as Bob’s source degrades while Eve’s remains the same, it is not possible to obtain more secret bits from the sources than for $\beta = h_2(\epsilon)$. Therefore, for $\beta > h_2(\epsilon)$,

$$I(V;B) - I(V;E) \leq 0, \quad (\text{A22})$$

which holds with equality if and only if $V = \emptyset$.

Combining Equations (A17), (A19), (A21), and (A22), we obtain the bound in Equation (14). This concludes the proof of Proposition 5. $\square$

References

- Wyner, A.D. The Wire-Tap Channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387, doi:10.1002/j.1538-7305.1975.tb02040.x. [\[CrossRef\]](#)
- Csiszár, I.; Körner, J. Broadcast Channels with Confidential Messages. *IEEE Trans. Inf. Theory* **1978**, *24*, 339–348, doi:10.1109/TIT.1978.1055892. [\[CrossRef\]](#)
- Shannon, C.E. Communication Theory of Secrecy Systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715, [\[CrossRef\]](#)
- Chorti, A.; Hollanti, C.; Belfiore, J.C.; Poor, H.V. Physical Layer Security: A Paradigm Shift in Data Confidentiality. In *Physical and Data-Link Security Techniques for Future Communication Systems*; Baldi, M., Tomasin, S., Eds.; Lecture Notes in Electrical Engineering; Springer International Publishing: Cham, Switzerland, 2016; Volume 358, pp. 1–15, doi:10.1007/978-3-319-23609-4_1.
- Narayan, P.; Tyagi, H. Multiterminal Secrecy by Public Discussion. In *Foundations and Trends® in Communications and Information Theory*; Now Publishers Inc.: Hanover, MA, USA, 2016; Volume 13, pp. 129–275, doi:10.1561/01000000072.
- Maurer, U.M. Secret Key Agreement by Public Discussion from Common Information. *IEEE Trans. Inf. Theory* **1993**, *39*, 733–742, doi:10.1109/18.256484. [\[CrossRef\]](#)
- Ahlsweide, R.; Csiszár, I. Common Randomness in Information Theory and Cryptography—Part I: Secret Sharing. *IEEE Trans. Inf. Theory* **1993**, *39*, 1121–1132, doi:10.1109/18.243431. [\[CrossRef\]](#)
- Csiszár, I.; Narayan, P. Common Randomness and Secret Key Generation with a Helper. *IEEE Trans. Inf. Theory* **2000**, *46*, 344–366, doi:10.1109/18.825796. [\[CrossRef\]](#)
- Csiszár, I.; Narayan, P. Secrecy Capacities for Multiterminal Channel Models. *IEEE Trans. Inf. Theory* **2008**, *54*, 2437–2452, doi:10.1109/TIT.2008.921705. [\[CrossRef\]](#)
- Csiszár, I.; Narayan, P. Secrecy Generation for Multiaccess Channel Models. *IEEE Trans. Inf. Theory* **2013**, *59*, 17–31, doi:10.1109/TIT.2012.2216254. [\[CrossRef\]](#)
- Gohari, A.A.; Anantharam, V. Information-Theoretic Key Agreement of Multiple Terminals—Part I. *IEEE Trans. Inf. Theory* **2010**, *56*, 3973–3996, doi:10.1109/TIT.2010.2050832. [\[CrossRef\]](#)
- Gohari, A.A.; Anantharam, V. Information-Theoretic Key Agreement of Multiple Terminals—Part II: Channel Model. *IEEE Trans. Inf. Theory* **2010**, *56*, 3997–4010, doi:10.1109/TIT.2010.2050925. [\[CrossRef\]](#)
- Khisti, A.; Diggavi, S.N.; Wornell, G.W. Secret-Key Generation Using Correlated Sources and Channels. *IEEE Trans. Inf. Theory* **2012**, *58*, 652–670, doi:10.1109/TIT.2011.2173629. [\[CrossRef\]](#)
- Prabhakaran, V.M.; Eswaran, K.; Ramchandran, K. Secrecy via Sources and Channels. *IEEE Trans. Inf. Theory* **2012**, *58*, 6747–6765, doi:10.1109/TIT.2012.2208579. [\[CrossRef\]](#)
- Bunin, A.; Piantanida, P.; Shamai, S. The Gaussian Wiretap Channel with Correlated Sources at the Terminals: Secret Communication and Key Generation. In Proceedings of the 2016 ICSEE International Conference on the Science of Electrical Engineering, Eilat, Israel, 16–18 November 2016; pp. 1–5.
- Salimi, S.; Skoglund, M.; Golic, J.D.; Salmasizadeh, M.; Aref, M.R. Key Agreement over a Generalized Multiple Access Channel Using Noiseless and Noisy Feedback. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 1765–1778, doi:10.1109/JSAC.2013.130910. [\[CrossRef\]](#)
- Tyagi, H. Common Information and Secret Key Capacity. *IEEE Trans. Inf. Theory* **2013**, *59*, 5627–5640, doi:10.1109/TIT.2013.2264355. [\[CrossRef\]](#)
- Hayashi, M.; Tyagi, H.; Watanabe, S. Secret Key Agreement: General Capacity and Second-Order Asymptotics. *IEEE Trans. Inf. Theory* **2016**, *62*, 3796–3810, doi:10.1109/TIT.2016.2567440. [\[CrossRef\]](#)
- Courtade, T.A.; Halford, T.R. Coded Cooperative Data Exchange for a Secret Key. *IEEE Trans. Inf. Theory* **2016**, *62*, 3785–3795, doi:10.1109/TIT.2016.2539347. [\[CrossRef\]](#)
- Boche, H.; Schaefer, R.F.; Poor, H.V. On the Computability of the Secret Key Capacity under Rate Constraints. In Proceedings of the 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Brighton, UK, 12–17 May 2019; pp. 2427–2431, doi:10.1109/ICASSP.2019.8683122. [\[CrossRef\]](#)
- Chen, Y.; Vinck, A.J.H. Wiretap Channel with Side Information. *IEEE Trans. Inf. Theory* **2008**, *54*, 395–402, doi:10.1109/TIT.2007.911157. [\[CrossRef\]](#)

22. Liu, W.; Chen, B. Wiretap Channel with Two-Sided Channel State Information. In Proceedings of the 2007 41st Asilomar Conference on Signals, Systems and Computers (ACSSC), Pacific Grove, CA, USA, 4–7 November 2007; pp. 893–897, doi:10.1109/ACSSC.2007.4487347. [[CrossRef](#)]
23. Gelfand, S.I.; Pinsker, M.S. Coding for Channel with Random Parameters. *Probl. Control Inf. Theory* **1980**, *9*, 19–31.
24. Muramatsu, J. General Formula for Secrecy Capacity of Wiretap Channel with Noncausal State. In Proceedings of the 2014 IEEE International Symposium on Information Theory (ISIT), Honolulu, HI, USA, 29 June–4 July 2014; pp. 21–25, doi:10.1109/ISIT.2014.6874787. [[CrossRef](#)]
25. Goldfeld, Z.; Cuff, P.; Permuter, H.H. Wiretap Channels with Random States Non-Causally Available at the Encoder. *arXiv* **2016**, arXiv:1608.00743.
26. Zibaeenejad, A. Key Generation over Wiretap Models with Non-Causal Side Information. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1456–1471, doi:10.1109/TIFS.2015.2407153. [[CrossRef](#)]
27. Bunin, A.; Goldfeld, Z.; Permuter, H.H.; Shamai, S.; Cuff, P.; Piantanida, P. Key and Message Semantic-Security over State-Dependent Channels. *IEEE Trans. Inf. Forensics Secur.* **2018**, doi:10.1109/TIFS.2018.2853108. [[CrossRef](#)]
28. Bassi, G.; Piantanida, P.; Shamai, S. The Wiretap Channel with Generalized Feedback: Secure Communication and Key Generation. *IEEE Trans. Inf. Theory* **2019**, *65*, 2213–2233, doi:10.1109/TIT.2018.2883299. [[CrossRef](#)]
29. El Gamal, A.; Kim, Y.H. *Network Information Theory*; Cambridge University Press: Cambridge, UK, 2011.
30. Bassi, G.; Piantanida, P.; Shamai, S. Secret Key Generation over Noisy Channels with Common Randomness. In Proceedings of the 2016 IEEE International Symposium on Information Theory (ISIT), Barcelona, Spain, 10–15 July 2016; pp. 510–514, doi:10.1109/ISIT.2016.7541351. [[CrossRef](#)]
31. Bassi, G.; Piantanida, P.; Shamai, S. Secret Key Generation over Noisy Channels with Correlated Sources. *arXiv* **2016**, arXiv:1609.08330.
32. Cao, D.; Kang, W. Secret key generation from correlated sources and secure link. In Proceedings of the 2017 9th International Conference on Wireless Communications and Signal Processing (WCSP), Nanjing, China, 11–13 October 2017; pp. 1–5, doi:10.1109/WCSP.2017.8171157. [[CrossRef](#)]
33. Nair, C. Capacity Regions of Two New Classes of 2-Receiver Broadcast Channels. In Proceedings of the 2009 IEEE International Symposium on Information Theory (ISIT), Seoul, Korea, 28 June–3 July 2009; pp. 1839–1843, doi:10.1109/ISIT.2009.5205399. [[CrossRef](#)]



© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).